

Lab5 Access Control Lists ACLs

Prepared by:

Nagham Kubba

Modified by Ali Nezhad

Group Number: **1**

Lab Theory

What Access Lists Do

Access lists **filter** network traffic by controlling whether routed packets should be **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. Follow the procedure of the lab and fulfill all requirements.
2. Answer all questions in the provided spaces (preferably in the red-bold font).
3. Add all required screenshots into corresponding spaces
4. Save the file again as a “ .pdf ” file
5. Submit the PDF file on Blackboard by the due date.

Network Topology

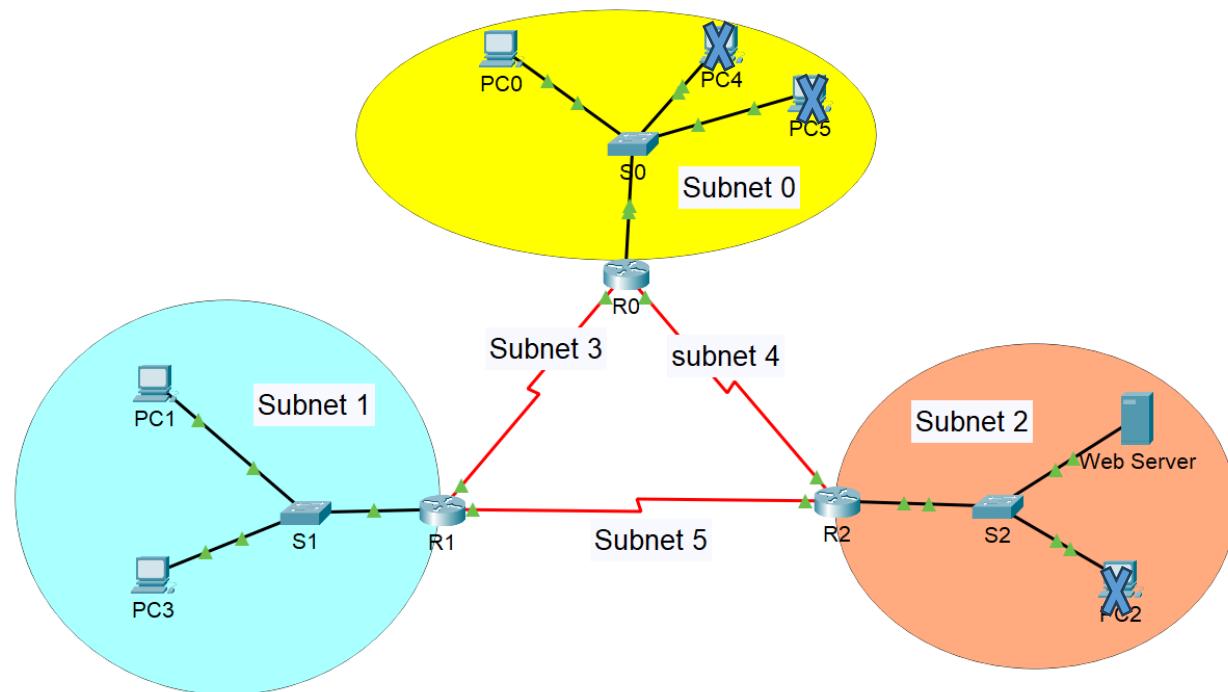


Fig1 Network Topology

Procedure

1. Use the following major network address where X is your group number: X.X.0.0/16
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 the **first available IP address of a range** in a LAN to the router.
5. For the serial links, assign the **lower IP address to the router with lower index**
6. Cable diagram in the lab using **1941 routers** and **2960 switches**. Put only one PC in subnet 0 (PC0), Two PCs in Subnet 1 (PC1 and PC3), and one in Subnet 2 (the server).
7. Since we are not adding PC2, PC4 and PC5 to the network, you can disregard S0 and S2 as well.
8. Assign the second available IP address in Subnet1 to PC3 and the last available IP address to PC1.
Assign the last available IP addresses in the corresponding ranges to the web server and to PC0.
9. Label your diagram with appropriate IP addresses. It may be easier to draw your diagram using Packet Tracer.
10. **Insert this labeled diagram below.** [1 marks]

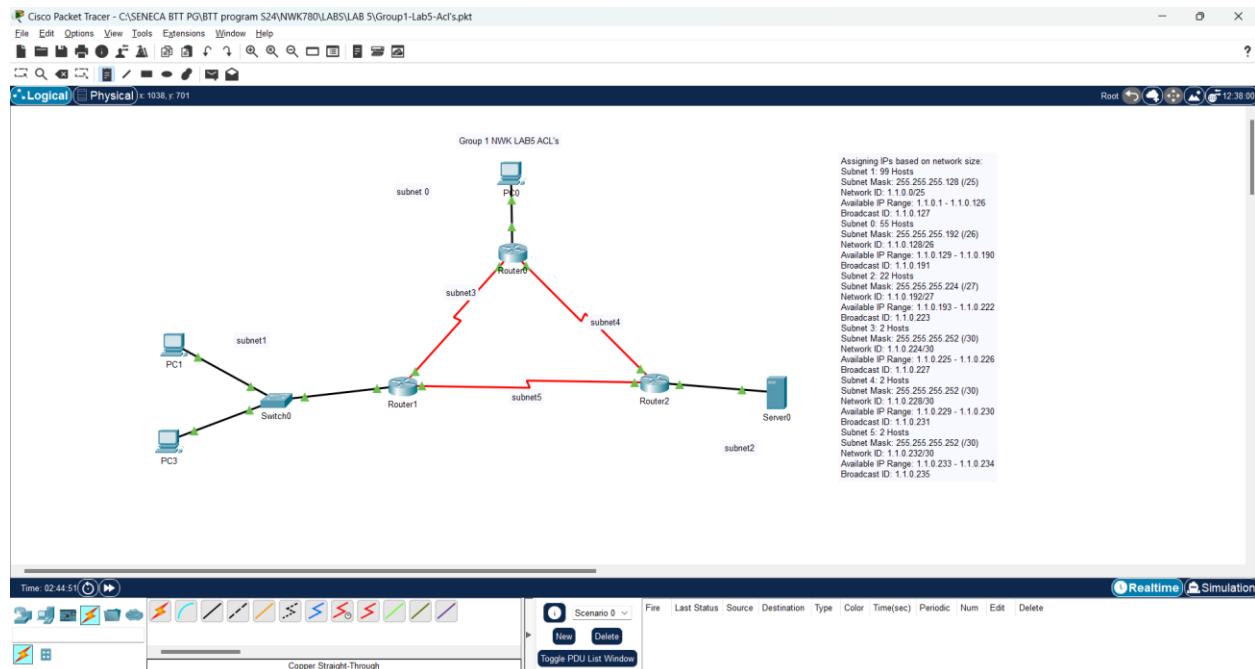


Fig2: Labeled Diagram

11. Use OSPF on all routers to ensure connectivity. Do not proceed further if you don't have full connectivity yet.
12. Install an Apache Web Server on one of your PCs, designated as Web Server in Subnet 2.
13. Edit the index.htm file to add your full names to it.
14. Access the webserver from PC1 using a Web Browser (Use <http://IP address of Server>)
15. Take a screen capture of the output and **insert it below** [1 mark]

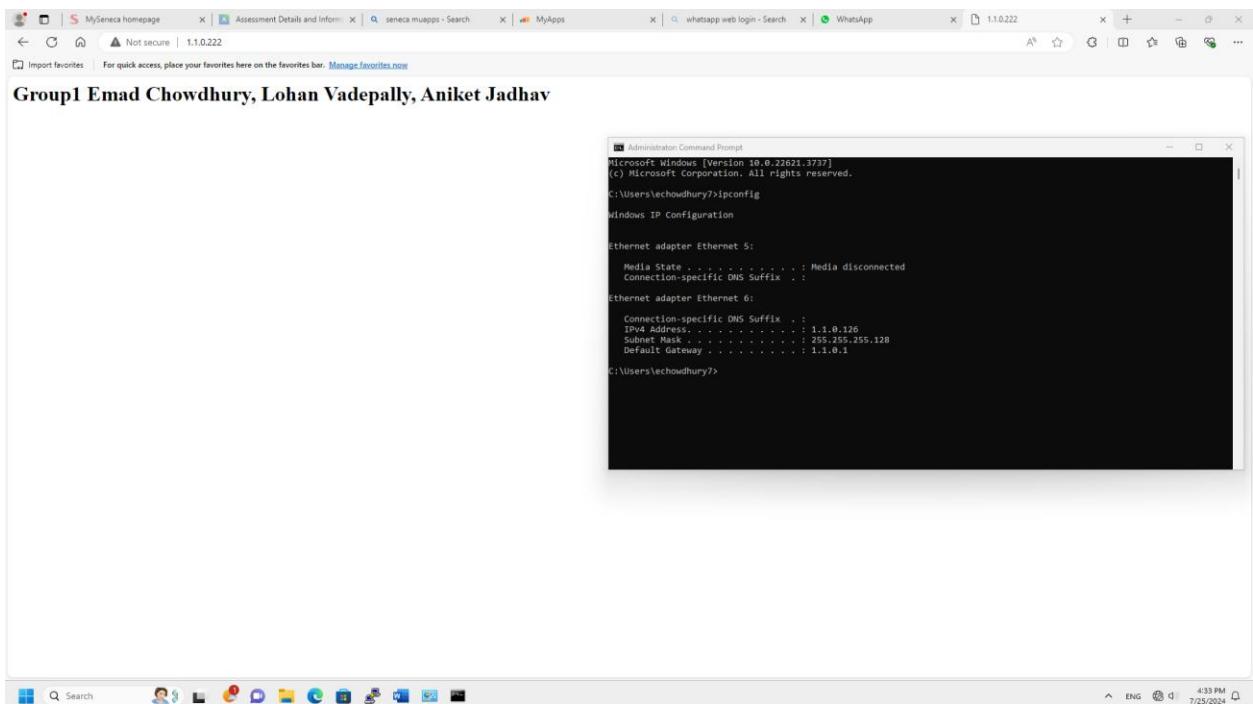


Fig3: Web Browser

Task1

16. **Allow only** PINGs from Subnet 0 to any other network. All other traffic must be blocked.
17. Insert the necessary ACL statements as a note on your diagram. You can copy/paste the relevant statements from the running configuration (not all of the running configuration). Where is the best place to deploy your ACL(s)?
18. Check your work:
 - a. Ping the web server in Subnet 2 from subnet 0. It must succeed.
 - b. Try connecting to the Apache server using a browser. This must fail.
19. Take screen captures of these outputs and **insert them below** along with the diagram showing the ACL statements. **[1 mark]**

Administrator: Command Prompt

```

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
C:\Users\echowdhury>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet 5:
    Connection-specific DNS Suffix . :
    IPv4 Address . . . . . : 1.1.0.198
    Subnet Mask . . . . . : 255.255.255.192
    Default Gateway . . . . . : 1.1.0.129

C:\Users\echowdhury>ping 1.1.0.222
Pinging 1.1.0.222 with 32 bytes of data:
Reply from 1.1.0.222: bytes=32 time=9ms TTL=126
Reply from 1.1.0.222: bytes=32 time=10ms TTL=126
Reply from 1.1.0.222: bytes=32 time=10ms TTL=126
Reply from 1.1.0.222: bytes=32 time=10ms TTL=126

Ping statistics for 1.1.0.222:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms
C:\Users\echowdhury>Group 1

```

COM3 - PuTTY

```

R0#s
*Jul 25 20:23:38.215: %SYS-5-CONFIG_I: Configured from console by console ip in
% Ambiguous command: "sh ip in"
R0#sh ip int br
Interface          IP-Address      OK? Method Status   Prot
G0/0               unassigned      YES unset administratively down down
GigabitEthernet0/0  1.1.0.129      YES manual up       up
GigabitEthernet0/1  unassigned     YES unset administratively down down
Serial0/0/0         1.1.0.225      YES manual up       up
Serial0/0/1         1.1.0.230      YES manual up       up

R0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#access-list 100 permit icmp 1.1.0.128 0.0.0.63 any echo
R0(config)#access-list 101 permit icmp any 1.1.0.128 0.0.0.63 echo-reply
R0(config)#access-list 100 deny ip any any
R0(config)#int g0/0
R0(config-if)#ip access-group 100 in
R0(config-if)#Group 1

```

MySeneca homepage | MyApps | WhatsApp | Lab5- ACLs Step-by-Step Procedure | 1.1.0.222 | +

Import favorites | For quick access, place your favorites here on the favorites bar. [Manage favorites now](#)

Hmmm... can't reach this page

1.1.0.222 took too long to respond

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_TIMED_OUT

[Diagnose issue](#) [Refresh](#)

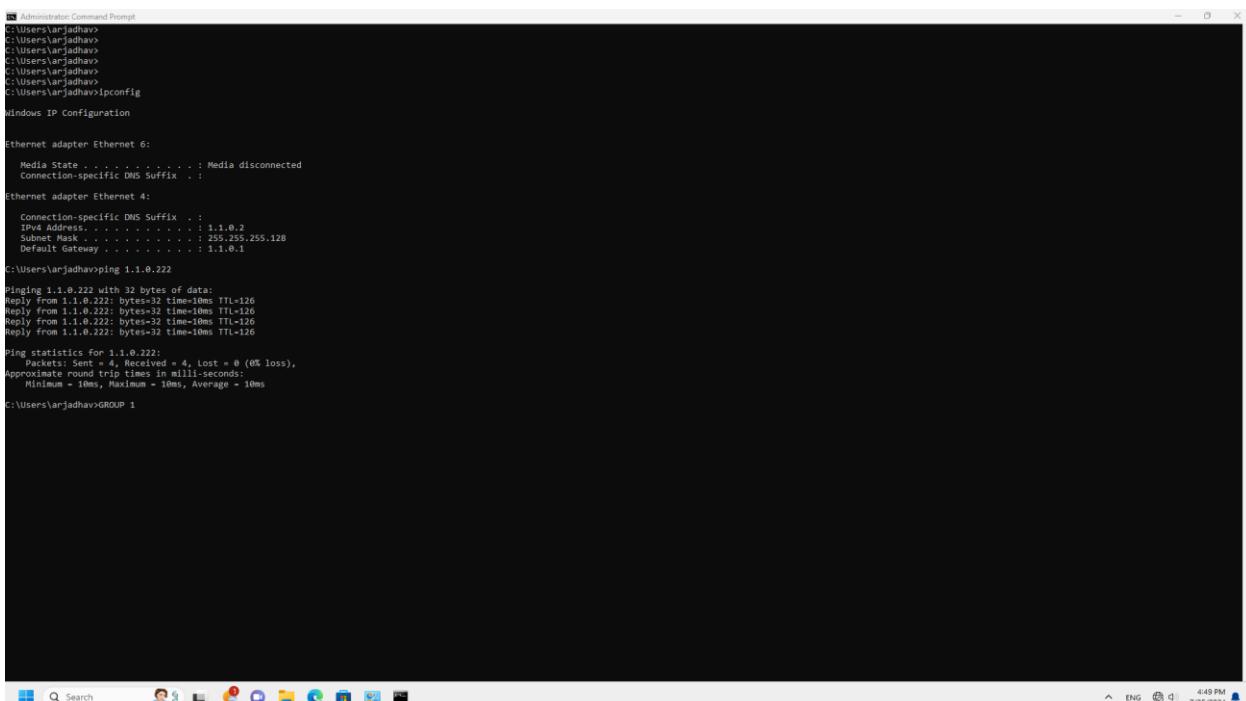
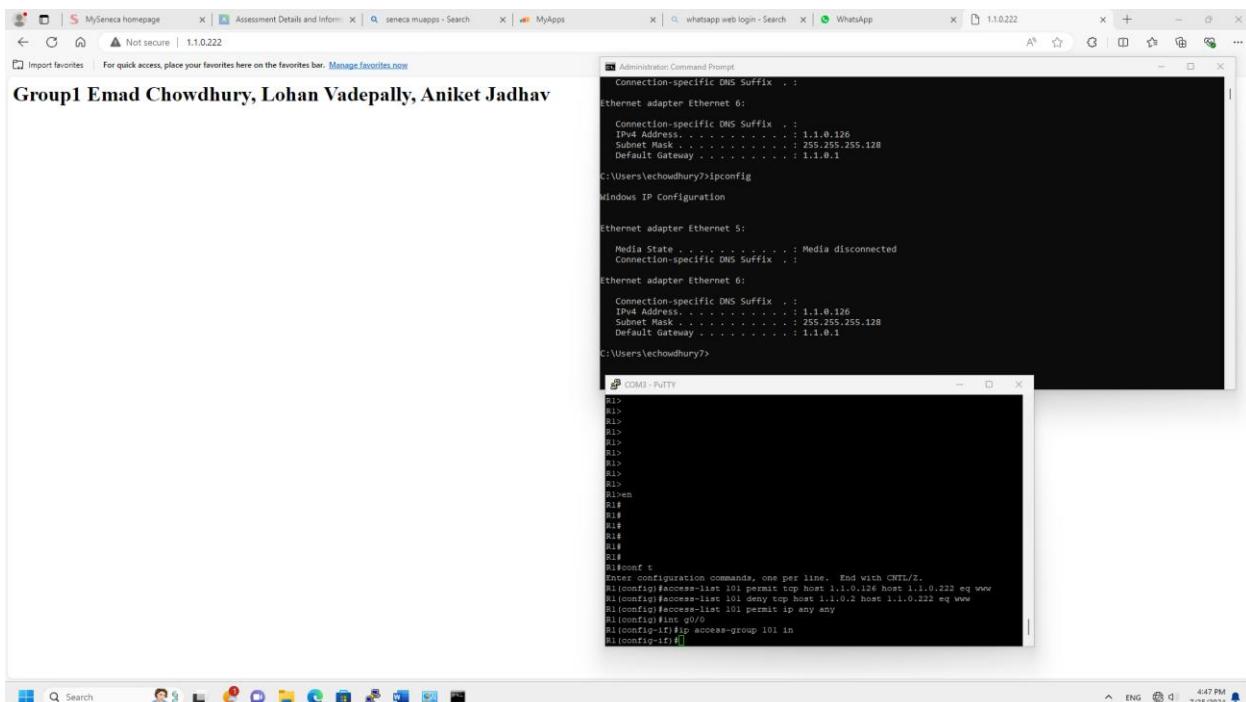
Fig4: Task1

Task2

20. **Allow only** PC1 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 the web pages on it.
22. Insert the necessary ACL statements as a note on your diagram as you did in Task1.
Where is the best place to deploy your ACL(s)?
23. Check your work:
 - a. Access the server from PC1 using a web browser. This should work.

- b. Ping the server from PC3. It should work.
c. Access the server from PC3 using a web browser. This should fail.

24. Take screen capture(s) of these outputs and insert them below as well as the diagram showing the ACL statements. **[1 mark]**



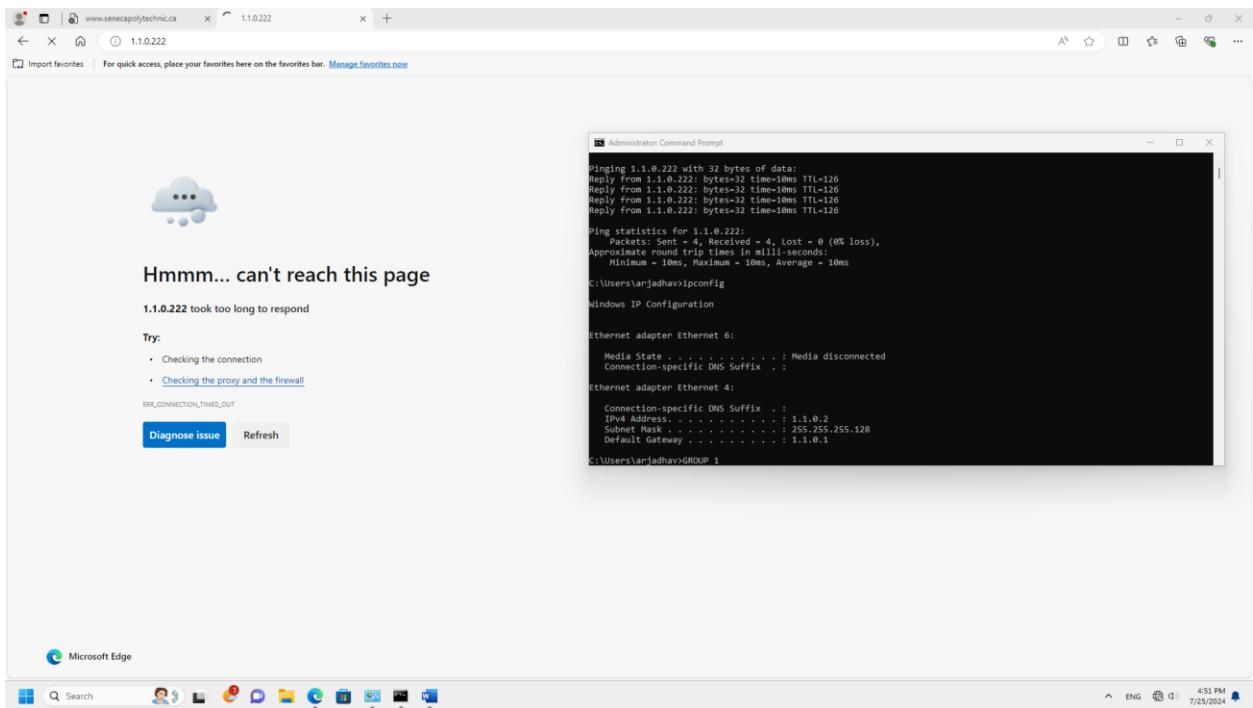


Fig5: Task2

Task3

25. **Allow** only the **first half** of Subnet 1 to PING Subnet 0. All the PCs of Subnet 0 should be able to PING all PCs of Subnet 1.
26. Insert the necessary ACL statements as a note on your diagram.
27. Remove the previous ACL(s) from R2.
28. Check your work:
 - a. Ping from PC1 to PC0 must fail.
 - b. Ping from PC3 to PC0 must succeed.
 - c. Pings from PC0 to PC1 and PC3 must succeed.
29. Take screen capture(s) of these outputs as well as the diagram showing the syntax of your ACL statements and, **insert them below [2 marks]**

```

Administrator: Command Prompt
C:\Users\echowdhury>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 5:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 6:
  Connection-specific DNS Suffix . :
    IPv4 Address . . . . . : 1.1.0.126
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 1.1.0.1

C:\Users\echowdhury>ping 1.1.0.190

Pinging 1.1.0.190 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 1.1.0.1: Destination net unreachable.
Request timed out.

Ping statistics for 1.1.0.190:
  Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
C:\Users\echowdhury>group 1

COM3 - PuTTY
R1#
R1#
R1#
R1#sh ip int br
Interface          IP-Address      OK? Method Status      Prot
o0/0               unassigned      YES unset administratively down down
GigabitEthernet0/0  1.1.0.1        YES manual up       up
GigabitEthernet0/1  unassigned      YES unset administratively down down
Serial0/0/0         1.1.0.233     YES manual up       up
Serial0/0/1         1.1.0.226     YES manual up       up

R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# 100 permit icmp 1.1.0.0 0.0.0.63 1.1.0.128 0.0.0.63 echo
R1(config)# 100 permit icmp 1.1.0.0 0.0.0.127 1.1.0.128 0.0.0.63 echo-reply
R1(config)#int go/0
R1(config-if)#ip access-group 100 in
R1(config-if)#group 1

Centre App lists

```

```

Administrator: Command Prompt
Ethernet adapter Ethernet 6:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 4:
  Connection-specific DNS Suffix . :
    IPv4 Address . . . . . : 1.1.0.2
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 1.1.0.1

C:\Users\arjad hav>ping 1.1.0.190

Pinging 1.1.0.190 with 32 bytes of data:
Reply from 1.1.0.190: bytes=32 time=14ms TTL=126
Reply from 1.1.0.190: bytes=32 time=10ms TTL=126
Reply from 1.1.0.190: bytes=32 time=10ms TTL=126
Reply from 1.1.0.190: bytes=32 time=10ms TTL=126

Ping statistics for 1.1.0.190:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 11ms

C:\Users\arjad hav>GROUP 1

```

```

Administrator: Command Prompt
C:\Users\echowdhury>ping 1.1.0.2

Pinging 1.1.0.2 with 32 bytes of data:
Reply from 1.1.0.2: bytes=32 time=10ms TTL=126

Ping statistics for 1.1.0.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\Users\echowdhury>ping 1.1.0.126

Pinging 1.1.0.126 with 32 bytes of data:
Reply from 1.1.0.126: bytes=32 time=10ms TTL=126

Ping statistics for 1.1.0.126:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\Users\echowdhury>Group 1

COM3 - PuTTY
R0(config)#
R0(config)#
R0(config)#
R0(config)no access-list 100
R0(config)access-list 100 permit icmp 1.1.0.0 0.0.0.63 1.1.0.128 0.0.0.63
R0(config)access-list 100 deny icmp 1.1.0.64 0.0.0.63 1.1.0.128 0.0.0.127
R0(config)access-list 100 permit ip any any
R0(config)int go/0
R0(config-if)#ip access-group 100 in
R0(config-if)#

```

Fig6: Task3

30. Save this document as word document for your own modifications and save another copy as ".PDF"
31. Submit the PDF file.

Appendix

1. Follow the instructions in the following video to install the Apache server on a PC.

https://www.youtube.com/watch?v=tYPQFztqV4I&ab_channel=DarcyDeClute

2. Task1 Hints:

```
# access-list 101 permit icmp subnet-id wildcard-mask any echo  
# access-list 102 permit icmp any subnet-id wildcard-mask echo-reply  
(interface)# ip access-group 101 in  
(interface)# ip access-group 102 out
```