Table of Contents

Introduction to ACL:

Access Control List (ACL) is a security feature that allows you to filter the network traffic based on configured statements. An ACL can be used to filter either inbound or outbound traffic on an interface. Once you applied an access list on a router, the router examines every packet moving from interface to another interface in the specified direction and takes the appropriate action.

Types of Access Lists :

An ACL can be either of the following two types.

1. **Standard access lists**

A Standard access list can use only the source IP address in an IP packet to filter the network traffic. Standard access lists are typically used permit or deny an entire system or network. They cannot be used to filter individual protocol or services such as FTP and Telnet.

2. **Extended access lists**

Extended access lists use the source and destination IP addresses. They can be used to filter specific protocol or service.

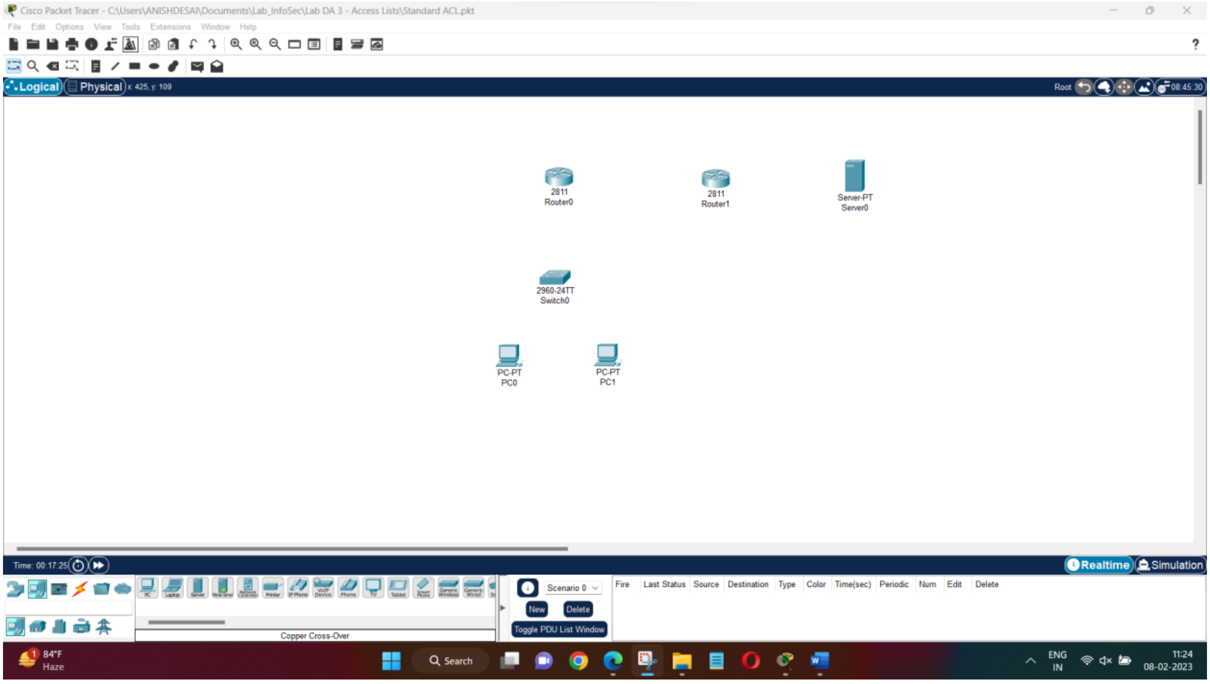
An ACL can be configured using either a number or a name. If you decide to use a name to configure an ACL, it is referred as Named ACL.

Configuration of Standard ACL using CISCO Packet Tracer :

Step 1 : Outlining the components and their connections

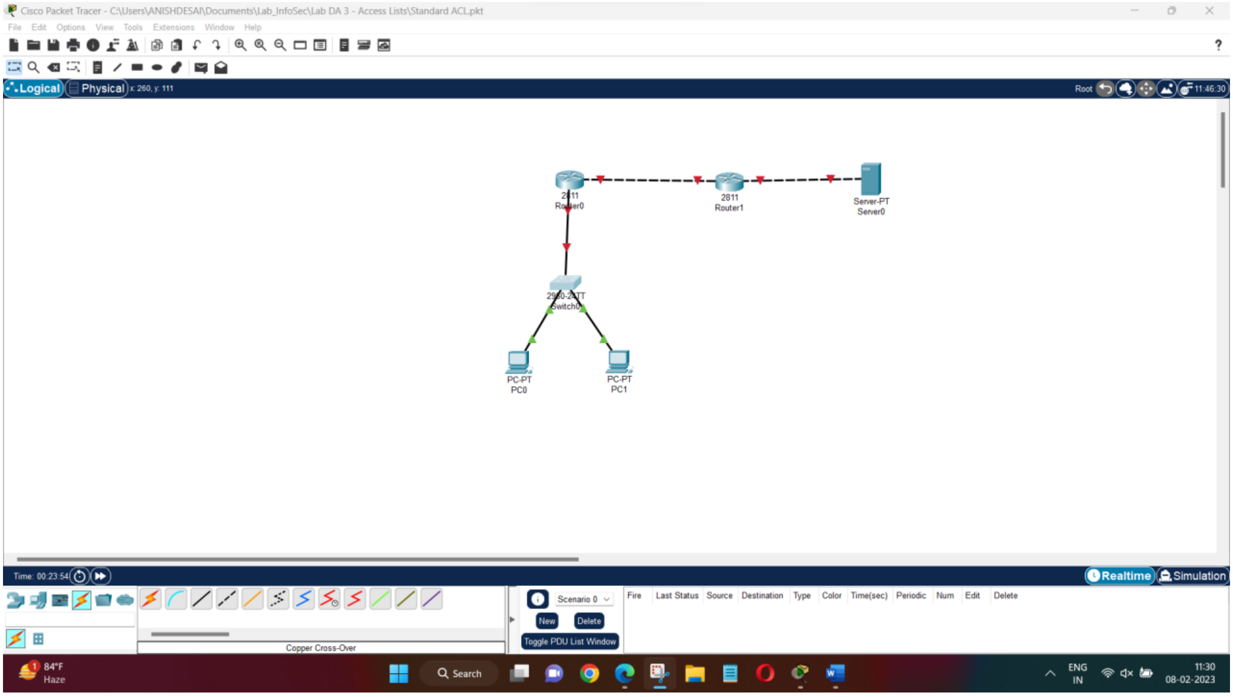
Components used include:

1. 2811-type Routers: Router0 and Router1
2. Switch 2960-24TT: Switch0
3. Server-PT: Server0
4. PC-PT: PC0 and PC1



Step 2 : Making the topology

Device	Connected to	Connected with
PC0 – FastEthernet0	Switch0 – FastEthernet0/1	Copper Straight-through
PC1 – FastEthernet0	Switch0 – FastEthernet0/2	Copper Straight-through
Switch0 – FastEthernet0/3	Router0 – FastEthernet0/0	Copper Straight-through
Router0 – FastEthernet0/1	Router1 – FastEthernet0/1	Copper Cross-Over
Router1 – FastEthernet0/0	Server0 – FastEthernet0	Copper Cross-Over



Step 3 : Assigning IP Addresses

Device	Connection	IP Address
PC0	FastEthernet0	10.0.0.2/8
PC1	FastEthernet0	10.0.0.3/8
Router0	FastEthernet0/0	10.0.0.1/8
Router0	FastEthernet0/1	192.168.0.1/24

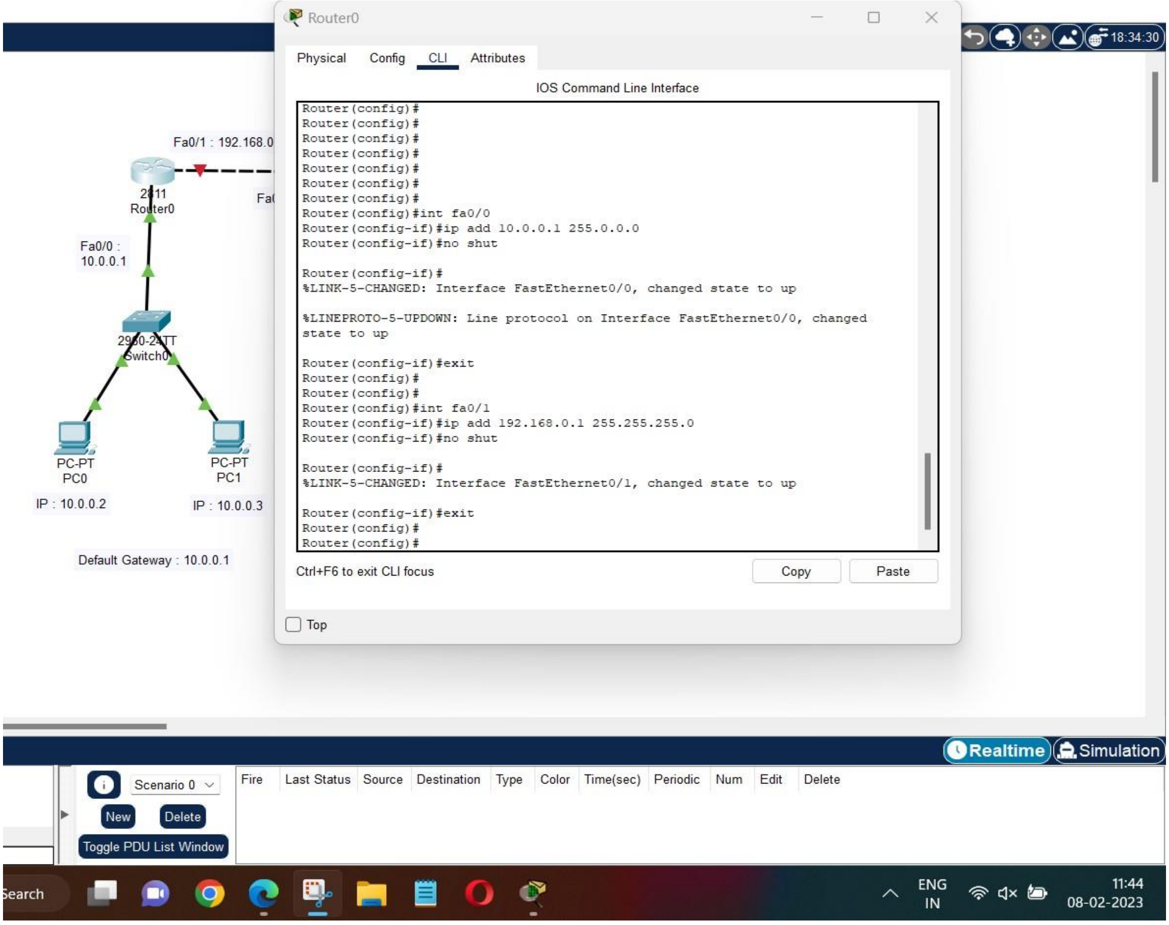
Router1	FastEthernet0/1	192.168.0.2/24
Router1	FastEthernet0/0	20.0.0.1/8
Server0	FastEthernet0	20.0.0.2/8

Default Gateway of PC0 and PC1 are set to ’10.0.0.1’ and that of Server-PT is set to ‘192.168.0.1’.

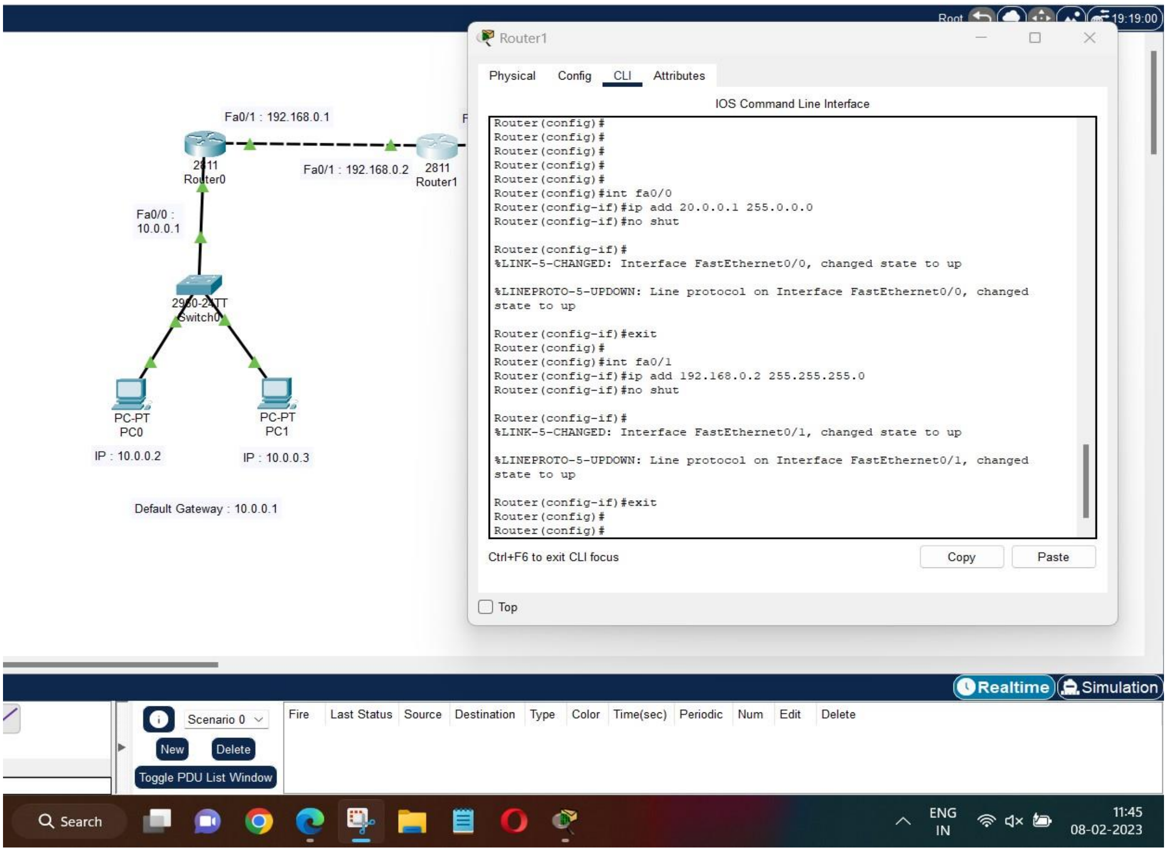
The IP Addresses can also be set using CLI of the routers.

```
Router0( config)# int fa0/ 0
Router0( config-if)# ip add 10.0.0.1 255.0.0.0
Router0( config-if)# no shut
Router0( config-if)# exit
Router0( config)# int fa0/ 1
Router0( config-if)# ip add 192.168.0.1 255.255.255.0
Router0( config-if)# no shut
Router0( config-if)# exit
```

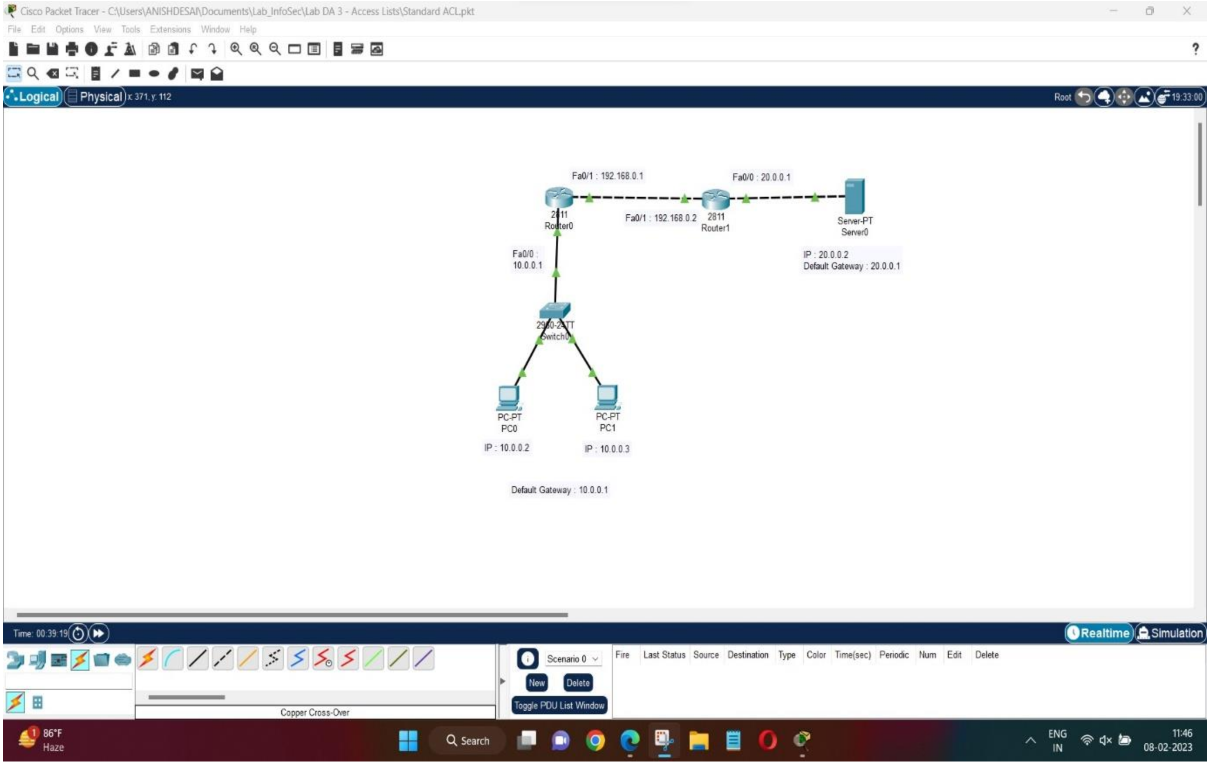
```
Router1( config)# int fa0/ 0
Router1( config-if)# ip add 20.0.0.1 255.0.0.0
Router1( config-if)# no shut
Router1( config-if)# exit
Router1( config)# int fa0/ 1
Router1( config-if)# ip add 192.168.0.2 255.255.255.0
Router1( config-if)# no shut
Router1( config-if)# exit
```



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#no shut

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#int fa0/1
Router(config-if)#ip add 192.168.0.1 255.255.255.0
Router(config-if)#no shut

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

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



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip add 20.0.0.1 255.0.0.0
Router(config-if)#no shut

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#
Router(config)#int fa0/1
Router(config-if)#ip add 192.168.0.2 255.255.255.0
Router(config-if)#no shut

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

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



Step 4 : Setting a routing method

Once you have configured appropriate IP addresses, use a routing method such as RIP. To do so, execute the following commands on Router0.

Router0(config)# router rip

Router0(config-router)# network 192.168.0.0

Router0(config-router)# network 10.0.0.0

Router0(config-router)# exit

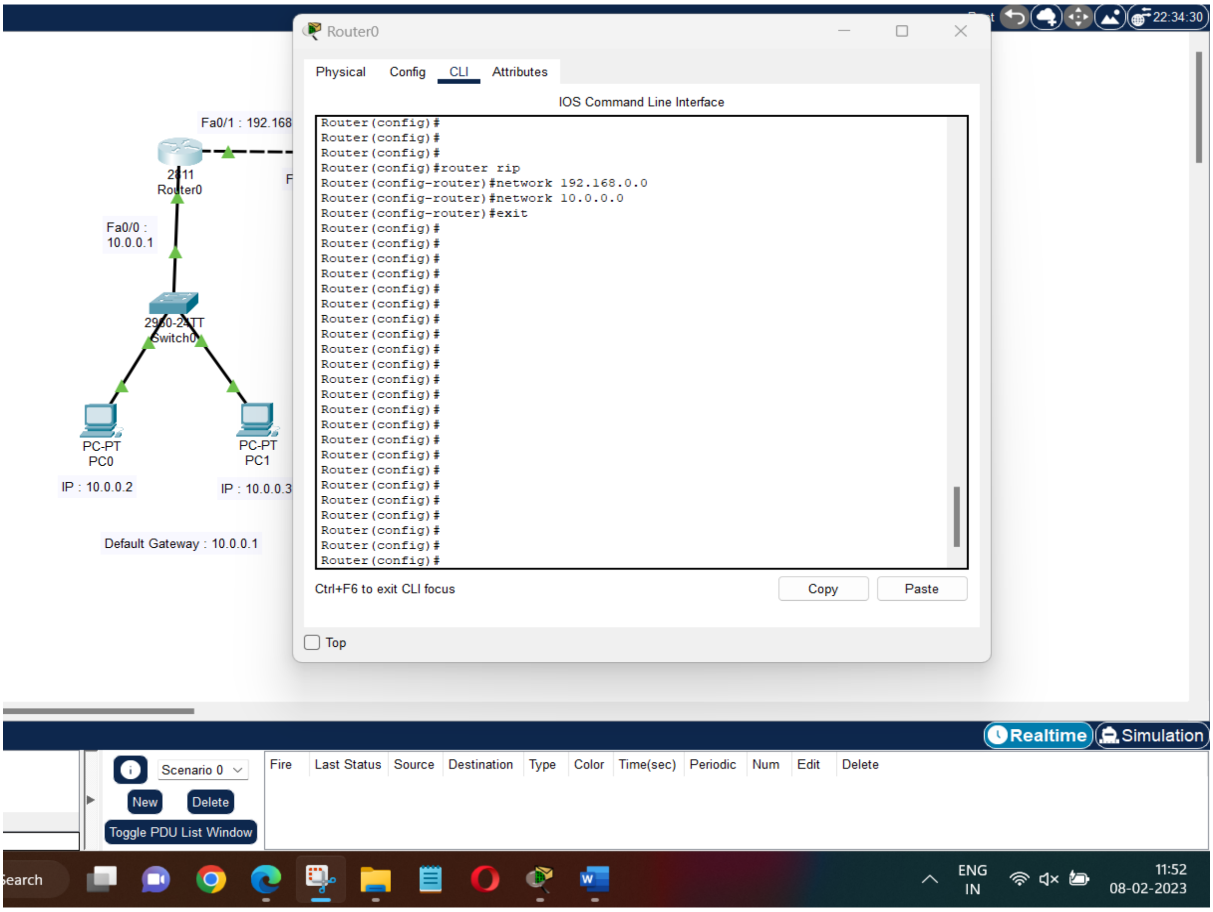
Next, move on to Router1 and execute the following commands to configure the RIP routing protocol.

Router1(config)# router rip

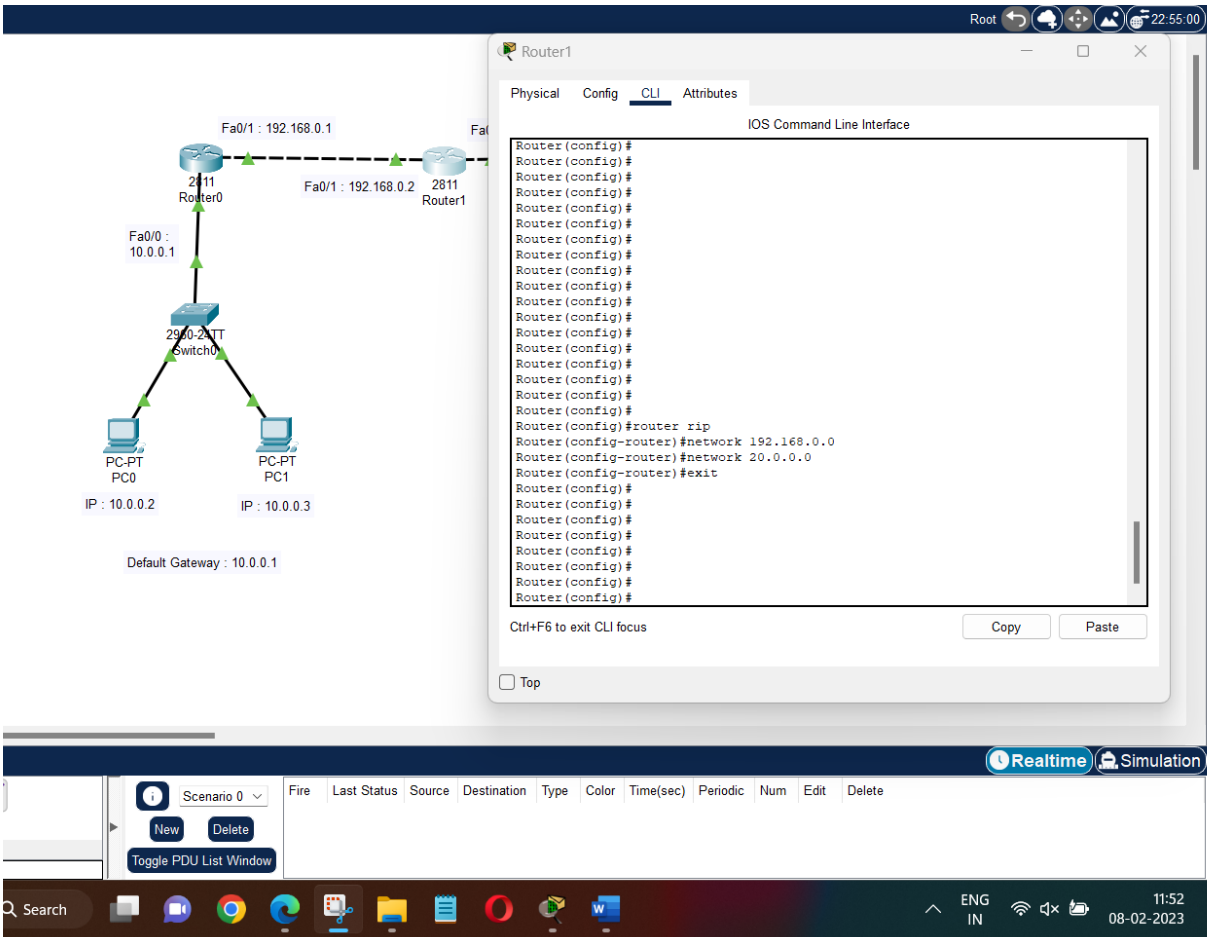
Router1(config-router)# network 192.168.0.0

Router1(config-router)# network 20.0.0.0

Router1(config-router)# exit



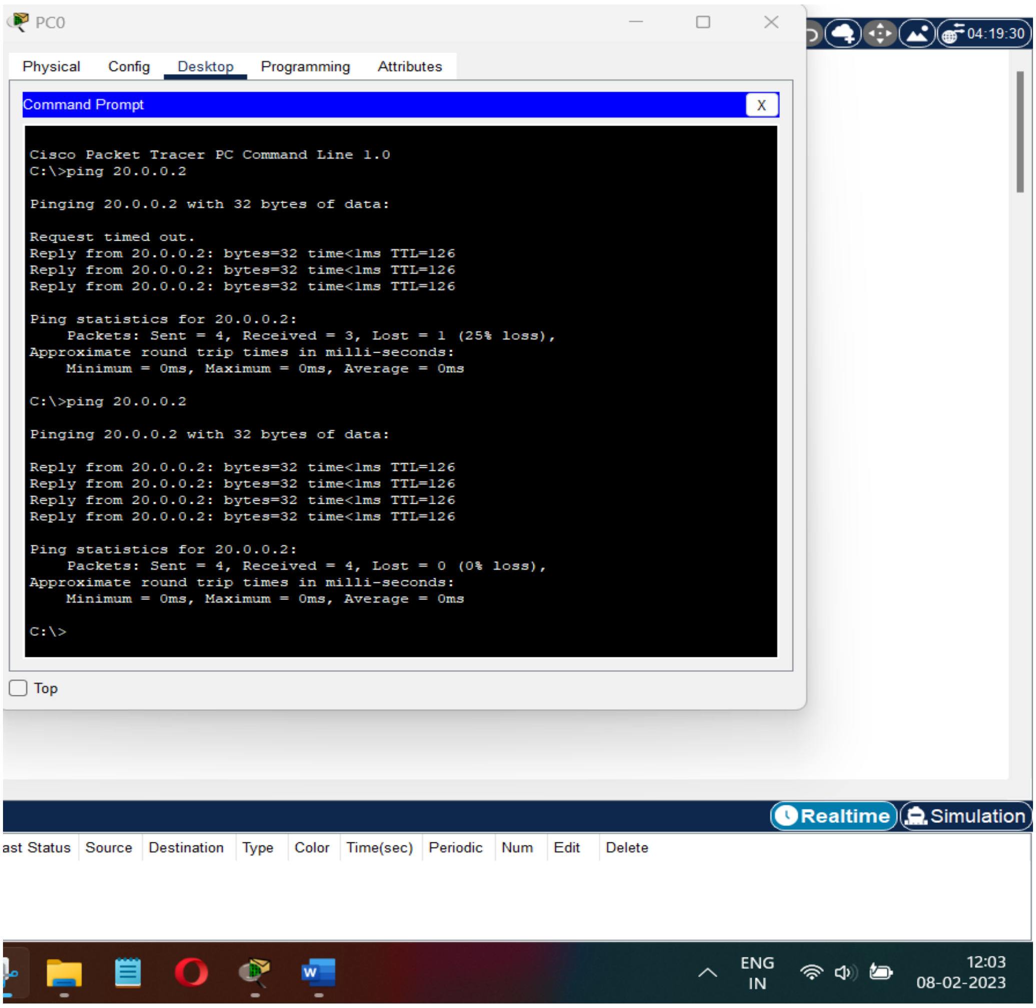
```
Router(config)#
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 10.0.0.0
Router(config-router)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

Step 5 : Configuring Standard ACL

As of now, we can ping the Server using PC0 or PC1.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 20.0.0.2: bytes=32 time<1ms TTL=126
Reply from 20.0.0.2: bytes=32 time<1ms TTL=126
Reply from 20.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time<1ms TTL=126
Reply from 20.0.0.2: bytes=32 time<1ms TTL=126
Reply from 20.0.0.2: bytes=32 time<1ms TTL=126
Reply from 20.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

In this configuration, we will restrict host 10.0.0.2 (PC0) from accessing Router1.

It can be configured using the following CLI commands :

Router1(config)# access-list 10 deny host 10.0.0.2

Router1(config)# access-list 10 permit any

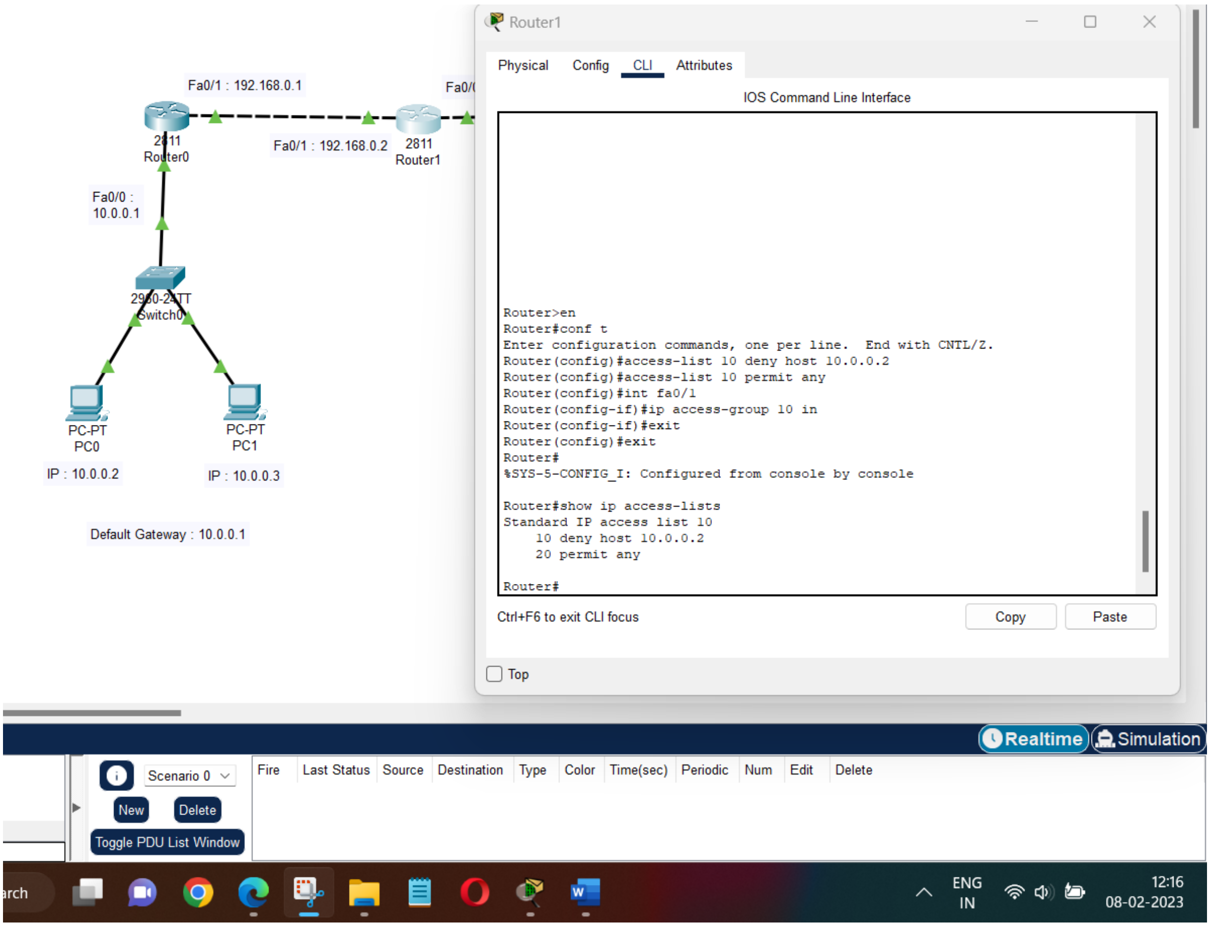
Router1(config)# int fa0/ 1

Router1(config-if)# ip access-group 10 in

Router1(config-if)# exit

Router1(config)# exit

Router1# show ip access-lists



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 deny host 10.0.0.2
Router(config)#access-list 10 permit any
Router(config)#int fa0/1
Router(config-if)#ip access-group 10 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip access-lists
Standard IP access list 10
    10 deny host 10.0.0.2
    20 permit any

Router#
```

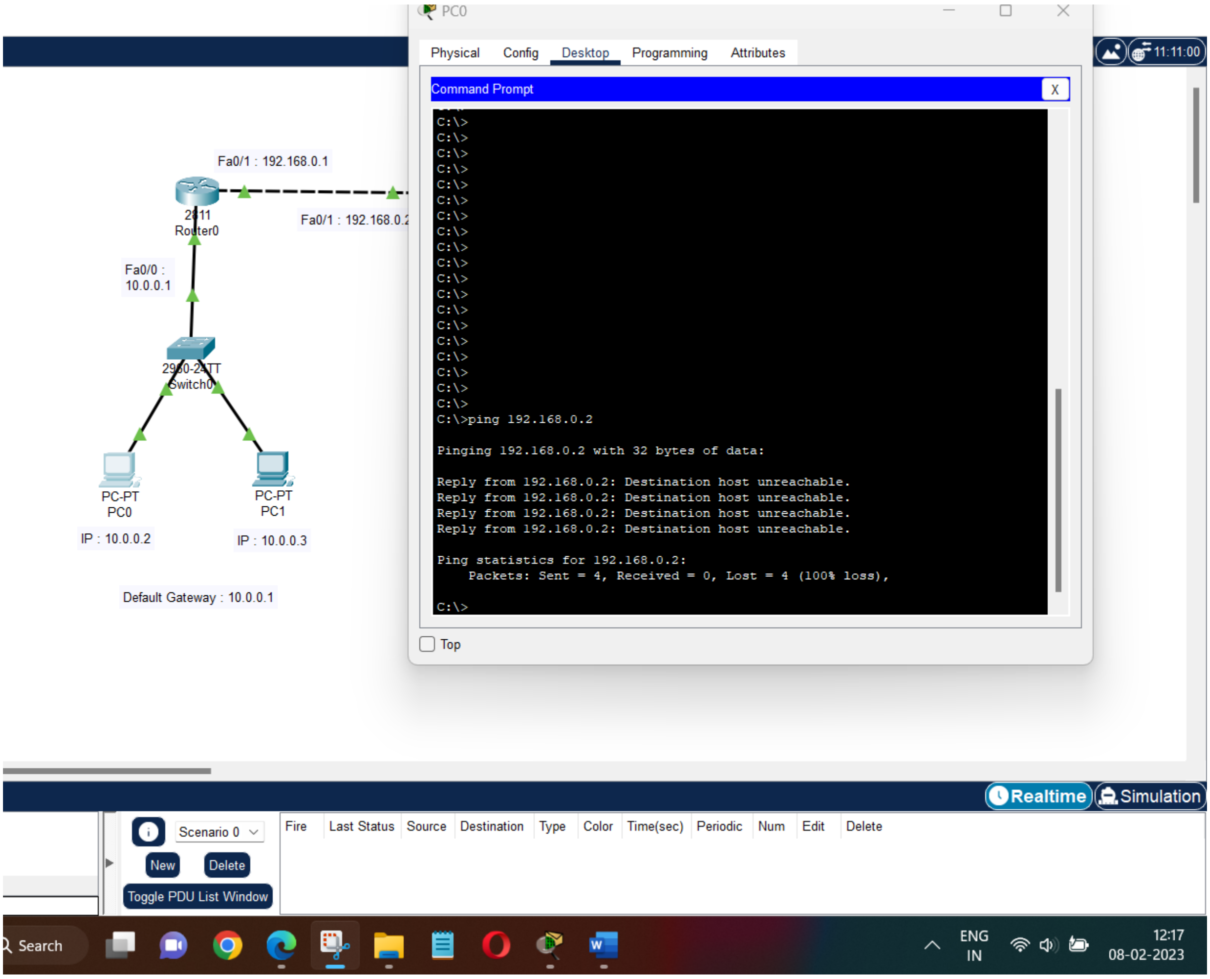
Step 6 : Verify Standard ACL Configuration

Now as we try to ping the Router1 using PC0, we can see that we can no longer reach that network.

For testing, enter

ping 192.168.0.2

from PC0.

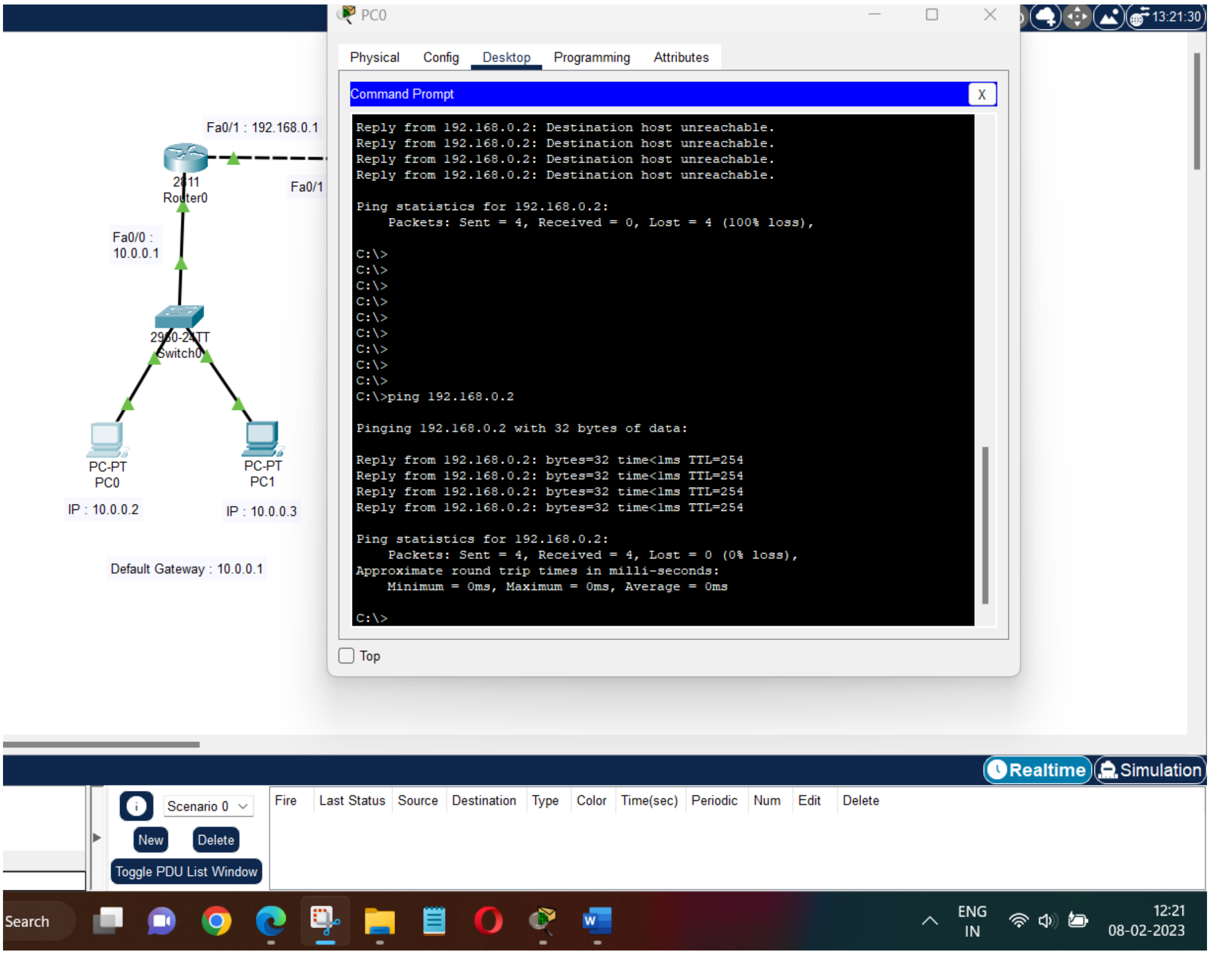


```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Now, after having tested the ACL configuration, we can remove the ACL configuration so the next test could be performed. To remove the configured ACL, execute the following command on Router1.

Router1(config)# no access-list 10 deny host 10.0.0.2

Try to ping again from PC0 to Router1, this time you should be able ping successfully, because the applied ACL has been removed.



```
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.
Reply from 192.168.0.2: Destination host unreachable.

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time<1ms TTL=254
Reply from 192.168.0.2: bytes=32 time<1ms TTL=254
Reply from 192.168.0.2: bytes=32 time<1ms TTL=254
Reply from 192.168.0.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

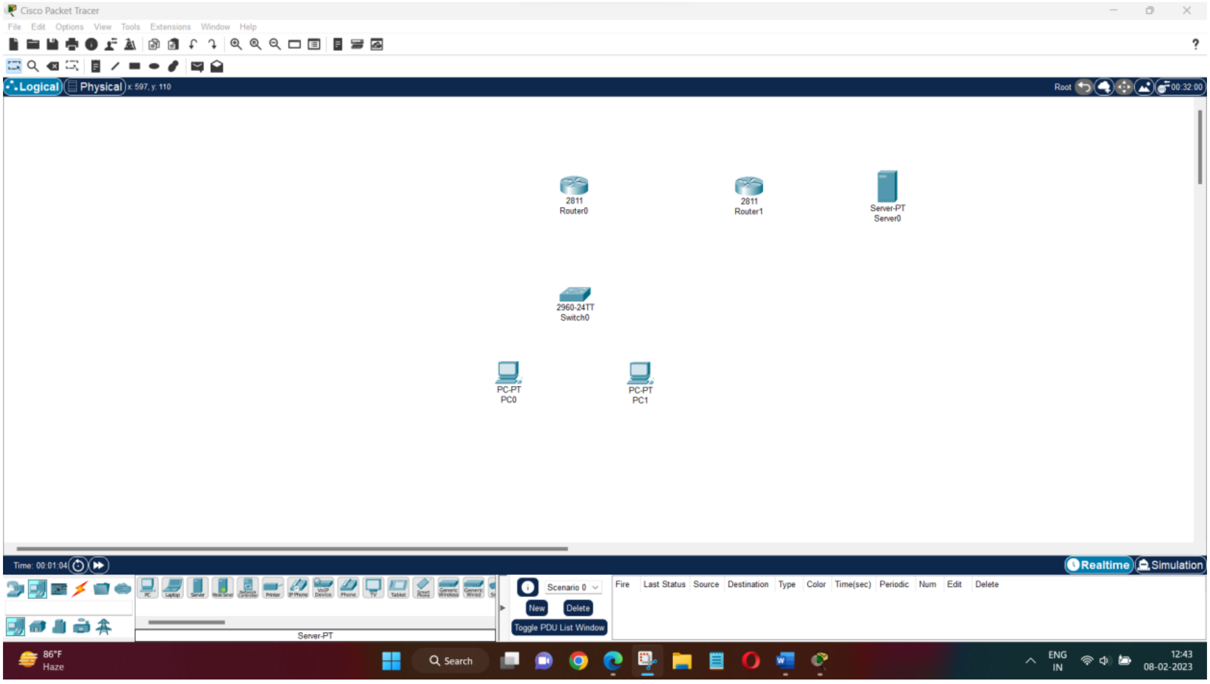
Successful Demonstration

Configuration of Extended ACL using CISCO Packet Tracer :

Step 1 : Outlining the components and their connections

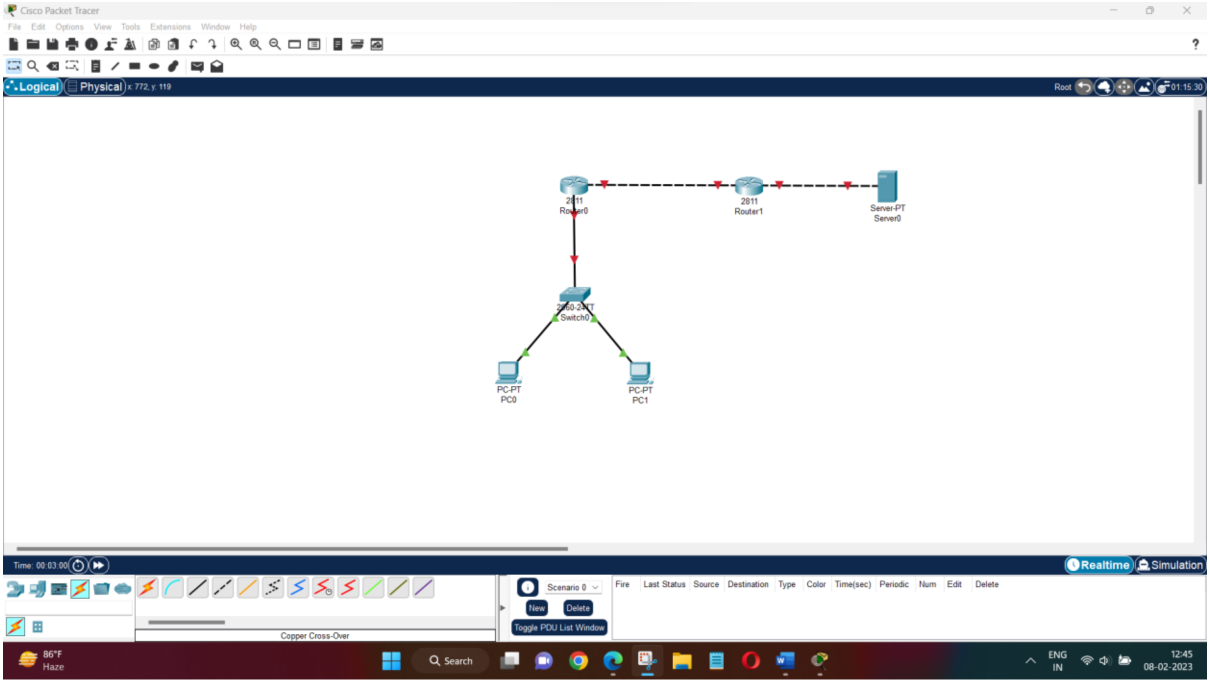
Components used include:

1. 2811-type Routers: Router0 and Router1
2. Switch 2960-24TT: Switch0
3. Server-PT: Server0
4. PC-PT: PC0 and PC1



Step 2 : Making the topology

Device	Connected to	Connected with
PC0 – FastEthernet0	Switch0 – FastEthernet0/1	Copper Straight-through
PC1 – FastEthernet0	Switch0 – FastEthernet0/2	Copper Straight-through
Switch0 – FastEthernet0/3	Router0 – FastEthernet0/0	Copper Straight-through
Router0 – FastEthernet0/1	Router1 – FastEthernet0/1	Copper Cross-Over
Router1 – FastEthernet0/0	Server0 – FastEthernet0	Copper Cross-Over



Step 3 : Assigning IP Addresses

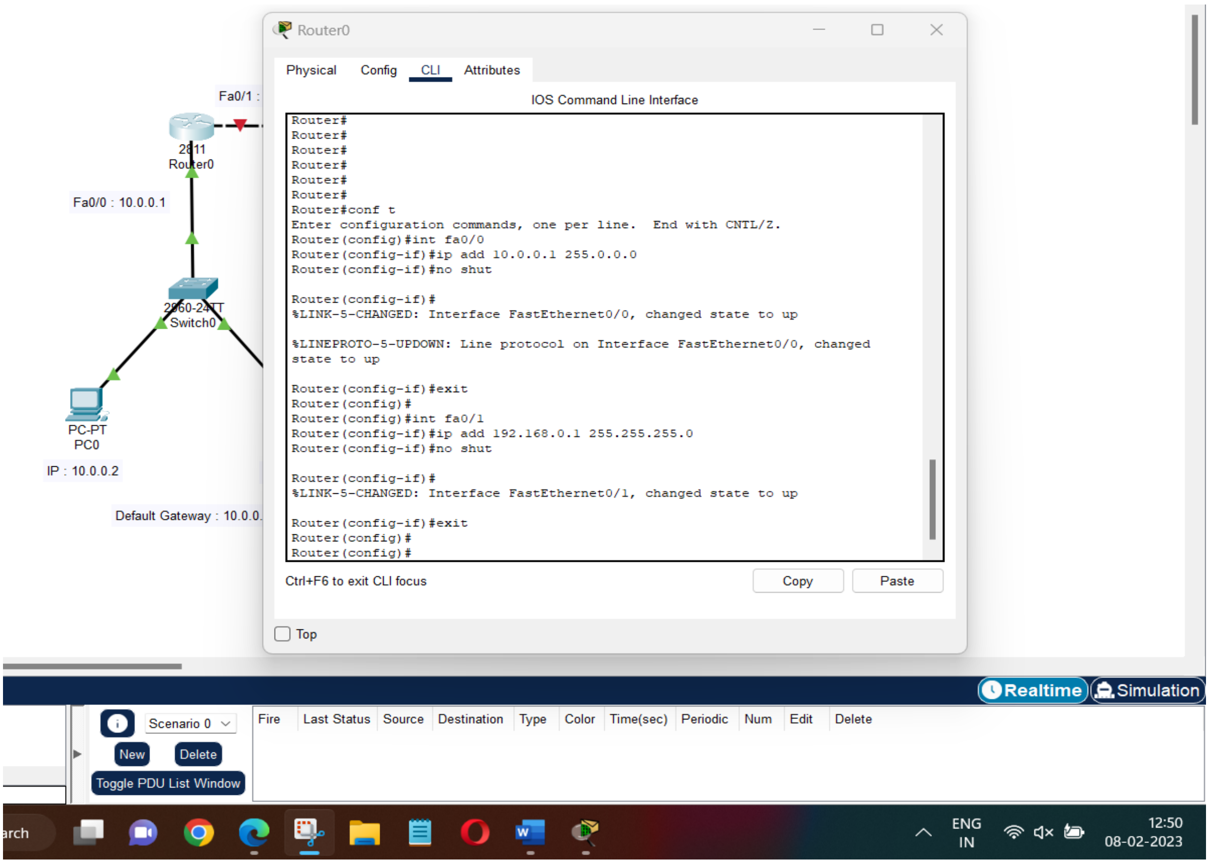
Device	Connection	IP Address
PC0	FastEthernet0	10.0.0.2/8
PC1	FastEthernet0	10.0.0.3/8
Router0	FastEthernet0/0	10.0.0.1/8
Router0	FastEthernet0/1	192.168.0.1/24
Router1	FastEthernet0/1	192.168.0.2/24

Router1	FastEthernet0/0	20.0.0.1/8
Server0	FastEthernet0	20.0.0.2/8

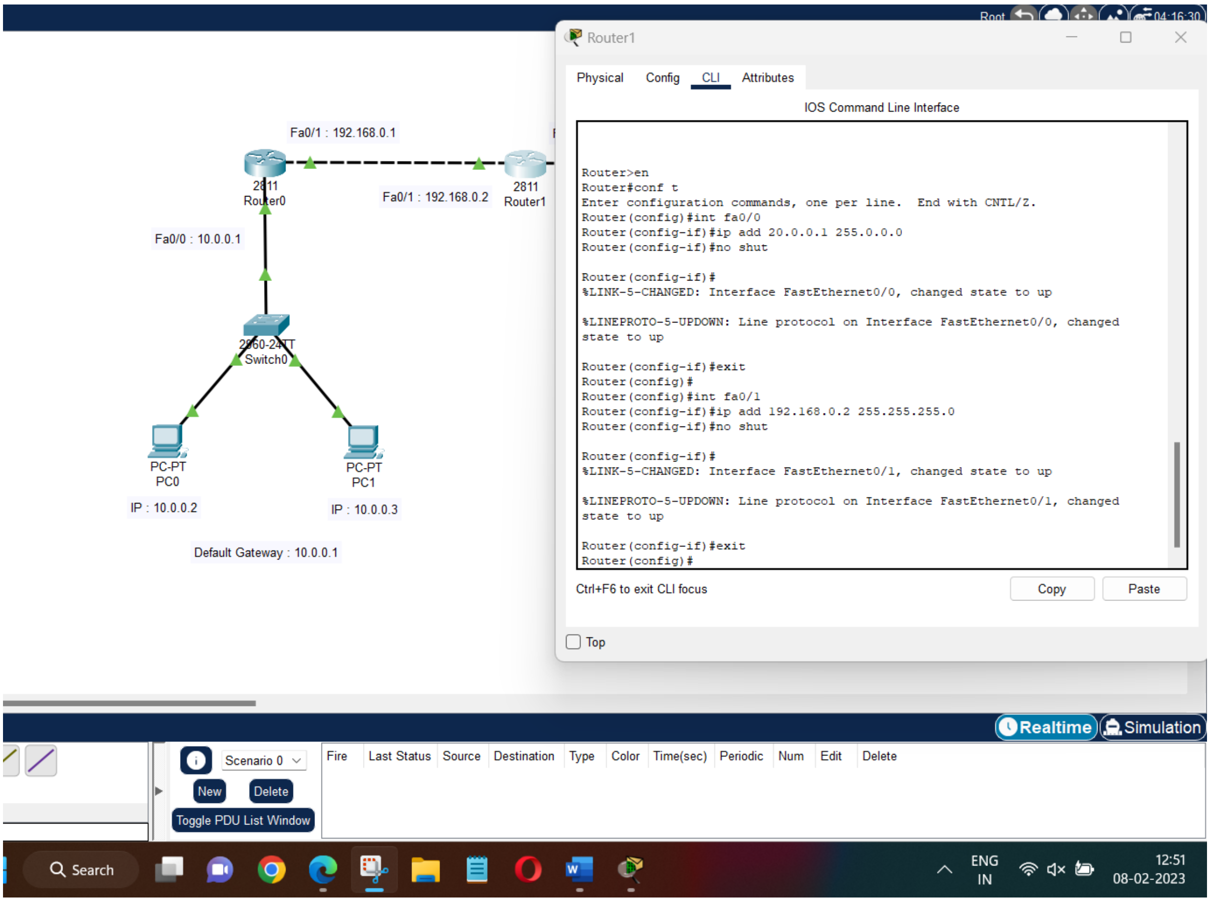
Default Gateway of PC0 and PC1 are set to ’10.0.0.1’ and that of Server-PT is set to ‘192.168.0.1’.

The IP Addresses can also be set using CLI of the routers.

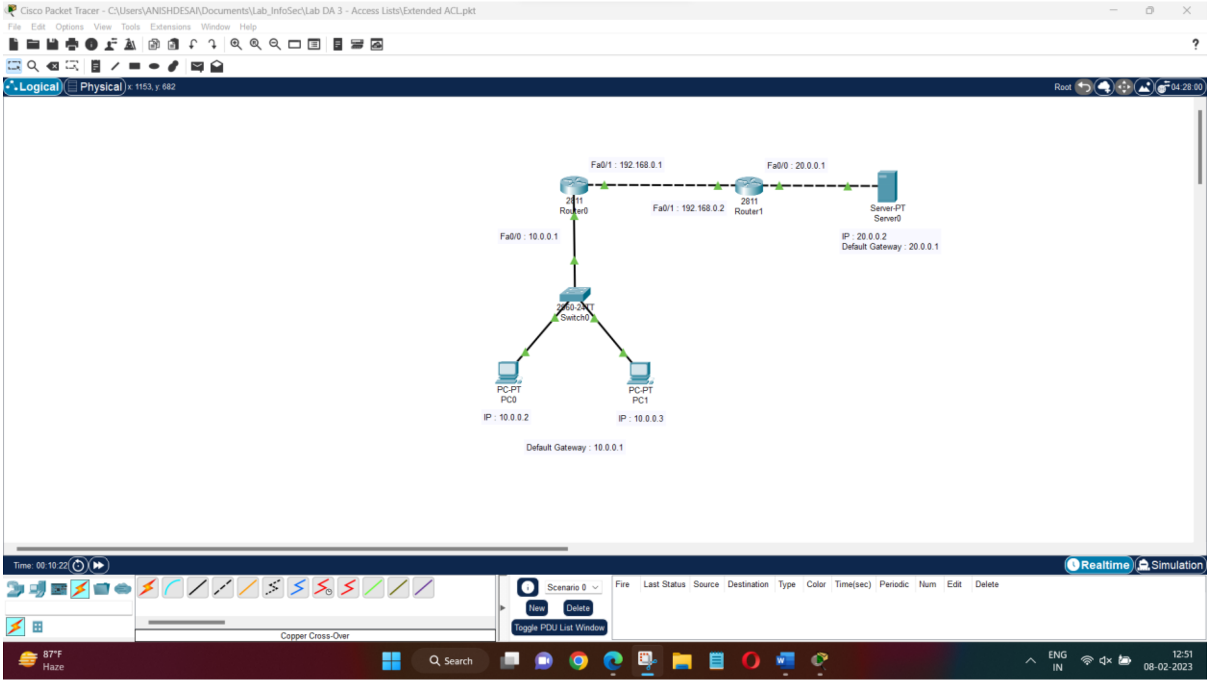
```
Router0( config)# int fa0/ 0
Router0( config-if)# ip add 10.0.0.1 255.0.0.0
Router0( config-if)# no shut
Router0( config-if)# exit
Router0( config)# int fa0/ 1
Router0( config-if)# ip add 192.168.0.1 255.255.255.0
Router0( config-if)# no shut
Router0( config-if)# exit

Router1( config)# int fa0/ 0
Router1( config-if)# ip add 20.0.0.1 255.0.0.0
Router1( config-if)# no shut
Router1( config-if)# exit
Router1( config)# int fa0/ 1
Router1( config-if)# ip add 192.168.0.2 255.255.255.0
Router1( config-if)# no shut
Router1( config-if)# exit
```



```
Router#
Router#
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#no shut

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#
Router(config)#int fa0/1
Router(config-if)#ip add 192.168.0.1 255.255.255.0
Router(config-if)#no shut

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

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



```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 20.0.0.1 255.0.0.0
Router(config-if)#no shut

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#
Router(config)#int fa0/1
Router(config-if)#ip add 192.168.0.2 255.255.255.0
Router(config-if)#no shut

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

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



Step 4 : Setting a routing method

Once you have configured appropriate IP addresses, use a routing method such as RIP. To do so, execute the following commands on Router0.

Router0(config)# router rip

Router0(config-router)# network 192.168.0.0

Router0(config-router)# network 10.0.0.0

Router0(config-router)# exit

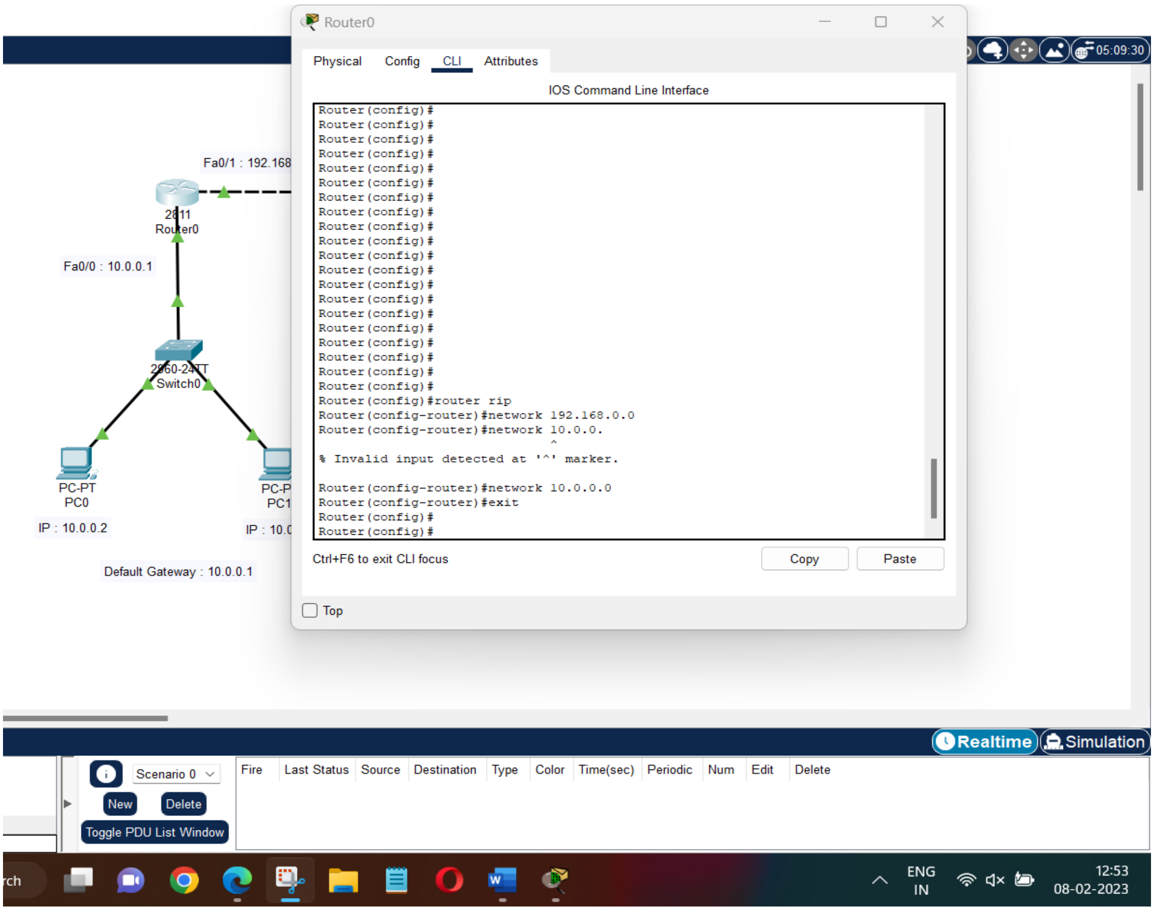
Next, move on to Router1 and execute the following commands to configure the RIP routing protocol.

Router1(config)# router rip

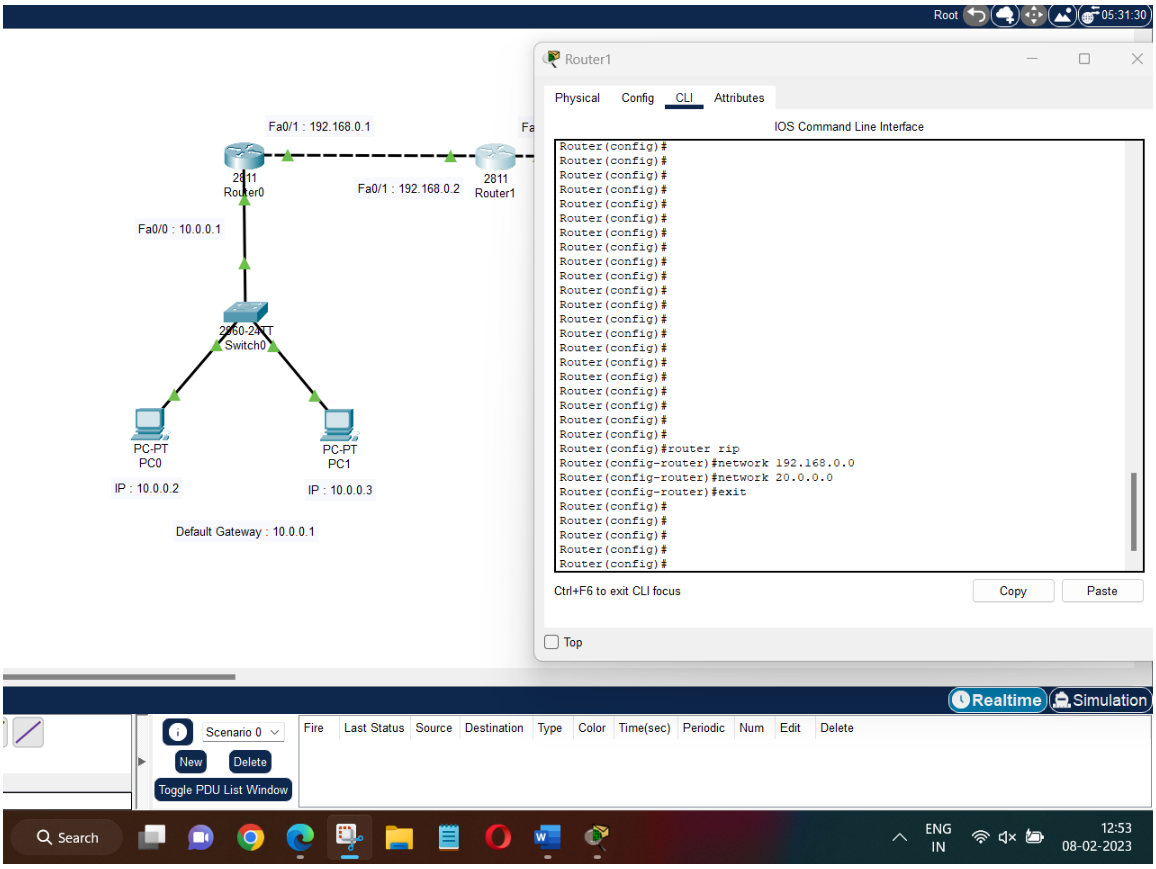
Router1(config-router)# network 192.168.0.0

Router1(config-router)# network 20.0.0.0

Router1(config-router)# exit



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 10.0.0.
                                     ^
% Invalid input detected at '^' marker.

Router(config-router)#network 10.0.0.0
Router(config-router)#exit
Router(config)#
Router(config)#
```



```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#network 192.168.0.0
Router(config-router)#network 20.0.0.0
Router(config-router)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
```

Step 5 : Configuring Extended ACL

To configure Extended ACL, we will deny the host 10.0.0.2 (PC0) from accessing the web server (20.0.0.2).

In order to prevent host 10.0.0.2 to access the Web server (20.0.0.2), you need to execute the following commands in the CLI of Router1.

Router1(config)# access-list 150 deny tcp host 10.0.0.2 20.0.0.2 0.0.0.0 eq www

Router1(config)# access-list 150 permit ip any any

Router1(config)# int fa0/ 1

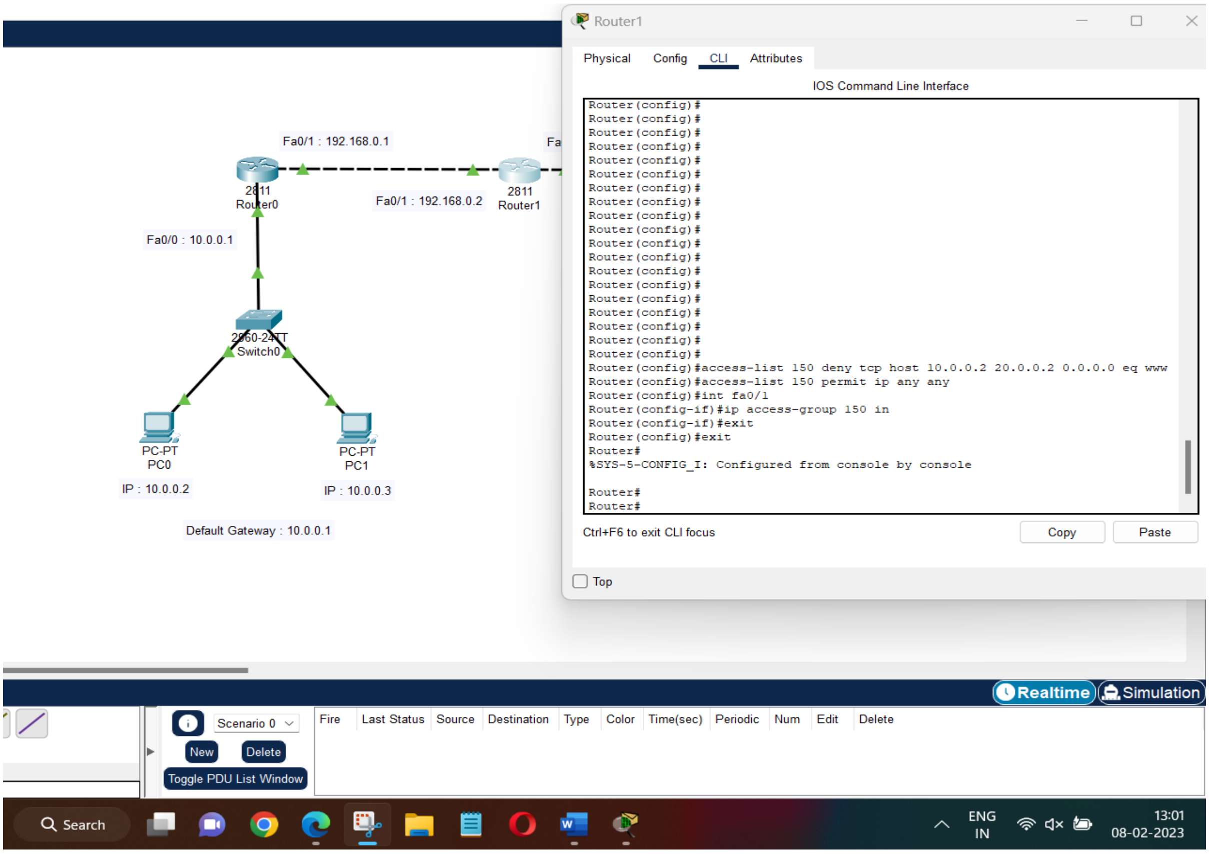
Router1(config-if)# ip access-group 150 in

Router1(config-if)# exit

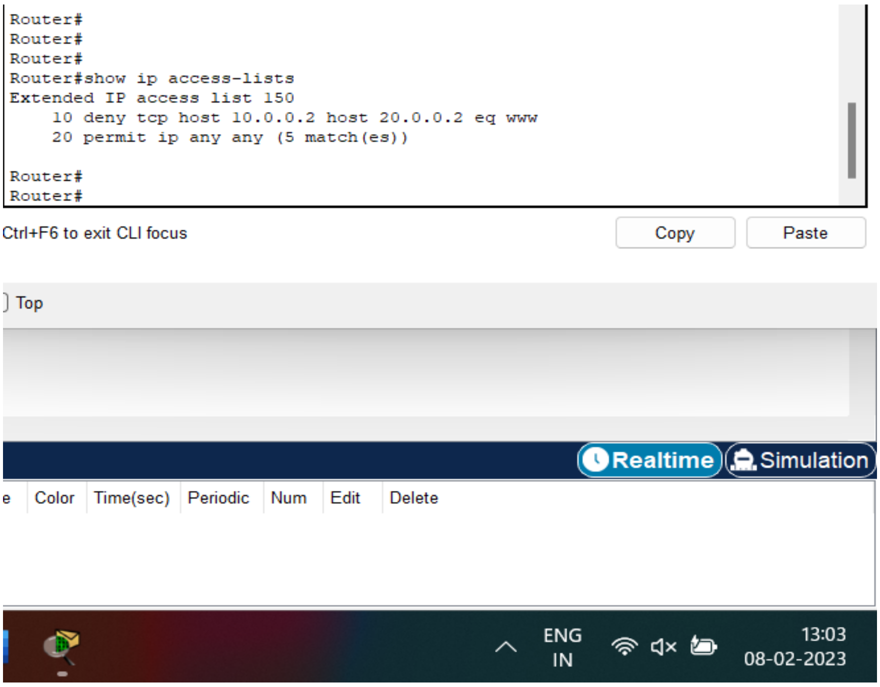
Router1(config)# exit

Once you applied an ACL on the desired interface, execute the following command to view the configured access lists.

Router1# show ip access-lists



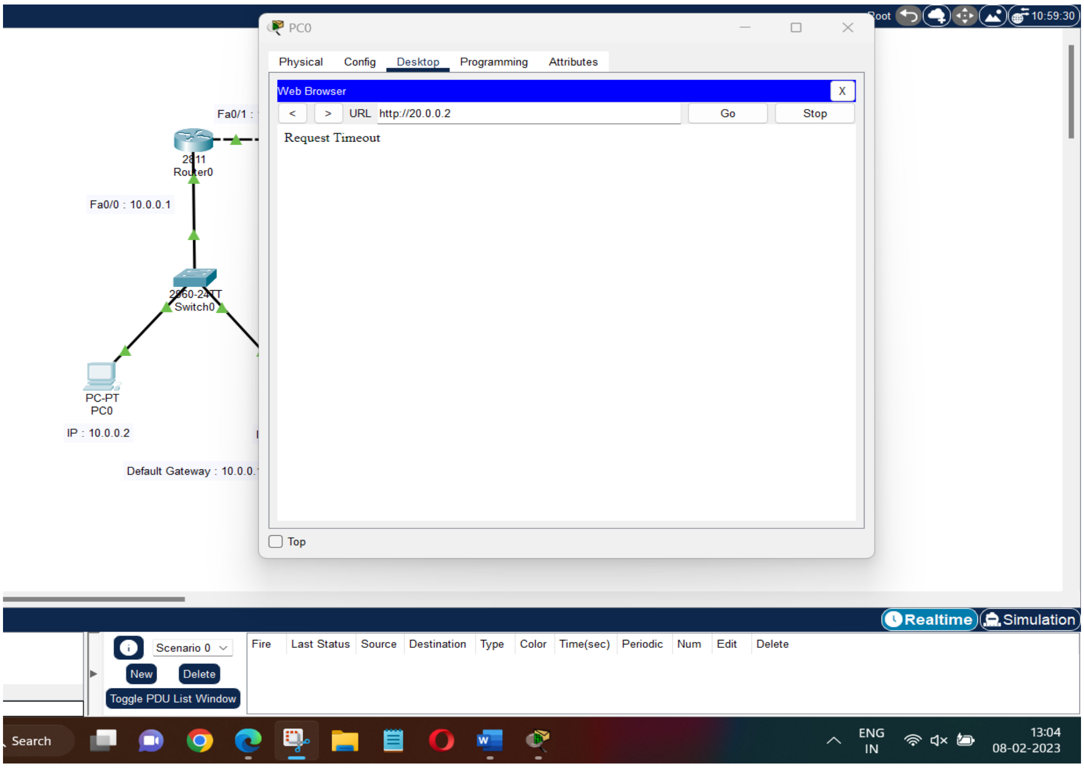
```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#access-list 150 deny tcp host 10.0.0.2 20.0.0.2 0.0.0.0 eq www
Router(config)#access-list 150 permit ip any any
Router(config)#int fa0/1
Router(config-if)#ip access-group 150 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#
```



```
Router#
Router#
Router#
Router#show ip access-lists
Extended IP access list 150
    10 deny tcp host 10.0.0.2 host 20.0.0.2 eq www
    20 permit ip any any (5 match(es))

Router#
Router#
```

Step 6 : Verify Extended ACL Configuration

To verify your configuration, open the Web browser on PC0, type http:// 20.0.0.2 and press Enter. You should not be able to access the Web server.

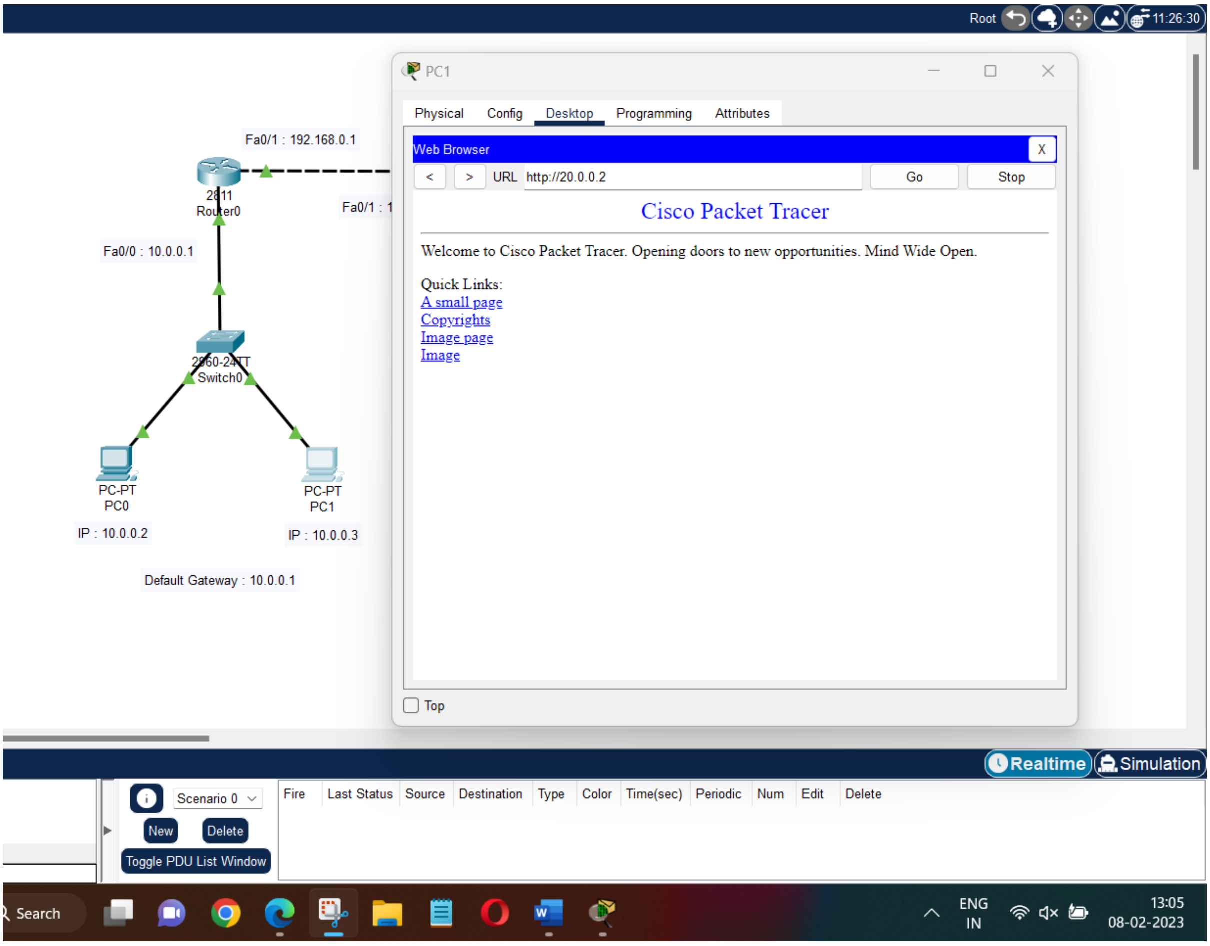


Web Browser

URL http://20.0.0.2

Request Timeout

Now move on to PC1 and try to access Web server, this time you should be able to access Web server. This is because we have not prevented PC1 to access Web server.



URL http://20.0.0.2

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Now, you have configured and verified the Extended ACL, you can remove the configured ACL. To do so, execute the following command on Router1.

Router1(config)# no access-list 150 deny tcp host 10.0.0.2 host 20.0.0.2 eq www

---