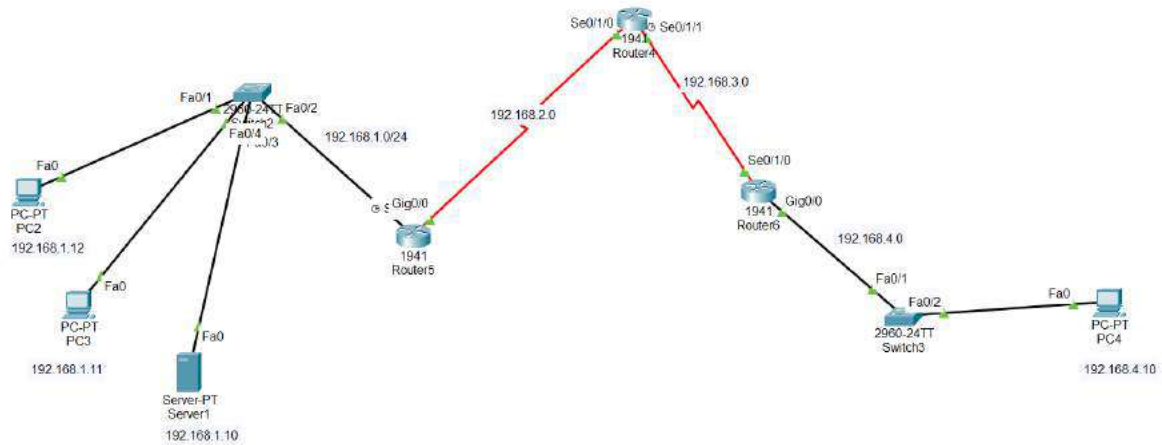
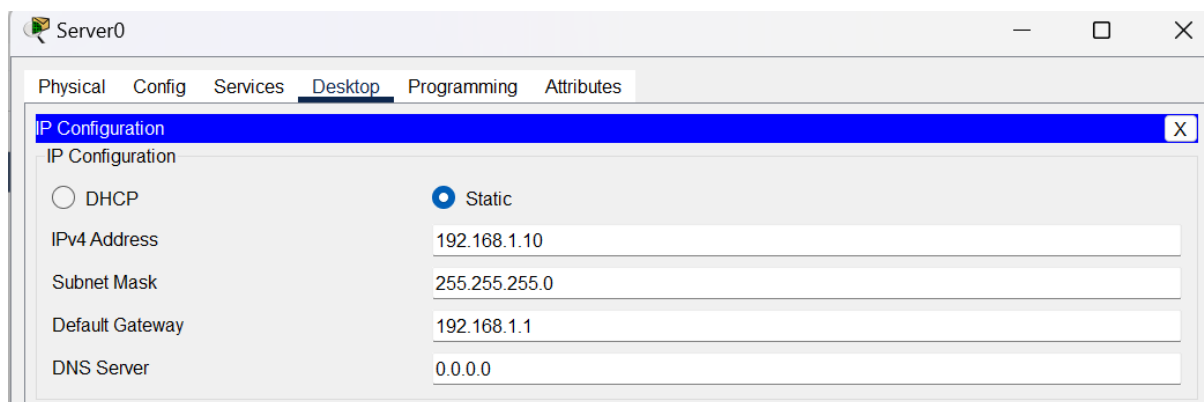


CONFIGURATION OF IPS



BEFORE IPS CONFIGURATION

ALL THE ROUTERS ARE CONFIGURED AS STATIC WITH THE IP GIVEN AND RIP PROTOCOL IS ENABLED



PC4

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>PING 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=8ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

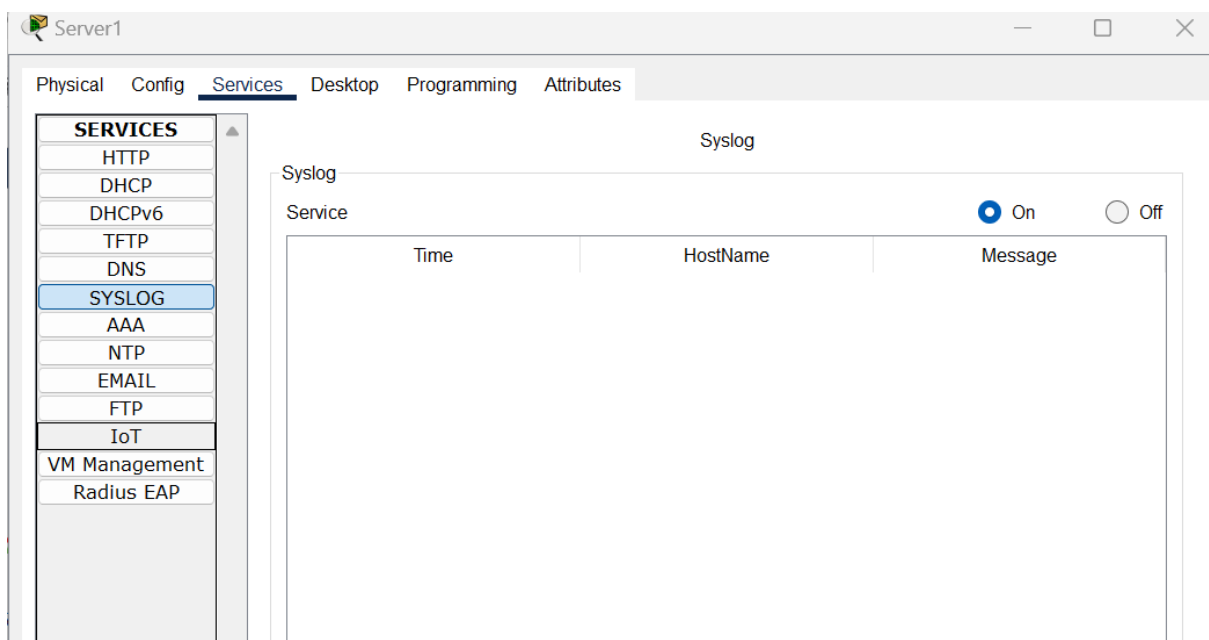
```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.11: bytes=32 time<1ms TTL=126
Reply from 192.168.1.11: bytes=32 time<1ms TTL=126
Reply from 192.168.1.11: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```



AFTER IPS CONFIGURATION

Router # show version

License Info:

License UDI:

Device# PID SN

*0 CISCO1941/K9 FTX1524TNA6-

Technology Package License Information for Module:'c1900'

Technology Technology-package Technology-package
Current Type Next reboot

ipbase ipbasek9 Permanent ipbasek9
security None None None
data None None None

Configuration register is 0x2102

Router (config)# license boot module c1900 technology-package security k9

It ill ask for yes to confirm (give yes)

Then give the command as do reload to reload your router

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.

Processor board ID FTX152400KS

2 Gigabit Ethernet interfaces

2 Low-speed serial(sync/async) network interface(s)

DRAM configuration is 64 bits wide with parity disabled.

255K bytes of non-volatile configuration memory.

249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

Device# PID SN

*0 CISCO1941/K9 FTX15248ZB8-

Technology Package License Information for Module:'c1900'

Technology Technology-package Technology-package
Current Type Next reboot

ipbase ipbasek9 Permanent ipbasek9
security securityk9 Evaluation securityk9
data disable None None

Configuration register is 0x2102

Router#

Router#mkdir ipsdir

Create directory filename [ipsdir]?

Created dir flash:ipsdir

Router#

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#ip ips config location ipsdir

Router(config)#ip ips name iosips

Router(config)#ip ips signature-category

Router(config-ips-category)#category all

Router(config-ips-category-action)#retired true

Router(config-ips-category-action)#

Router(config-ips-category-action)#exit

Router(config-ips-category)#category ios_ips basic

Router(config-ips-category-action)#

Router(config-ips-category-action)#retired false

Router(config-ips-category-action)#exit

Router(config-ips-category)#exit

Do you want to accept these changes? [confirm]

Applying Category configuration to signatures ...

%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines

%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

Router(config)#

Router(config)#in gigabitEthernet 0/0

Router(config-if)#ip ips iosips?

WORD

Router(config-if)#ip ips iosips out

Router(config-if)#

%IPS-6-ENGINE_BUILDS_STARTED: 00:04:40 UTC Mar 01 1993

%IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

%IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned

%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms

```
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#logging host 192.168.1.10
Router(config)#
Router(config)#service timestamps log datetime msec
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature ?
```

<1-65535> signature id value

Router(config-sigdef)#signature 2004?

<0-65535> signature subid value

<cr>

```
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline //it acts as ips not ids
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
```

Do you want to accept these changes? [confirm]

%IPS-6-ENGINE_BUILDS_STARTED:

%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines

%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned

%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

```
Router(config)#
Router(config)#
Router(config)#do show ip ips all
IPS Signature File Configuration Status
Configured Config Locations: ipsdir
Last signature default load time:
Last signature delta load time:
Last event action (SEAP) load time: -none-
```

General SEAP Config:

Global Deny Timeout: 3600 seconds

Global Overrides Status: Enabled

Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status

Event notification through syslog is enabled

Event notification through SDEE is enabled

IPS Signature Status

Total Active Signatures: 1

Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status

IPS Rule Configuration

IPS name iosips

IPS fail closed is disabled

IPS deny-action ips-interface is false

Fastpath ips is enabled

Quick run mode is enabled

Interface Configuration

Interface GigabitEthernet0/0

Inbound IPS rule is not set

Outgoing IPS rule is iosips

IPS Category CLI Configuration:

Category all

Retire: True

Category ios_ips basic

Retire: False

Router(config)#

*Mar 01, 00:12:29.1212: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25

*Mar 01, 00:12:35.1212: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25

*Mar 01, 00:12:41.1212: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25

*Mar 01, 00:12:47.1212: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25

*Mar 01, 00:14:42.1414: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25

*Mar 01, 00:14:48.1414: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25

*Mar 01, 00:14:54.1414: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25

*Mar 01, 00:15:00.1515: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25



Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.4.10: bytes=32 time=16ms TTL=125

Ping statistics for 192.168.4.10:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 16ms, Average = 16ms

C:\>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Reply from 192.168.4.10: bytes=32 time=26ms TTL=125
Reply from 192.168.4.10: bytes=32 time=2ms TTL=125
Reply from 192.168.4.10: bytes=32 time=2ms TTL=125
Reply from 192.168.4.10: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.4.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 26ms, Average = 8ms

C:\>
```



Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.10

Pinging 192.168.4.10 with 32 bytes of data:

Reply from 192.168.4.10: bytes=32 time=2ms TTL=125
Reply from 192.168.4.10: bytes=32 time=2ms TTL=125
Reply from 192.168.4.10: bytes=32 time=25ms TTL=125
Reply from 192.168.4.10: bytes=32 time=20ms TTL=125

Ping statistics for 192.168.4.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 25ms, Average = 12ms

C:\>
```

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

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

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

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

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

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

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```


Server1

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

Syslog

Service

On

Off

| | Time | HostName | Message |
|----|----------------------------|-------------|------------------------------|
| 1 | 03.01.1993 12:02:00.564 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 2 | 03.01.1993 12:02:06.594 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 3 | 03.01.1993 12:02:12.627 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 4 | 03.01.1993 12:02:25.671 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 5 | 03.01.1993 12:02:31.680 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 6 | 03.01.1993 12:02:37.699 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 7 | 03.01.1993 12:02:43.713 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 8 | 03.01.1993 12:02:53.227 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 9 | 03.01.1993 12:02:59.241 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 10 | 03.01.1993 12:03:05.272 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 11 | 03.01.1993 12:03:11.283 AM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |

Clear Log

Router5

PhysicalConfigCLIAttributes

IOS Command Line Interface

DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

*Mar 01, 00:00:00.000: %IPS-6-ENGINE_BUILDS_STARTED: 00:00:00 UTC Mar 01 1993
*Mar 01, 00:00:00.000: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Mar 01, 00:00:00.000: %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
*Mar 01, 00:00:00.000: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
*Mar 01, 00:00:00.000: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.10 port 514 started - CLI initiated
*Mar 01, 00:00:00.000: %LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
*Mar 01, 00:00:00.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Mar 01, 00:00:00.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
*Mar 01, 00:01:54.011: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.11:0] RiskRating:25
*Mar 01, 00:02:00.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.11:0] RiskRating:25
*Mar 01, 00:02:06.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.11:0] RiskRating:25
*Mar 01, 00:02:12.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.11:0] RiskRating:25
*Mar 01, 00:02:25.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25
*Mar 01, 00:02:31.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25
*Mar 01, 00:02:37.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25
*Mar 01, 00:02:43.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.10:0] RiskRating:25
*Mar 01, 00:02:53.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25
*Mar 01, 00:02:59.022: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25
*Mar 01, 00:03:05.033: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25
*Mar 01, 00:03:11.033: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.4.10 -> 192.168.1.12:0] RiskRating:25

CopyPaste

☐ Top

Basic Firewall Configuration in Cisco Packet Tracer

Steps to Configure and Verify Firewall in Cisco Packet Tracer:

Step 1: First, open the Cisco packet tracer desktop and select the devices given below:

| S.NO | Device | Model Name | Quantity |
|------|--------|------------|----------|
| 1. | PC | PC | 3 |
| 2. | server | PT-Server | 1 |
| 3. | switch | PT-Switch | 1 |

IP Addressing Table:

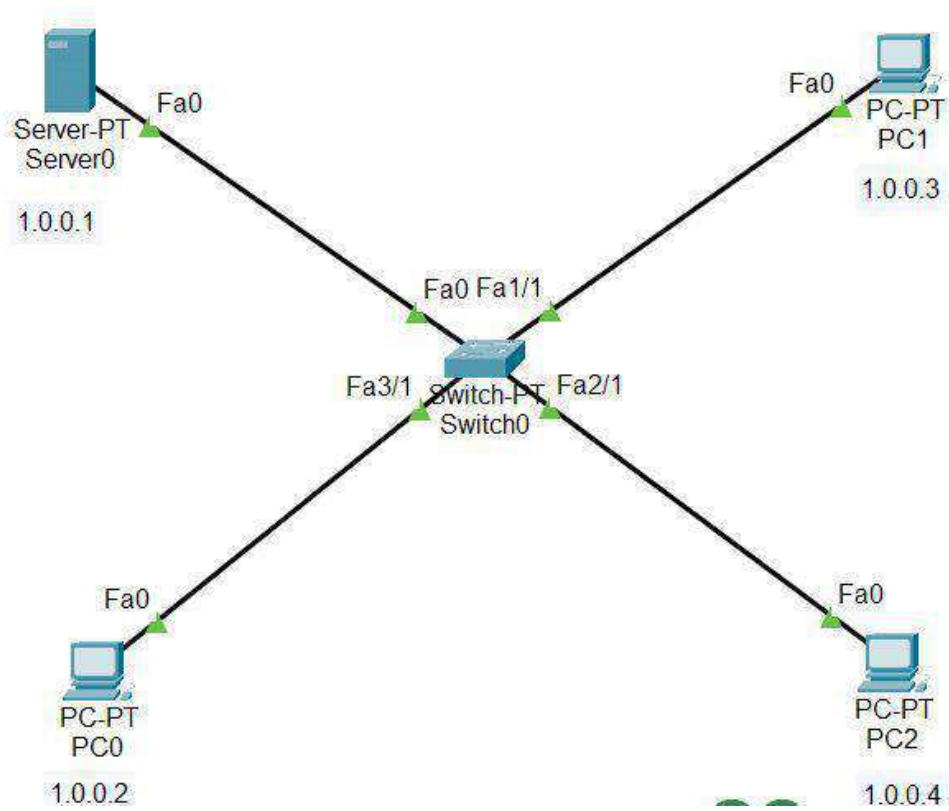
| S.NO | Device | IPv4 Address | Subnet Mask |
|------|--------|--------------|-------------|
| 1. | Server | 1.0.0.1 | 255.0.0.0 |
| 2. | PC0 | 1.0.0.2 | 255.0.0.0 |
| 3. | PC1 | 1.0.0.3 | 255.0.0.0 |
| 4. | PC2 | 1.0.0.4 | 255.0.0.0 |

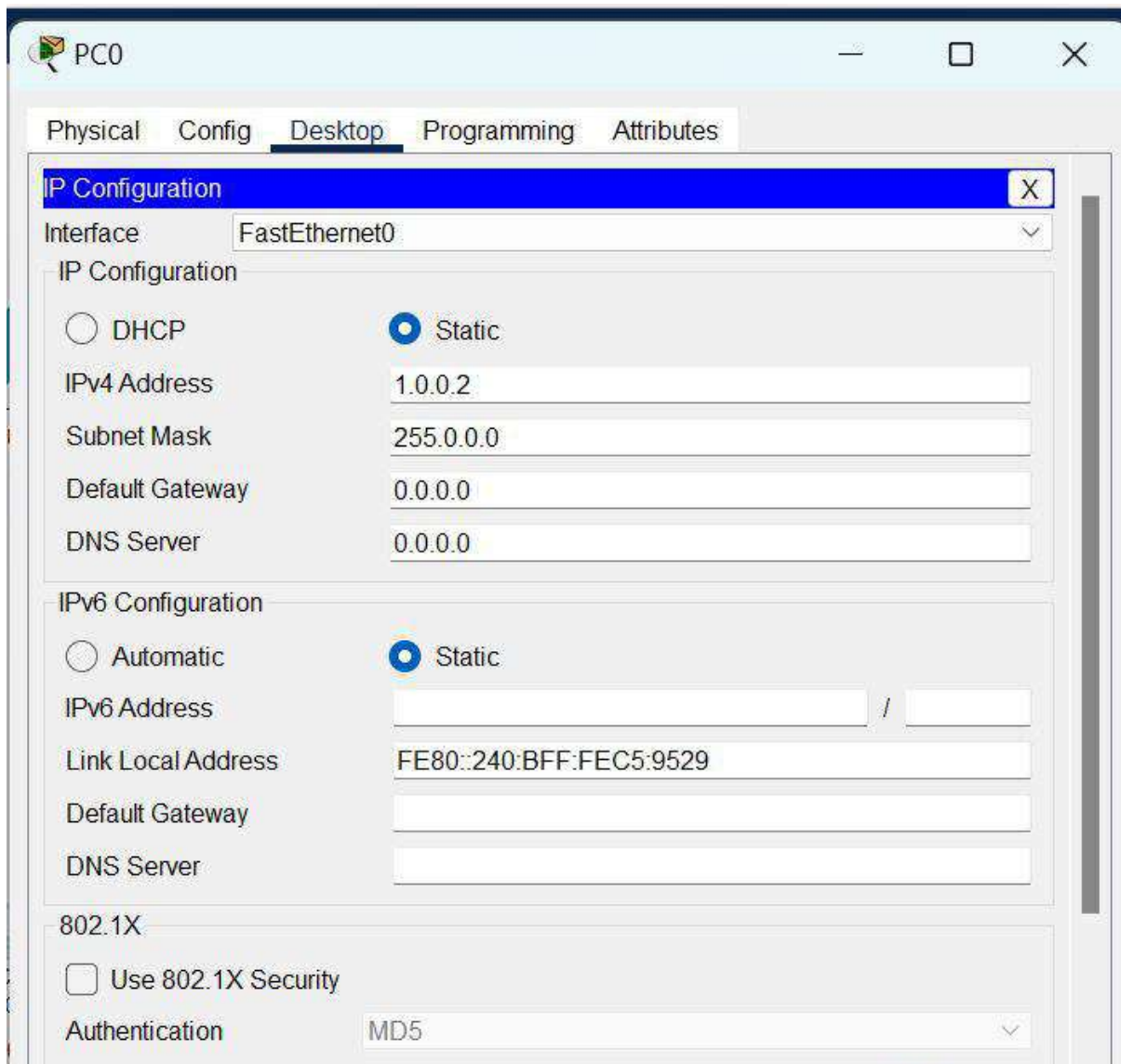
- Then, create a network topology as shown below the image.
- Use an Automatic connecting cable to connect the devices with others.

Step 2: Configure the PCs (hosts) and server with IPv4 address and Subnet Mask according to the IP addressing table given above.

- To assign an IP address in PC0, click on PC0.
- Then, go to desktop and then IP configuration and there you will IPv4 configuration.
- Fill IPv4 address and subnet mask.

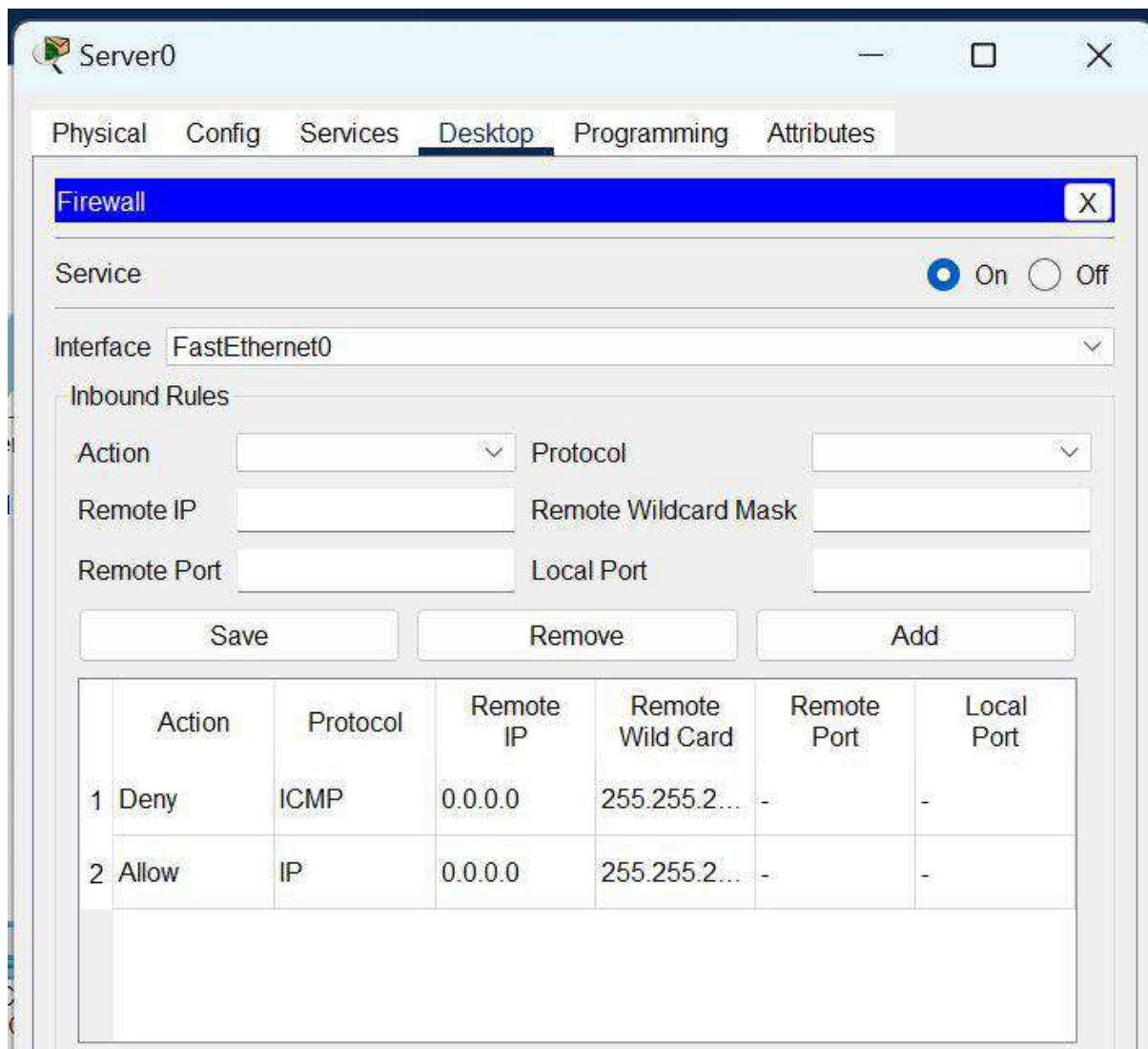
- Repeat the same procedure with the server





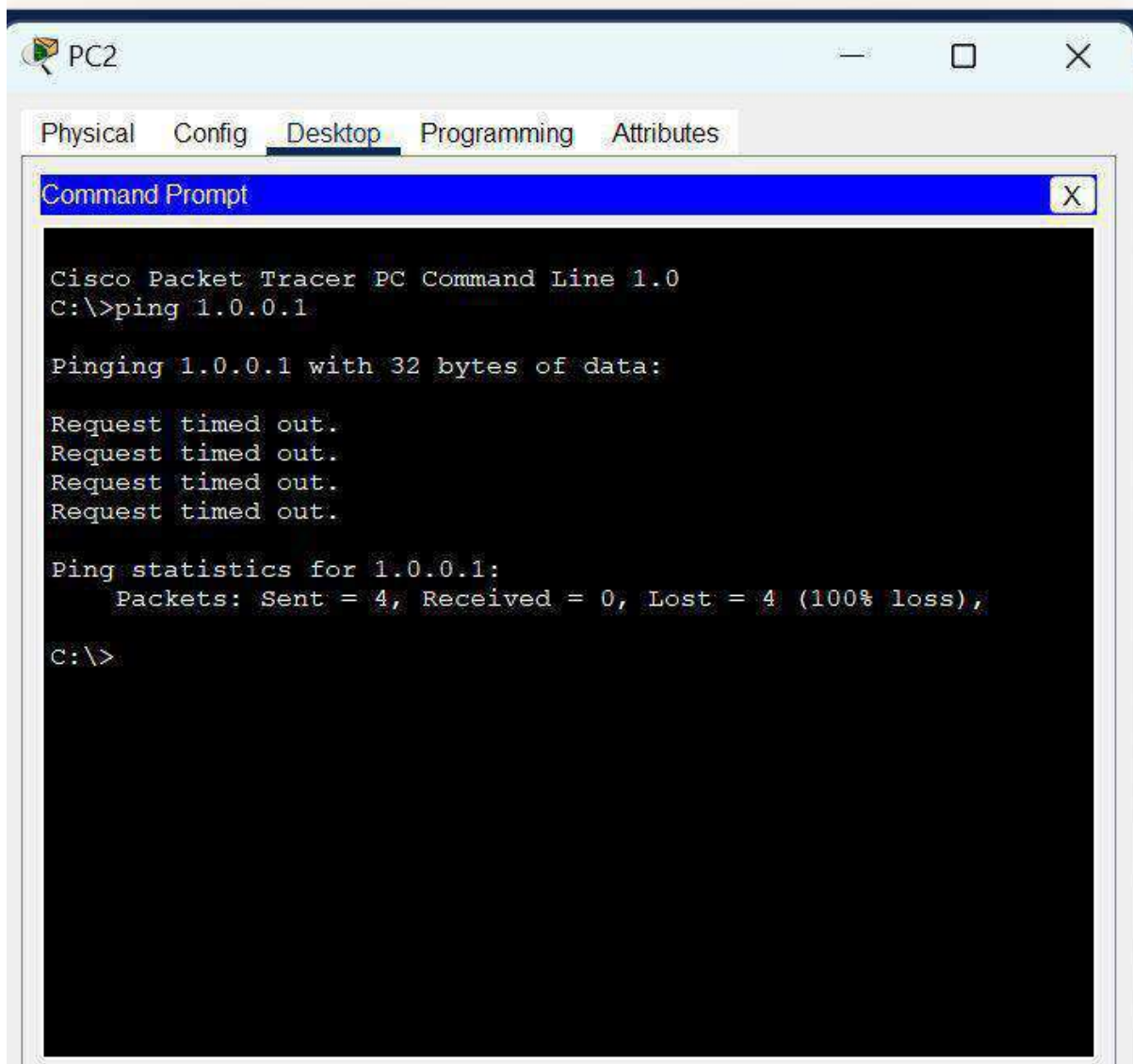
Step 3: Configuring the firewall in a server and blocking packets and allowing web browser.

- Click on server0 then go to the desktop.
- Then click on firewall IPv4.
- Turn on the services.
- First, Deny the ICMP protocol and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255.
- Then, allow the IP protocol and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255.
- And add them.



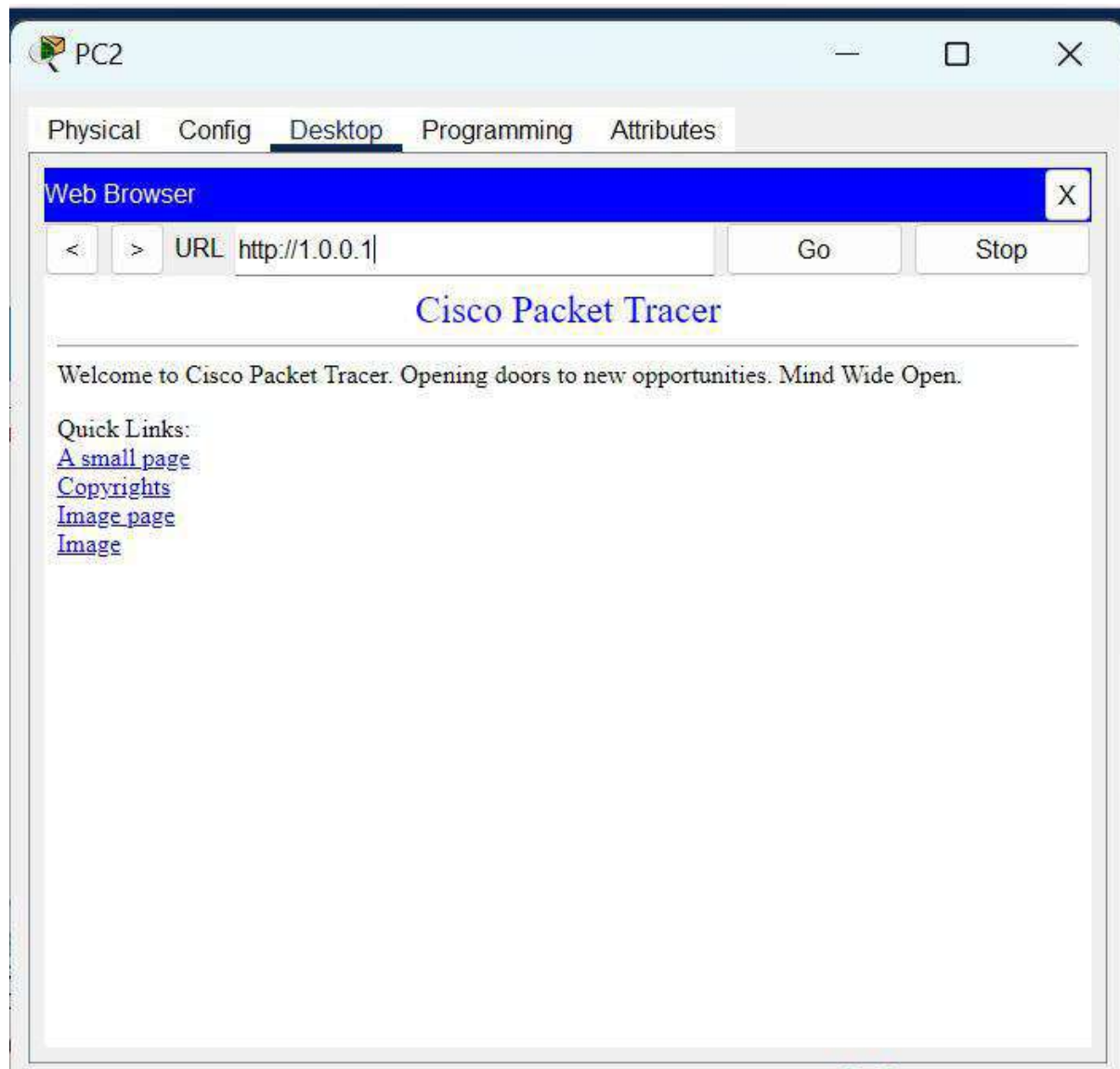
Step 4: Verifying the network by pinging the IP address of any PC.

- We will use the ping command to do so.
- First, click on PC2 then Go to the command prompt.
- Then type ping <IP address of targeted node>.
- We will ping the IP address of the server0.
- As we can see in the below image we are getting no replies which means the packets are blocked.

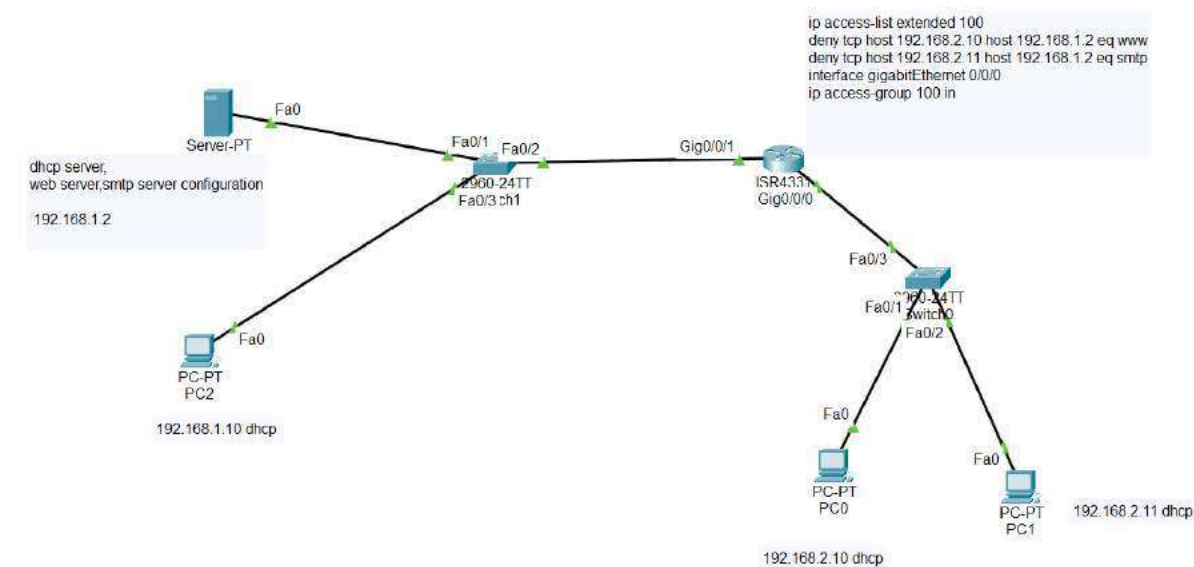


Check the web browser by entering the IP address in the URL.

- Click on PC2 and go to desktop then web browser.



EXTENDED ACL USING DHCP, SMTP, WEB SERVER



Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool1

Default Gateway: 192.168.1.1

DNS Server: 192.168.1.2

Start IP Address: 192 168 1 10

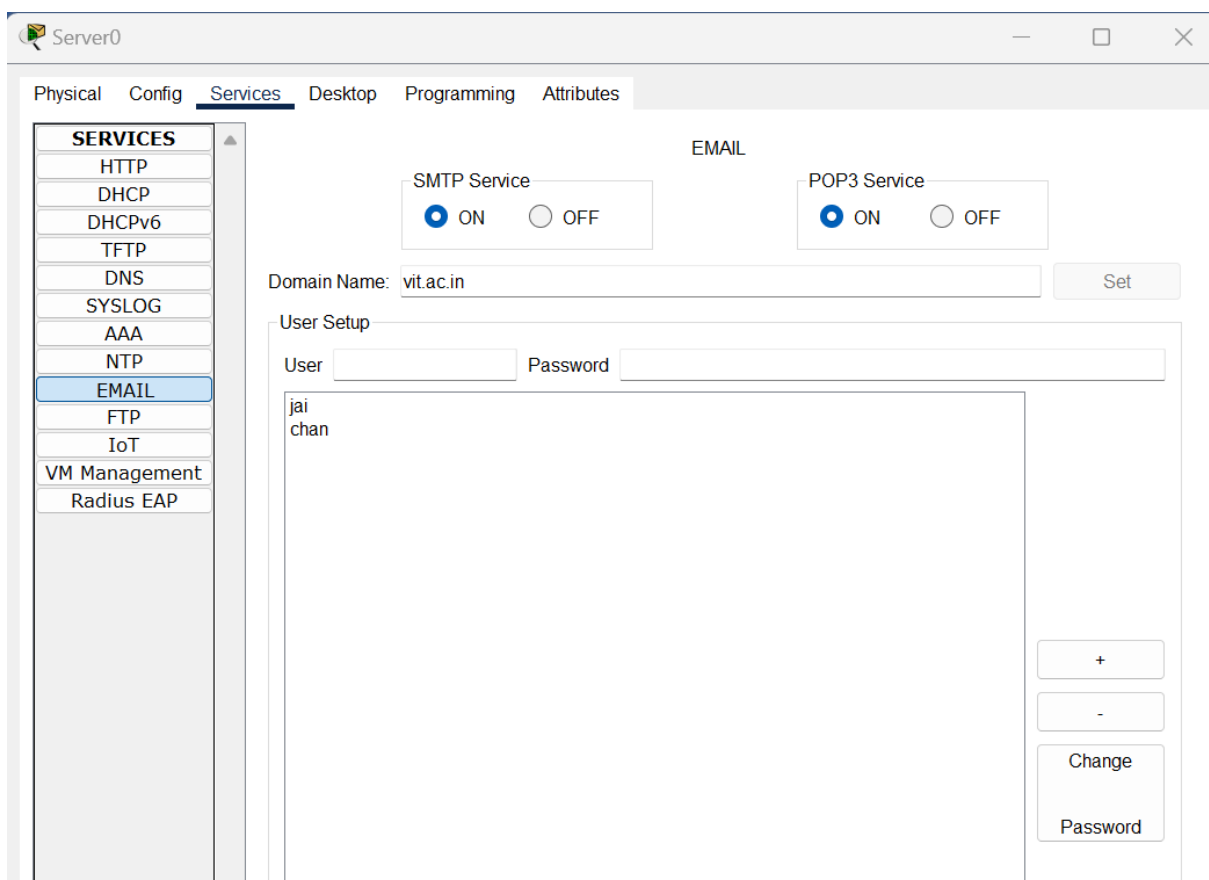
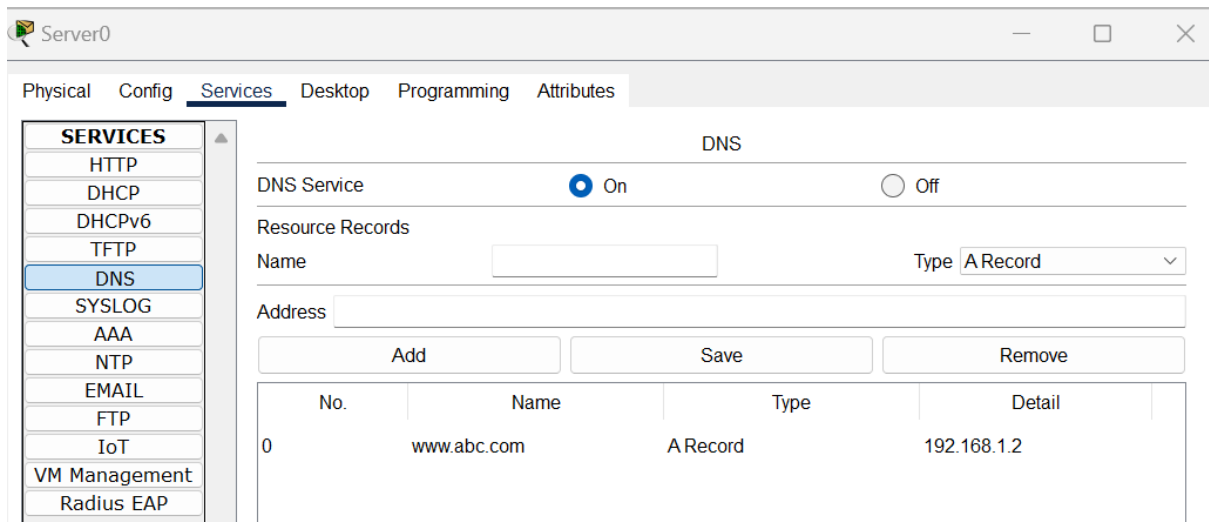
Subnet Mask: 255 255 255 0

Maximum Number of Users: 20

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

| Pool Name | Default Gateway | DNS Server | Start IP Address | Subnet Mask | Max User | TFTP Server | WLC Address |
|-------------|-----------------|-------------|------------------|--------------|----------|-------------|-------------|
| serverPool1 | 192.168.1.1 | 192.168.1.2 | 192.168.1.10 | 255.255.2... | 20 | 0.0.0.0 | 0.0.0.0 |
| serverPool | 192.168.2.1 | 192.168.1.2 | 192.168.2.10 | 255.255.2... | 20 | 0.0.0.0 | 0.0.0.0 |



Before ACL configuration

Router>enable

Router#

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface GigabitEthernet0/0/1

```
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 GigabitEthernet0/0/1, changed state to
up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1, changed state to up
```

```
Router(config-if)#
Router(config-if)#ip helper-address 192.168.1.2
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to
up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
Router(config-if)#ip helper-address 192.168.1.2
Router(config-if)#exit
```

PC1

Physical Config **Desktop** Programming Attributes

Configure Mail [X]

User Information

Your Name:

Email Address:

Server Information

Incoming Mail Server:

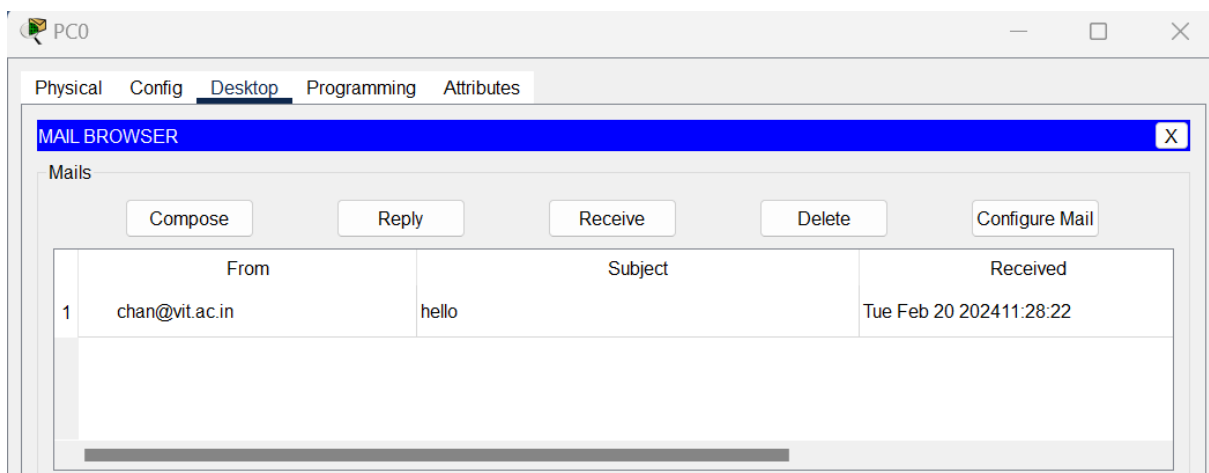
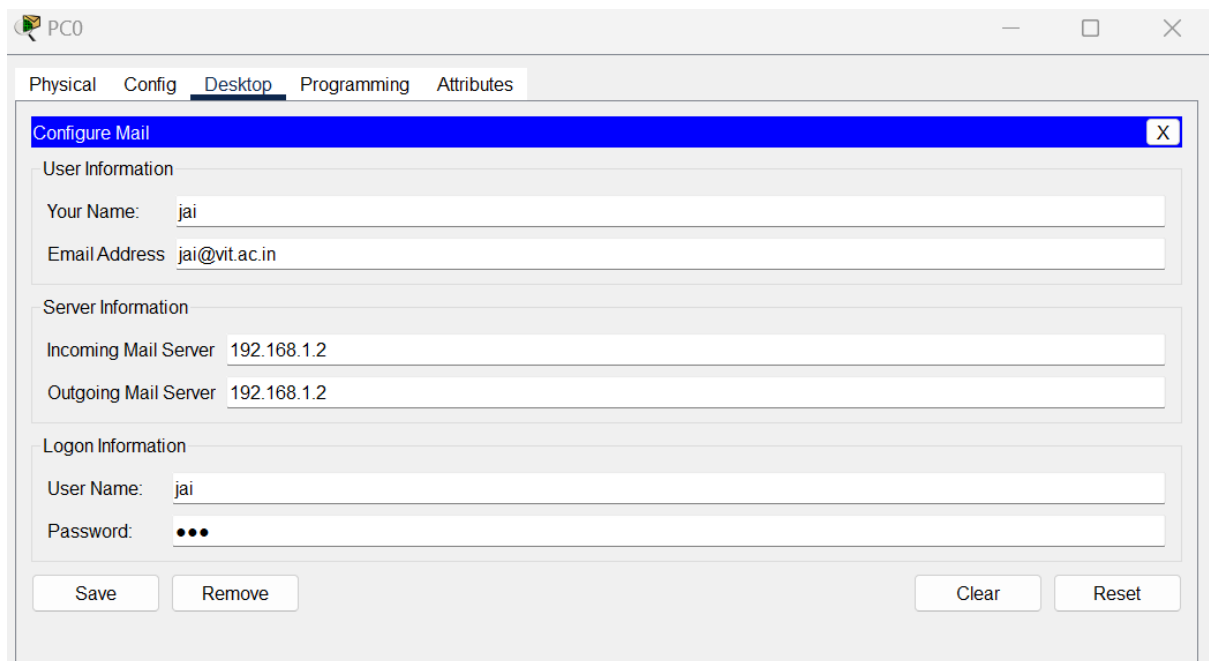
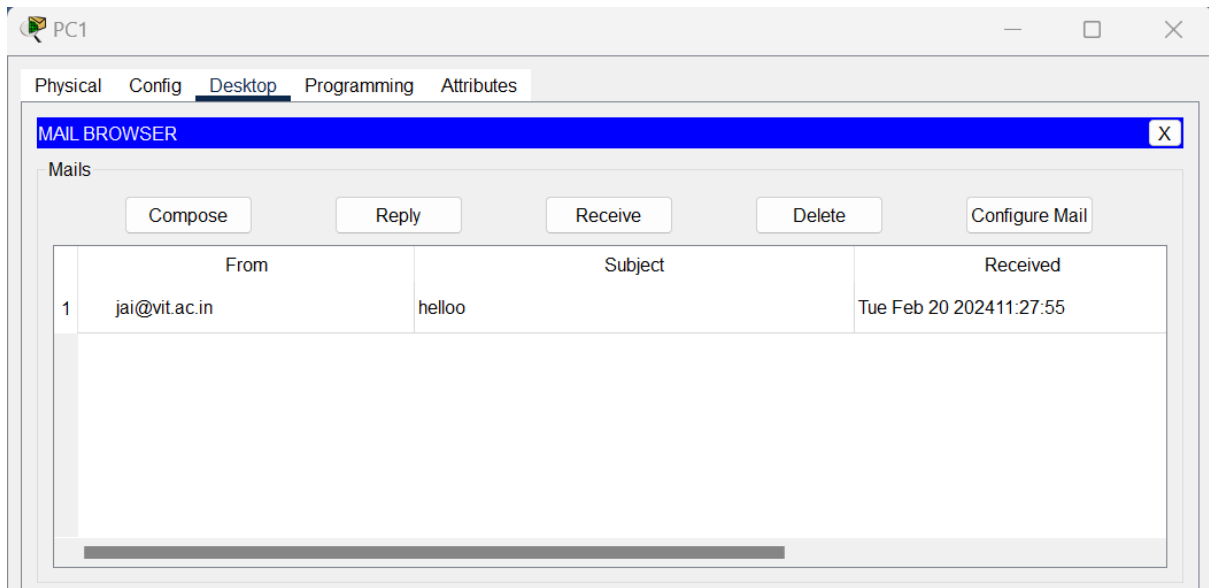
Outgoing Mail Server:

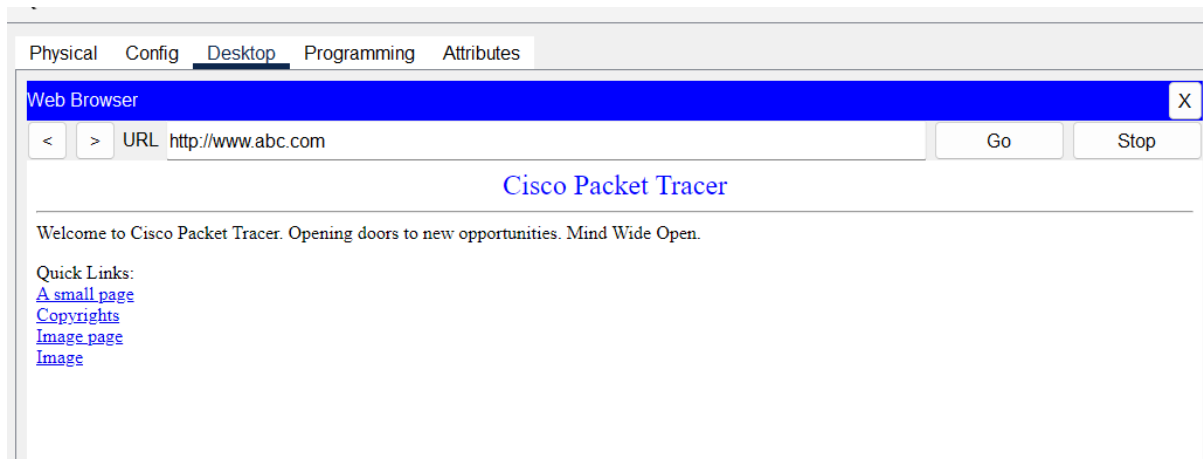
Logon Information

User Name:

Password:

Save Remove Clear Reset

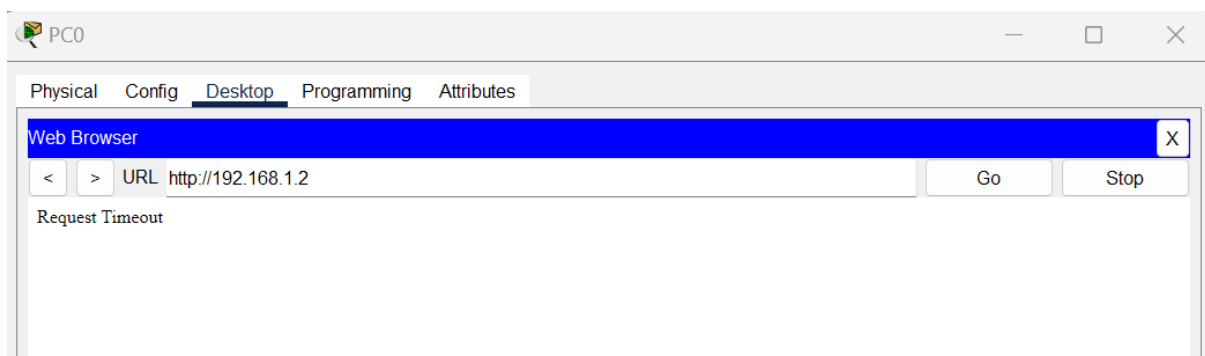


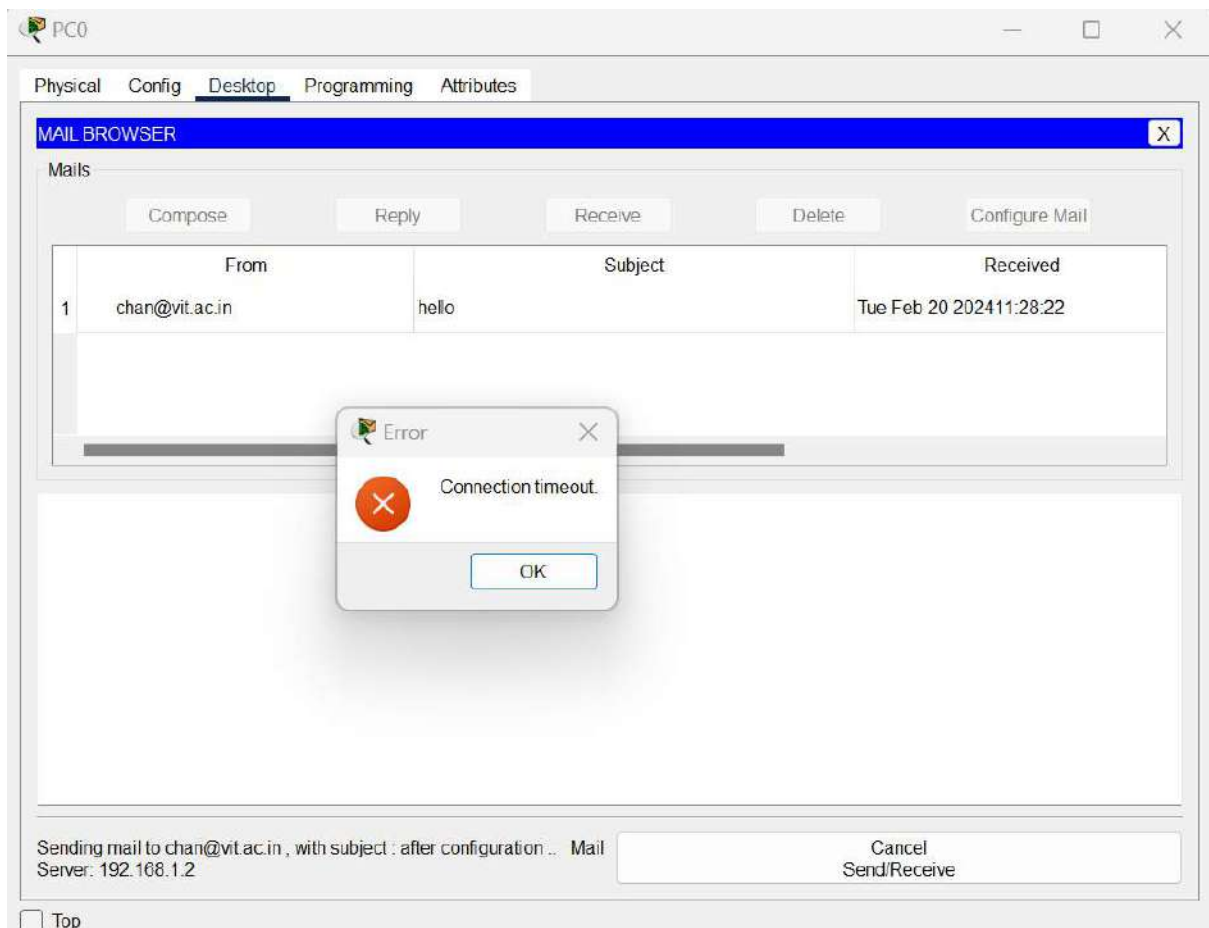


After ACL configuration

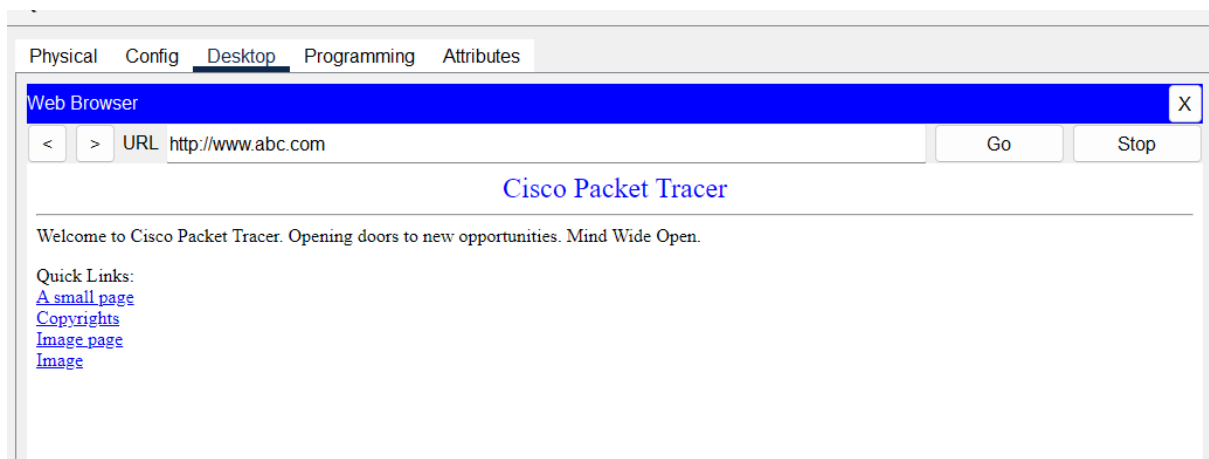
Router(config)#ip access-list ?
extended Extended Access List
standard Standard Access List
Router(config)#ip access-list standard ?
<1-99> standard IP access-list number
WORD name
Router(config)#ip access-list extended ?
<100-199> standard IP access-list number
WORD name
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#?
<1-2147483647> Sequence Number
default Set a command to its defaults
deny Specify packets to reject
exit Exit from access-list configuration mode
no Negate a command or set its defaults
permit Specify packets to forward
remark Access list entry comment
Router(config-ext-nacl)#deny ?
ahp Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol

tcp Transmission Control Protocol
udp User Datagram Protocol
Router(config-ext-nacl)#deny tcp host 192.168.2.10 eq ?
<0-65535> Port number
domain Domain Name Service (DNS, 53)
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnet Telnet (23)
www World Wide Web (HTTP, 80)
Router(config-ext-nacl)#deny tcp host 192.168.2.10 host 192.168.1.2 eq
www or 80
Router(config-ext-nacl)#deny tcp host 192.168.2.11 host 192.168.1.2 eq
smtp or 25
Router(config-ext-nacl)#exit
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#





Pc1





VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Information Security Management

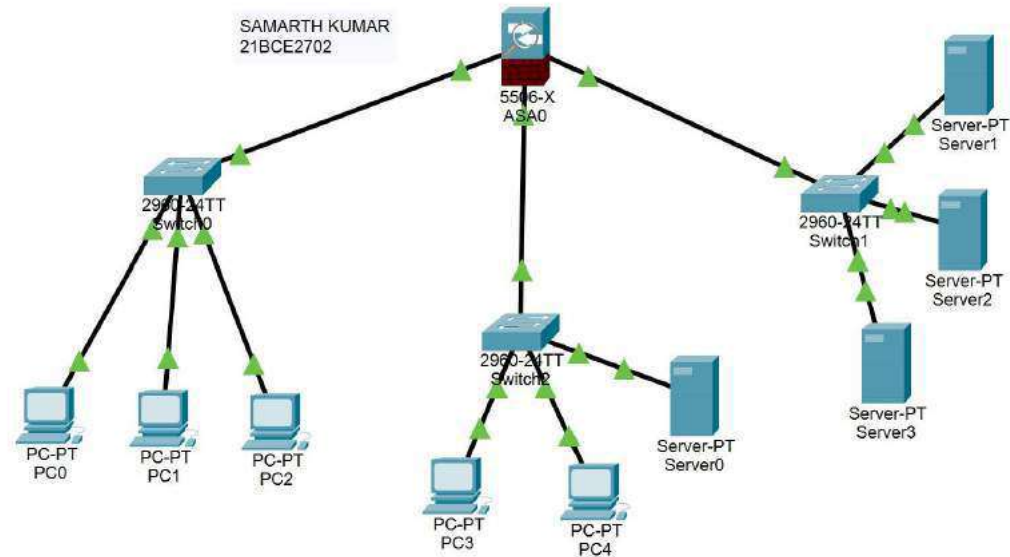
BCSE454E

DA-4

NAME: SAMARTH KUMAR
REGISTRATION NO : 21BCE2702
COURSE CODE: BCSE354E
FACULTY : VIMALA DEVI K

ASA FIREWALL

TOPOLOGY:



1. Open a the asa firewall, by default the name seems to be ciscoasa and by default password ill be empty

```
ciscoasa>en Password:
```

```
ciscoasa#conf t
```

```
ciscoasa(config)#
```

2. Change the name of the firewall to identify it easily here I name the firewall as basefirewall

```
ciscoasa(config)# host name basefirewall
```

```
basefirewall(config)#
```

3. Enable the password for security purpose as I had given the password as hello123

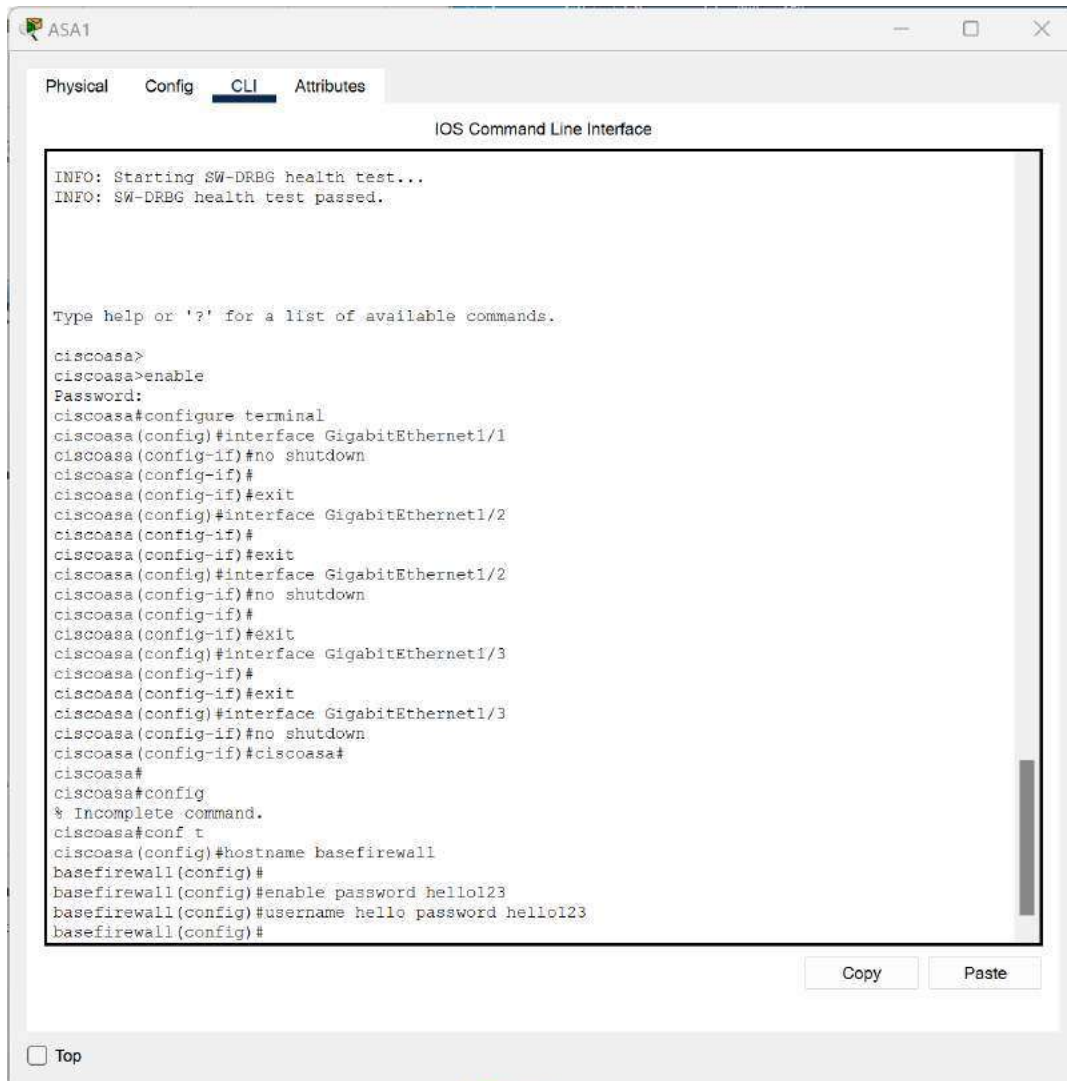
```
basefirewall(config)#
```

```
basefirewall(config)# enable password hello123
```

4. Need to configure the host name for connecting to the ssh (remote desktop)

```
basefirewall(config)#username hello password hello123
```

STEPS 1-4

A screenshot of a web-based CLI interface for a Cisco ASA device named ASA1. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The CLI tab shows the 'IOS Command Line Interface' with a text area containing the following commands and their outputs:

```
INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

Type help or '?' for a list of available commands.

ciscoasa>
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#ciscoasa#
ciscoasa#
ciscoasa#conf
% Incomplete command.
ciscoasa#conf t
ciscoasa(config)#hostname basefirewall
basefirewall(config)#
basefirewall(config)#enable password hello123
basefirewall(config)#username hello password hello123
basefirewall(config)#
```

At the bottom of the CLI window, there are 'Copy' and 'Paste' buttons, and a 'Top' link with a checkbox.

5. Need to set the clock and date for the present firewall

```
basefirewall(config)# clock set hh:mm:ss date month in words year
```

6. Configure the interface port 1/1 with an ip address

```
basefirewall (config)#int g1/1
```

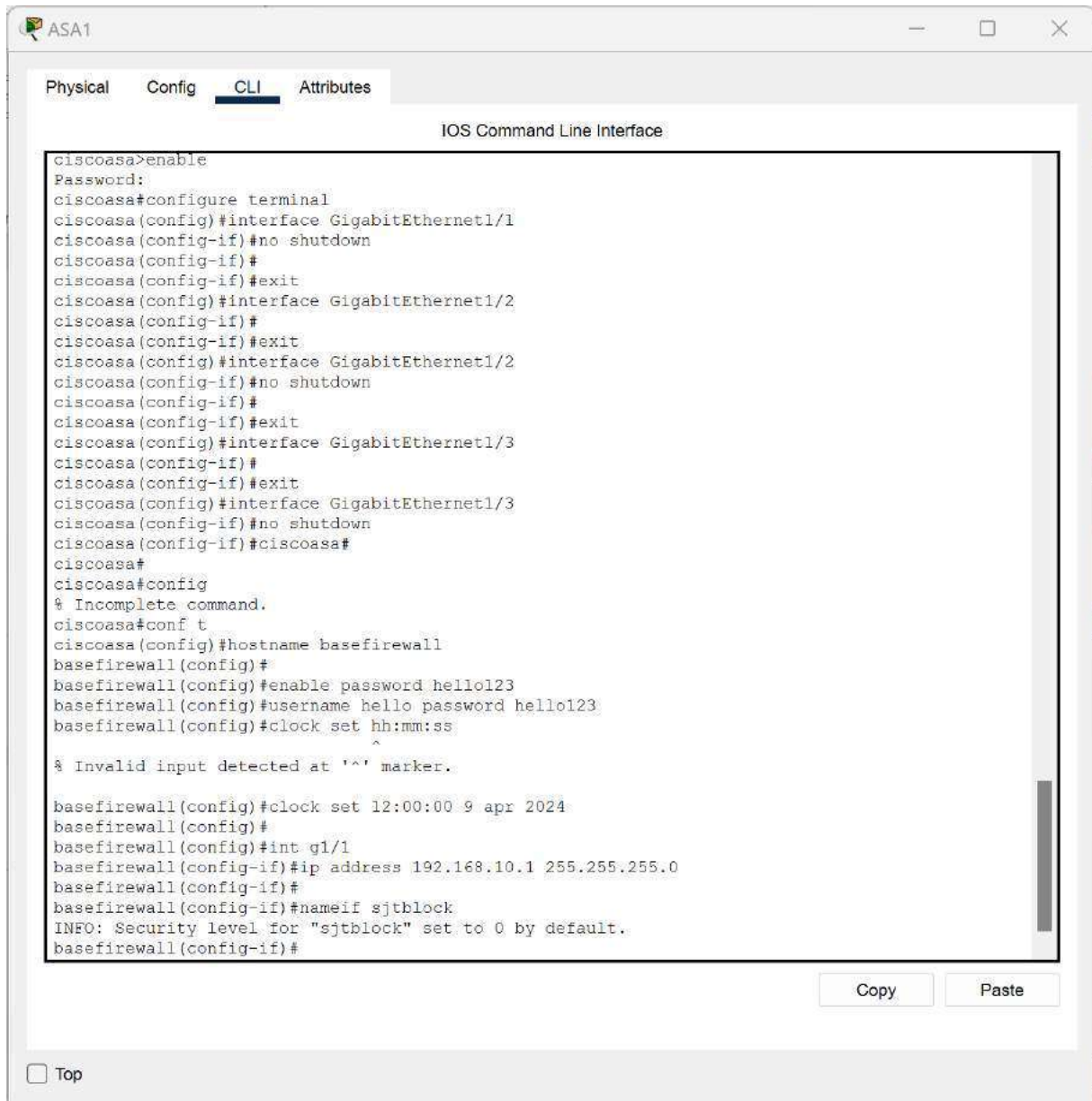
```
basefirewall (config-if)#ip address 192.168.10.1 255.255.255.0
```

7. We need to name the interface port for our easy identification let I name that port as sjtblock

```
basefirewall (config-if)#nameif sjtblock
```

INFO: Security level for "sjtblock" set to 0 by default.

STEPS 5-7



The screenshot shows the Cisco ASA CLI interface with the following commands and output:

```

ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#interface GigabitEthernet1/1
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/2
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#
ciscoasa(config-if)#exit
ciscoasa(config)#interface GigabitEthernet1/3
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#ciscoasa#
ciscoasa#
ciscoasa#config
% Incomplete command.
ciscoasa#conf t
ciscoasa(config)#hostname basefirewall
basefirewall(config)#
basefirewall(config)#enable password hello123
basefirewall(config)#username hello password hello123
basefirewall(config)#clock set hh:mm:ss
^
% Invalid input detected at '^' marker.
basefirewall(config)#clock set 12:00:00 9 apr 2024
basefirewall(config)#
basefirewall(config)#int g1/1
basefirewall(config-if)#ip address 192.168.10.1 255.255.255.0
basefirewall(config-if)#
basefirewall(config-if)#nameif sjtblock
INFO: Security level for "sjtblock" set to 0 by default.
basefirewall(config-if)#
  
```

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" link.

8. Next we need to set the security level of each and every port which has connected to that particular firewall it varies from 0 to 100

Here 0 means no security all are allowed, 100 means it is more trusted port, other numbers are like how much trust u have on that particular port

```
basefirewall (config-if)#security-level 100
```

```
basefirewall (config-if)#exit
```

```
basefirewall (config)#
```

```
basefirewall(config-if)#  
basefirewall(config-if)#nameif sjtblock  
INFO: Security level for "sjtblock" set to 0 by default.  
basefirewall(config-if)#  
basefirewall(config-if)#security-level 100  
basefirewall(config-if)#exit  
basefirewall(config)#
```

9.Next we need to configure the asa firewall as a dhcp server

basefirewall (config)#dhcp ?

basefirewall (config)#dhcp add

basefirewall (config)#dhcpd address

basefirewall (config)#dhcp address 192.168.1.10-192.168.1.15 sjtblock

basefirewall (config)#dhcp dns 192.168.1.1

basefirewall (config)#dhcp en

basefirewall (config)#dhcp enable sjtblock

basefirewall (config)#int gig1/1

basefirewall (config-if)#no shut

basefirewall (config-if)#

basefirewall (config-if)#exit

```
basefirewall(config)#dhcp?  
configure mode commands/options:  
dhcpd  
basefirewall(config)#dhcp address 192.168.1.10-192.168.1.15 sjtblock  
Address range subnet 192.168.1.10 or 192.168.1.15 is not the same as inside interface subnet  
192.168.10.1  
basefirewall(config)#dhcp address 192.168.10.1-192.168.10.15 sjtblock  
basefirewall(config)#dhcp dns 192.168.1.1  
basefirewall(config)#  
basefirewall(config)#dhcp enable sjtblock  
basefirewall(config)#int gig1/1  
basefirewall(config-if)#no shut  
basefirewall(config-if)#  
basefirewall(config-if)#exit  
basefirewall(config)#
```

Copy

Paste

DHCP OUTPUT:

PC0

Physical Config Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.10.12

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 8.8.8.8

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::200:CFF:FE8A:85A5

Default Gateway

DNS Server

802.1X

PC2

Physical Config Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.10.10

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server 8.8.8.8

IPv6 Configuration

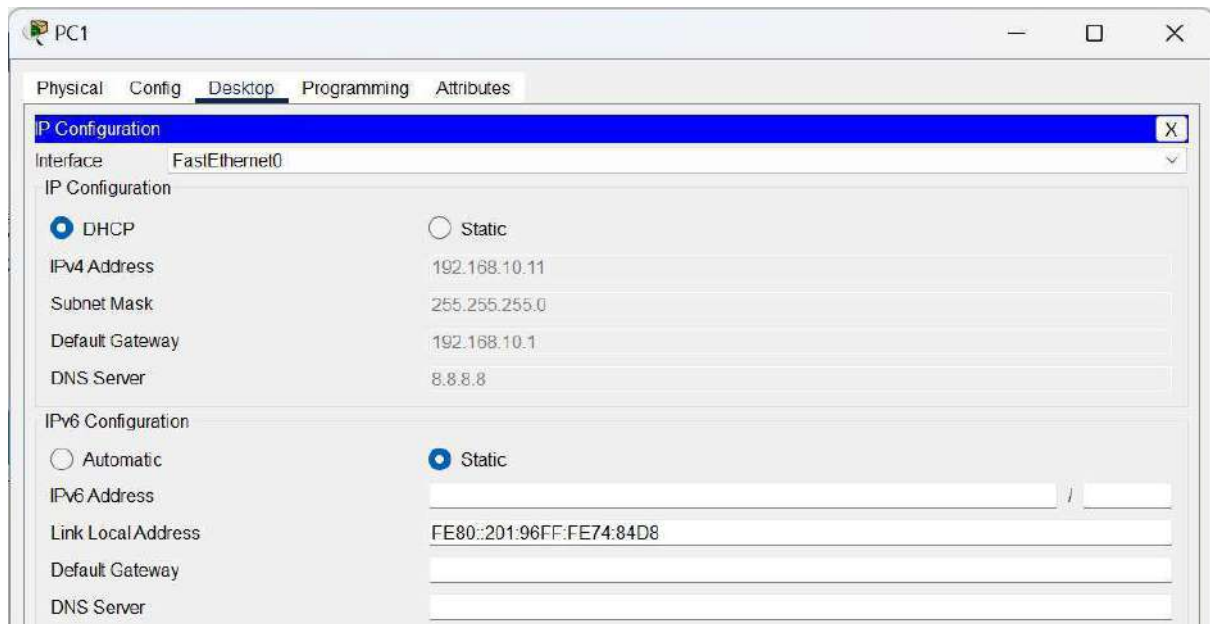
☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:A3FF:FED1:5B5B

Default Gateway

DNS Server



10. For enabling the ssh (remote desktop) we need to configure the local authentication (AAA services)

```
basefirewall (config)#aaa authentication ?  
basefirewall (config)#aaa authentication ssh console ?  
basefirewall (config)#aaa authentication ssh console local
```

11. For providing the encryption security we need to give the type of encryption and their module and the number

```
basefirewall (config)#crypto key generate rsa module 1024  
Do you really want to replace them? [yes/no]: y Keypair
```

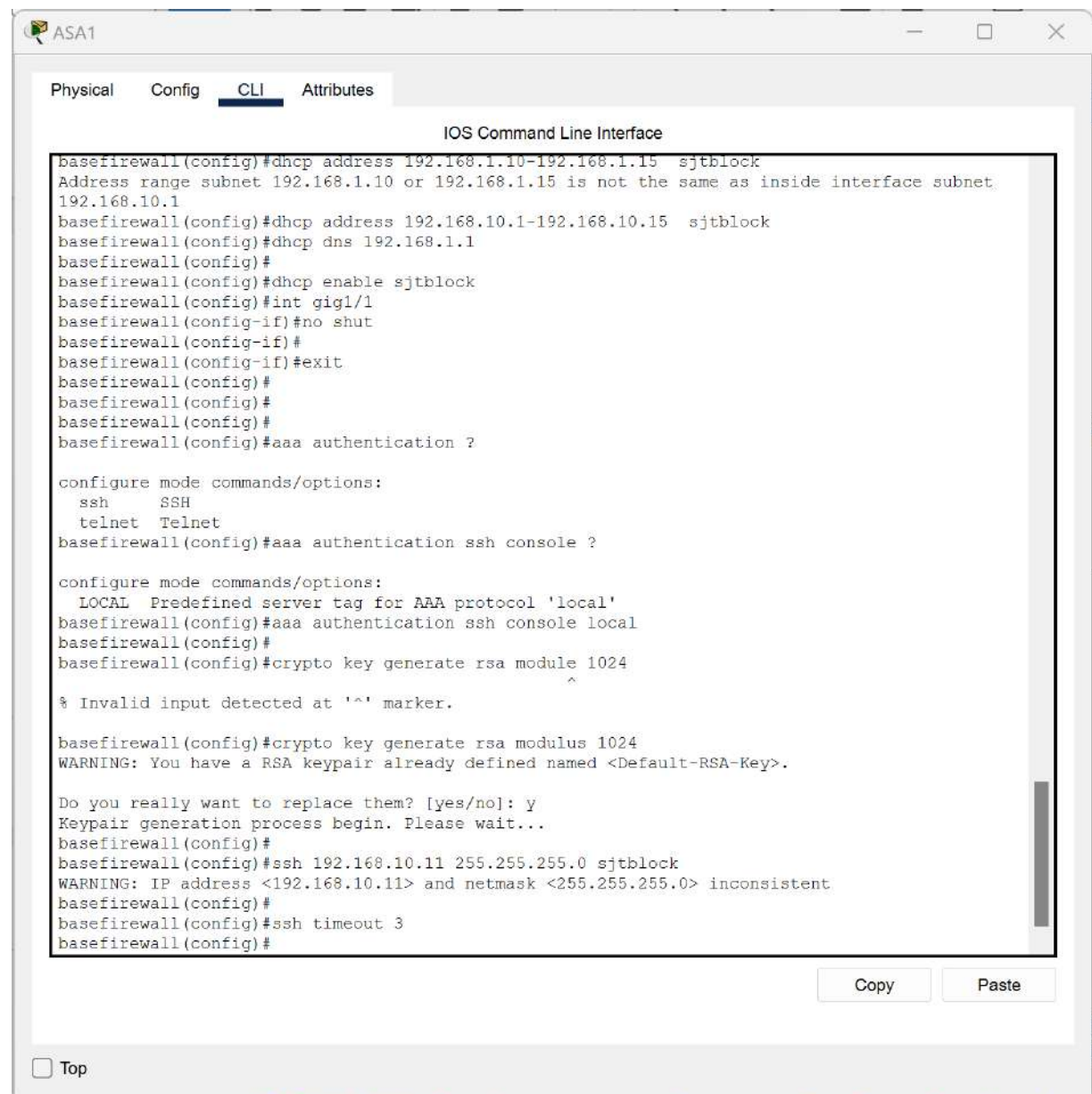
12. Next step to create a blocking process: ssh ip range /single ip wat ever u need u can give to block using for ssh services with their subnet mask and also followed by interface port name

```
basefirewall (config)#ssh 192.168.10.11 255.255.255.0 sjtblock
```

13. Next step is to provide the ssh timeout how many minutes u have to specify

```
basefirewall (config)#ssh timeout 3
```

STEPS 10-13:



The screenshot shows the ASA1 CLI interface with the following commands and output:

```
basefirewall(config)#dhcp address 192.168.1.10-192.168.1.15 sjtblock
Address range subnet 192.168.1.10 or 192.168.1.15 is not the same as inside interface subnet
192.168.10.1
basefirewall(config)#dhcp address 192.168.10.1-192.168.10.15 sjtblock
basefirewall(config)#dhcp dns 192.168.1.1
basefirewall(config)#
basefirewall(config)#dhcp enable sjtblock
basefirewall(config)#int gig1/1
basefirewall(config-if)#no shut
basefirewall(config-if)#
basefirewall(config-if)#exit
basefirewall(config)#
basefirewall(config)#
basefirewall(config)#
basefirewall(config)#aaa authentication ?

configure mode commands/options:
  ssh      SSH
  telnet   Telnet
basefirewall(config)#aaa authentication ssh console ?

configure mode commands/options:
  LOCAL   Predefined server tag for AAA protocol 'local'
basefirewall(config)#aaa authentication ssh console local
basefirewall(config)#
basefirewall(config)#crypto key generate rsa module 1024
% Invalid input detected at '^' marker.

basefirewall(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: y
Keypair generation process begin. Please wait...
basefirewall(config)#
basefirewall(config)#ssh 192.168.10.11 255.255.255.0 sjtblock
WARNING: IP address <192.168.10.11> and netmask <255.255.255.0> inconsistent
basefirewall(config)#
basefirewall(config)#ssh timeout 3
basefirewall(config)#
```

14. **Once u had configured all the things write all the things in the memory for asa firewall the command is write memory**

basefirewall (config)#wr mem Building configuration...

Cryptochecksum: 7ff79915 ffffffffedcb2eee 5cbc628d 5cfc17b5

1213 bytes copied in 1.12 secs (1083 bytes/sec)

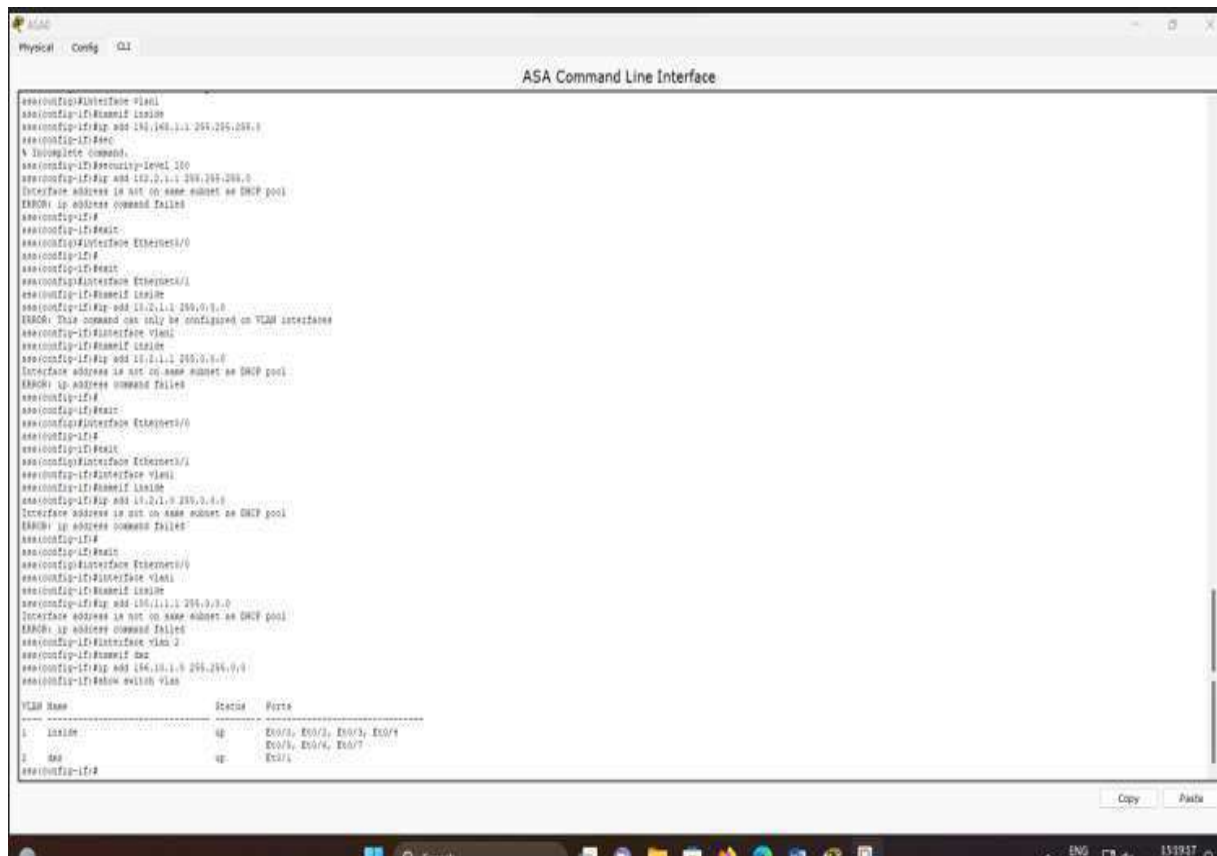
[OK

15. Once u had done all the configurations and saved it in memory if u want to see the configuration wat u had done earlier the command is show start

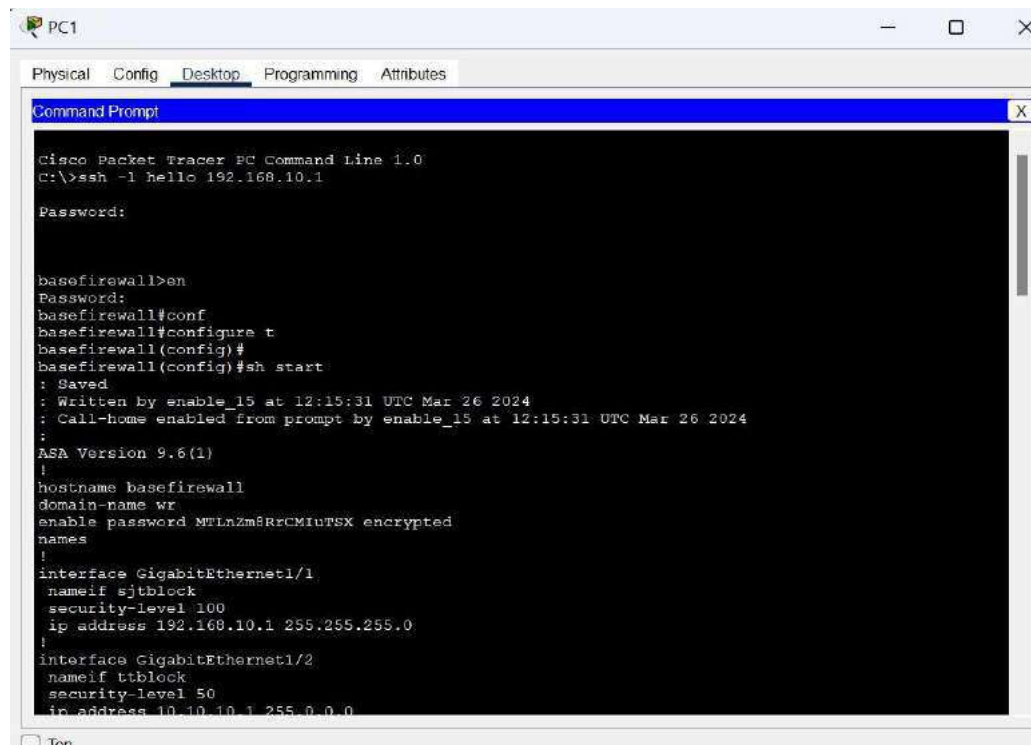
```
basefw(config)#show start
: Saved
: Written by enable_15 at 13:01:41 UTC Mar 26 2024
: Call-home enabled from prompt by enable_15 at 13:01:41 UTC Mar 26 2024
:
ASA Version 9.6(1)
!
hostname basefw domain-name
wr
enable password MTLnZm8RrCMJuTSX encrypted names
!
interface GigabitEthernet1/1 nameif
sjtblock security-level 100 ip address
192.168.10.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif ttblock security-level
50 ip address 10.10.10.1
255.0.0.0
!
interface GigabitEthernet1/3
nameif prpblock security-level
0
ip address 20.20.20.1 255.0.0.0
!
interface GigabitEthernet1/4
no nameif no security-level
no ip address shutdown
!
interface GigabitEthernet1/5
no nameif no security-level
no ip address shutdown
!
interface GigabitEthernet1/6
no nameif no security-level
no ip address shutdown
!
interface GigabitEthernet1/7
no nameif no security-level
no ip address shutdown
!
```

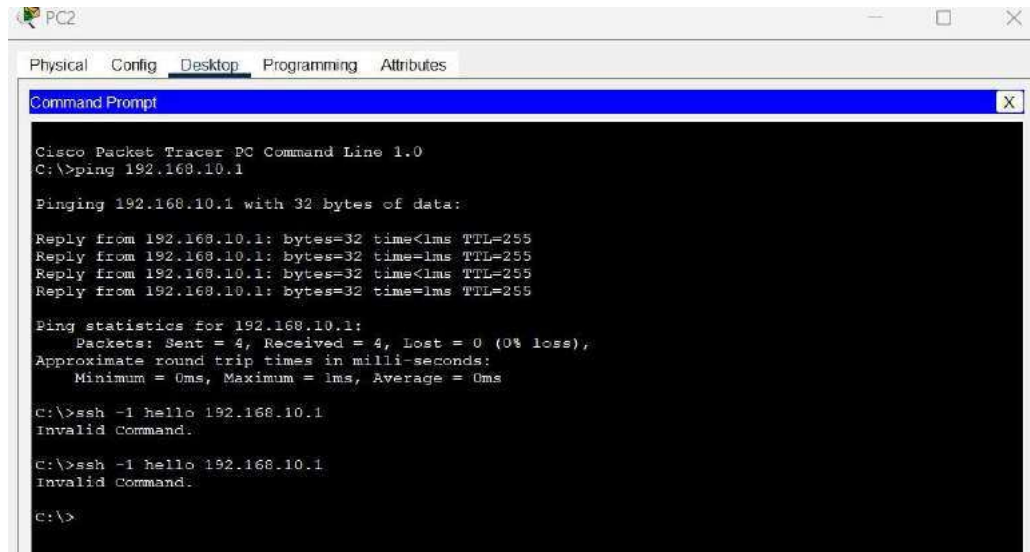


```
interface GigabitEthernet1/8
no nameif no security-level
no ip address shutdown
!
interface Management1/1
management-only no
nameif no security-level
no ip address shutdown
!
!
!
!
!
aaa authentication ssh console LOCAL
!
username hello password MTLnZm8RrCMluTSX encrypted
!
class-map inspection_default match
default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters message-length
maximum 512 policy-map
global_policy class
inspection_default inspect dns
preset_dns_map
inspect ftp
inspect tftp !
service-policy global_policy global
!
telnet timeout 5
ssh 192.168.10.11 255.255.255.0 sgtblock ssh
timeout 3
!
dhcpd dns 8.8.8.8
!
dhcpd address 192.168.10.10-192.168.10.20 sgtblock dhcpd
enable sgtblock
!
!
!
!
basefw(config)# basefw(config)#
```



Ssh output:





```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ssh -l hello 192.168.10.1
Invalid Command.

C:\>ssh -l hello 192.168.10.1
Invalid Command.

C:\>
```



VIT[®]

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

NAME: SAMARTH KUMAR

REG NO : 21BCE2702

COURSE NAME: Information Security Management

FACULTY : VIMALA DEVI K

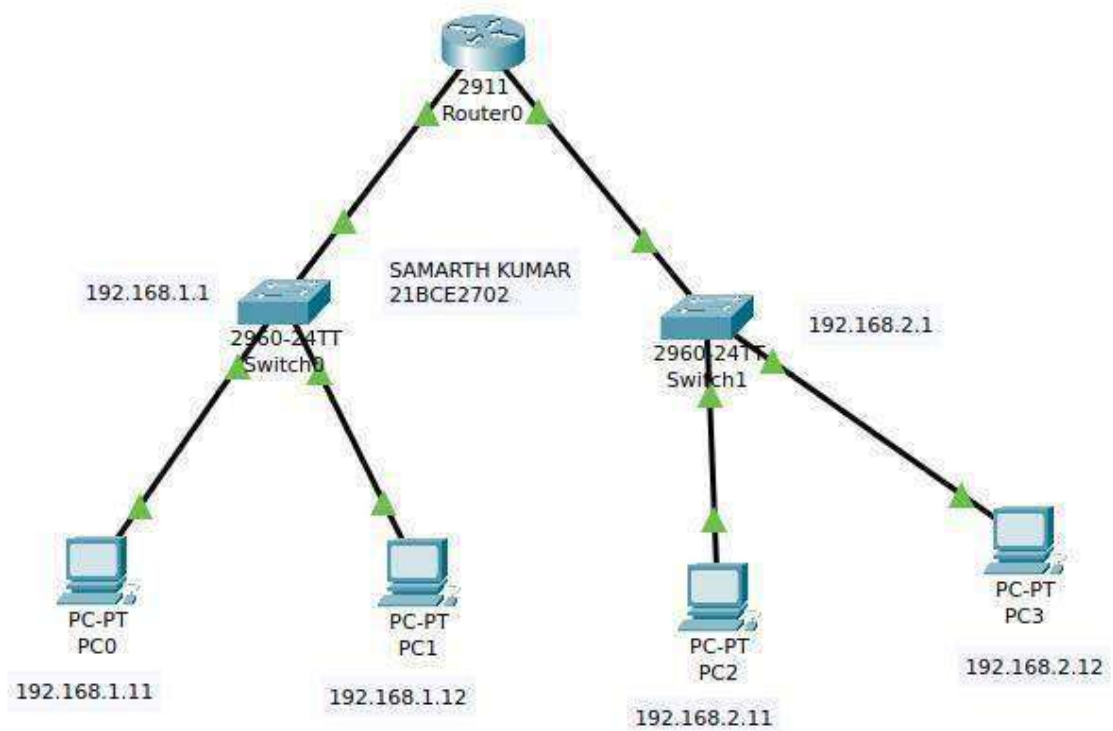
ISM LAB

EXPERIMENT 1

AIM: CONNECTING TWO NETWORKS USING A ROUTER

PROCEDURE:

1. Select a 2911 router
2. Select 2960 2 switches
3. Select 3 PC's



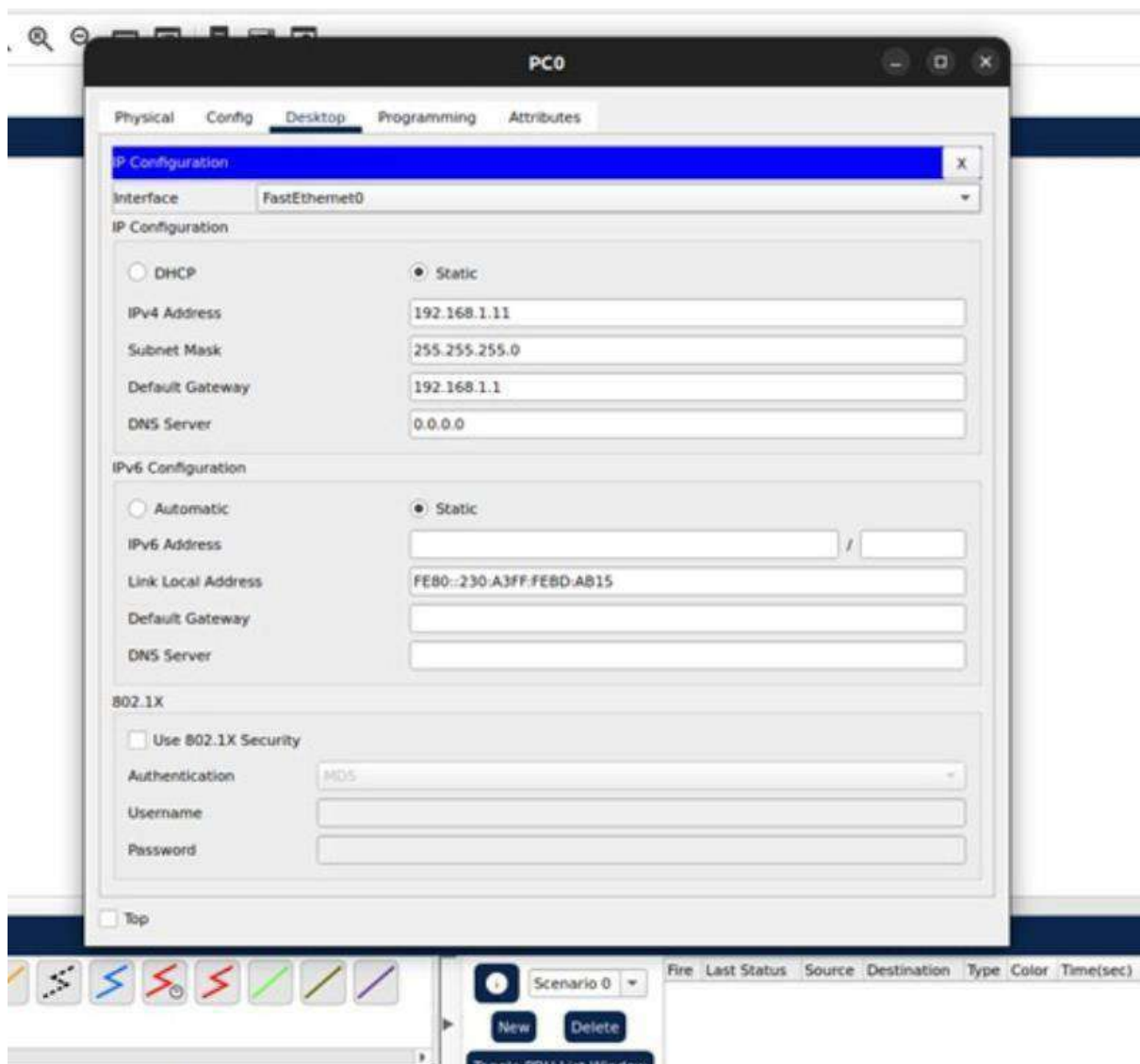
4. From router select gigabitethernet 0/0 to switch0
gigabitethernet 0/1
From router select gigabitethernet 0/1 to switch1
gigabitethernet 0/1
5. PC Configuration:

Give addresses for Pcs in Network1 as : 192.168.1.11 to 192.168.1.13

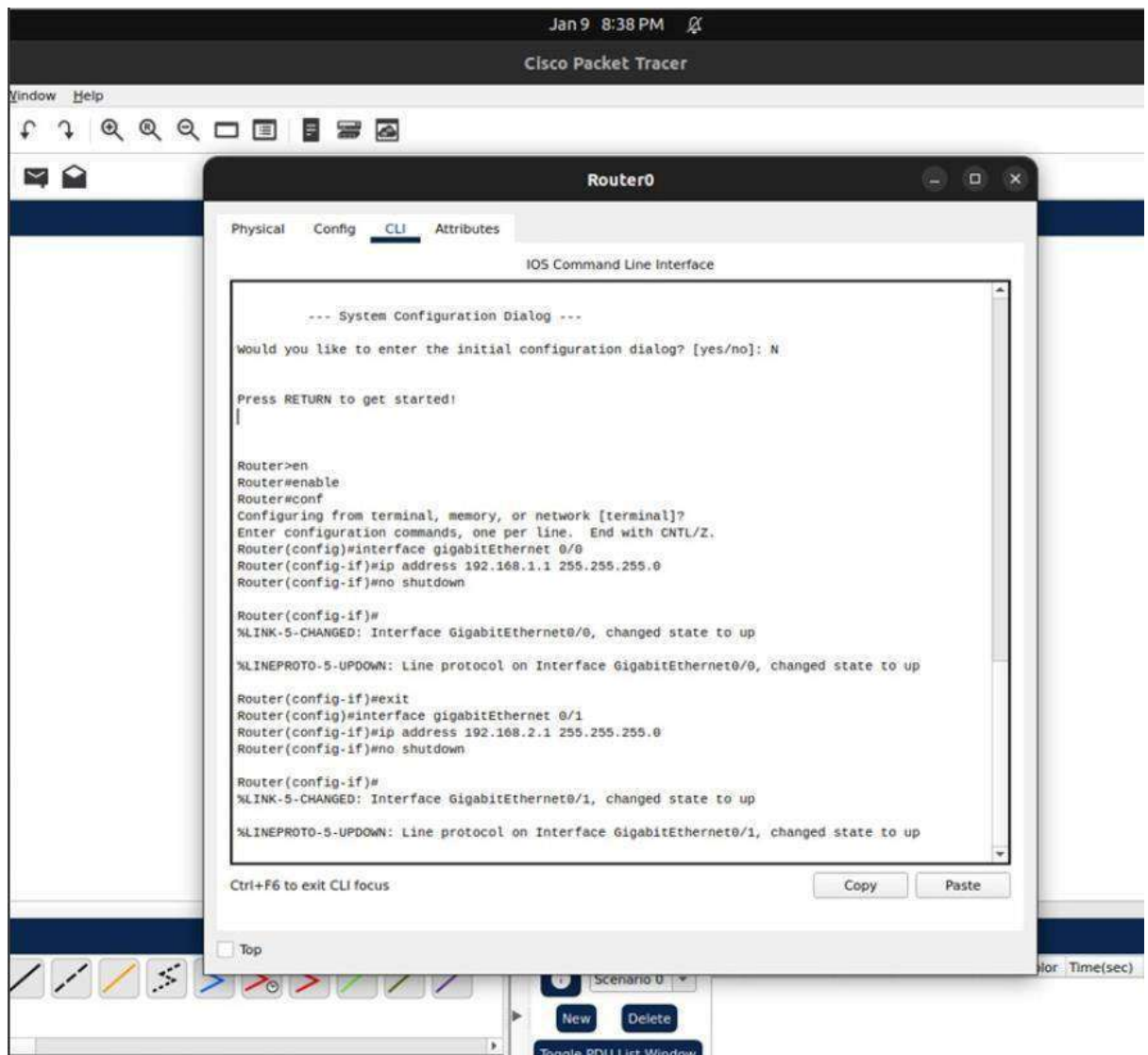
Give addresses for Pcs in Network2 as : 192.168.2.11 to 192.168.2.13

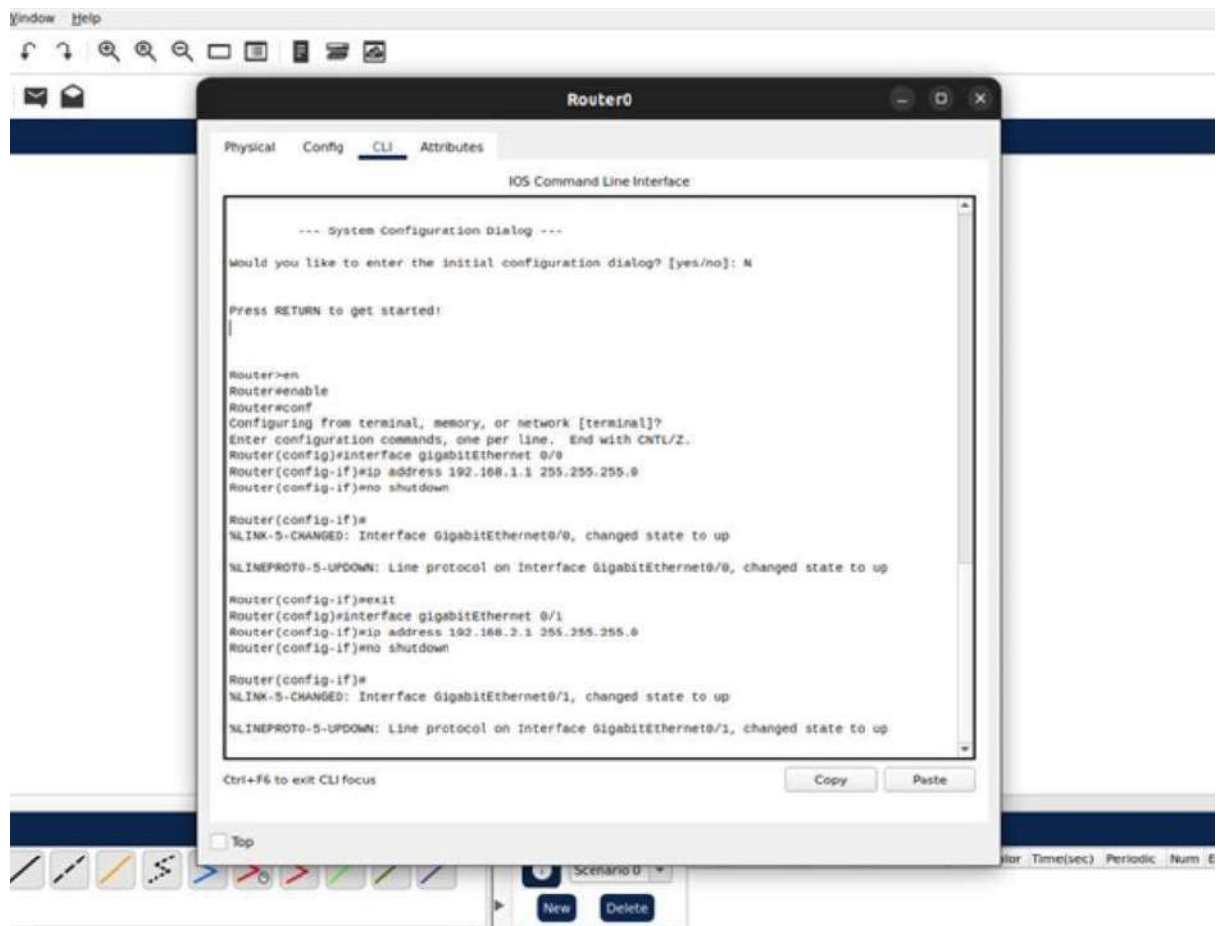
Set default gateway for the leftside network as 192.168.1.1 (as
Similar to router gigabitEthernet 0/0)

Set default gateway for the leftside network as 192.168.2.1 (as
Similar to router gigabitEthernet 0/1)



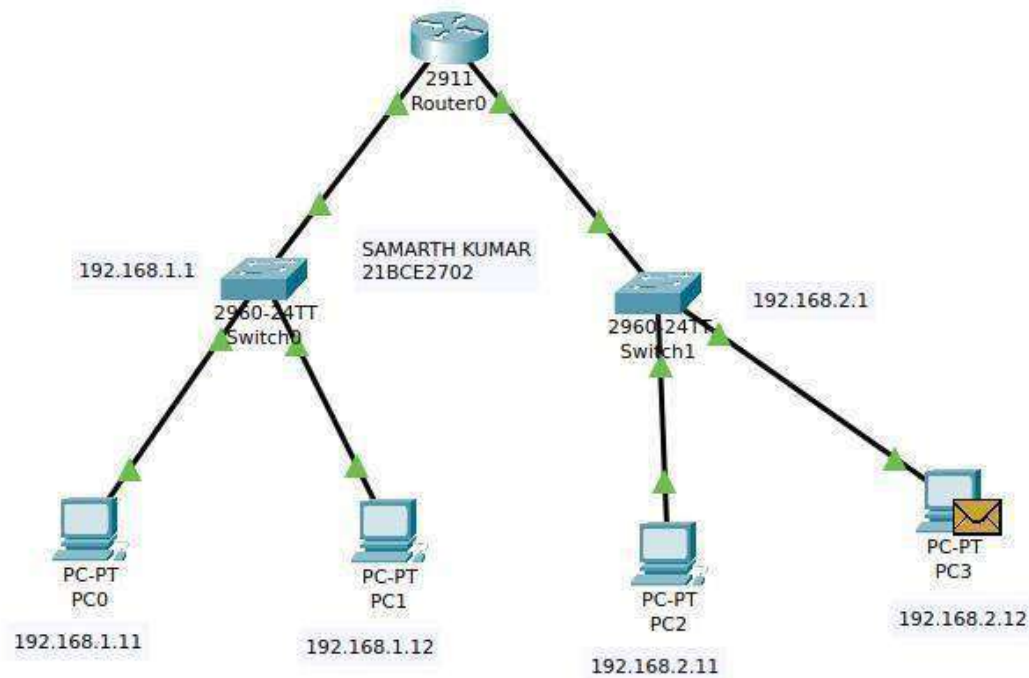
6. Router Configuration: Go to Router and CLI WRITE THE FOLLOWING COMMANDS:





RESULT

- The two networks are successfully connected via the router, allowing communication between devices in different networks.
- PCs within each network can communicate with each other and access resources within their respective networks.
- PCs from Network1 can communicate with PCs from Network2 through the router.



CONCLUSION

The configuration demonstrates the basic setup of interconnecting multiple networks using a router in Cisco Packet Tracer.

It highlights the importance of proper IP addressing and default gateway configuration for devices to communicate across different networks.

This setup serves as a fundamental building block for more complex network configurations and scenarios.

EXPERIMENT 2

AIM: TO CONFIGURE STANDARD ACCESS CONTROL LIST

PROCEDURE :

- Open Cisco Packet tracer • connect 3PC to switch • switch connected to router
- router again to a Server.
- Router has Access control List (ACL) on his outbound direction.
- deny PC 2 for accessing server

SERVER – 10.10.10.11 255.0.0.0

GATEWAY – INT FA 0/1
10.10.10.10

PC 01- 192.168.10.1

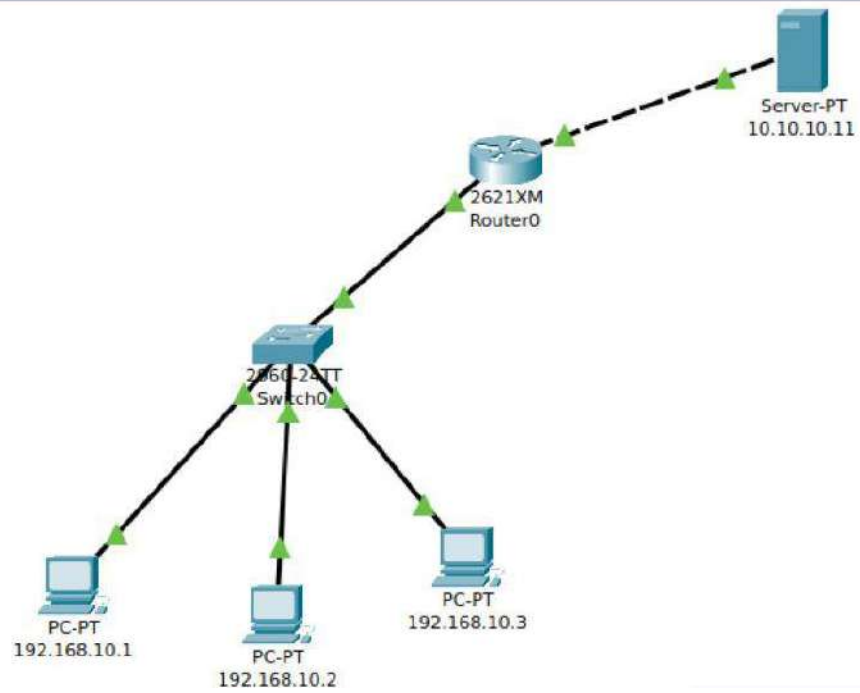
PC 02- 192.168.10.2

PC 03- 192.168.10.3 **GATEWAY**
– INT FA 0/0

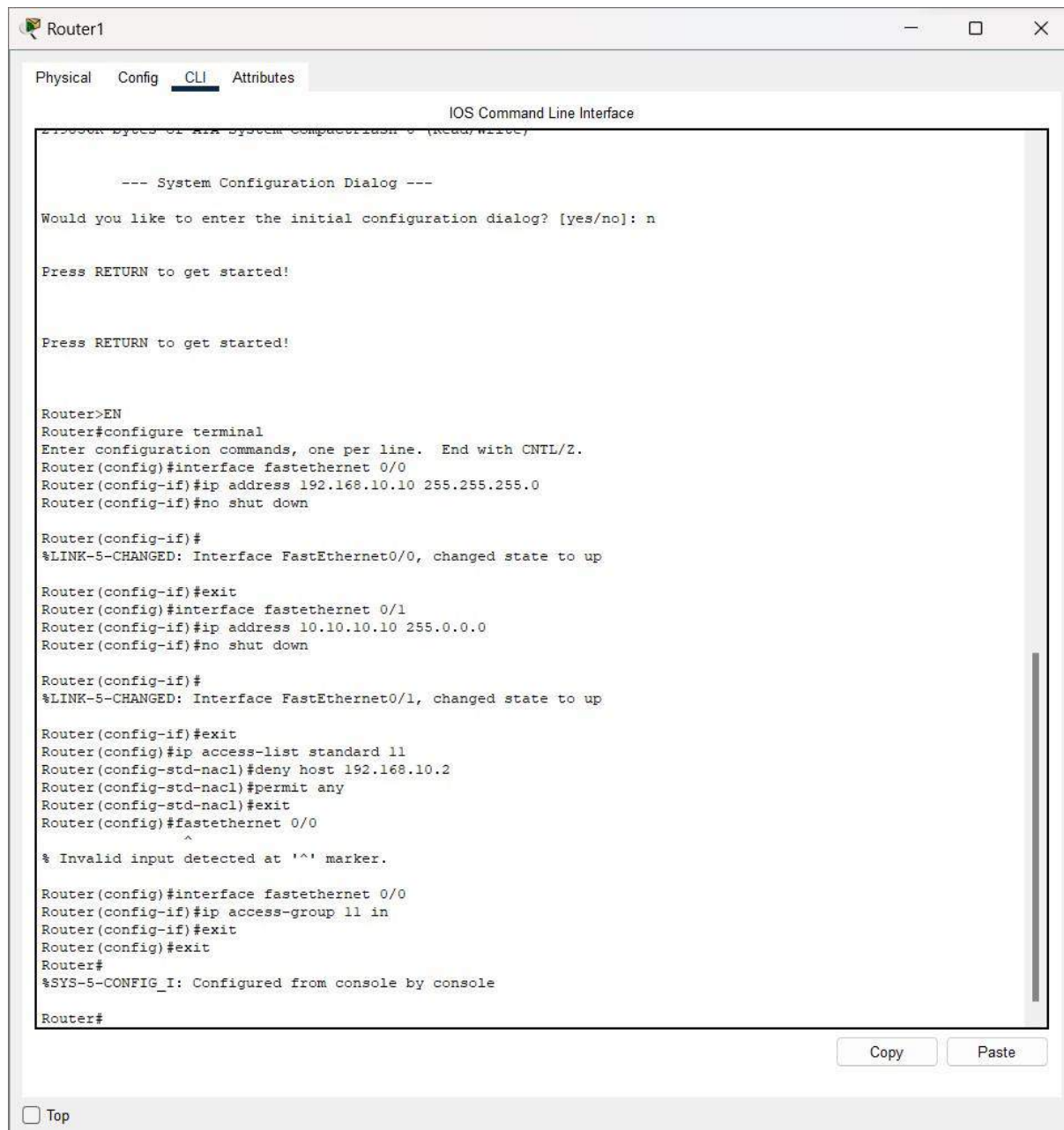
192.168.10.10

SCREENSHOTS:

TOPOLOGY



ROUTER CONFIGURATION



The screenshot shows a web-based interface for configuring a router named 'Router1'. The 'CLI' tab is selected, displaying the 'IOS Command Line Interface'. The interface shows a series of commands entered to configure the router, including setting the terminal configuration mode, configuring two FastEthernet interfaces (0/0 and 0/1) with IP addresses and no shutdown, and configuring an access list (11) to deny traffic from 192.168.10.2 and permit any other traffic. The configuration is applied to interface 0/0. The window includes a 'Copy' button and a 'Paste' button at the bottom right, and a 'Top' link at the bottom left.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

--- System Configuration Dialog ---

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

Press RETURN to get started!

Press RETURN to get started!

Router>EN
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.10.10 255.255.255.0
Router(config-if)#no shut down

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface fastethernet 0/1
Router(config-if)#ip address 10.10.10.10 255.0.0.0
Router(config-if)#no shut down

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#ip access-list standard 11
Router(config-std-nacl)#deny host 192.168.10.2
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#fastethernet 0/0
Router(config-if)#
^
% Invalid input detected at '^' marker.

Router(config)#interface fastethernet 0/0
Router(config-if)#ip access-group 11 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

☐ Top

Copy Paste

SERVER CONFIGURATION

Server0

Physical

Config

Services

Desktop

Programming

Attributes

IP Configuration

X

IP Configuration

☐ DHCP

☒ Static

IPv4 Address

10.10.10.11

Subnet Mask

255.0.0.0

Default Gateway

10.10.10.10

DNS Server

0.0.0.0

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

/

Link Local Address

FE80::260:2FFF:FEBC:A6A8

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication

MD5

Username

Password

☐ Top

PC CONFIGURATION

The screenshot shows a configuration window for PC0 with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying the IP Configuration for the FastEthernet0 interface. The IP Configuration section has two radio buttons: DHCP (unselected) and Static (selected). The Static configuration fields are filled with the following values: IPv4 Address: 192.168.10.1, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.10.10, and DNS Server: 0.0.0.0. The IPv6 Configuration section also has two radio buttons: Automatic (unselected) and Static (selected). The Static configuration fields are filled with the following values: IPv6 Address: (empty), Link Local Address: FE80::250:FFF:FE2E:C518, Default Gateway: (empty), and DNS Server: (empty). The 802.1X section has a checkbox for Use 802.1X Security (unchecked), an Authentication dropdown menu set to MD5, and fields for Username and Password (both empty). A Top button is located at the bottom left of the window.

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.10.1

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.10

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::250:FFF:FE2E:C518

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

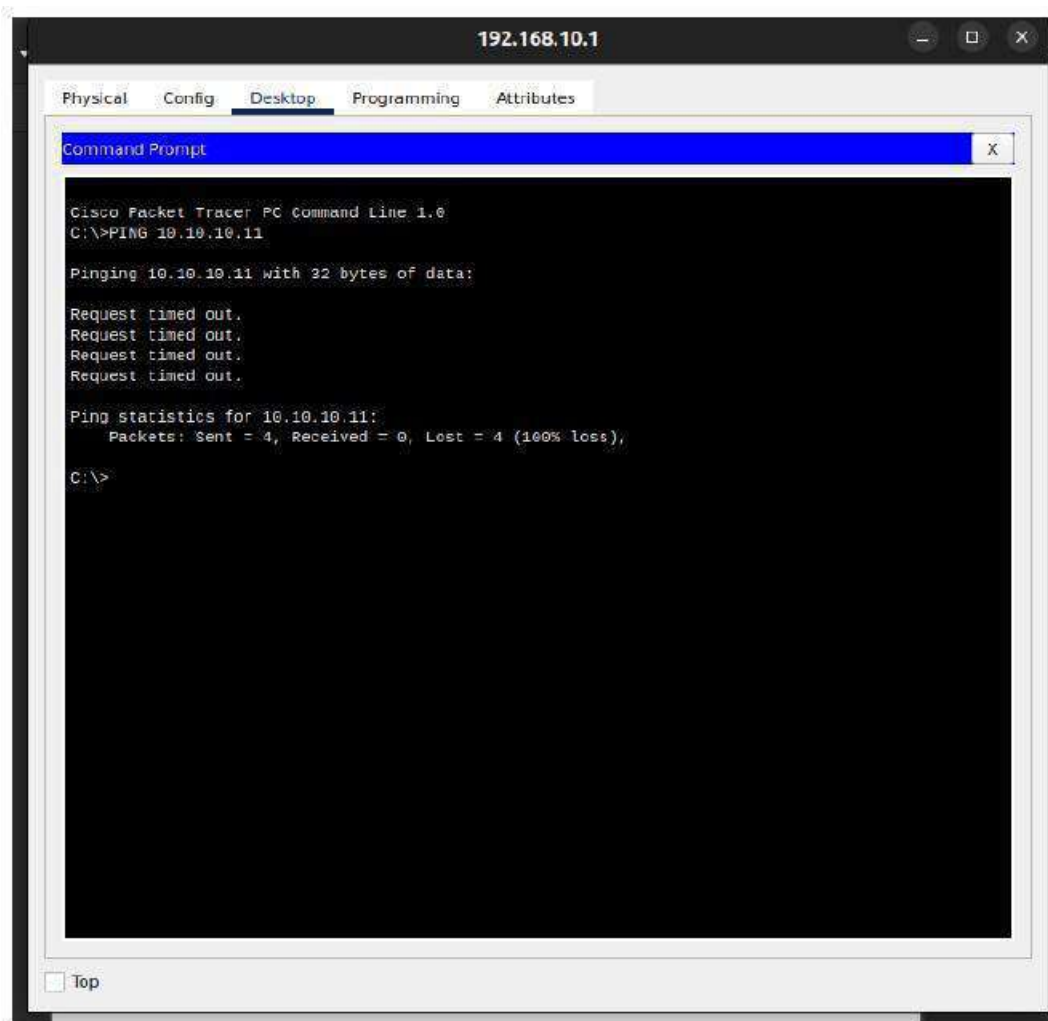
☐ Top

RESULT:

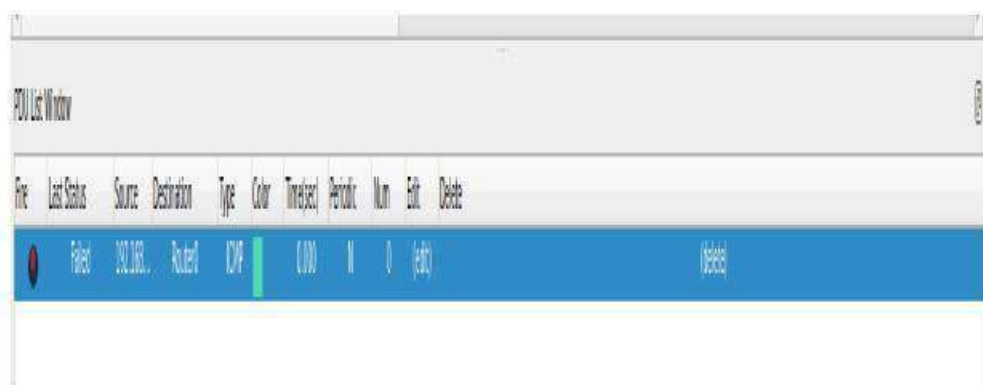
ACL VERIFICATION

```
Router#SHOW ACCESS-LISTS
Standard IP access list 11
 10 deny host 192.168.10.2
 20 permit any
```

- DENY ACCESS TO PC2



- EVENT LIST FAILED



CONCLUSION:

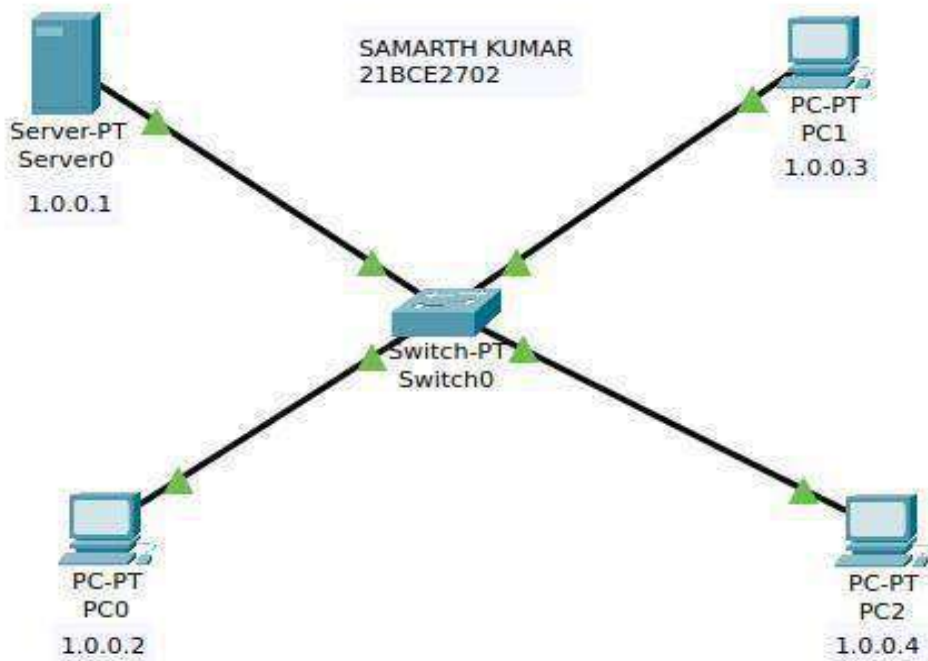
- PC 2 will be unable to access the server due to the Access Control List (ACL) on the router's outbound direction.

- The ACL specifically denies traffic originating from PC 2 from reaching the server. When PC 2 sends packets towards the server:
- The packets will reach the switch and be forwarded to the router.
- The router will analyze the source IP address of the packets, identifying them as originating from PC 2.
- The router will compare the source IP address with the ACL entries.
- Since the ACL contains a "deny" rule for traffic from PC 2, the packets will be dropped, not forwarded to the server.
- PC 2 will receive no response from the server, effectively blocked from accessing it.

EXPERIMENT 3

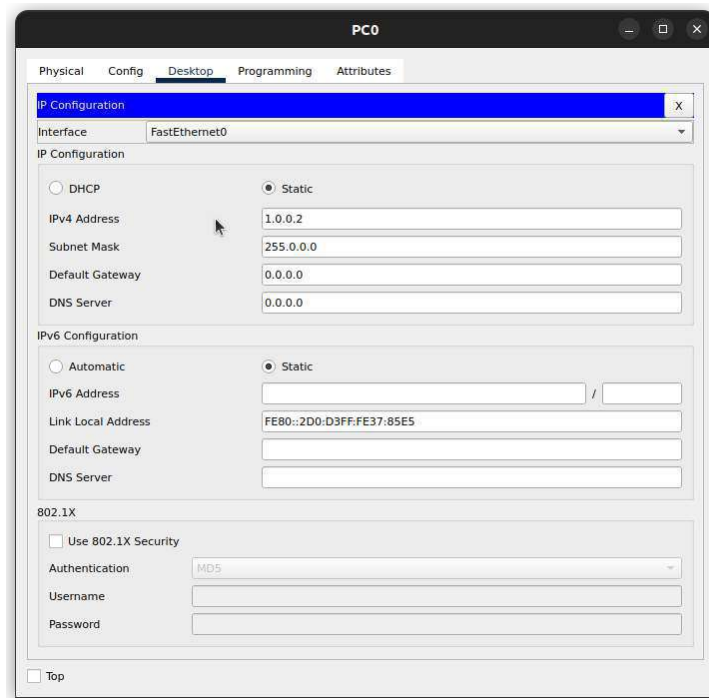
AIM: Configure and Verify Firewall in Cisco Packet Tracer **PROCEDURE:**

1. First, open the Cisco packet tracer desktop and select the devices 3 PC's, 1 server and 1 Switch and assign the following IP Address



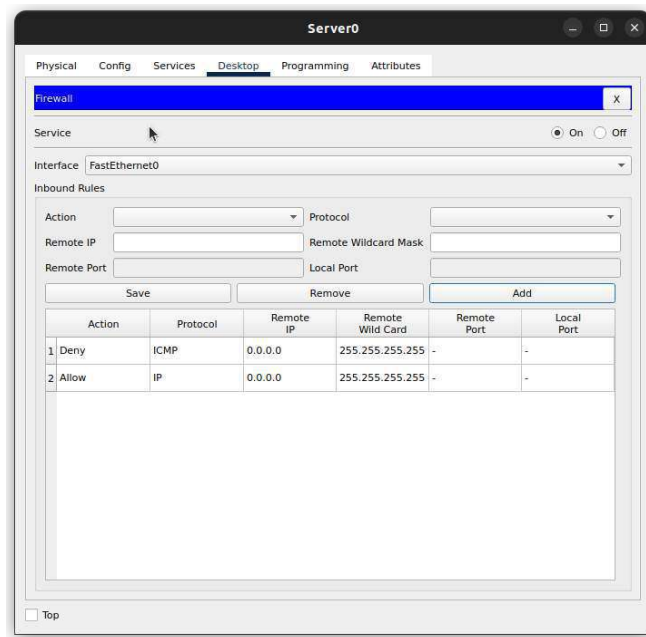
2. Configure the PCs (hosts) and server with IPv4 address and Subnet Mask according to the IP addressing table given above.
 - To assign an IP address in PC0, click on PC0.
 - Then, go to desktop and then IP configuration and there you will IPv4 configuration.
 - Fill IPv4 address and subnet mask.

- Repeat the same procedure with the server



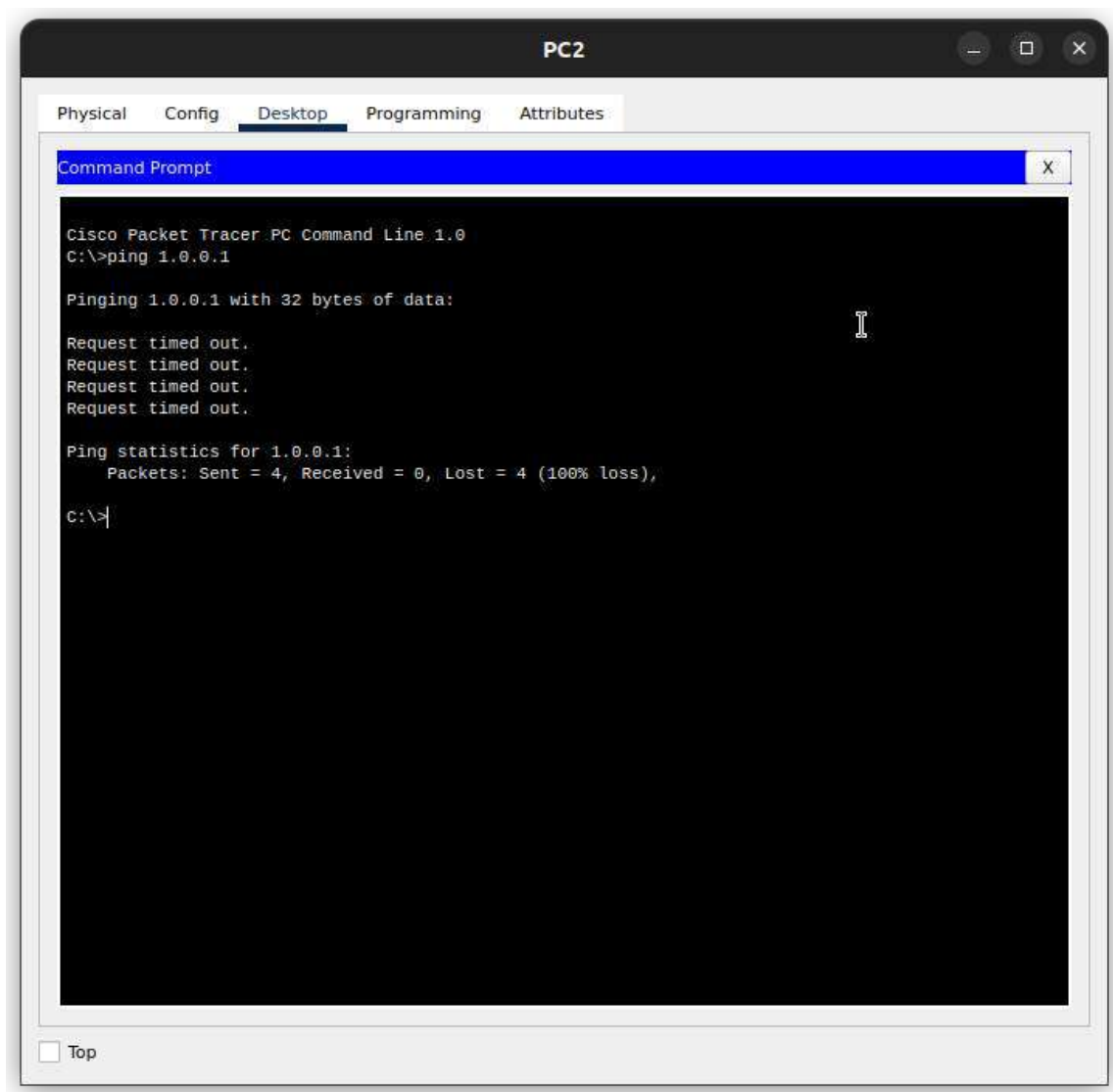
3. Configuring the firewall in a server and blocking packets and allowing web browser.

- Click on server0 then go to the desktop.
- Then click on firewall IPv4.
- Turn on the services.
- First, Deny the ICMP protocol and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255.
- Then, allow the IP protocol and set remote IP to 0.0.0.0 and Remote wildcard mask to 255.255.255.255.
- And add them.



4. Verifying the network by pinging the IP address of any PC.

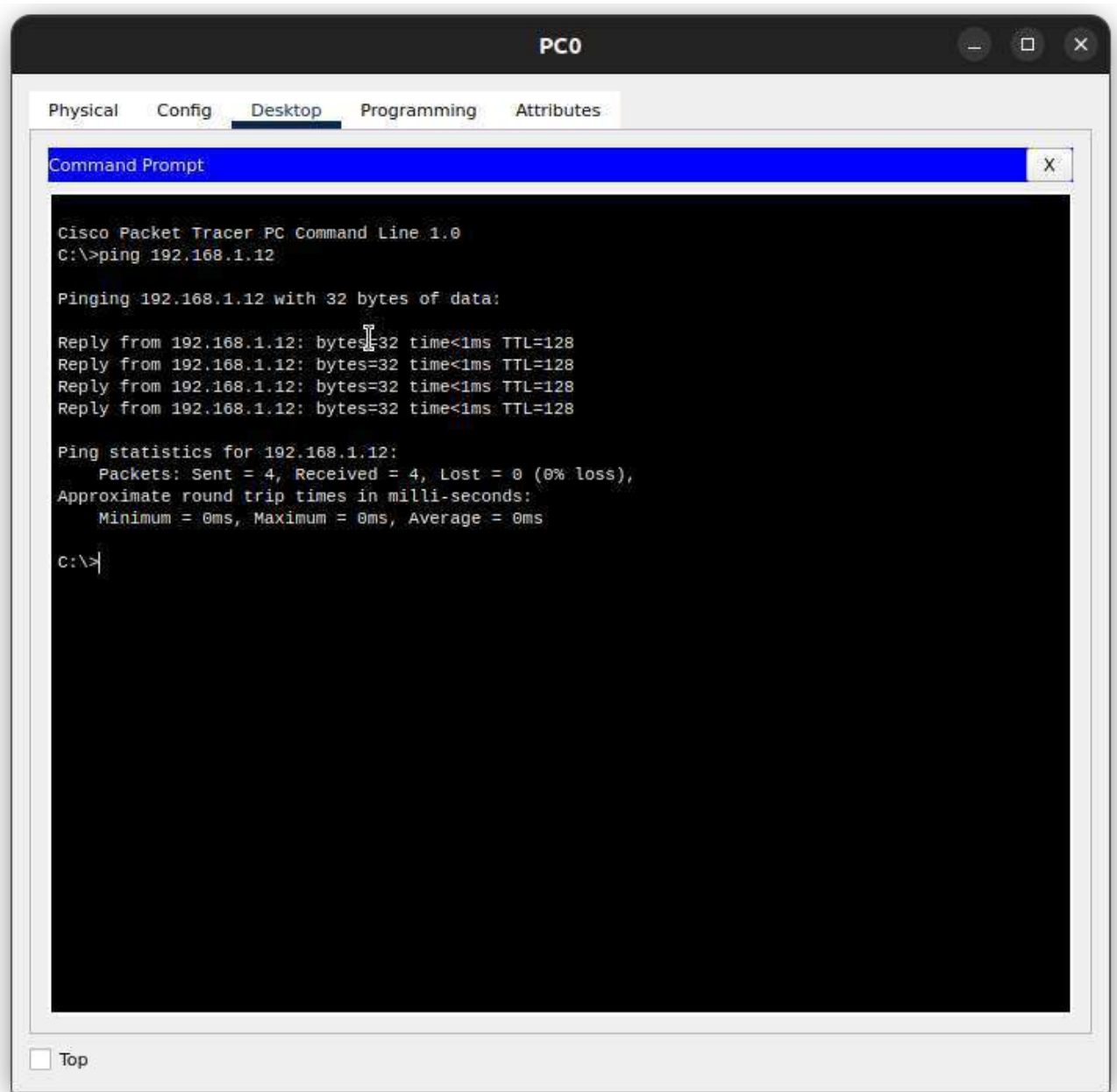
- We will use the ping command to do so.
- First, click on PC2 then Go to the command prompt.
- Then type ping <IP address of targeted node>.
- We will ping the IP address of the server0.
- As we can see in the below image we are getting no replies which means the packets are blocked.



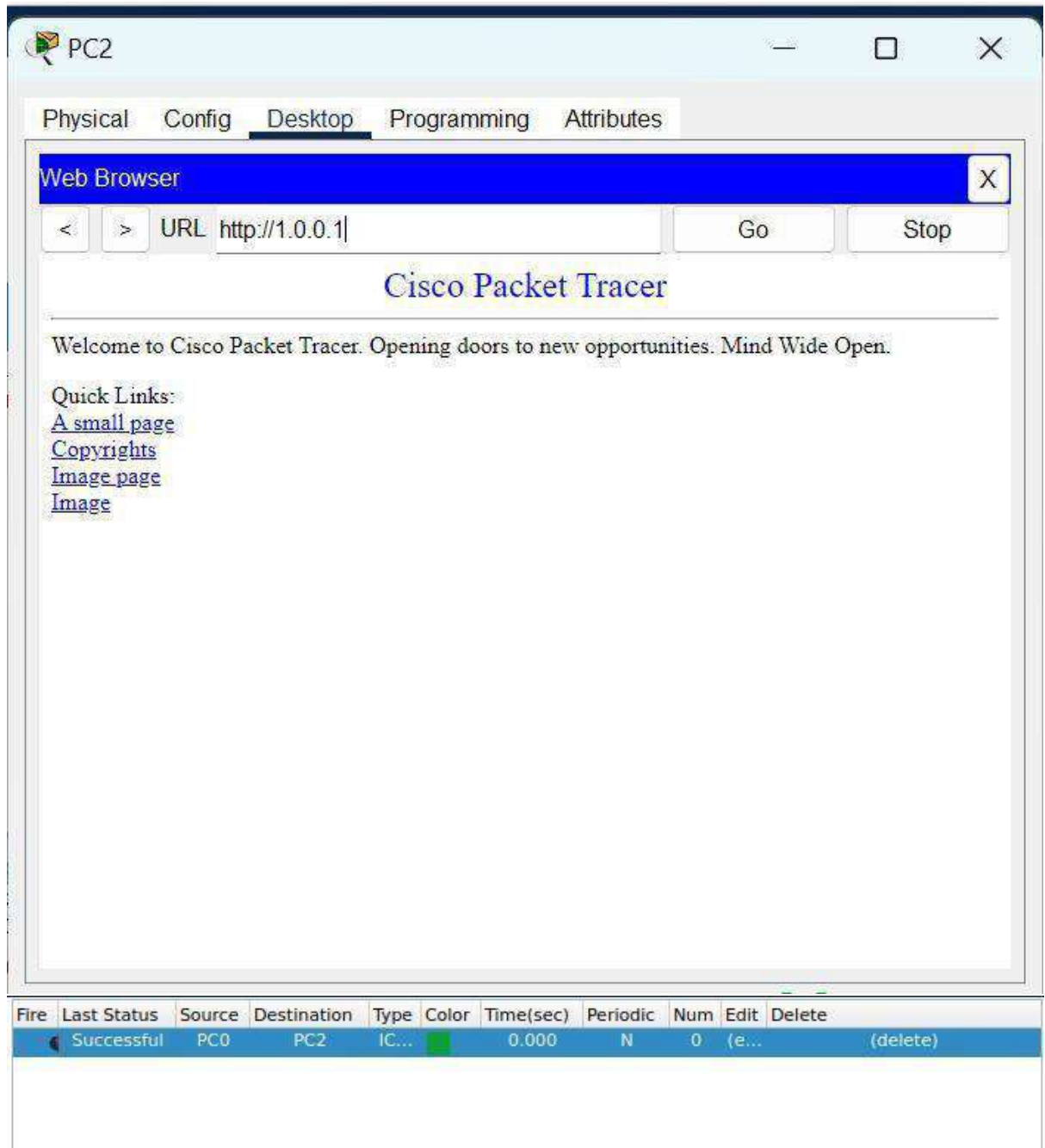
Check the web browser by entering the IP address in the URL.

Click on PC2 and go to desktop then web browser.

After unblocking all the packets



RESULT



The firewall was successfully configured and verified to restrict and control the traffic flow between different network segments. The firewall rules were implemented to allow or deny specific types of traffic based on the defined criteria, and the access control lists were applied to filter traffic based on source and destination IP addresses.

CONCLUSION

In conclusion, the experiment demonstrated the importance of implementing a firewall to enhance network security and protect against unauthorized access and malicious attacks. By configuring and verifying the firewall in

Cisco Packet Tracer, it was evident that network administrators can effectively manage and control the flow of traffic to ensure the confidentiality, integrity, and availability of the network resources. Overall, the experiment provided valuable insights into the practical application of firewall technology in a simulated network environment.



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Digital Assessment - 3

INFORMATION SECURITY AND MANAGEMENT

NAME: SAMARTH KUMAR

REG NO. 21BCE2702

Course Code : BCSE354E

Faculty: VIMALA DEVI K

Traffic and color Analysis for different protocols

1. TCP:

tcp

Interface

Channel

802.11 Preferences

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------------------------|-----------------|------------------------------------|----------|--|---|
| 345 | 2024-03-12 08:28:42.286022553 | 172.217.166.170 | 10.30.158.54 | TCP | 74 | 443 → 45448 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 |
| 346 | 2024-03-12 08:28:42.286112389 | 10.30.158.54 | 172.217.166.170 | TCP | 66 | 45448 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=899449 |
| 347 | 2024-03-12 08:28:42.286323345 | 10.30.158.54 | 172.217.166.170 | TLSv1 | 621 | Client Hello |
| 348 | 2024-03-12 08:28:42.286162710 | 172.217.166.170 | 10.30.158.54 | TCP | 60 | 443 → 45448 [RST, ACK] Seq=1 Ack=556 Win=128512 Len=0 |
| 386 | 2024-03-12 08:28:59.857423177 | 10.30.158.54 | 142.250.183.206 | TCP | 74 | 44588 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM= |
| 387 | 2024-03-12 08:28:59.882689332 | 142.250.183.206 | 10.30.158.54 | TCP | 74 | 443 → 44588 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 |
| 388 | 2024-03-12 08:28:59.882701218 | 10.30.158.54 | 142.250.183.206 | TCP | 66 | 44588 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=233513 |
| 389 | 2024-03-12 08:28:59.882938802 | 10.30.158.54 | 142.250.183.206 | TLSv1 | 605 | Client Hello |
| 28 | 2024-03-12 08:26:00.288982317 | 172.217.166.170 | 10.30.158.54 | TCP | 66 | 443 → 40762 [RST, ACK] Seq=1 Ack=620 Win=128512 Len=0 |
| 237 | 2024-03-12 08:27:33.348632107 | 10.30.158.54 | 37.59.29.33 | TCP | 74 | [TCP Retransmission] [TCP Port numbers reused] 37498 → 656 |
| 238 | 2024-03-12 08:27:33.830671821 | Cisco_6b:cd:96 | Cisco_6b:cd:96 | LOOP | 60 | Reply |
| 239 | 2024-03-12 08:27:33.95135501 | Cisco_6b:cd:96 | Spanning-tree (for bridges)_00 STP | 80 | RST, Root = 32768/150/00:00:2f:01:cd:96 Cost = 35 Port = | |
| 240 | 2024-03-12 08:27:34.372645089 | 10.30.158.54 | 37.59.29.33 | TCP | 74 | [TCP Retransmission] [TCP Port numbers reused] 37498 → 656 |
| 241 | 2024-03-12 08:27:35.956425523 | Cisco_6b:cd:96 | Spanning-tree (for bridges)_00 STP | 80 | RST, Root = 32768/150/00:00:2f:01:cd:96 Cost = 35 Port = | |

Analysis:

1. Packet Information:

- Timestamp: 2024-03-12 08:26:00.287272076
- Source IP: 10.30.158.54
- Destination IP: 172.217.166.170
- Protocol: TCP
- Length: 66 bytes
- Message: 40762 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
TSval=899287075 TSecr=1022103074

2. Explanation:

- TCP (Transmission Control Protocol): TCP is a connection-oriented protocol used for reliable and ordered delivery of data between devices over an IP network.
- Source Port (40762) and Destination Port (443): These are port numbers representing the source and destination endpoints of the TCP connection. Port 443 is commonly used for HTTPS traffic, which is secured with SSL/TLS.
- [ACK]: This TCP flag indicates that the packet is acknowledging receipt of data from the other end of the connection.
- Seq=1 Ack=1: These fields indicate the sequence and acknowledgment numbers of the TCP segments. In this case, it suggests that the next expected sequence number from the sender is 1, and the acknowledgment number indicates the sender has received data up to sequence number 1 from the receiver.

- Win=64256: This field represents the TCP window size, which is the amount of data (in bytes) that can be sent without receiving an acknowledgment. A larger window size indicates more available buffer space for receiving data.
- Len=0: Indicates the length of the TCP segment's payload in bytes. In this case, it's zero, indicating that there is no payload in this particular TCP segment.

3. Traffic Analysis:

- This packet represents an acknowledgment (ACK) sent from the source (IP: 10.30.158.54) to the destination (IP: 172.217.166.170) in response to data received over a TCP connection.
- The connection appears to be initiated from port 40762 on the source side and directed towards port 443 on the destination side, commonly associated with HTTPS traffic.
- The acknowledgment confirms the receipt of data up to sequence number 1 and acknowledges the readiness to receive further data.

4. Color:

- In Wireshark, TCP traffic is represented by a light purple colour. This colour coding simplifies the analysis process, making it easier for users to distinguish and focus on TCP-related packets within the network capture.
- In Wireshark, yellow text on a red background typically indicates a packet with a checksum error. This color scheme helps highlight potential issues with data integrity, prompting further investigation by network analysts to ensure the reliability and accuracy of transmitted data.
- Wireshark highlights potential issues by displaying them in red text on a black background. This distinctive colour scheme draws attention to critical problems, aiding network administrators in quickly identifying and resolving issues within network traffic.

2. SSDP

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------------------------|--------------|-----------------|----------|--------|---------------------|
| 94 | 2024-03-12 08:26:16.097222972 | 10.30.158.40 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 95 | 2024-03-12 08:26:16.352636790 | 10.30.158.58 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 97 | 2024-03-12 08:26:17.098506648 | 10.30.158.40 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 104 | 2024-03-12 08:26:20.831207793 | 10.30.158.21 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 106 | 2024-03-12 08:26:21.832173861 | 10.30.158.21 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 107 | 2024-03-12 08:26:22.833944891 | 10.30.158.21 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 110 | 2024-03-12 08:26:23.834794541 | 10.30.158.21 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 116 | 2024-03-12 08:26:32.634906315 | 10.30.158.72 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 117 | 2024-03-12 08:26:33.636238598 | 10.30.158.72 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 121 | 2024-03-12 08:26:34.636350588 | 10.30.158.72 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 120 | 2024-03-12 08:26:35.636582483 | 10.30.158.72 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 137 | 2024-03-12 08:26:45.752554460 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 138 | 2024-03-12 08:26:46.753831830 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 140 | 2024-03-12 08:26:47.754189182 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 143 | 2024-03-12 08:26:48.754842125 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 144 | 2024-03-12 08:26:49.883462227 | 10.30.158.46 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 146 | 2024-03-12 08:26:50.584403297 | 10.30.158.46 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 147 | 2024-03-12 08:26:51.386883836 | 10.30.158.46 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 149 | 2024-03-12 08:26:52.387344116 | 10.30.158.46 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 157 | 2024-03-12 08:27:00.585891451 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 159 | 2024-03-12 08:27:02.586279581 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 162 | 2024-03-12 08:27:02.586906287 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 165 | 2024-03-12 08:27:03.588126195 | 10.30.158.34 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 173 | 2024-03-12 08:27:09.716598138 | 10.30.158.44 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 175 | 2024-03-12 08:27:10.718038696 | 10.30.158.44 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 176 | 2024-03-12 08:27:11.719278365 | 10.30.158.44 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 178 | 2024-03-12 08:27:12.726095597 | 10.30.158.44 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 179 | 2024-03-12 08:27:13.863714565 | 10.30.158.70 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 181 | 2024-03-12 08:27:13.489641978 | 10.30.158.16 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
| 185 | 2024-03-12 08:27:14.004986287 | 10.30.158.70 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |

1. Packet Information:

| | | | | | | |
|----|-------------------------------|--------------|-----------------|------|-----|---------------------|
| 94 | 2024-03-12 08:26:16.097222972 | 10.30.158.40 | 239.255.255.250 | SSDP | 215 | M-SEARCH * HTTP/1.1 |
|----|-------------------------------|--------------|-----------------|------|-----|---------------------|

- Timestamp: 2024-03-12 08:26:16.097222972
- Source IP: 10.30.158.40
- Destination IP: 239.255.255.250
- Protocol: SSDP
- Length: 215 bytes
- Message: M-SEARCH * HTTP/1.1

2. Explanation:

- **SSDP (Simple Service Discovery Protocol):** This is a network protocol primarily used for discovery of network services in Universal Plug and Play (UPnP) devices. It operates over UDP (User Datagram Protocol) and utilizes multicast for communication.
- **M-SEARCH:** This is an SSDP method used for discovering devices or services available on the network. It is akin to a multicast query sent by a client to discover services. In this case, the asterisk (*) denotes that the client is looking for all services available on the network.
- **HTTP/1.1:** SSDP uses a simple HTTP-like protocol for communication. This portion indicates that the message follows the format of HTTP version 1.1.

3. Traffic Analysis:

- This packet represents a client's (source IP: 10.30.158.40) search for available services on the network. It sends an SSDP M-SEARCH request to the multicast address 239.255.255.250.
- The M-SEARCH request is a broadcast-like message, seeking responses from any devices or services that support SSDP.
- Typically, devices such as printers, media servers, or routers may respond to such requests if they support SSDP.
- This type of traffic is common in network discovery processes, especially in home networks or environments where UPnP devices are prevalent.

4. Color:

In Wireshark, SSDP (Simple Service Discovery Protocol) packets are displayed in **light blue colour**. This distinctive colour makes it easy for users to identify and focus on SSDP traffic within network captures, aiding in the analysis of devices and services discovery processes on the network.

3. DNS

| Interface | Channel | Source | Destination | Protocol | Length | Info |
|-----------|---------|--------------|--------------|----------|--------|--|
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 100 | Standard query 0xbf26 A optimizationguide-pa.googleapis.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 100 | Standard query 0xee23 HTTPS optimizationguide-pa.googleapis.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 100 | Standard query response 0xee23 HTTPS optimizationguide-pa.googleapis.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 100 | Standard query response 0xbf26 A optimizationguide-pa.googleapis.com A 172.217.166.170 |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 91 | Standard query 0x3828 A boot.net.anydesk.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 91 | Standard query 0x3e73 AAAA boot.net.anydesk.com OPT |
| eth0 | | 10.30.158.40 | 10.30.158.54 | DNS | 172 | Standard query response 0x3e73 AAAA boot.net.anydesk.com SOA ns-889.awsdns-47.net OPT |
| eth0 | | 10.30.158.40 | 10.30.158.54 | DNS | 187 | Standard query response 0x3828 A boot.net.anydesk.com A 37.59.29.33 OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 91 | Standard query 0xd5bd AAAA boot.net.anydesk.com OPT |
| eth0 | | 10.30.158.40 | 10.30.158.54 | DNS | 172 | Standard query response 0xd5bd AAAA boot.net.anydesk.com SOA ns-889.awsdns-47.net OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 91 | Standard query 0x7b95 AAAA boot.net.anydesk.com OPT |
| eth0 | | 10.30.158.40 | 10.30.158.54 | DNS | 172 | Standard query response 0x7b95 AAAA boot.net.anydesk.com SOA ns-889.awsdns-47.net OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 98 | Standard query 0x3961 A accounts.google.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 98 | Standard query 0xf2da HTTPS accounts.google.com OPT |
| eth0 | | 10.30.158.40 | 10.30.158.54 | DNS | 106 | Standard query response 0x3961 A accounts.google.com A 142.250.4.84 OPT |
| eth0 | | 10.30.158.40 | 10.30.158.54 | DNS | 98 | Standard query response 0xf2da HTTPS accounts.google.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 98 | Standard query 0x38fe A clients2.google.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 98 | Standard query 0x5e1f HTTPS clients2.google.com OPT |
| eth0 | | 10.30.158.40 | 10.30.158.54 | DNS | 98 | Standard query response 0x5e1f HTTPS clients2.google.com OPT |
| eth0 | | 10.30.158.40 | 10.10.4.10 | DNS | 138 | Standard query response 0x39f6 A clients2.google.com CNAME clients.l.google.com A 142. |

Analysis for ->

15 2024-03-12 08:26:00.261859748 10.10.4.10 10.30.158.54 DNS 362

Standard query response 0xbf26 A optimizationguide-pa.googleapis.com A

172.217.166.170 A 172.217.174.234 A 216.58.203.10 A 142.250.71.106 A 142.250.183.42

A 142.250.183.74 A 142.250.183.106 A 142.250.192.10 A 142.250.192.42 A

142.250.192.74 A 142.250.192.106 A 142.250.192.138 A 142.251.42.10 A 142.251.42.42 A

142.251.42.74 A 172.217.166.74 OPT

1. Packet Information:

26:00.261859748 10.10.4.10 10.30.158.54 DNS 362 Standard query response 0xbfd6 A optimizationguide

- Timestamp: 2024-03-12 08:26:00.261859748
- Source IP: 10.10.4.10
- Destination IP: 10.30.158.54
- Protocol: DNS
- Length: 362 bytes
- Message: Standard query response

2. Explanation:

- DNS (Domain Name System): This is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates domain names to IP addresses and vice versa.
- Standard Query Response: This part of the DNS message indicates that the packet is a response to a DNS query. It contains the resolved IP addresses for the queried domain name.

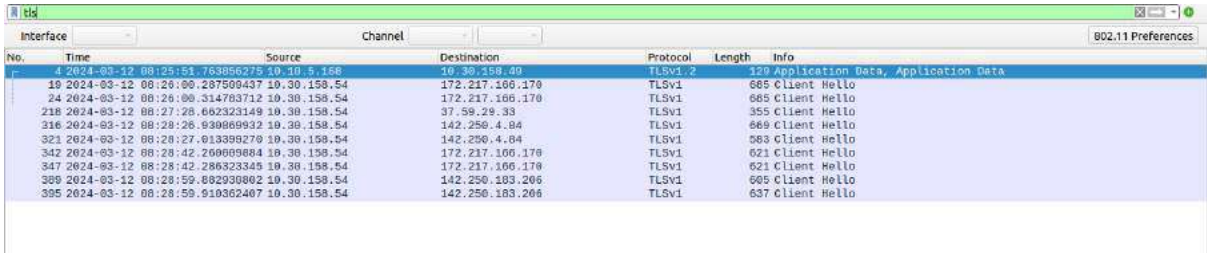
3. Traffic Analysis:

- This packet represents a DNS response from a DNS server (source IP: 10.10.4.10) to a client (destination IP: 10.30.158.54) that queried for the domain name "optimizationguide-pa.googleapis.com".
- The DNS server has resolved the domain name to multiple IP addresses (A records). These IP addresses are provided in the response.
- The IP addresses provided are for the domain "optimizationguide-pa.googleapis.com" and include a list of IPv4 addresses (A records) that can be used to reach the specified domain.
- The DNS response also includes an OPT record, which is an extension mechanism in DNS for adding extra data to DNS messages.

4. Color:

In Wireshark, DNS packets are displayed in **light blue color**. This distinctive colour makes it easy for users to identify and focus on SSDP traffic within network captures, aiding in the analysis of devices and services discovery processes on the network.

4. TLS



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------------------------|--------------|-----------------|----------|--------|------------------------------------|
| 4 | 2024-03-12 08:25:51.763856275 | 10.10.5.168 | 10.30.158.49 | TLSv1.2 | 129 | Application Data, Application Data |
| 19 | 2024-03-12 08:28:00.287500437 | 10.30.158.54 | 172.217.166.170 | TLSv1 | 685 | Client Hello |
| 24 | 2024-03-12 08:28:00.314703712 | 10.30.158.54 | 172.217.166.170 | TLSv1 | 355 | Client Hello |
| 218 | 2024-03-12 08:27:28.662323149 | 10.30.158.54 | 37.59.29.33 | TLSv1 | 689 | Client Hello |
| 316 | 2024-03-12 08:28:26.930869932 | 10.30.158.54 | 142.250.4.04 | TLSv1 | 583 | Client Hello |
| 321 | 2024-03-12 08:28:27.013398270 | 10.30.158.54 | 142.250.4.04 | TLSv1 | 621 | Client Hello |
| 342 | 2024-03-12 08:28:42.260009684 | 10.30.158.54 | 172.217.166.170 | TLSv1 | 621 | Client Hello |
| 347 | 2024-03-12 08:28:42.286323345 | 10.30.158.54 | 172.217.166.170 | TLSv1 | 605 | Client Hello |
| 389 | 2024-03-12 08:28:59.582930802 | 10.30.158.54 | 142.250.183.206 | TLSv1 | 637 | Client Hello |
| 395 | 2024-03-12 08:28:59.510362407 | 10.30.158.54 | 142.250.183.206 | TLSv1 | | |

Analysis for->

4 2024-03-12 08:25:51.763856275 10.10.5.168 10.30.158.49 TLSv1.2 129
Application Data, Application Data

1. Packet Information:



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------------------------|-------------|--------------|----------|--------|------------------------------------|
| 4 | 2024-03-12 08:25:51.763856275 | 10.10.5.168 | 10.30.158.49 | TLSv1.2 | 129 | Application Data, Application Data |

- Timestamp: 2024-03-12 08:25:51.763856275
- Source IP: 10.10.5.168
- Destination IP: 10.30.158.49
- Protocol: TLSv1.2
- Length: 129 bytes
- Message: Application Data, Application Data

2. Explanation:

- TLS (Transport Layer Security): TLS is a cryptographic protocol used to secure communication over a network. It ensures privacy, data integrity, and authentication between communicating applications.
- TLSv1.2: This indicates the version of the TLS protocol being used for the communication. TLSv1.2 is one of the widely used versions, providing strong security features.
- Application Data: This part of the TLS packet indicates that the payload contains application-layer data encrypted and secured by the TLS protocol.

3. Traffic Analysis:

- This packet represents encrypted data being transmitted securely between a client (source IP: 10.10.5.168) and a server (destination IP: 10.30.158.49) over TLSv1.2.
- The packet carries application data, suggesting that it contains information exchanged between the client and server at the application layer.
- Since the data is encrypted under TLS, its contents are not visible in plaintext without proper decryption keys.
- The exchange of application data over TLS ensures that the communication remains confidential and protected from eavesdropping or tampering.

4. Color:

Light purple for TLS

5. ICMPV6

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------------------------|---------------------------|-------------------|----------|--------|---|
| 35 | 2024-03-12 08:26:03.601468500 | :: | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 39 | 2024-03-12 08:26:04.146172099 | :: | ff02::1:ff5b:2d8d | ICMPv6 | 86 | Neighbor Solicitation for fe80::2740:930d:925b:2d8d |
| 40 | 2024-03-12 08:26:04.148415173 | :: | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 46 | 2024-03-12 08:26:05.170588065 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 47 | 2024-03-12 08:26:05.173432466 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 53 | 2024-03-12 08:26:05.652507554 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 69 | 2024-03-12 08:26:09.486330146 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 99 | 2024-03-12 08:26:18.439950118 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 128 | 2024-03-12 08:26:37.226894135 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 158 | 2024-03-12 08:27:01.179292024 | fe80::7f07:1ad:1362:6ads | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 182 | 2024-03-12 08:27:13.837788691 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 307 | 2024-03-12 08:28:24.838297324 | fe80::2740:930d:925b:2d8d | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 406 | 2024-03-12 08:29:02.722011437 | fe80::32df:2000:69ed:5619 | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 547 | 2024-03-12 08:30:10.747802083 | :: | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 549 | 2024-03-12 08:30:11.623837399 | :: | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 561 | 2024-03-12 08:30:14.891144609 | :: | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 566 | 2024-03-12 08:30:15.180643602 | :: | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 569 | 2024-03-12 08:30:15.302502762 | :: | ff02::1:ff63:55de | ICMPv6 | 86 | Neighbor Solicitation for fe80::23a5:51f1:9483:55de |
| 582 | 2024-03-12 08:30:16.327217205 | fe80::23a5:51f1:9483:55de | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 584 | 2024-03-12 08:30:16.501929544 | fe80::23a5:51f1:9483:55de | ff02::1 | ICMPv6 | 62 | Router Solicitation |
| 586 | 2024-03-12 08:30:16.872556065 | fe80::23a5:51f1:9483:55de | ff02::1 | ICMPv6 | 110 | Multicast Listener Report Message v2 |
| 611 | 2024-03-12 08:30:26.487576417 | fe80::23a5:51f1:9483:55de | ff02::1 | ICMPv6 | 62 | Router Solicitation |

Analysis for->

39 2024-03-12 08:26:04.146172099 :: ff02::1:ff5b:2d8d
 ICMPv6 86 Neighbor Solicitation for
 fe80::2740:930d:925b:2d8d

1.Packet Information:

| | | | |
|-------------------------------------|-------------------|--------|--|
| 39 2024-03-12 08:26:04.146172099 :: | ff02::1:ff5b:2d8d | ICMPv6 | 86 Neighbor Solicitation for fe80::2740:930d:925b:2d8d |
|-------------------------------------|-------------------|--------|--|

- Timestamp: 2024-03-12 08:26:04.146172099
- Source IP: ::
- Destination IP: ff02::1:ff5b:2d8d
- Protocol: ICMPv6
- Length: 86 bytes
- Message: Neighbor Solicitation for fe80::2740:930d:925b:2d8d

2. Explanation:

- ICMPv6 (Internet Control Message Protocol version 6): ICMPv6 is a network layer protocol used in IPv6 networks for diagnostic and error reporting purposes, as well as for the management of network devices.
- Neighbor Solicitation: This ICMPv6 message type is used by IPv6 hosts to resolve the link-layer address of a neighbor (e.g., another host or router) on the same link when its IPv6 address is known.

3. Traffic Analysis:

- This packet represents a Neighbor Solicitation message sent by a node (::) to the IPv6 multicast address ff02::1:ff5b:2d8d.
- The Neighbor Solicitation is seeking the link-layer address (MAC address) of the IPv6 address fe80::2740:930d:925b:2d8d.
- IPv6 multicast addresses beginning with ff02::/16 are used for various purposes, including link-local multicast.
- Neighbor Solicitation messages are part of the Neighbor Discovery Protocol (NDP) in IPv6, which is essential for address resolution, neighbor unreachability detection, and other functions in IPv6 networks.

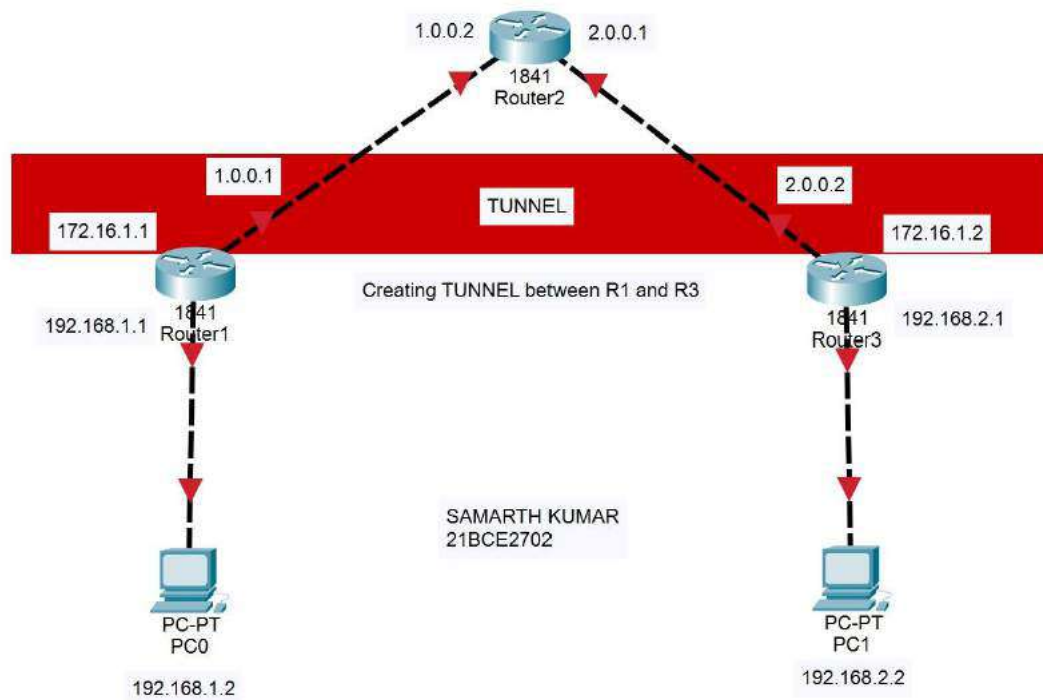
4. Color:

Pink

In Wireshark, ICMPv6 packets are displayed in pink colour. This distinct colour helps users identify and track ICMPv6 traffic within network captures, facilitating efficient analysis and troubleshooting of IPv6 network communications.

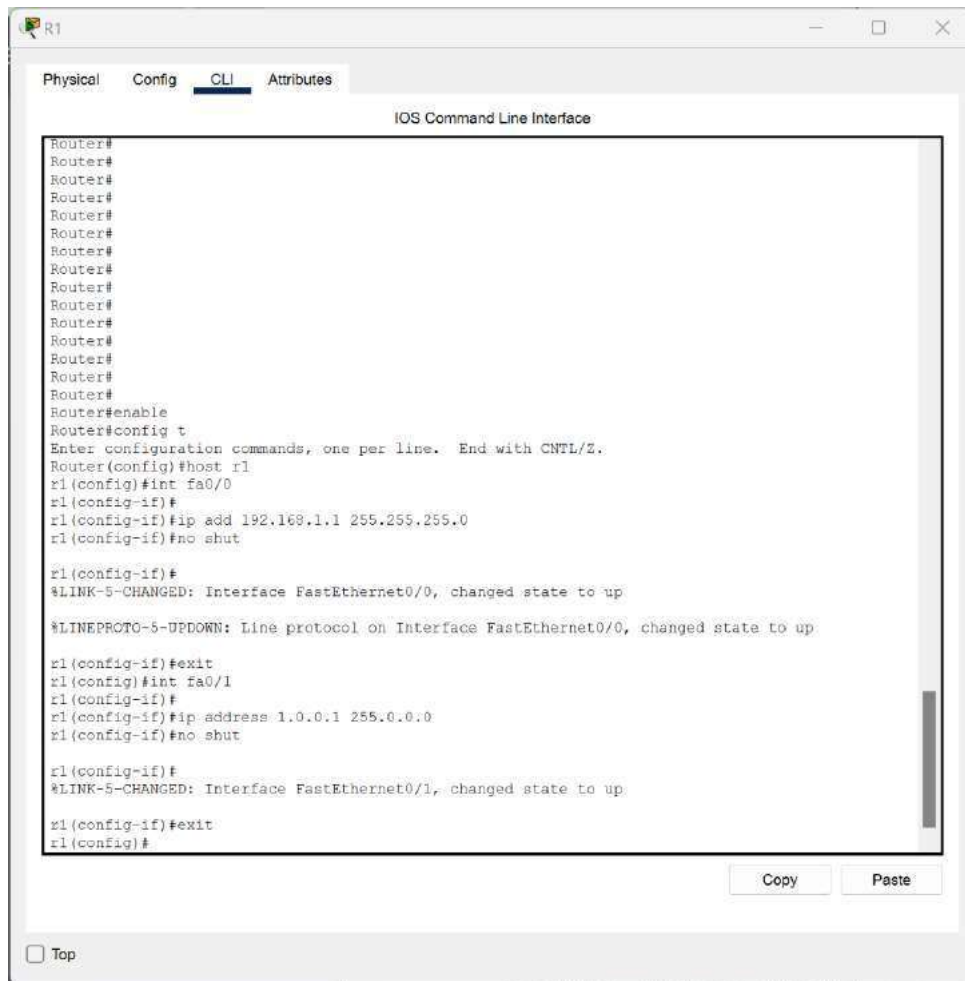
DA 3

VPN configuration Topology:



CONFIGURATION ON ROUTER R1:

```
Router>enable
Router#config t
Router(config)#host r1
r1(config)#int fa0/0
r1(config-if)#ip add 192.168.1.1 255.255.255.0
r1(config-if)#no shut
r1(config-if)#exit
r1(config)#int fa0/1
r1(config-if)#ip address 1.0.0.1 255.0.0.0
r1(config-if)#no shut
```



CONFIGURATION ON ROUTER R2:

Router>enable

Router#config t

Router(config)#host r2

r2(config)#int fa0/0

r2(config-if)#ip add 1.0.0.2 255.0.0.0

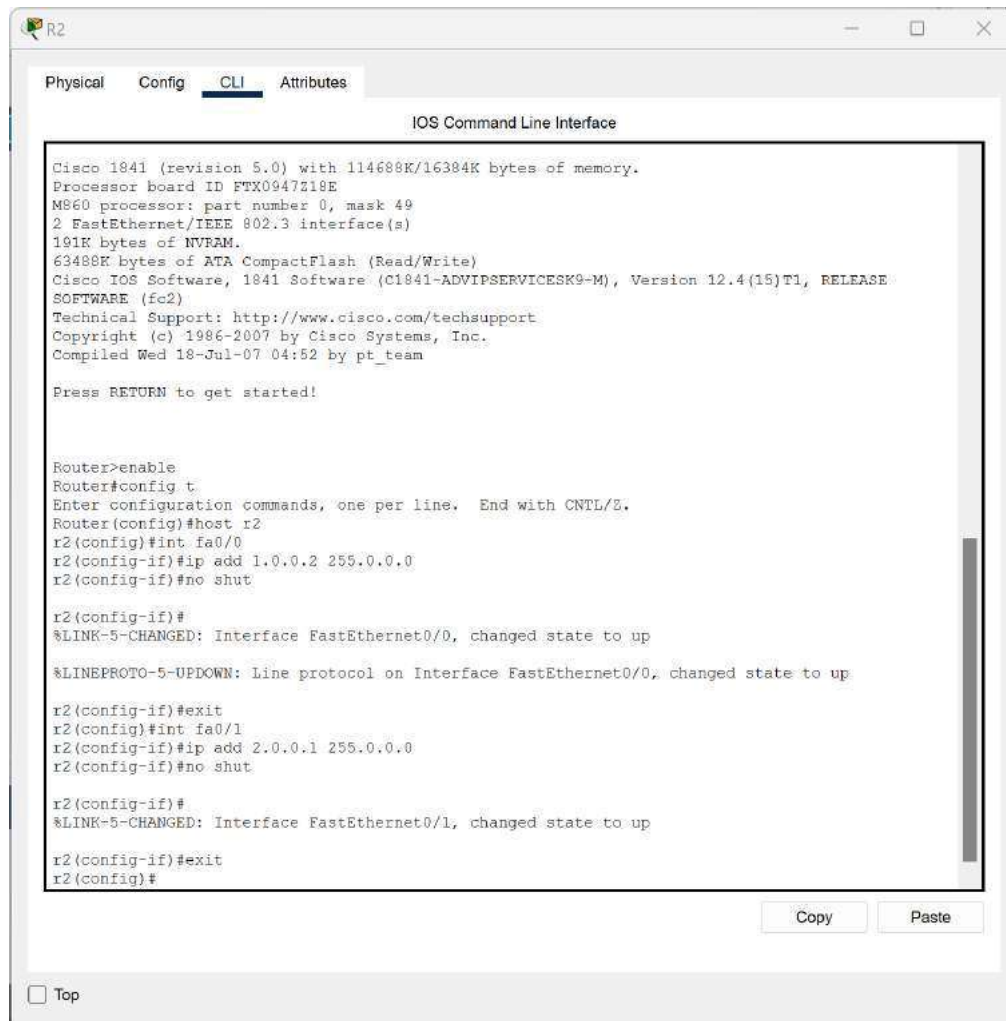
r2(config-if)#no shut

r2(config-if)#exit

r2(config)#int fa0/1

r2(config-if)#ip add 2.0.0.1 255.0.0.0

r2(config-if)#no shut



CONFIGURATION ON ROUTER R3:

Router>enable

Router#config t

Router(config)#host r3

r3(config)#int fa0/0

r3(config-if)#ip add 2.0.0.2 255.0.0.0

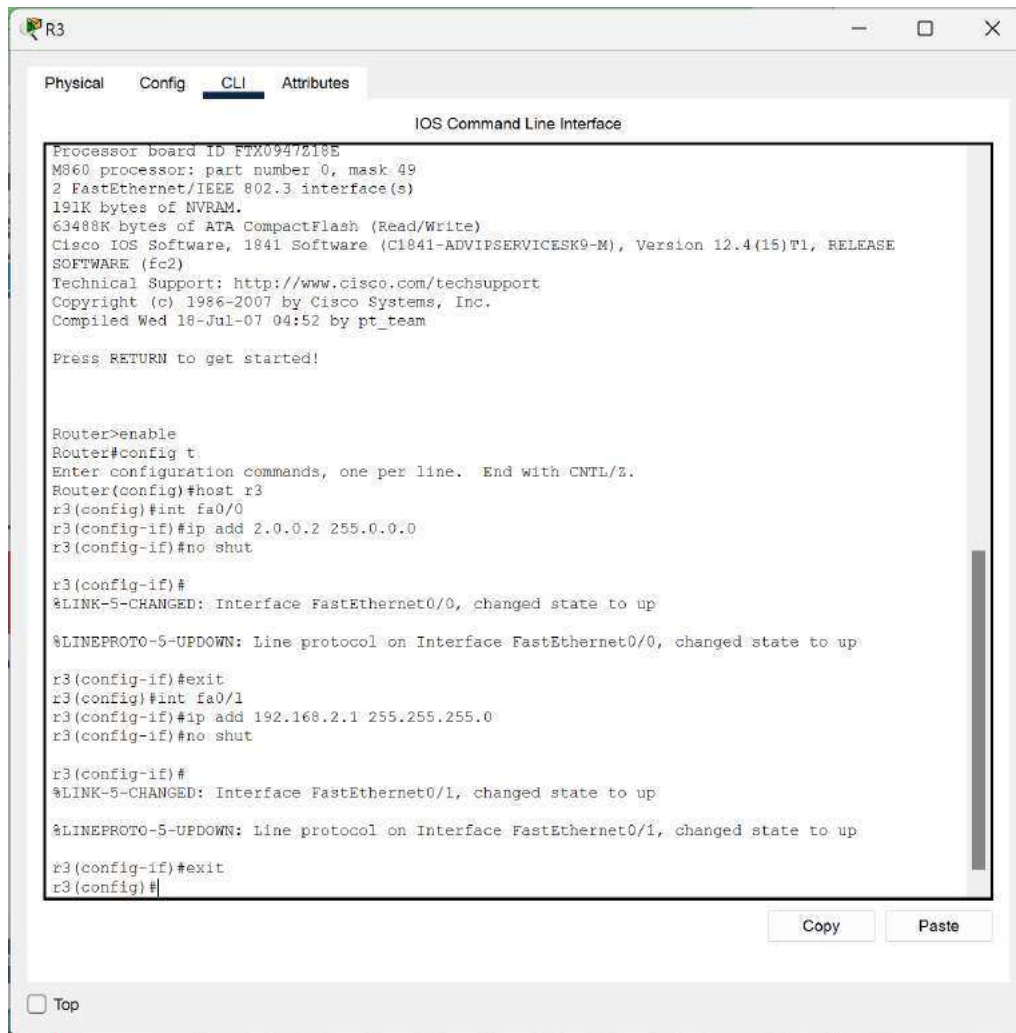
r3(config-if)#no shut

r3(config-if)#exit

r3(config)#int fa0/1

r3(config-if)#ip add 192.168.2.1 255.255.255.0

r3(config-if)#no shut



DEFAULT ROUTING CONFIGURATION ON

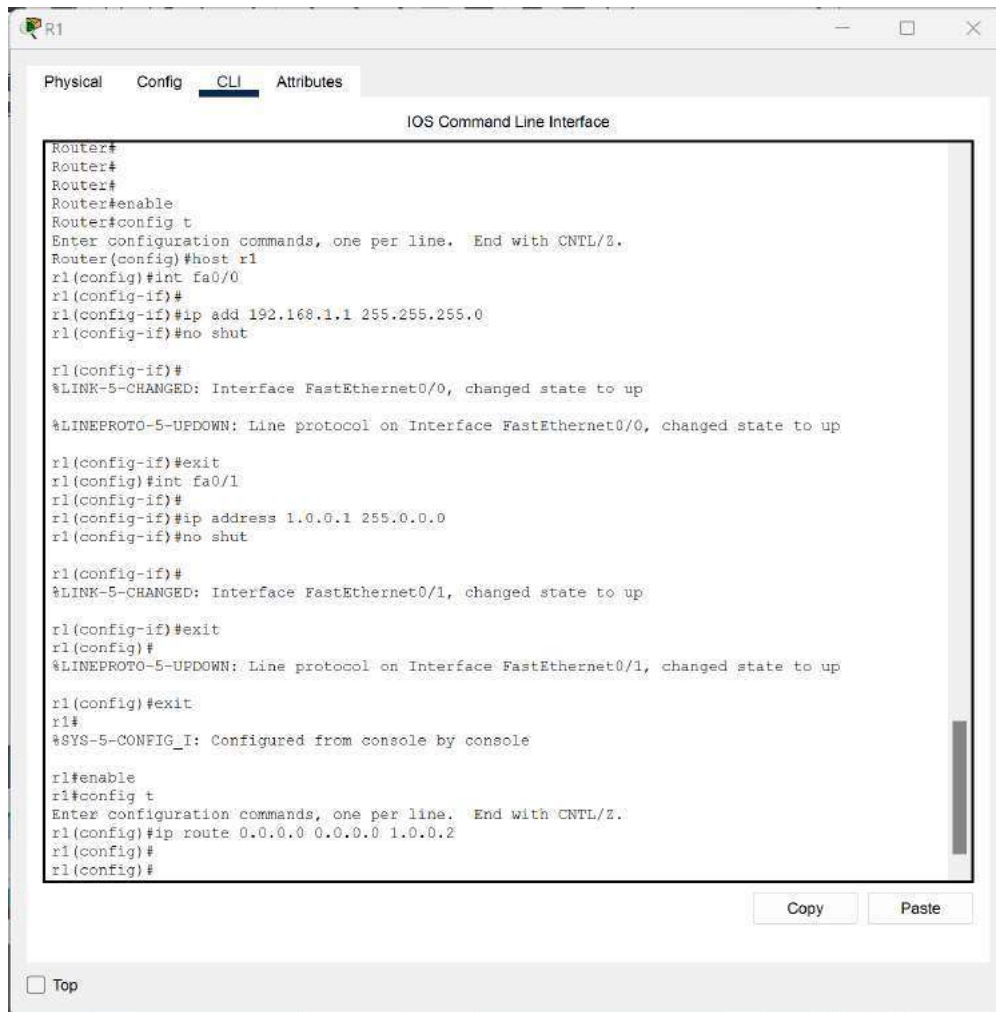
ROUTER R1:

r1>enable r1#config t

Enter configuration commands, one per line. End with CNTL/Z.

r1(config)#ip route 0.0.0.0 0.0.0.0 1.0.0.2

r1(config)#



r3>enable r3#config t

Enter configuration commands, one per line. End with CNTL/Z.

r3(config)#ip route 0.0.0.0 0.0.0.0 2.0.0.1

r3(config)#

DEFAULT ROUTING CONFIGURATION ON

ROUTER r3:

Now check the connection by pinging each other.**First we go to router r1 and ping with router r3:**

```
r1>ping 2.0.0.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 2.0.0.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

SUCCESSFUL PING**NOW CREATE VPN TUNNEL between R1 & R3****FIRST CREATE A VPN TUNNEL ON ROUTER R1:**

```
r1#config t r1(config)#interface tunnel 10 r1(config-if)#ip address 172.16.1.1 255.255.0.0
r1(config-if)#tunnel source fa0/1 r1(config-if)#tunnel destination 2.0.0.2 r1(config-if)#no
shut
```

```
r1(config)#interface tunnel 10
r1(config-if)#
%LINK-5-CHANGED: Interface Tunnel10, changed state to up
r1(config-if)#172.16.1.1 255.255.0.0
^
% Invalid input detected at '^' marker.
r1(config-if)#ip address 172.16.1.1 255.255.0.0
r1(config-if)#tunnel source fa0/1
r1(config-if)#tunnel destination 2.0.0.2
r1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel10, changed state to up
r1(config-if)#no shut
r1(config-if)#
```

Copy

Paste

NOW CREATE A VPN TUNNEL ON ROUTER R3:

```
r3#config t r3(config)#interface tunnel 100 r3(config-
if)#ip address 172.16.1.2 255.255.0.0 r3(config-
if)#tunnel source fa0/0 r3(config-if)#tunnel destination
1.0.0.1 r3(config-if)#no shut
```

```
r3#config t
Enter configuration commands, one per line. End with CNTL/Z.
r3(config)#interface tunnel 100

r3(config-if)#
%LINK-5-CHANGED: Interface Tunnel100, changed state to up

r3(config-if)#ip address 172.16.1.2 255.255.0.0
r3(config-if)#tunnel source fa0/0
r3(config-if)#tunnel destination 1.0.0.1
r3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100, changed state to up

r3(config-if)#no shut|
r3(config-if)#
```

[Copy](#)[Paste](#)

Now test communication between these two routers

again by pinging each other:

```
r1>ping 172.16.1.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/5 ms
```

SUCCESSFUL PING

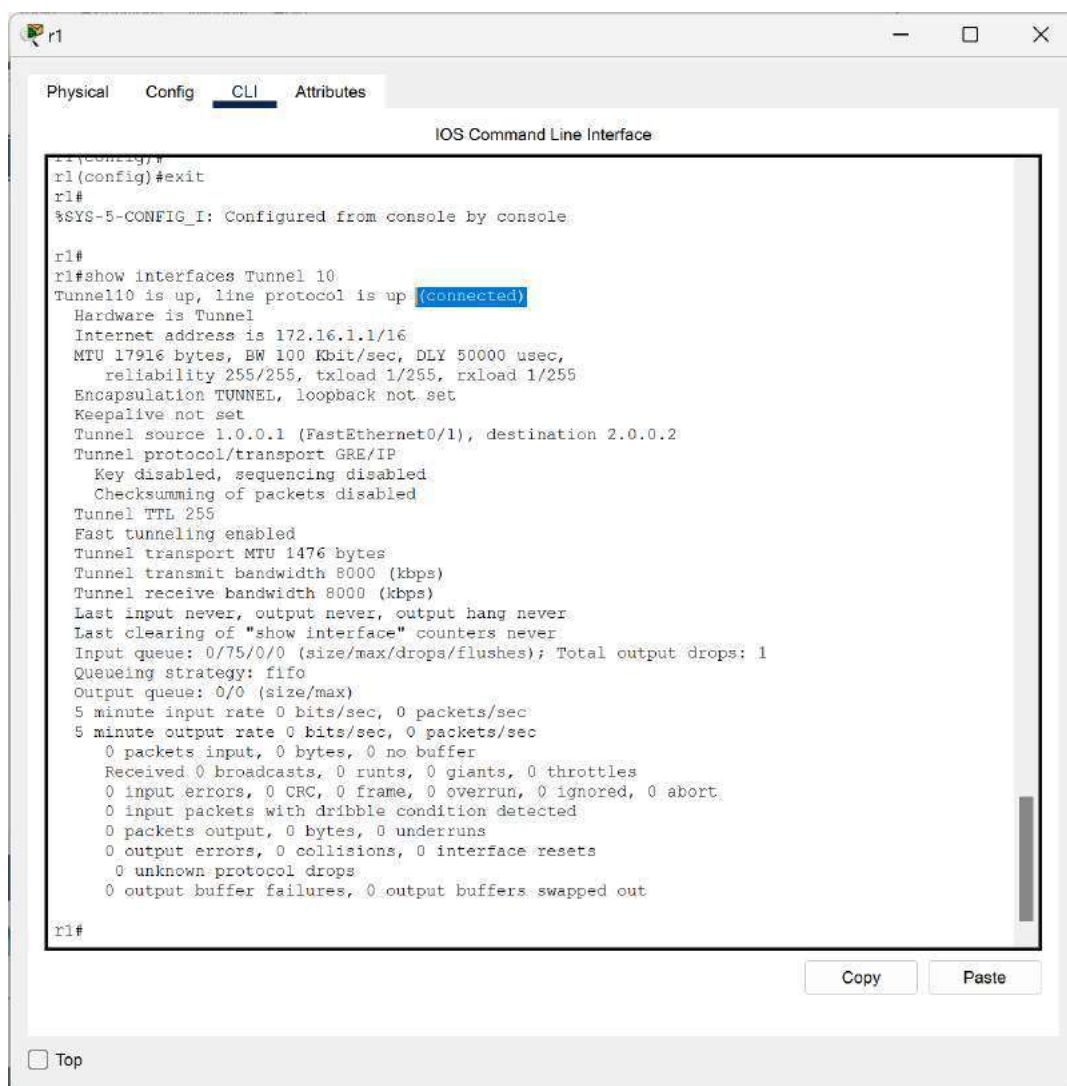
Now Do routing for created VPN Tunnel on Both R1&R3:

```
r1(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2
```

```
r3(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1
```

TEST VPN TUNNEL CONFIGURATION:

r1#show interfaces Tunnel 10



The screenshot shows a network device CLI window titled "r1". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main content area is titled "IOS Command Line Interface" and displays the following text:

```
r1(config)#
r1(config)#exit
r1#
%SYS-5-CONFIG_I: Configured from console by console

r1#
r1#show interfaces Tunnel 10
Tunnel10 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 172.16.1.1/16
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 1.0.0.1 (FastEthernet0/1), destination 2.0.0.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out

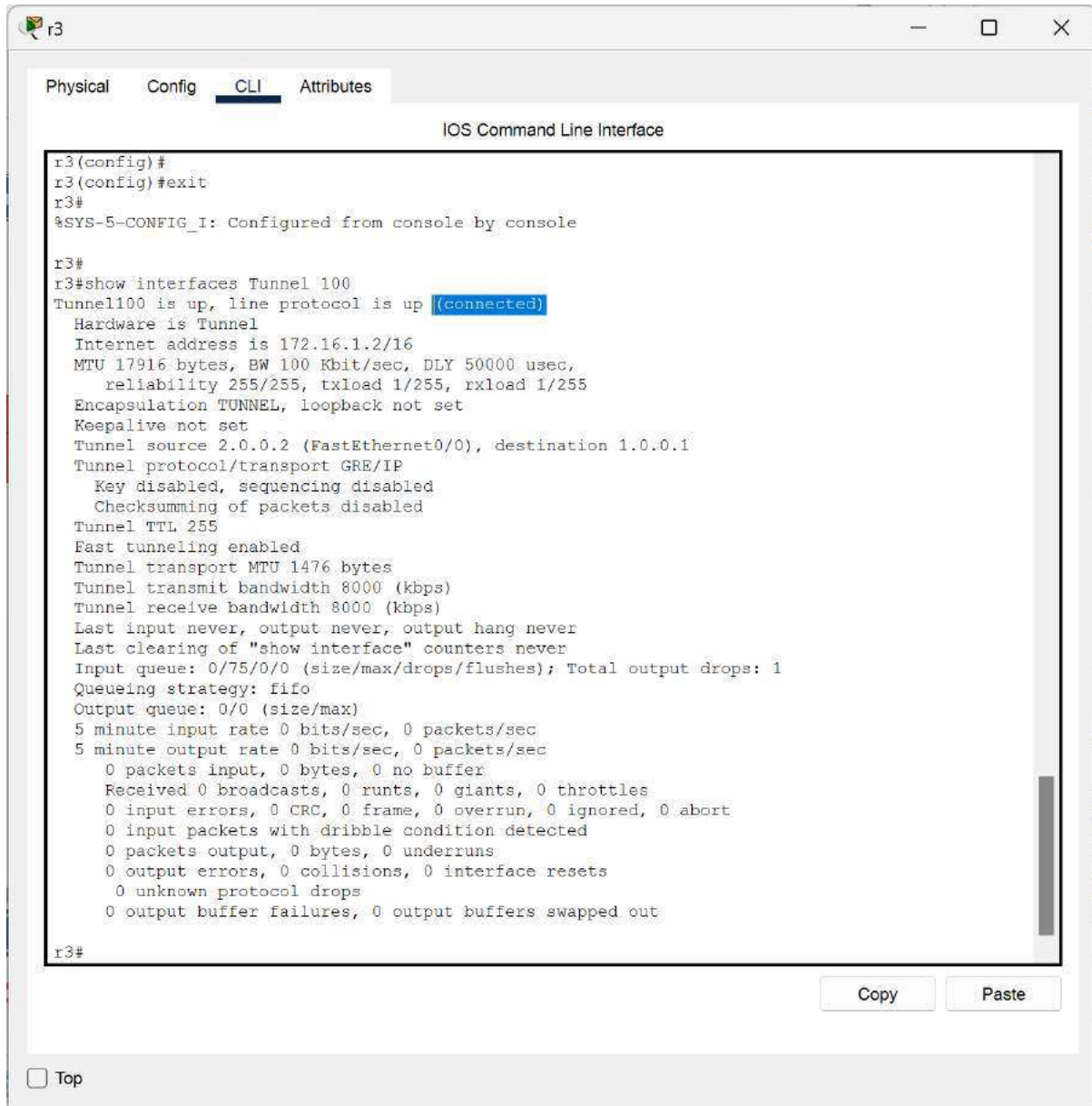
r1#
```

At the bottom of the window, there are "Copy" and "Paste" buttons, and a "Top" link.

Now going to Router R3 and test VPN Tunnel Creation:

r3#show interface Tunnel 100

Tunnel100 is up, line protocol is up (connected)



The screenshot shows a Cisco IOS Command Line Interface window for Router R3. The window has tabs for Physical, Config, CLI (selected), and Attributes. The CLI tab displays the following text:

```
r3(config)#
r3(config)#exit
r3#
%SYS-5-CONFIG_I: Configured from console by console

r3#
r3#show interfaces Tunnel 100
Tunnel100 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 172.16.1.2/16
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 2.0.0.2 (FastEthernet0/0), destination 1.0.0.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out

r3#
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons, and a 'Top' link with a checkbox.

CONCLUSION:

Therefore, a Tunnel is set up between Routers R1 and R3 in a VPN

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.