NWK780 – Traditional Networks

Seneca | SCHOOL OF INFORMATION TECHNOLOGY ADMINISTRATION & SECURITY

Lab5 Access Control Lists ACLs

Prepared by:

Nagham Kubba

[redacted]

What Access Lists Do

Access lists ***filter*** network traffic by controlling whether routed packets are ***forwarded or blocked*** at the router's interfaces.

Routers ***examine*** each packet to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists.

Access list criteria could be the ***source address*** of the traffic, the ***destination address*** of the traffic, the ***upper-layer protocol***, or other ***information***. Note that sophisticated users can sometimes successfully evade or fool basic access lists because no authentication is required.*(1)*

Lab Objectives

1. To understand how to configure web servers
2. To understand how to configure ACLs on routers
3. To understand how to test ACLs

Lab Instructions

1. Type your name, student ID
2. Launch Packet Tracer and perform the lab
3. Follow the procedure of the lab and fulfill all requirements.
4. Answer all questions in the provided spaces (preferably in the red-bold font).
5. Add all required screenshots into corresponding spaces
6. Save the file again as a " .pdf " file
7. Submit the PDF file and the packet tracer file in Blackboard by the due date.

(1) https://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/15-2mt/sec-acl-ov-gdl.html

Network Topology

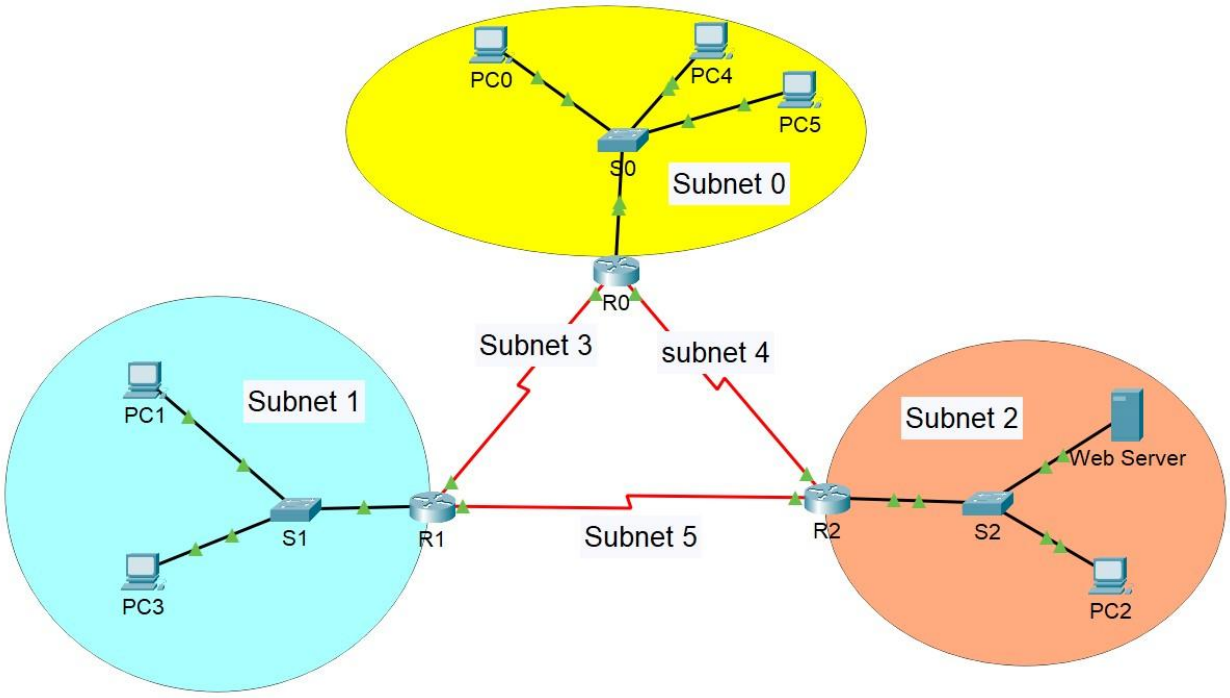


Fig1

Procedure

1. Your major address for this lab is **192.ab.0.0/16**, where **ab** represent the last two digits of your student ID.
2. The networks in the diagram above have the following requirements

Network	Number of hosts
Subnet 0	55
Subnet 1	99
Subnet 2	22
All other subnets	2

3. Use VLSM to assign addresses to routers and devices
4. Assign first IP address of the range to the router and last address(es) to devices connected to each router
5. For the serial links, assign the lower IP address to the router with lower index
6. Connect the full diagram on packet tracer using **PT-Router** for all routers and **2960 switch** for S1
7. Label your diagram using your personalized IP address
8. Take a screen capture of this labeled diagram insert the image below

[2 marks]

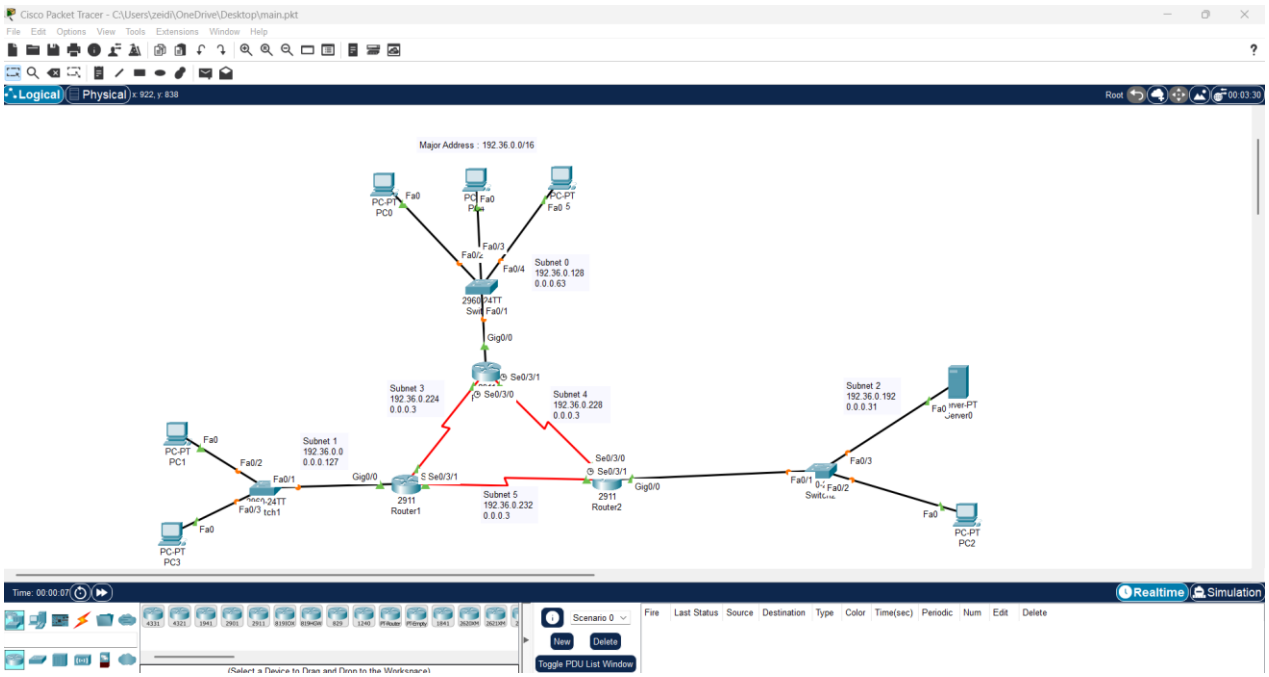


Fig2: Labeled Diagram

9. Use OSPF on all routers to ensure connectivity
10. Click on Services on the Web Server, then click on the index.html file
11. Edit the file to add your full name and student ID to the Welcome line
12. Access the webserver from PC1 by clicking on the Web Brouser (Use ***http://[IP_address]***)
13. Take a screen capture of the output and insert it below ***[3 marks]***

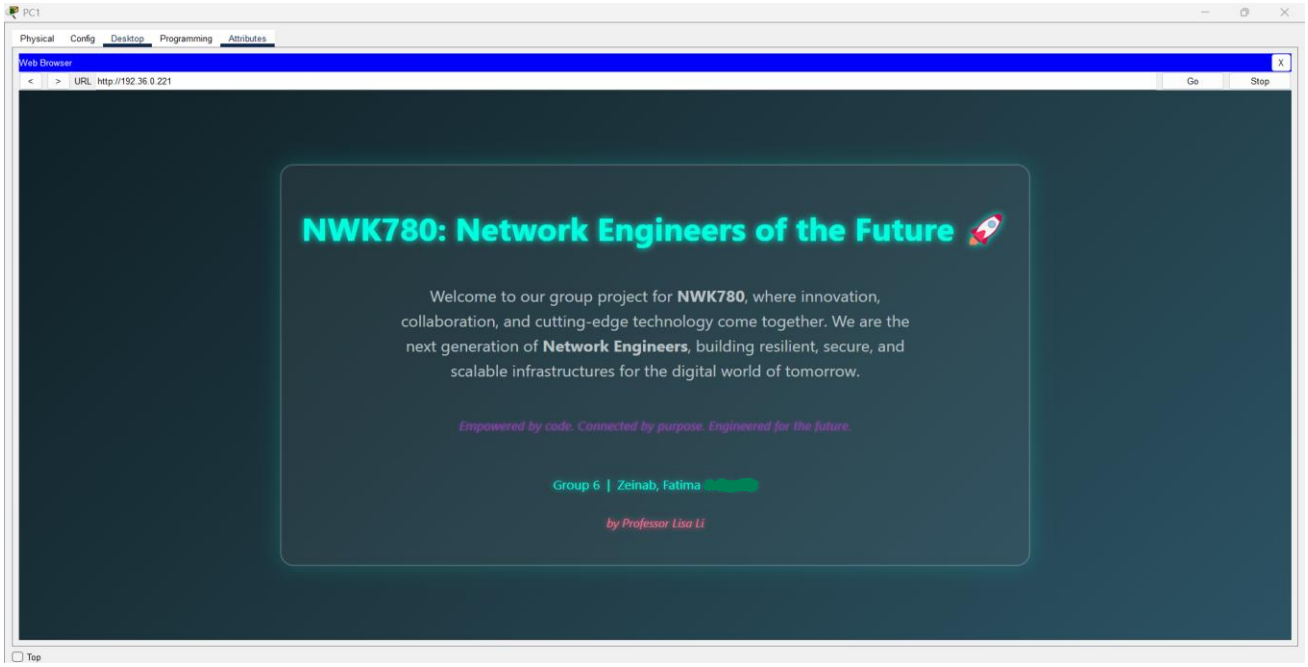
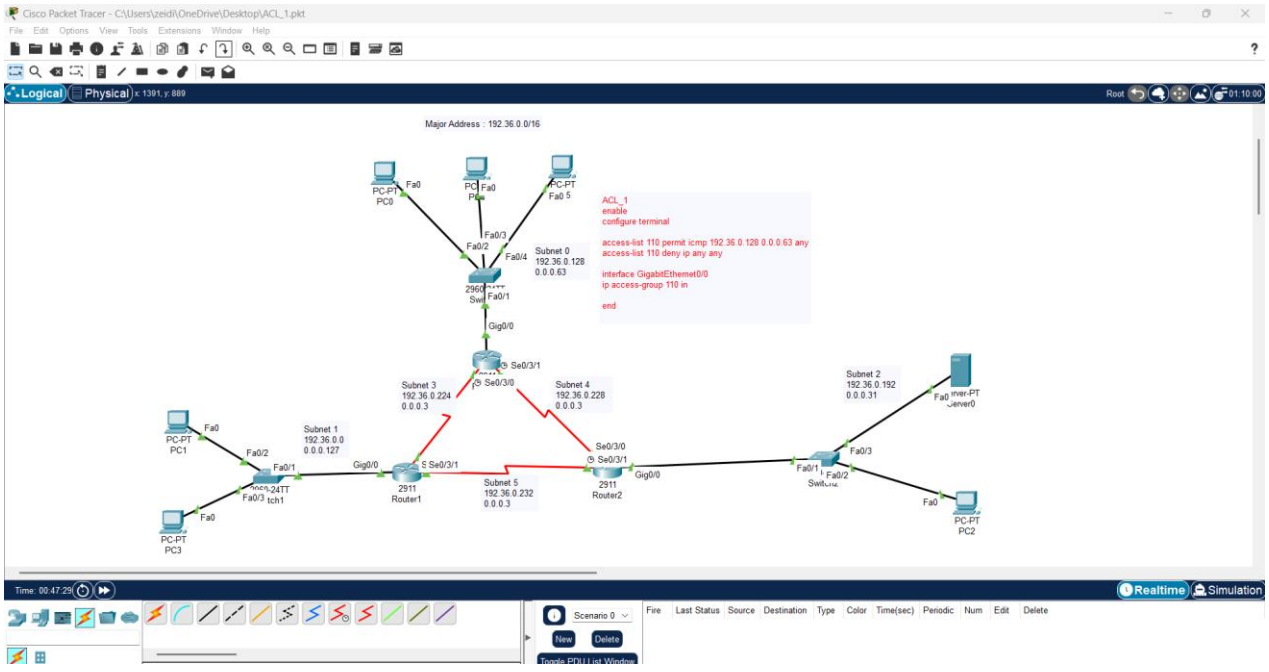


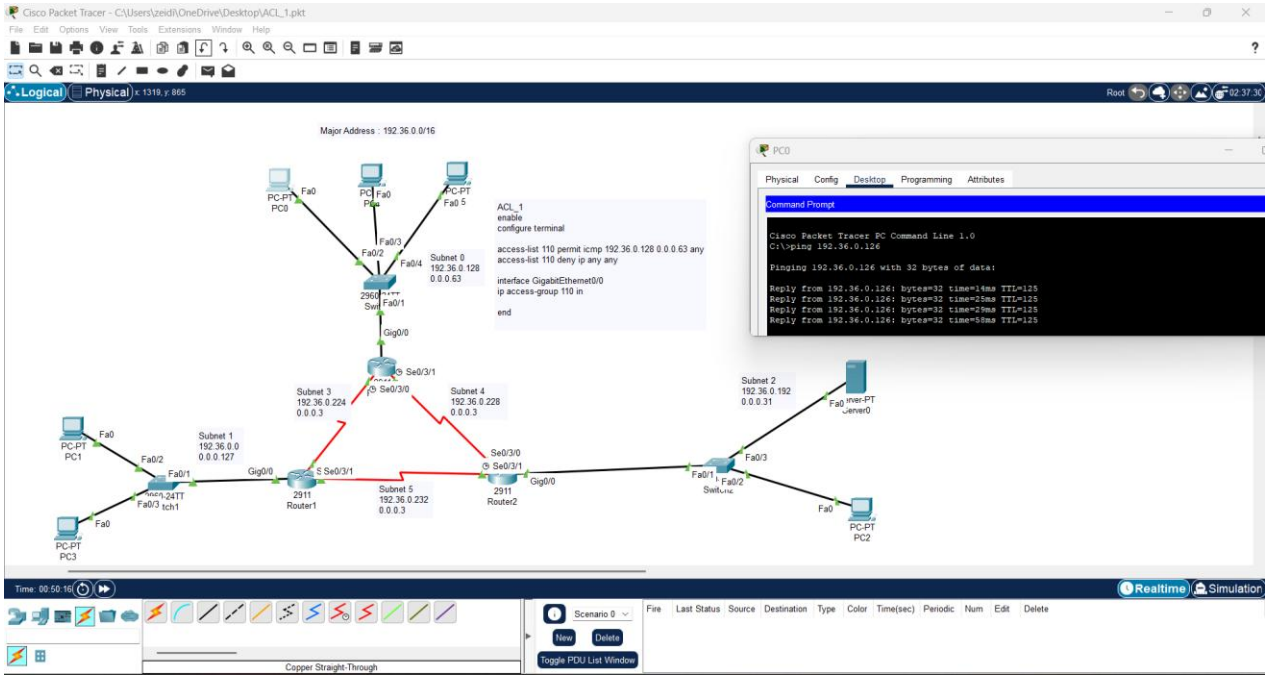
Fig3: Web Browser

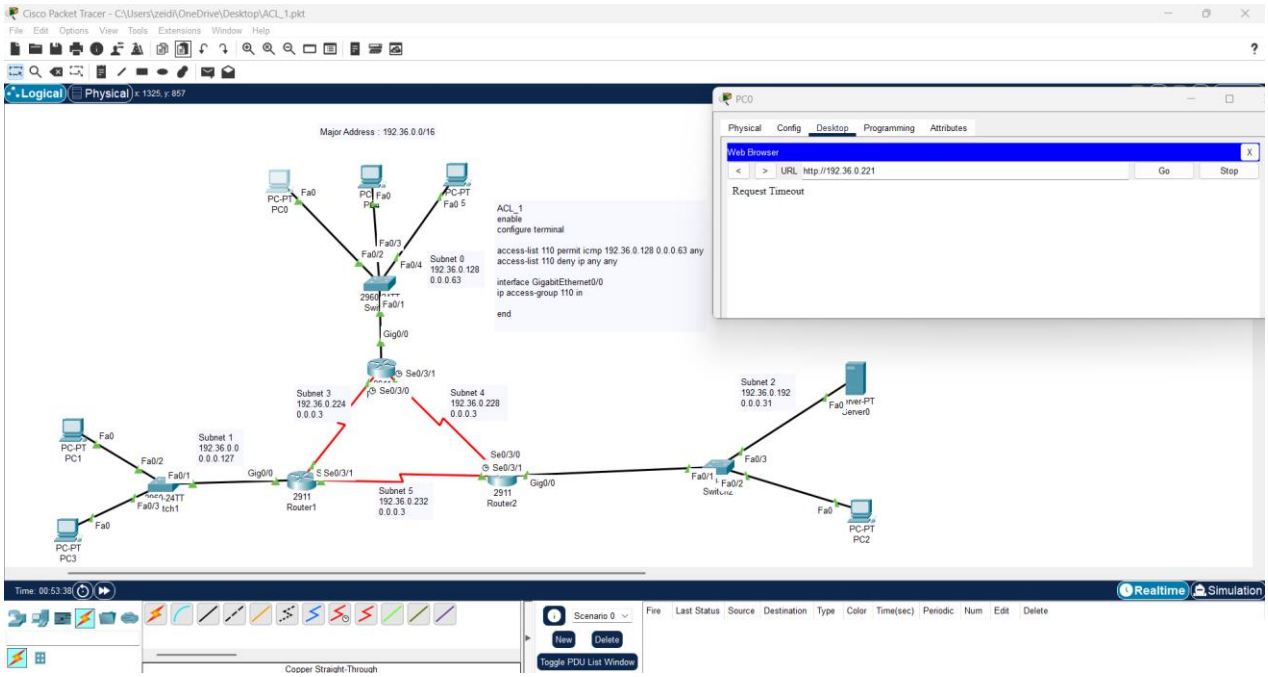
14. Save the above version of your file as the main version (save the file as main.pkt)

ACL_1

15. ***Allow*** PINGs from Subnet 0 ***only*** to any other network. All other traffic must be blocked.
16. Insert the syntax of ACL_1 as a note on your diagram
17. Check that ACL_1 works and save the file as ACL_1.pkt
18. Take a screen capture of the output including the syntax of ACL_1, insert it below [5 marks]





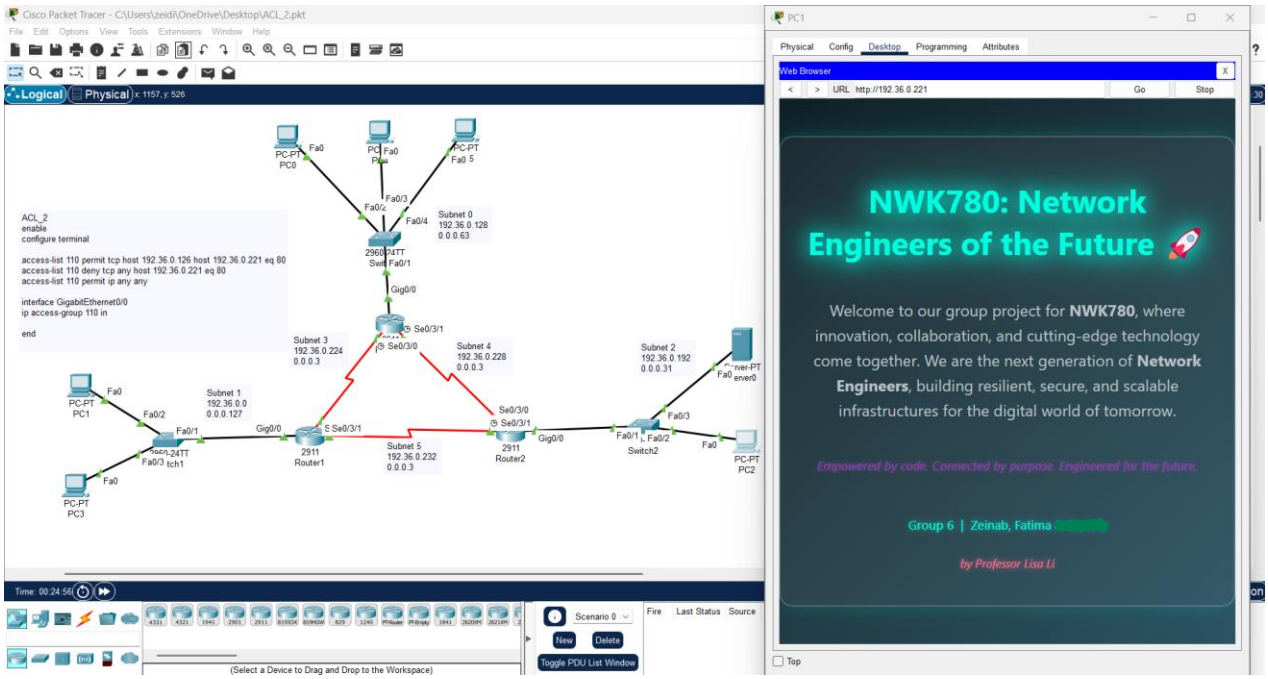


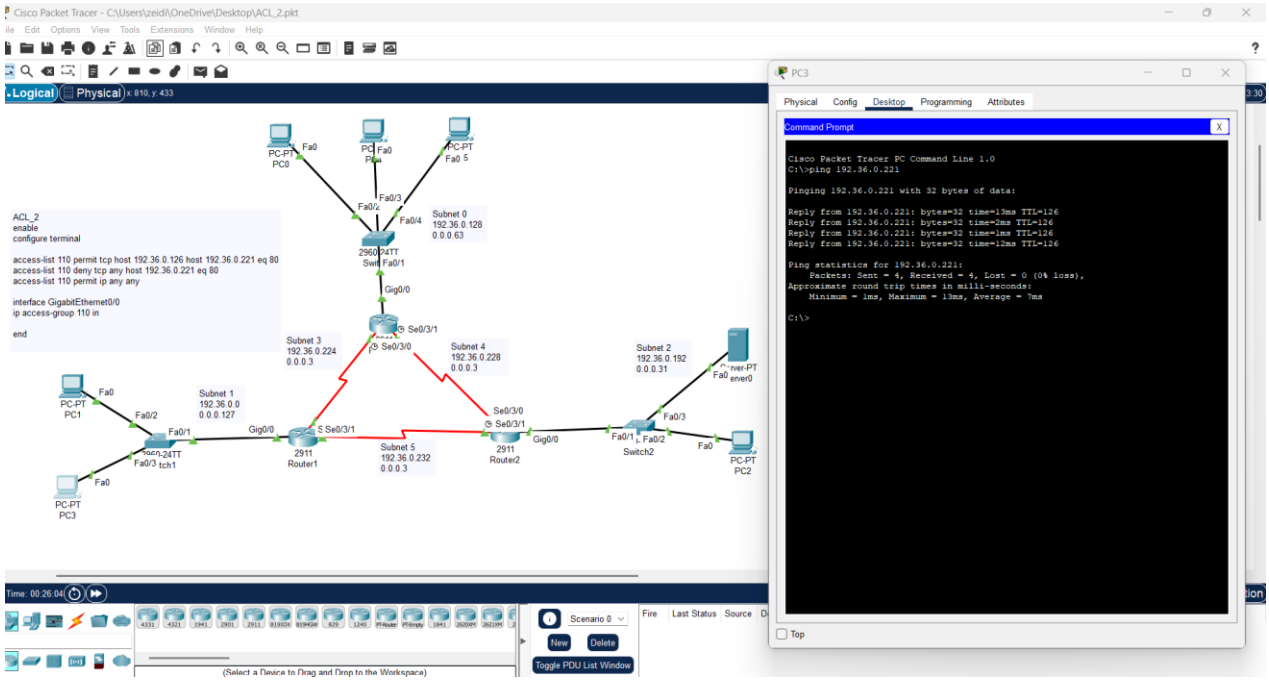

```
Router0(config)#do sh access-list
Extended IP access list 110
    10 permit icmp 192.36.0.128 0.0.0.63 any
    20 deny ip any any

Router0(config)#
```

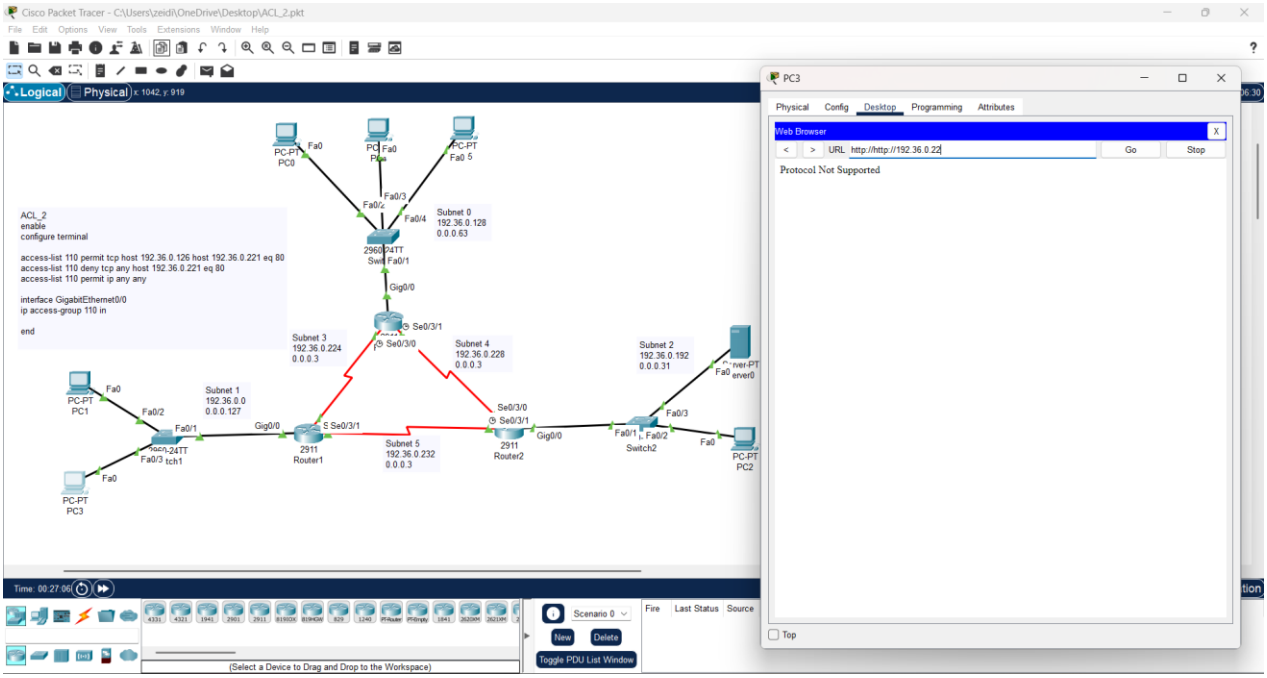
Fig4: ACL_1

ACL_2

19. Re-load the main.pkt file
20. ***Allow*** PC1 ***only*** from Subnet1 to access the Web Server on Subnet2.
21. All other PCs in Subnet 1 should be able to ping the Web Server but not access it
22. Insert the syntax of ACL_2 as a note on your diagram
23. Check that ACL_2 works and save the file as ACL_2.pkt
24. Take one or more screen capture(s) of the output including the syntax of ACL_2, insert it below ***[5 marks]***





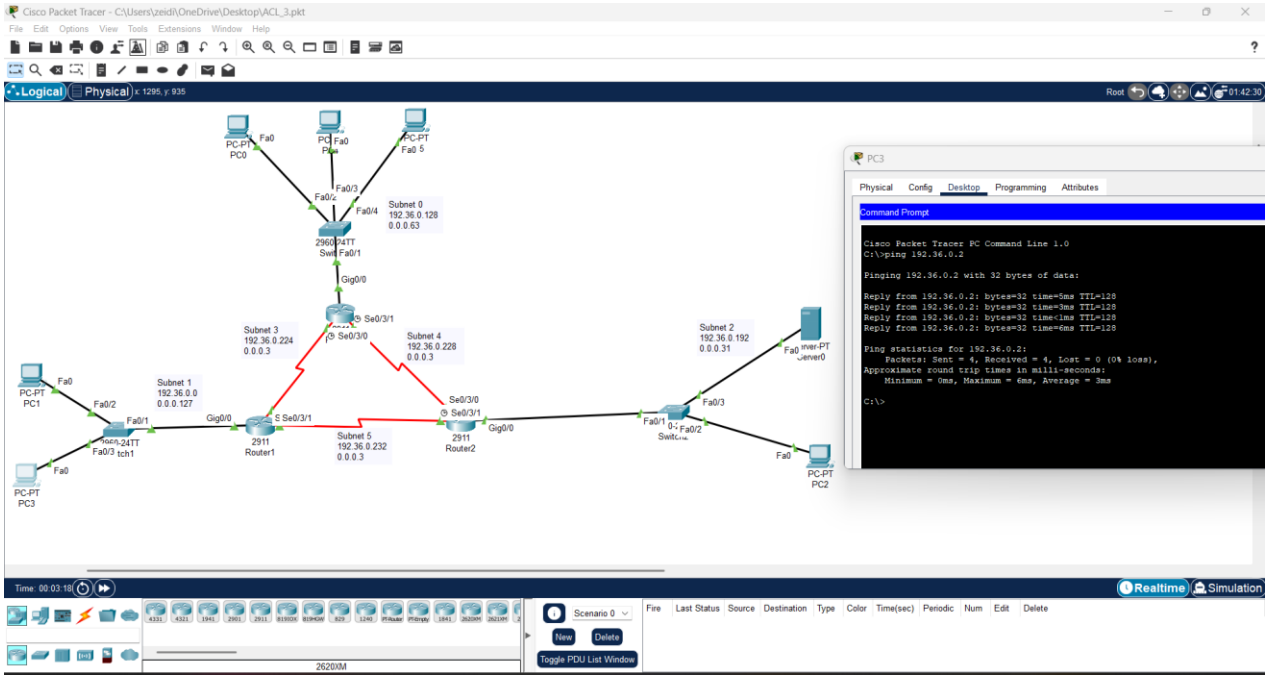


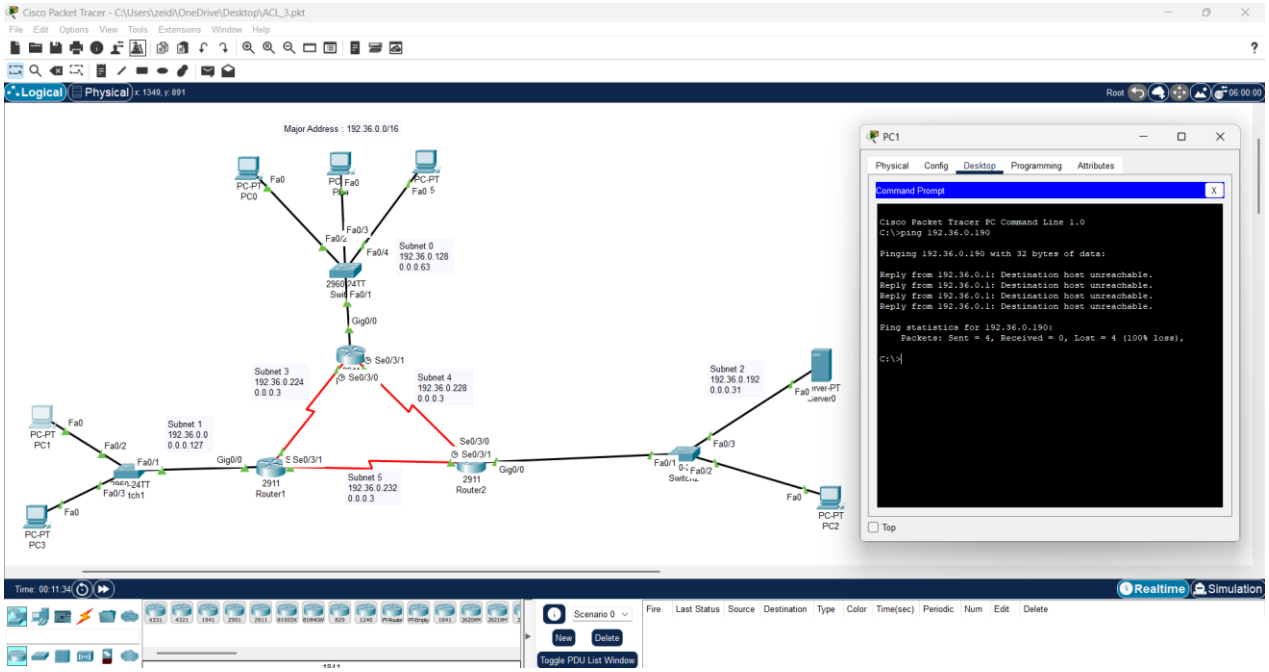

```
R1>en
R1#show access-lists 110
Extended IP access list 110
    permit tcp host 192.36.0.126 host 192.36.0.221 eq www
    deny tcp any host 192.36.0.221 eq www
    permit ip any any

R1#
```

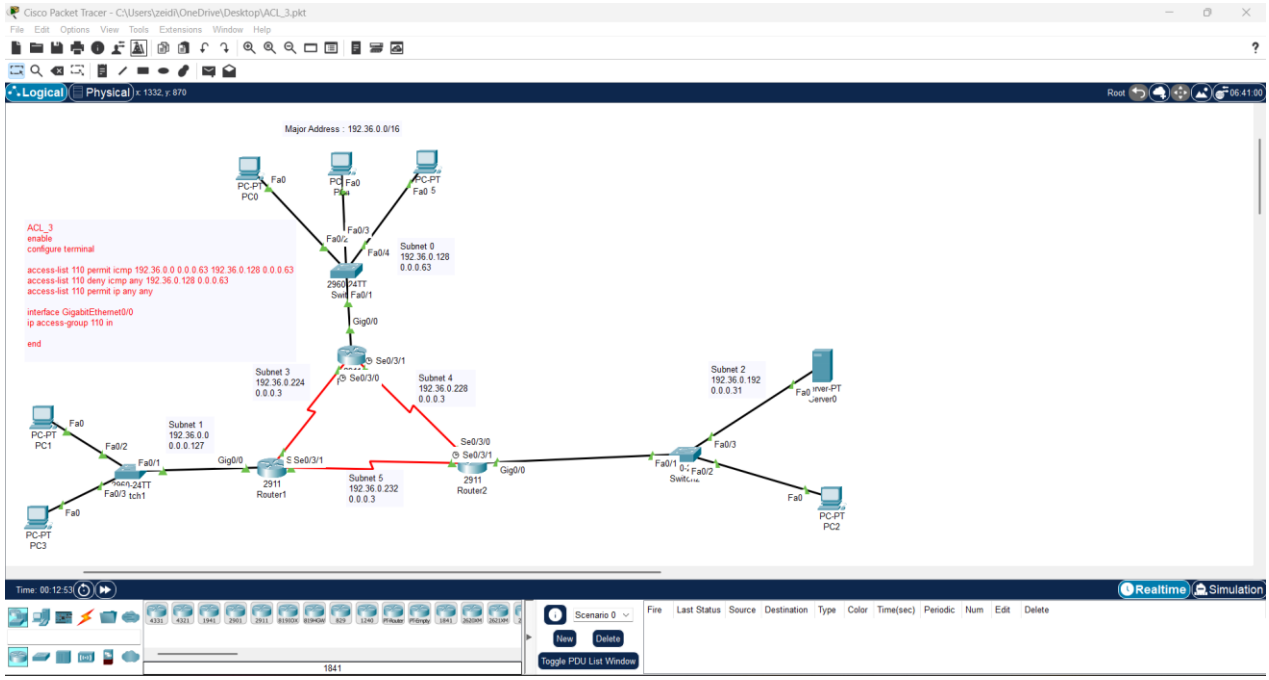
Fig5a: ACL_2

ACL_3

25. Re-load the main.pkt file
26. ***Assign*** PC1 the ***last*** address of the range of subnet 1
27. ***Assign*** PC3 the ***second*** address of the range. (R1 must have the first address)
28. ***Allow*** the ***first half*** of Subnet 1 to PING Subnet 0, (PCs of Subnet 0 should be able to PING all PCs of Subnet 1)
29. Check your ACL by pinging from PC1 and PC3 and capturing the results.
30. Insert the syntax of ACL_3 as a note on your diagram
31. Check that ACL_3 works and save the file as ACL_3.pkt
32. Take one or more screen capture(s) of the output including the syntax of ACL_3, insert it below ***[5 marks]***


Cisco Packet Tracer - C:\Users\zeidi\OneDrive\Desktop\ACL_3.pkt
Logical
Physical
PC3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.36.0.2
Pinging 192.36.0.2 with 32 bytes of data:
Reply from 192.36.0.2: bytes=32 time=5ms TTL=128
Reply from 192.36.0.2: bytes=32 time=3ms TTL=128
Reply from 192.36.0.2: bytes=32 time<1ms TTL=128
Reply from 192.36.0.2: bytes=32 time=6ms TTL=128
Ping statistics for 192.36.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 6ms, Average = 3ms
C:\>
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT Server0
2960-24TT Switch1
2911 Router1
2911 Router2
Subnet 0 192.36.0.128 0.0.0.63
Subnet 1 192.36.0.0 0.0.0.127
Subnet 2 192.36.0.192 0.0.0.31
Subnet 3 192.36.0.224 0.0.0.3
Subnet 4 192.36.0.228 0.0.0.3
Subnet 5 192.36.0.232 0.0.0.3
Time: 00:03:18
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
2620XM






```
R1#sh access-list
Extended IP access list 110
    10 permit icmp 192.36.0.0 0.0.0.63 192.36.0.128 0.0.0.63 (4 match(es))
    20 deny icmp any 192.36.0.128 0.0.0.63 (8 match(es))
    30 permit ip any any

R1#
```

Fig6a: ACL_3

33. You will have many .pkt files for this lab, keep them all as they will be useful for you in your studies
34. Save this document as word document for your own modifications and save another copy as “.PDF”
35. Submit the PDF file with the packet tracer files to your Lab5 submission tab.