



Birzeit University
Faculty of Engineering and Technology
Electrical and Computer Engineering Department
Computer Networks Laboratory ENCS413

EXP. No. 6. Access Lists

Leyan Burait

1211439

Objective :

Configuring Extended Access List In this section, you will use only extended access list, and make sure in each step to copy the main topology. Extended ACL takes IDs of 100 to 199. A. Prevent PC0 from accessing PC2. (all other traffic is allowed).

First, create an access list to deny PC0, we can use one of the following methods:

Method 1:

```
Router0(config)#access-list 101 deny ip host 192.X.10.2 host 192.X.20.2
Router0(config)#access-list 101 permit ip any any
```

Method 2:

```
Router0(config)#access-list 101 deny ip 192.X.10.2 0.0.0.0 192.X.20.2 0.0.0.0
Router0(config)#access-list 101 permit ip any any
```

The command `access-list 101 permit ip any any` is used because after assigning an access list, by default there is an implicit deny all traffic the end of every ACL see sec 3.4 in the introduction. Anything that is not explicitly permitted is denied. Then you must give the ACL to an interface, in our case give it to fa0/0 for the inbound, using the following commands: `Router0(config)# interface fa0/0` `Router0(config-if)#ip access-group 101 in`

B. Allow PC0 to access PC2 all other traffic is denied.

C. Add a server to the topology to network 192.X.20.0/24 and activate http service on it, then deny PC0 to make HTTP request to this server. (Hint: use command: `access list 101 deny tcp host 192.X.10.2 host 192.X.20.4 eq 80` Where 80 is the port number for HTTP requests.)

D. Prevent PC0 from accessing PC4 all other traffic is allowed. (Think about in which router should you put the rule).

E. Enable telnet on Router1 then, deny all the host from making telnet with interface se2/0 of Router1 expect PC0, it can make telnet with any interface. [try to minimize the traffic on the serial line as much as possible]. All other traffic should be allowed.

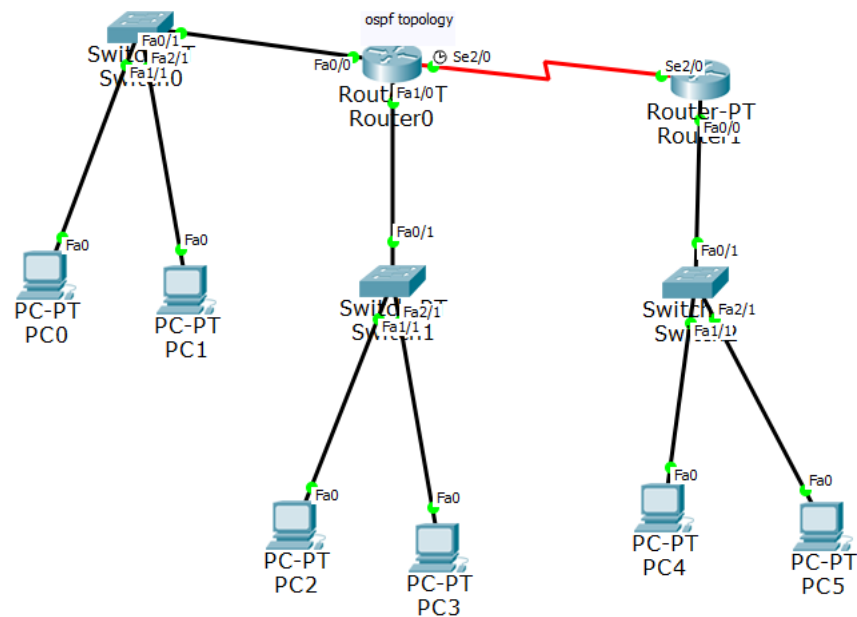


Figure 1: originally topology

Area	Network	Device	Interface	IP	Subnet Mask	Wildcard Mask
Area 0	192.X.40.0/24	Router 0	Se2/0	192.X.40.1	255.255.255.0	0.0.0.255
		Router 1	Se2/0	192.X.40.2	255.255.255.0	0.0.0.255
	192.X.10.0/24	Router 0	Fa0/0	192.X.10.1	255.255.255.0	0.0.0.255
		PC0	Fa0	192.X.10.2	255.255.255.0	0.0.0.255
		PC1	Fa0	192.X.10.3	255.255.255.0	0.0.0.255
	192.X.20.0/24	Router 0	Fa1/0	192.X.20.1	255.255.255.0	0.0.0.255
		PC2	Fa0	192.X.20.2	255.255.255.0	0.0.0.255
		PC3	Fa0	192.X.20.3	255.255.255.0	0.0.0.255
	192.X.30. 0/24	Router 1	Fa0/0	192.X.30. 1	255.255.255.0	0.0.0.255
		PC4	Fa0	192.X.30. 2	255.255.255.0	0.0.0.255
		PC5	Fa0	192.X.30. 3	255.255.255.0	0.0.0.255

Contents

Objective :	2
A. Prevent PC0 from accessing PC2. (all other traffic is allowed).	5
B. Allow PC0 to access PC2 all other traffic is denied.	5
C. Add a server to the topology to network 192.X.20.0/24 and activate http service on it, then deny PC0 to make HTTP request to this server. (Hint: use command: access list 101 deny tcp host 192.X.10.2 host 192.X.20.4 eq 80 Where 80 is the port number for HTTP requests.)	6

Test pc0 to server http port 80.....	8
D. Prevent PC0 from Accessing PC4, Allowing All Other Traffic	9
E. Enable Telnet on Router1 and Restrict Telnet Access on se2/0 to Only PC0	12

Contents of figure

Figure 1: originally topology.....	3
Figure 2:command expander to Allow PC0 to access PC2 all other traffic is denied.....	5
Figure 3: test command expander to Allow PC0 to access PC2 all other traffic is denied.....	6
Figure 4: topology of part c.....	6
Figure 5topology & command of part c	7
Figure 6ping 192.39.20.4	8
Figure 7: request time out	8
Figure 8: command of part D	9
Figure 9: test fail PC0 from Accessing PC4	9
Figure 10: successful all other to pc4 except pc0	10
Figure 11: all of part D.....	11
Figure 12: enable telnet	12
Figure 13: command of part E.....	12
Figure 14: test pc0 to router1	13

A. Prevent PC0 from accessing PC2. (all other traffic is allowed).

First, create an access list to deny PC0, we can use one of the following methods:

Method 1:

```
Router0(config)#access-list 101 deny ip host 192.X.10.2 host 192.X.20.2
```

```
Router0(config)#access-list 101 permit ip any any
```

Method 2:

```
Router0(config)#access-list 101 deny ip 192.X.10.2 0.0.0.0 192.X.20.2 0.0.0.0
```

```
Router0(config)#access-list 101 permit ip any any
```

B. Allow PC0 to access PC2 all other traffic is denied.

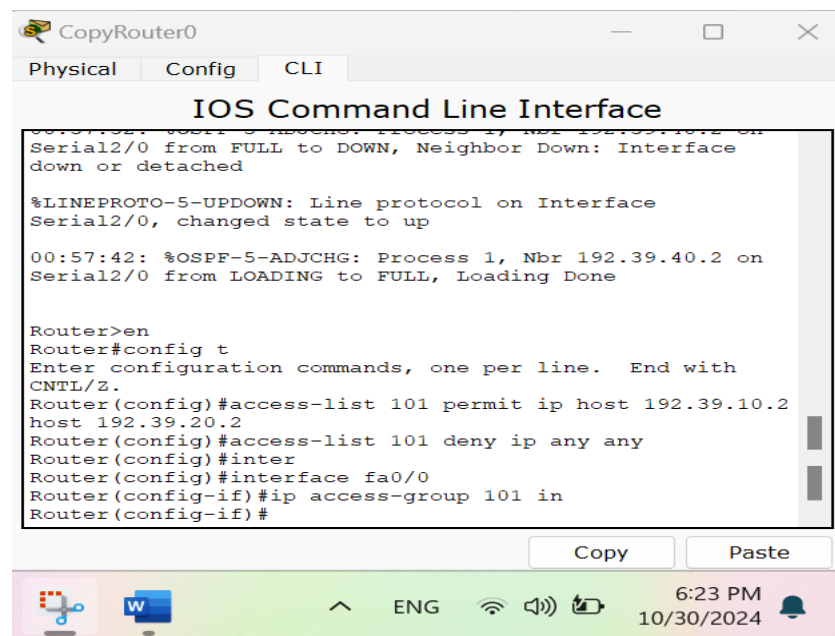


Figure 2:command expander to Allow PC0 to access PC2 all other traffic is denied.

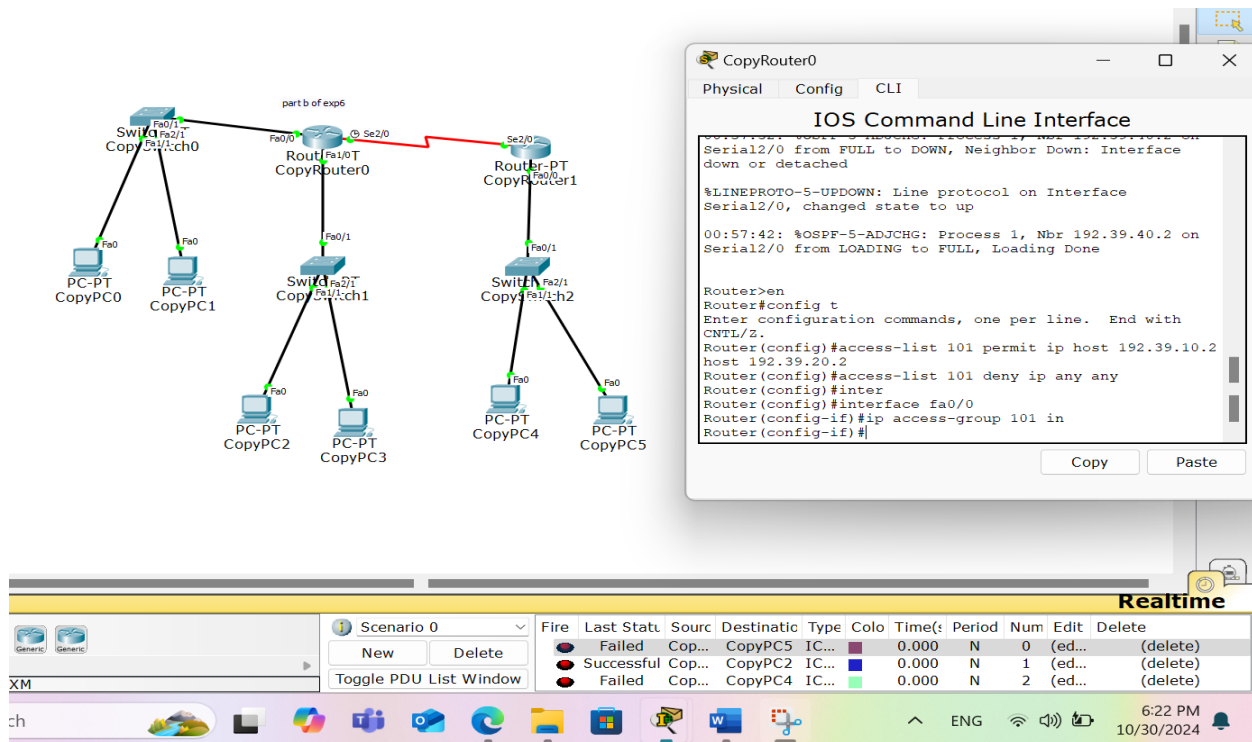


Figure 3: test command expander to Allow PC0 to access PC2 all other traffic is denied.

C. Add a server to the topology to network 192.X.20.0/24 and activate http service on it, then deny PC0 to make HTTP request to this server. (Hint: use command: access list 101 deny tcp host 192.X.10.2 host 192.X.20.4 eq 80 Where 80 is the port number for HTTP requests.)

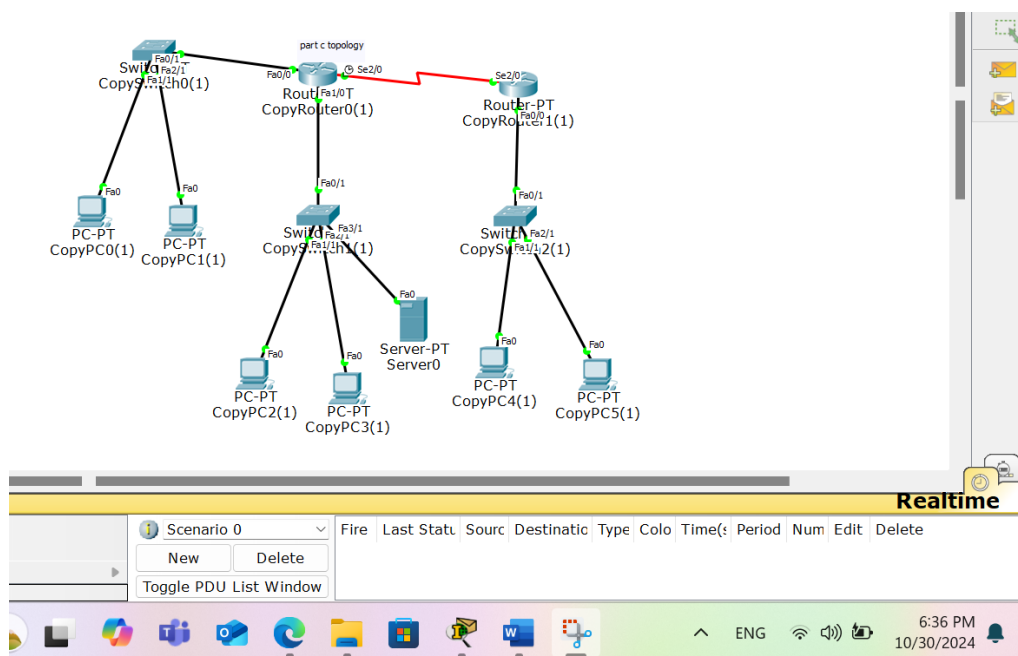


Figure 4: topology of part c

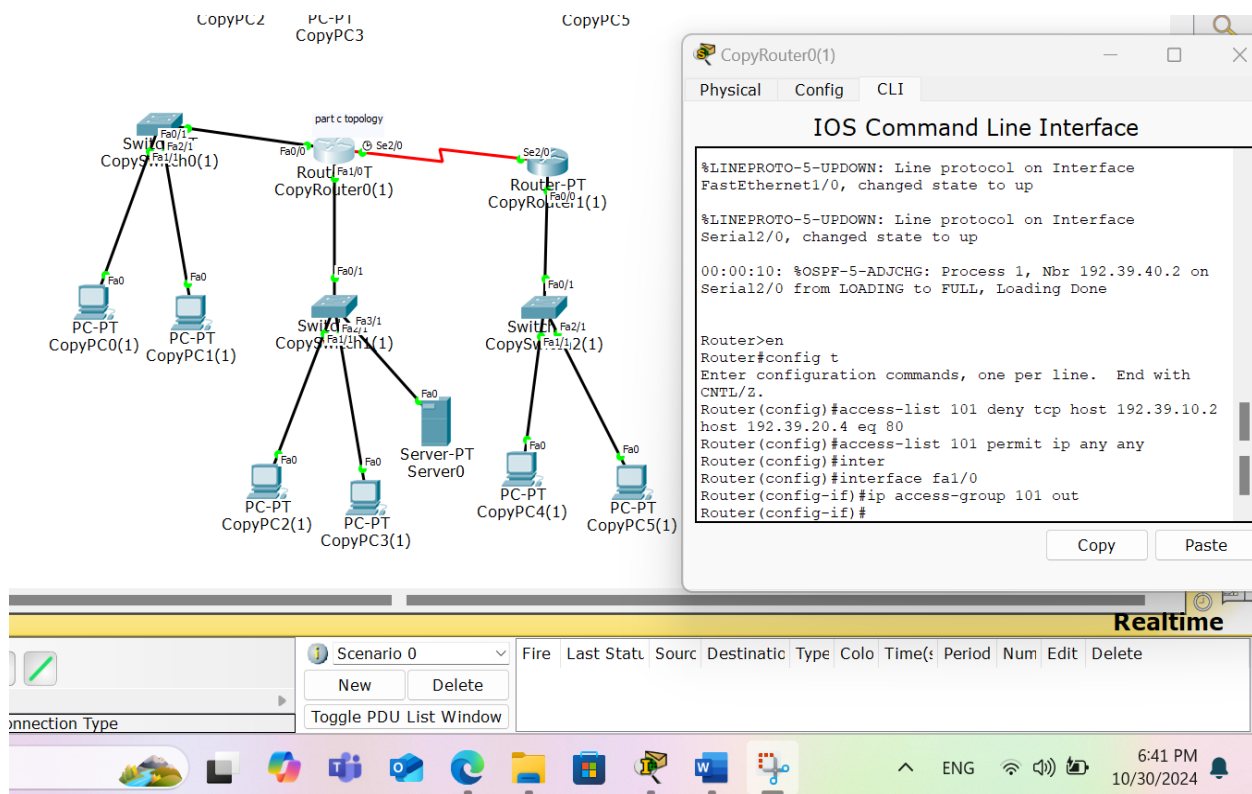
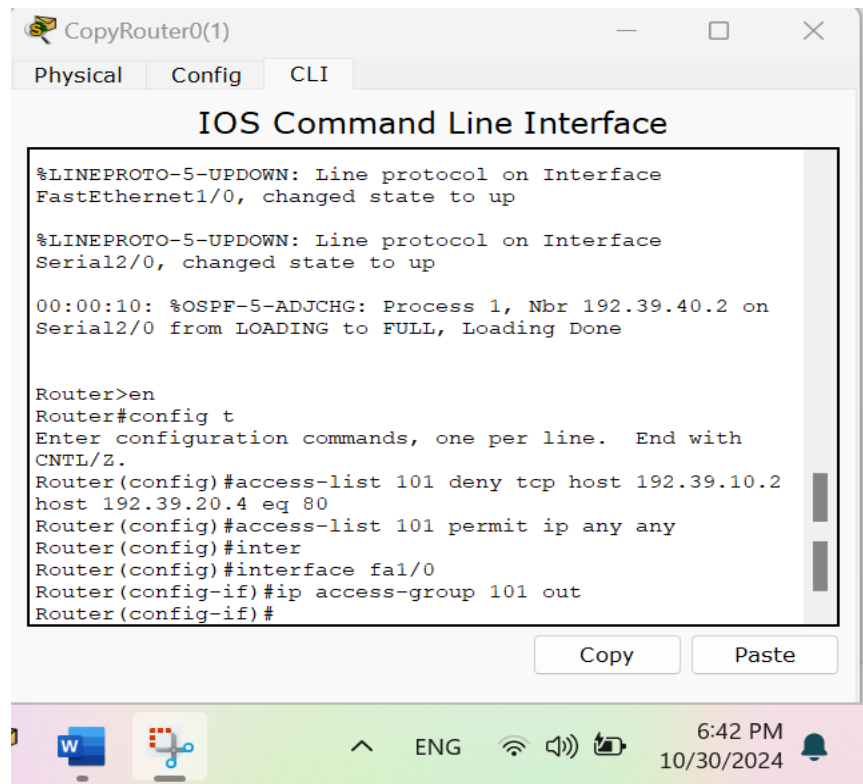


Figure 5 topology & command of part c

Test pc0 to server http port 80

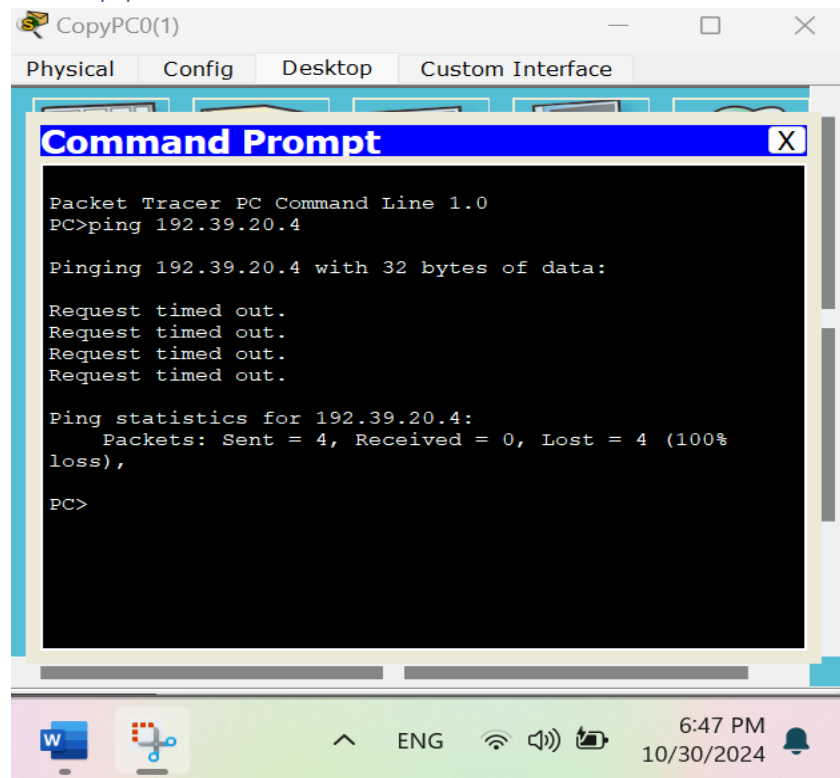


Figure 6 ping 192.39.20.4

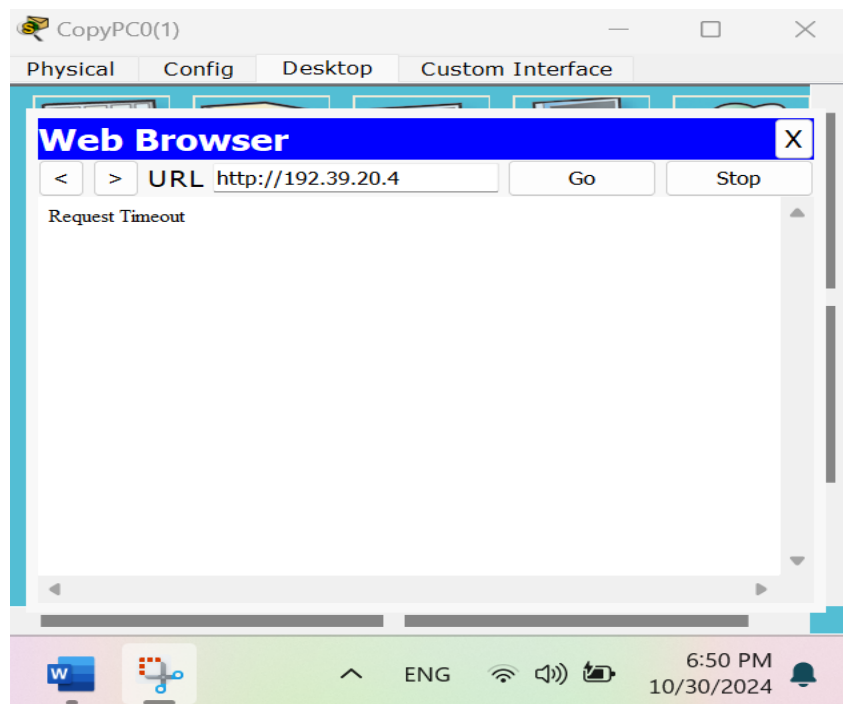
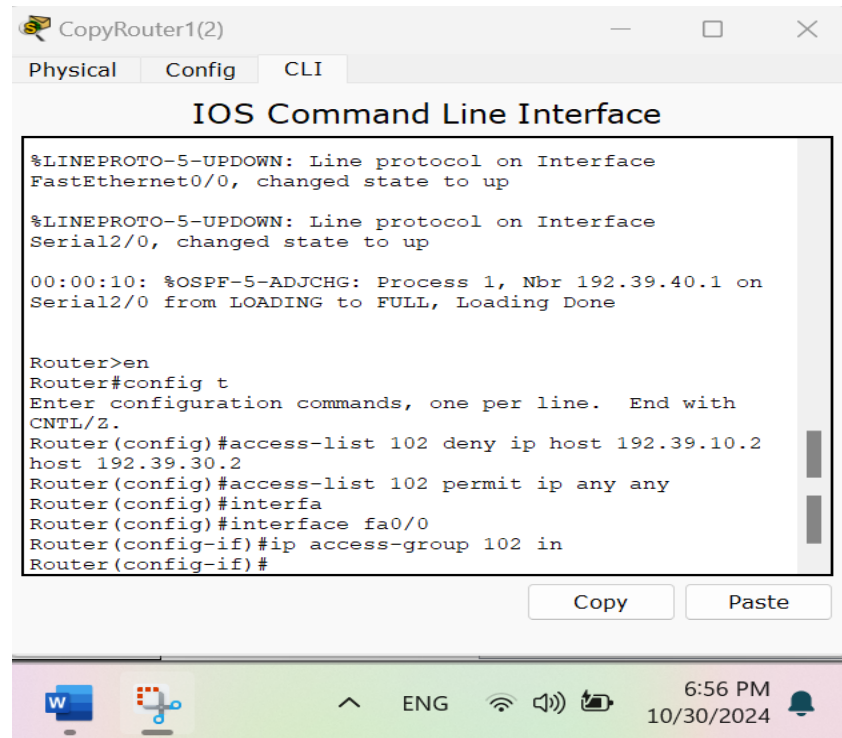


Figure 7: request time out

D. Prevent PC0 from Accessing PC4, Allowing All Other Traffic



```
CopyRouter1(2)
Physical Config CLI
IOS Command Line Interface

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial2/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.39.40.1 on
Serial2/0 from LOADING to FULL, Loading Done

Router>en
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#access-list 102 deny ip host 192.39.10.2
host 192.39.30.2
Router(config)#access-list 102 permit ip any any
Router(config)#interfa
Router(config)#interface fa0/0
Router(config-if)#ip access-group 102 in
Router(config-if)#
```

Figure 8: command of part D

When test it fail PC0 from Accessing PC4 as shown bellow

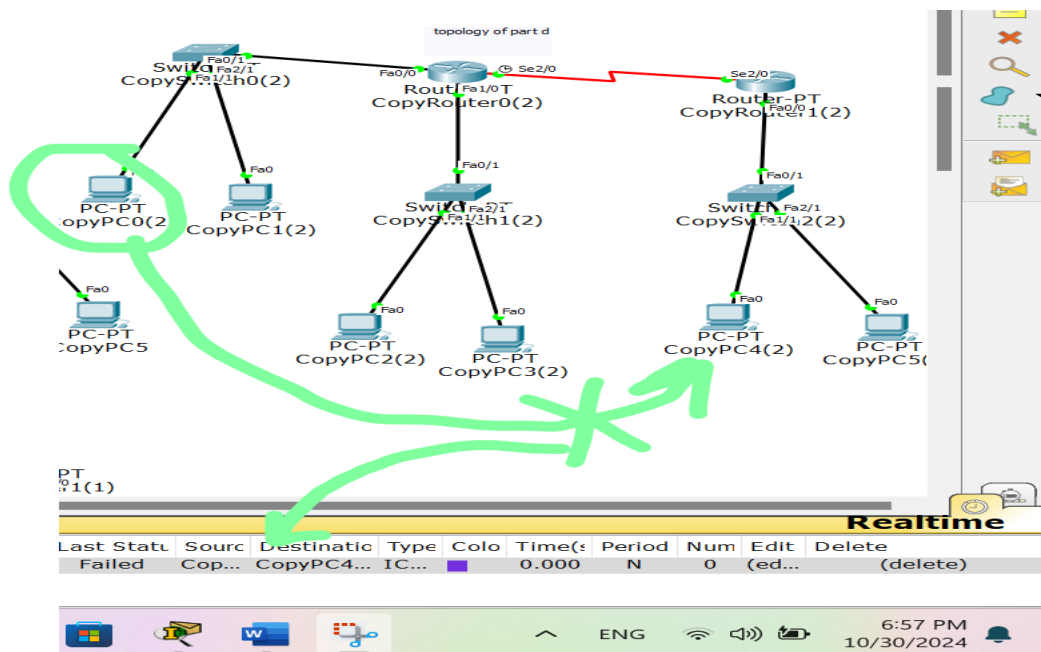


Figure 9: test fail PC0 from Accessing PC4

But the other successful when sent to pc4 as shown bellow

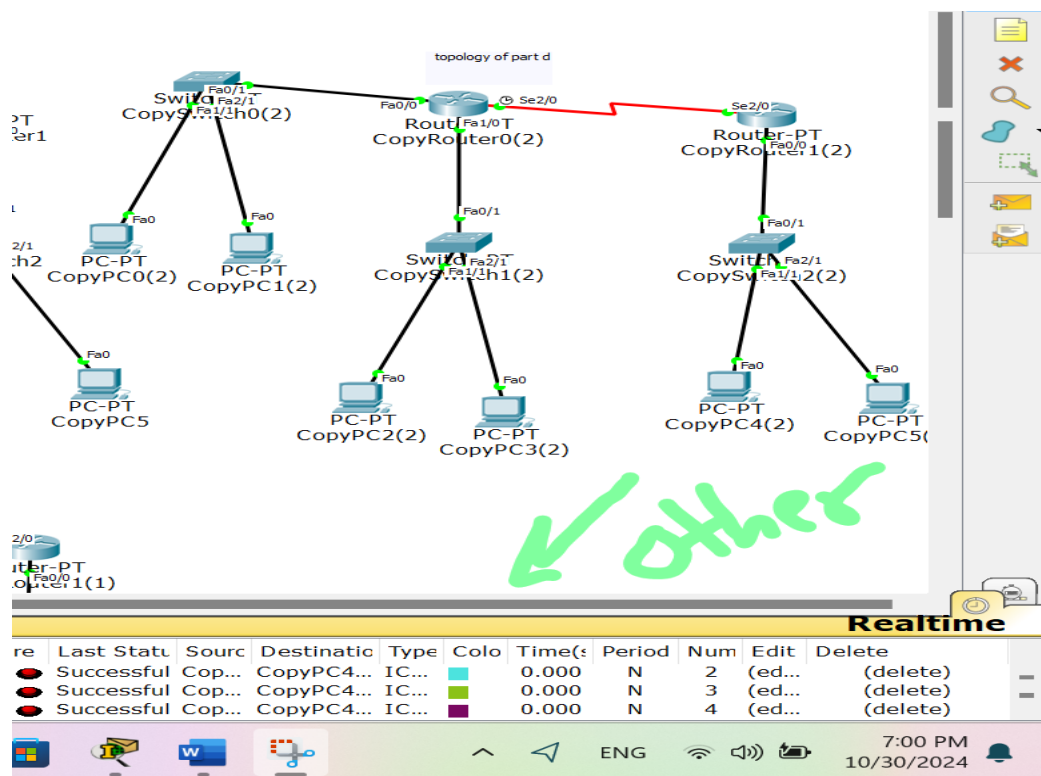


Figure 10: successful all other to pc4 except pc0

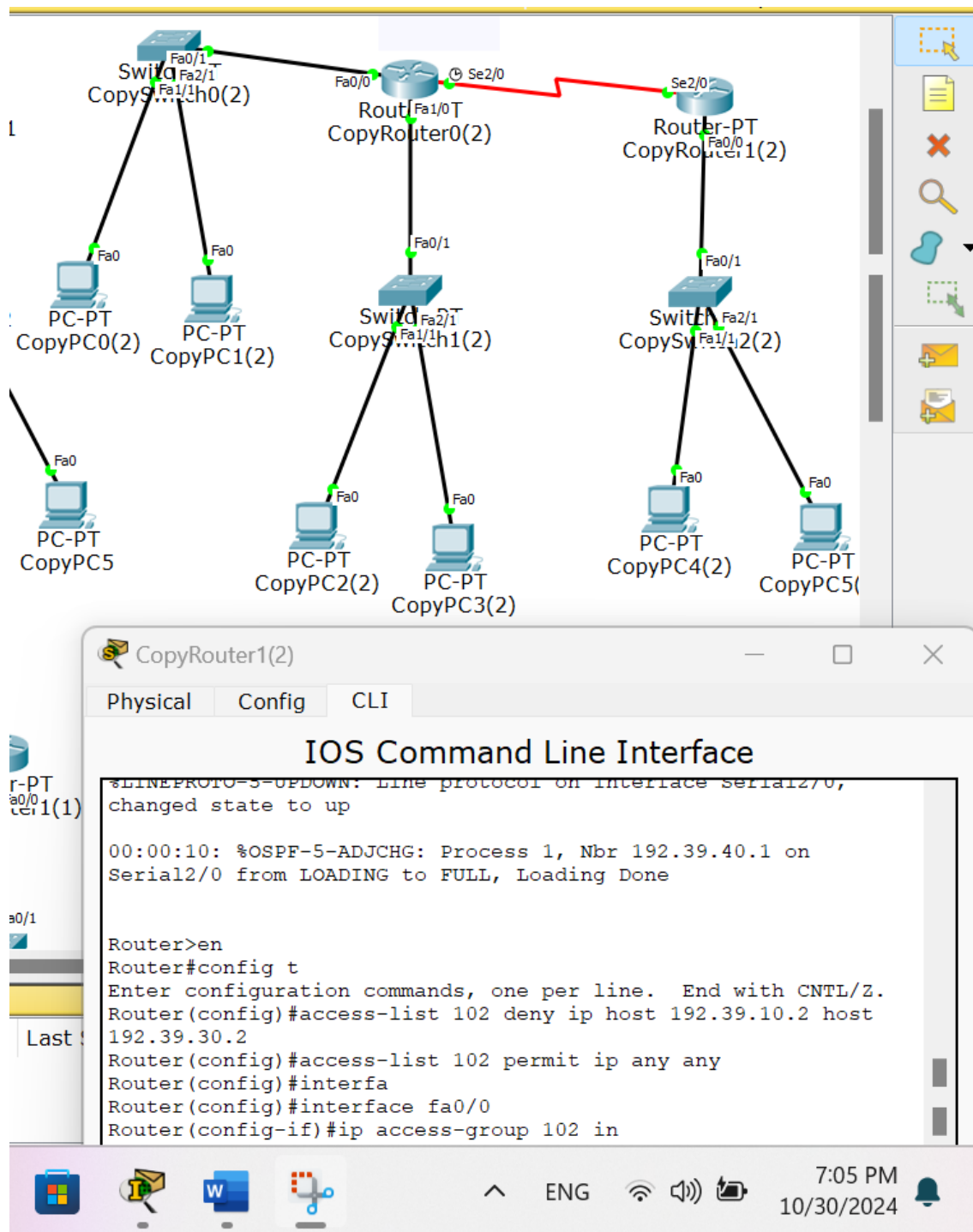
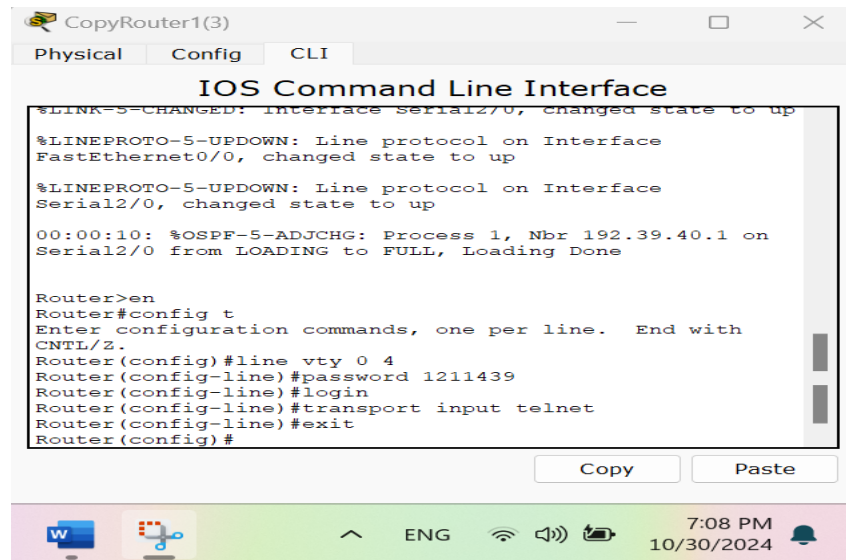


Figure 11: all of part D

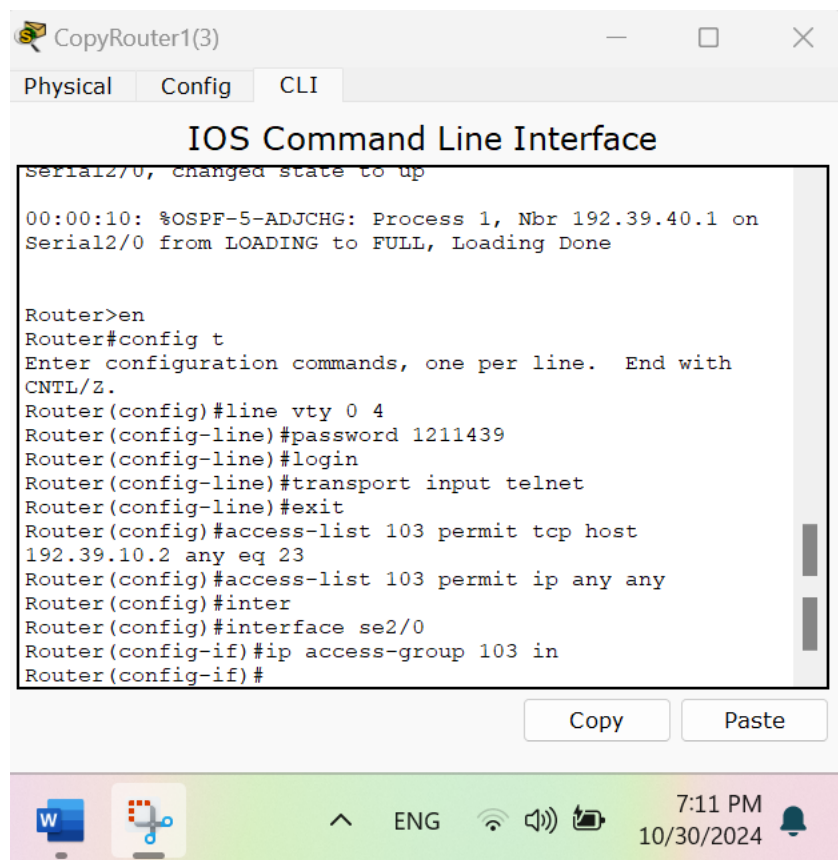
E. Enable Telnet on Router1 and Restrict Telnet Access on se2/0 to Only PC0



```
CopyRouter1(3)
Physical Config CLI
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial2/0, changed state to up
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.39.40.1 on
Serial2/0 from LOADING to FULL, Loading Done

Router>en
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password 1211439
Router(config-line)#login
Router(config-line)#transport input telnet
Router(config-line)#exit
Router(config)#
```

Figure 12: enable telnet



```
CopyRouter1(3)
Physical Config CLI
IOS Command Line Interface
Serial2/0, changed state to up
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 192.39.40.1 on
Serial2/0 from LOADING to FULL, Loading Done

Router>en
Router#config t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password 1211439
Router(config-line)#login
Router(config-line)#transport input telnet
Router(config-line)#exit
Router(config)#access-list 103 permit tcp host
192.39.10.2 any eq 23
Router(config)#access-list 103 permit ip any any
Router(config)#inter
Router(config)#interface se2/0
Router(config-if)#ip access-group 103 in
Router(config-if)#
```

Figure 13: command of part E

Test pc0 to router1

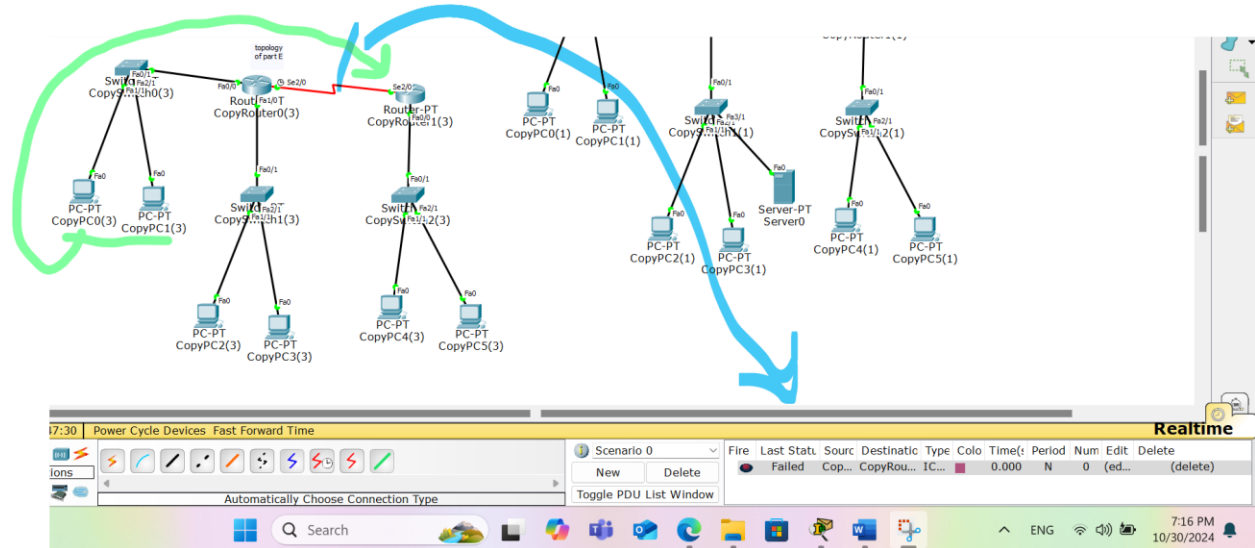
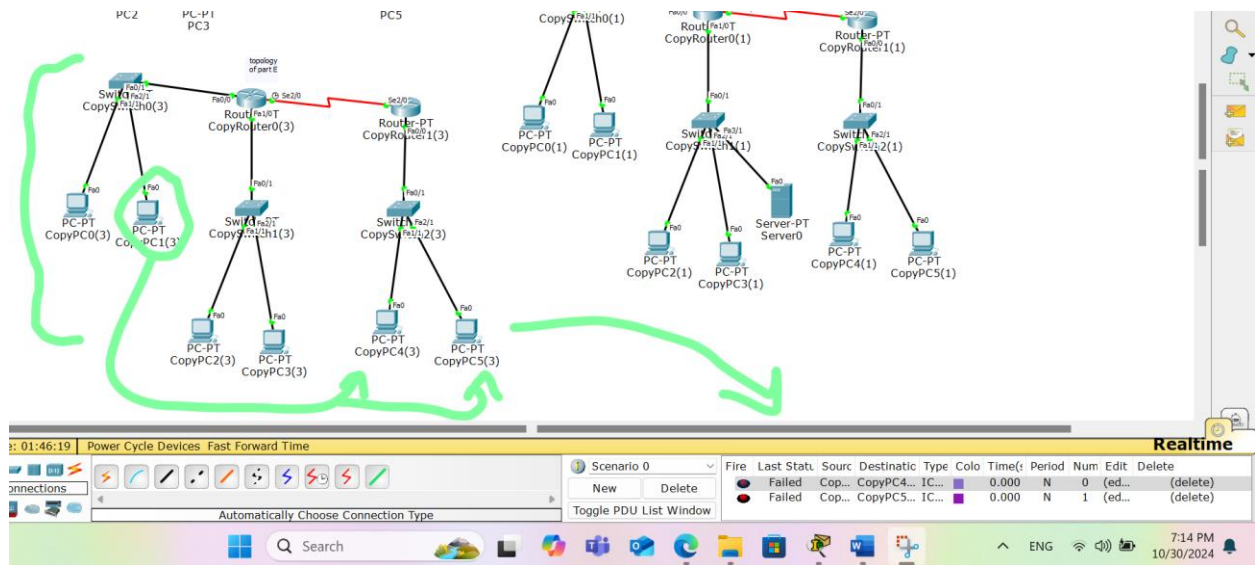


Figure 14: test pc0 to router1