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.

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

Network Topology

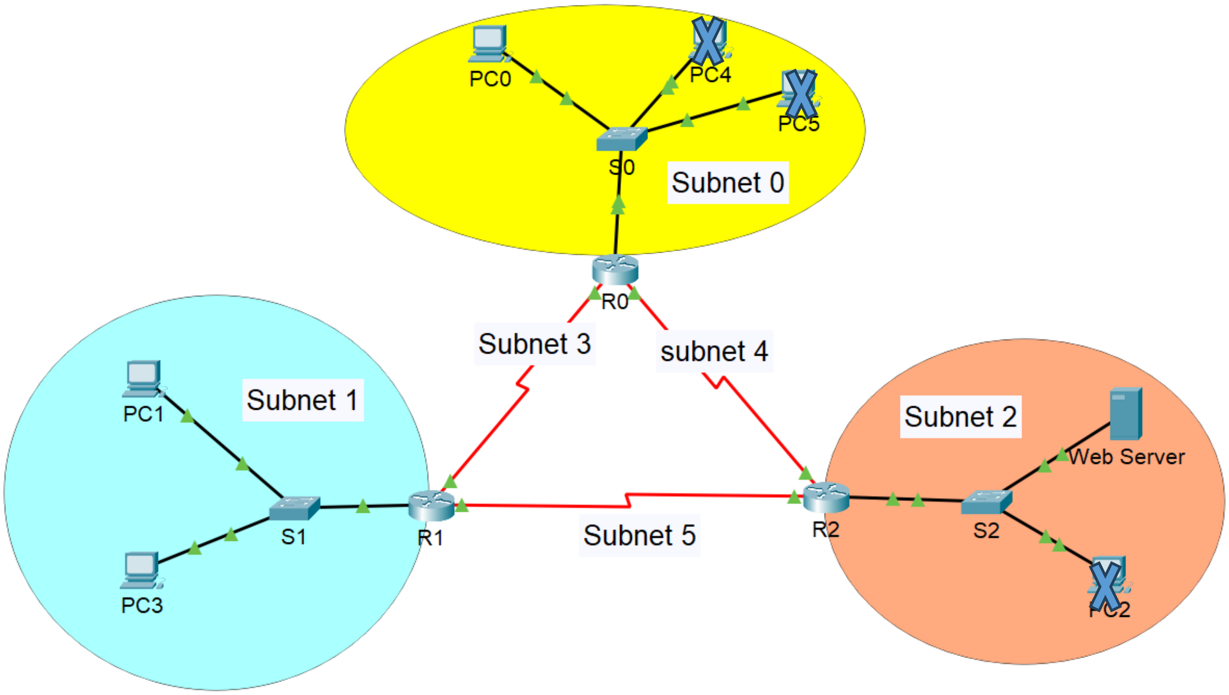


Fig1 Network Topolgy

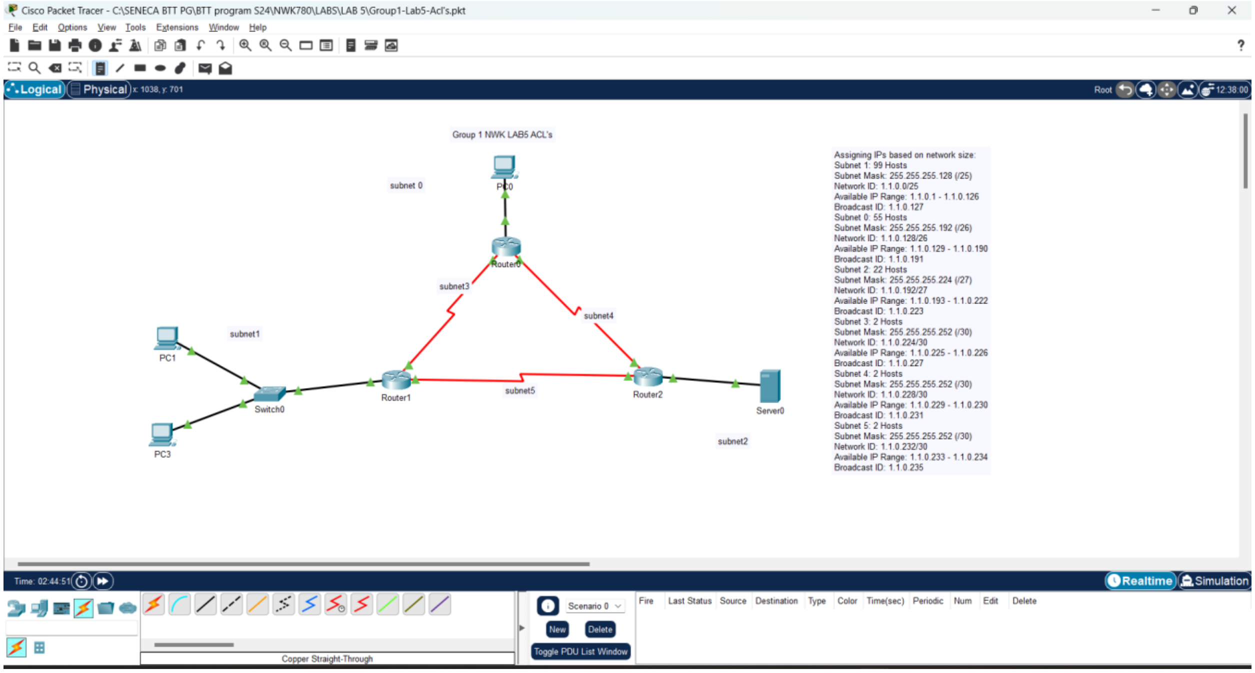
Procedure

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]***

Insert your image here

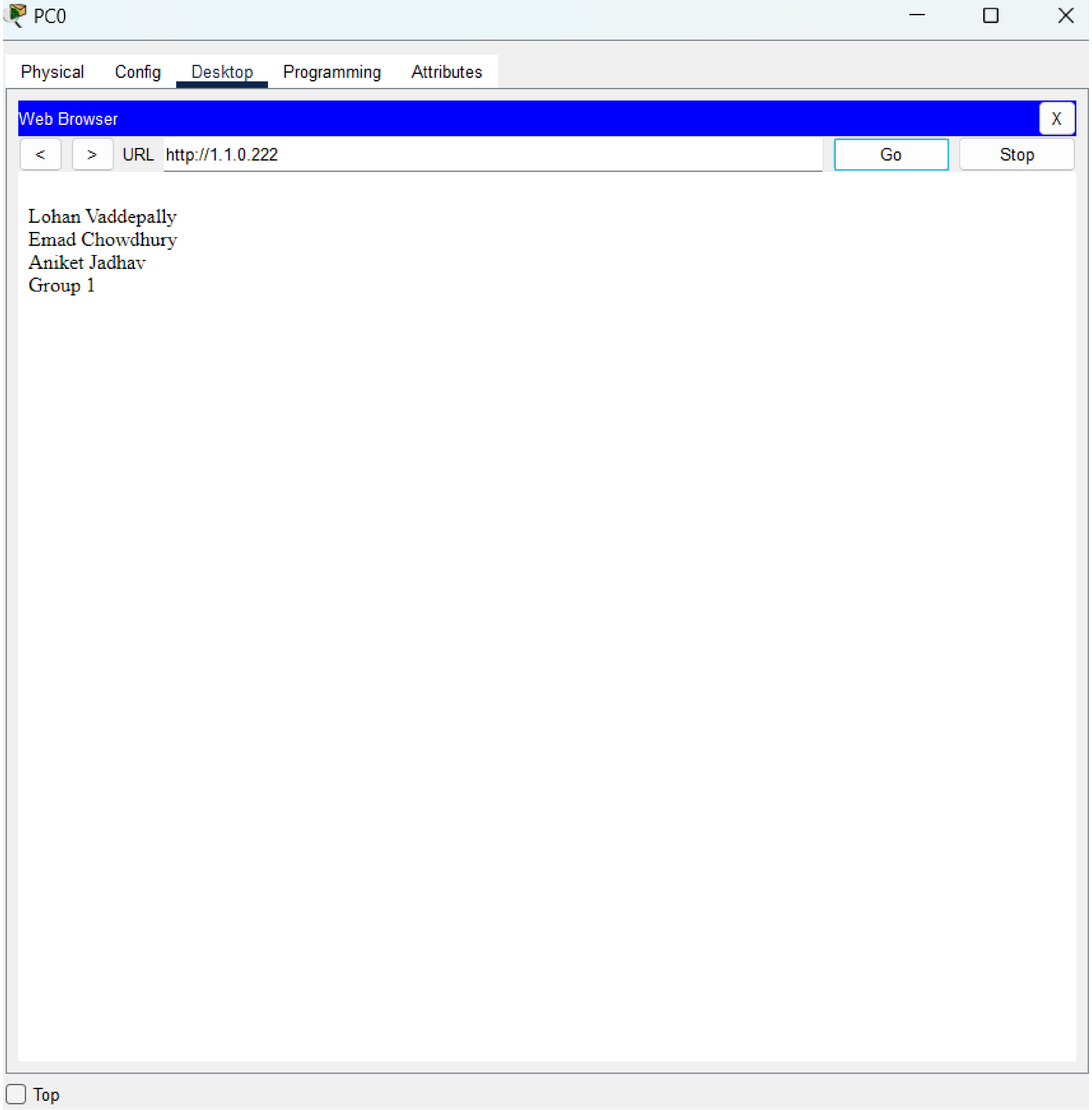


Assigning IPs based on network size:
Subnet 1: 99 Hosts
Subnet Mask: 255.255.255.128 (/25)
Network ID: 1.1.0.0/25
Available IP Range: 1.1.0.1 - 1.1.0.126
Broadcast ID: 1.1.0.127
Subnet 0: 55 Hosts
Subnet Mask: 255.255.255.192 (/26)
Network ID: 1.1.0.128/26
Available IP Range: 1.1.0.129 - 1.1.0.190
Broadcast ID: 1.1.0.191
Subnet 2: 22 Hosts
Subnet Mask: 255.255.255.224 (/27)
Network ID: 1.1.0.192/27
Available IP Range: 1.1.0.193 - 1.1.0.222
Broadcast ID: 1.1.0.223
Subnet 3: 2 Hosts
Subnet Mask: 255.255.255.252 (/30)
Network ID: 1.1.0.224/30
Available IP Range: 1.1.0.225 - 1.1.0.226
Broadcast ID: 1.1.0.227
Subnet 4: 2 Hosts
Subnet Mask: 255.255.255.252 (/30)
Network ID: 1.1.0.228/30
Available IP Range: 1.1.0.229 - 1.1.0.230
Broadcast ID: 1.1.0.231
Subnet 5: 2 Hosts
Subnet Mask: 255.255.255.252 (/30)
Network ID: 1.1.0.232/30
Available IP Range: 1.1.0.233 - 1.1.0.234
Broadcast ID: 1.1.0.235

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 Apachi 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]***

Insert your image here



URL http://1.1.0.222

Lohan Vaddepally
Emad Chowdhury
Aniket Jadhav
Group 1

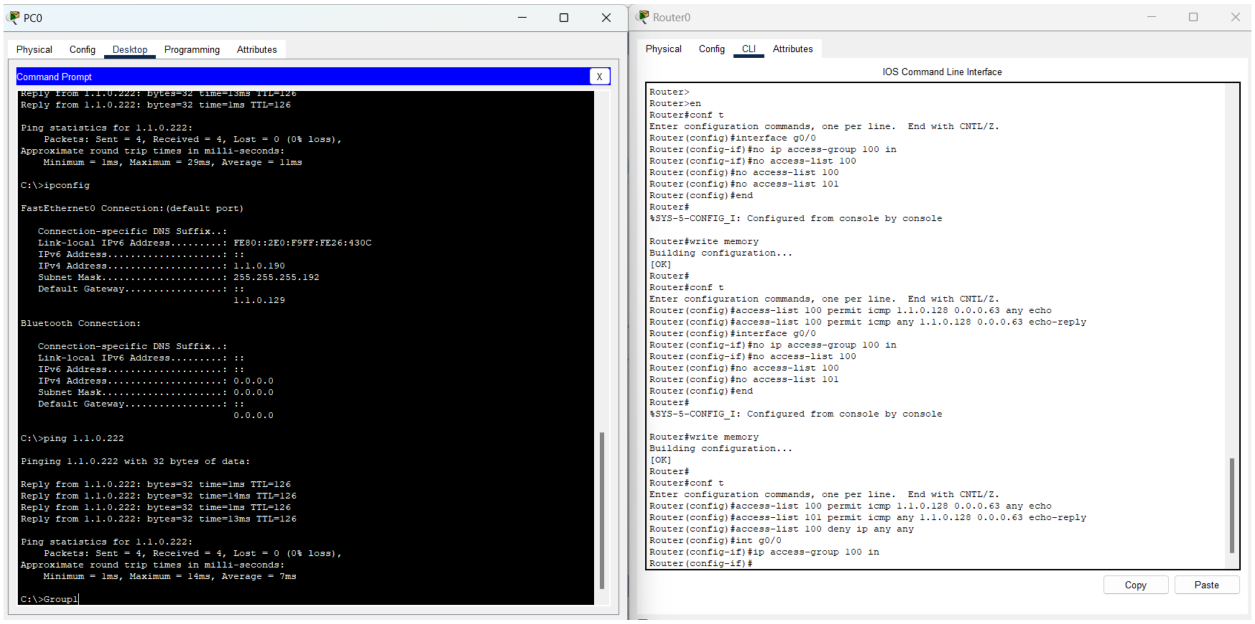
Fig3: Web Browser

Task1

16. ***Allow only*** PINGs from Subnet 0 to any other network. All other traffic must be blocked.

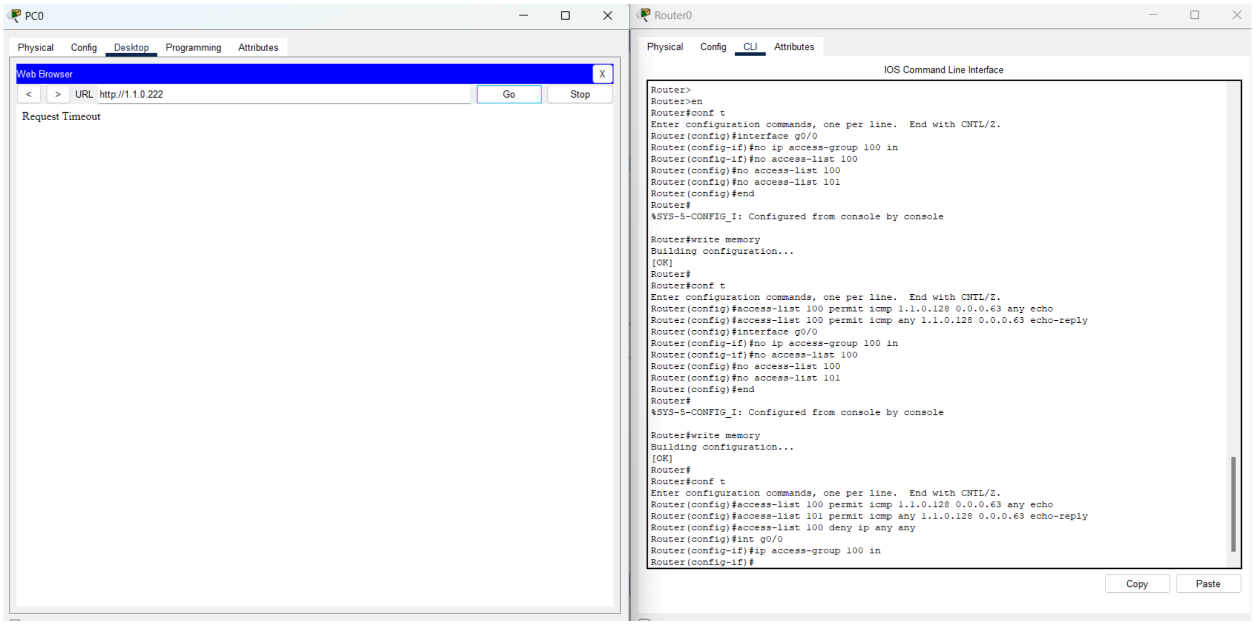
17. Insert the necessary ACL statements as a note on your diagram. You can copy/paste the relevant statements from the running configuration (not all of the running configuration). Where is the best place to deploy your ACL(s)?
18. Check your work:
    a. Ping the web server in Subnet 2 from subnet 0. 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]***

Insert your images here



```
Reply from 1.1.0.222: bytes=32 time=13ms TTL=126
Reply from 1.1.0.222: bytes=32 time=1ms 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 = 1ms, Maximum = 29ms, Average = 11ms

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2E0:F9FF:FE26:430C
   IPv6 Address....................: ::
   IPv4 Address....................: 1.1.0.190
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: ::
                                     1.1.0.129

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 1.1.0.222

Pinging 1.1.0.222 with 32 bytes of data:

Reply from 1.1.0.222: bytes=32 time=1ms TTL=126
Reply from 1.1.0.222: bytes=32 time=14ms TTL=126
Reply from 1.1.0.222: bytes=32 time=1ms TTL=126
Reply from 1.1.0.222: bytes=32 time=13ms 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 = 1ms, Maximum = 14ms, Average = 7ms

C:\>Group1
```

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/0
Router(config-if)#no ip access-group 100 in
Router(config-if)#no access-list 100
Router(config)#no access-list 100
Router(config)#no access-list 101
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit icmp 1.1.0.128 0.0.0.63 any echo
Router(config)#access-list 100 permit icmp any 1.1.0.128 0.0.0.63 echo-reply
Router(config)#interface g0/0
Router(config-if)#no ip access-group 100 in
Router(config-if)#no access-list 100
Router(config)#no access-list 100
Router(config)#no access-list 101
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit icmp 1.1.0.128 0.0.0.63 any echo
Router(config)#access-list 101 permit icmp any 1.1.0.128 0.0.0.63 echo-reply
Router(config)#access-list 100 deny ip any any
Router(config)#int g0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
```



Request Timeout

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/0
Router(config-if)#no ip access-group 100 in
Router(config-if)#no access-list 100
Router(config)#no access-list 100
Router(config)#no access-list 101
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit icmp 1.1.0.128 0.0.0.63 any echo
Router(config)#access-list 100 permit icmp any 1.1.0.128 0.0.0.63 echo-reply
Router(config)#interface g0/0
Router(config-if)#no ip access-group 100 in
Router(config-if)#no access-list 100
Router(config)#no access-list 100
Router(config)#no access-list 101
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit icmp 1.1.0.128 0.0.0.63 any echo
Router(config)#access-list 101 permit icmp any 1.1.0.128 0.0.0.63 echo-reply
Router(config)#access-list 100 deny ip any any
Router(config)#int g0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

Fig4: Task1

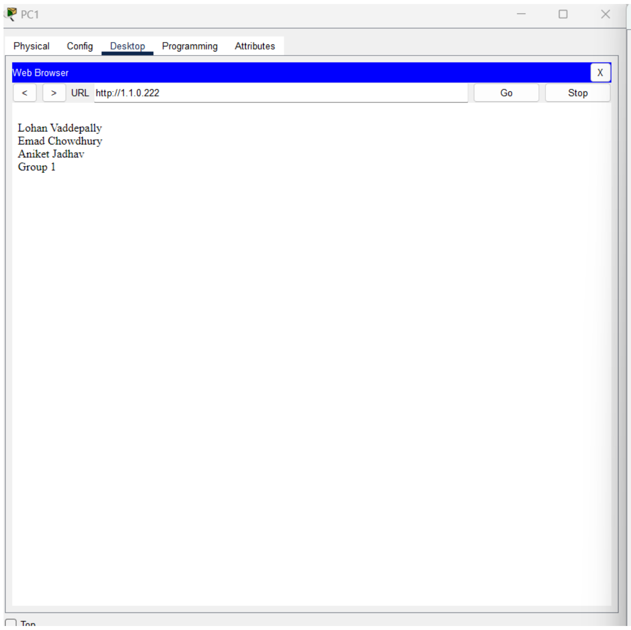
Task2

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.

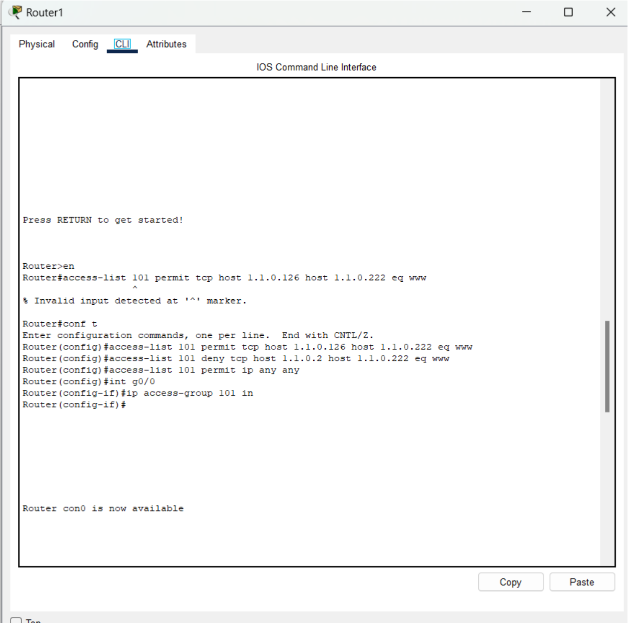
24. Take screen capture(s) of these outputs and insert them below as well as the diagram showing the ACL statements.*[1 mark]*

Insert your images here

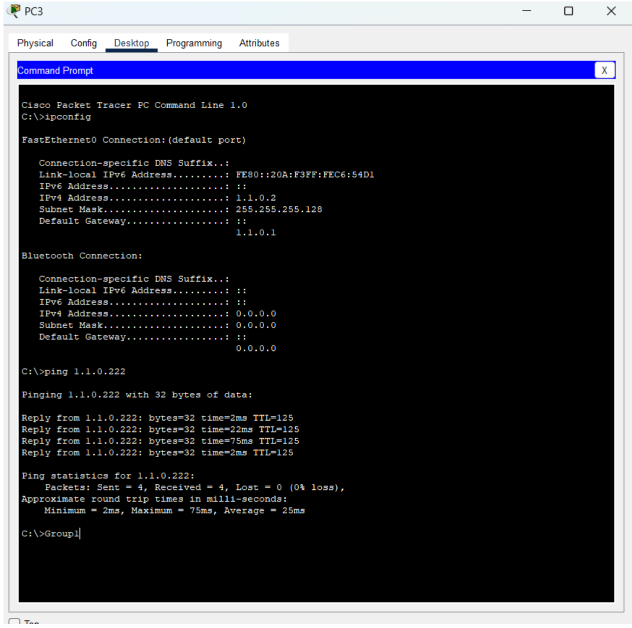


http://1.1.0.222

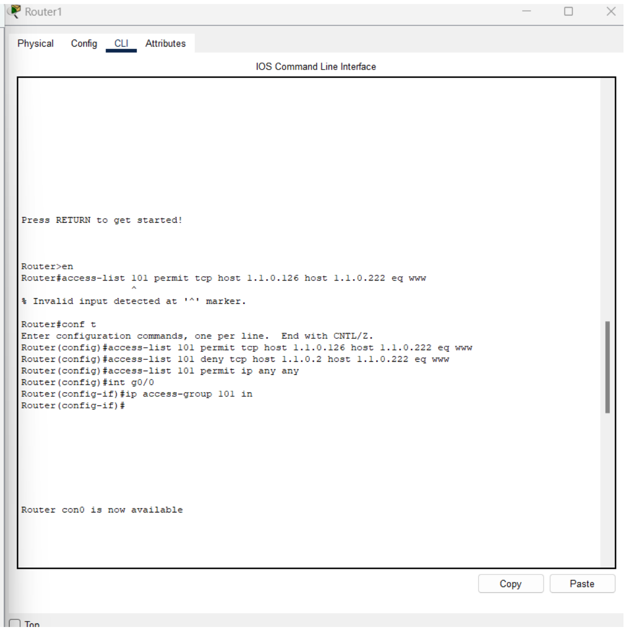
Lohan Vaddepally
Emad Chowdhury
Aniket Jadhav
Group 1



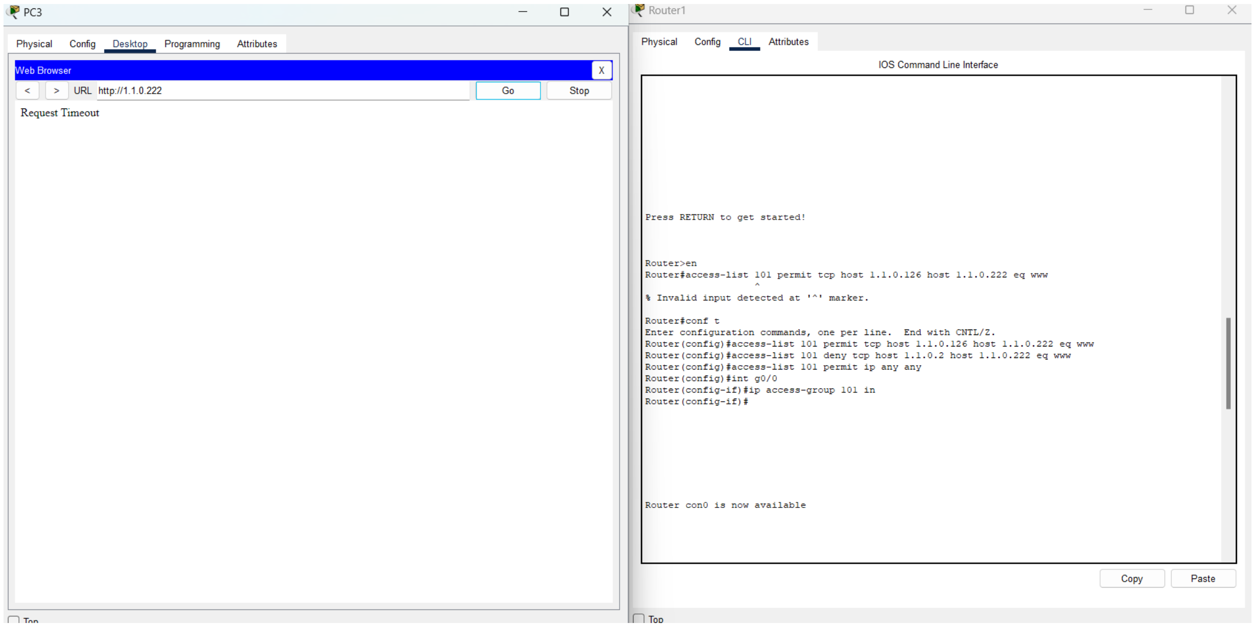
```
Press RETURN to get started!


Router>en
Router#access-list 101 permit tcp host 1.1.0.126 host 1.1.0.222 eq www
                   ^
% Invalid input detected at '^' marker.

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit tcp host 1.1.0.126 host 1.1.0.222 eq www
Router(config)#access-list 101 deny tcp host 1.1.0.2 host 1.1.0.222 eq www
Router(config)#access-list 101 permit ip any any
Router(config)#int g0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#



Router con0 is now available
```



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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEC6:54D1
   IPv6 Address....................: ::
   IPv4 Address....................: 1.1.0.2
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     1.1.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 1.1.0.222

Pinging 1.1.0.222 with 32 bytes of data:

Reply from 1.1.0.222: bytes=32 time=2ms TTL=125
Reply from 1.1.0.222: bytes=32 time=22ms TTL=125
Reply from 1.1.0.222: bytes=32 time=75ms TTL=125
Reply from 1.1.0.222: bytes=32 time=2ms TTL=125

Ping statistics for 1.1.0.222:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 75ms, Average = 25ms

C:\>Group1
```



```
Press RETURN to get started!


Router>en
Router#access-list 101 permit tcp host 1.1.0.126 host 1.1.0.222 eq www
                   ^
% Invalid input detected at '^' marker.

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit tcp host 1.1.0.126 host 1.1.0.222 eq www
Router(config)#access-list 101 deny tcp host 1.1.0.2 host 1.1.0.222 eq www
Router(config)#access-list 101 permit ip any any
Router(config)#int g0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#



Router con0 is now available
```



URL http://1.1.0.222

Request Timeout

```
Press RETURN to get started!


Router>en
Router#access-list 101 permit tcp host 1.1.0.126 host 1.1.0.222 eq www
                   ^
% Invalid input detected at '^' marker.

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 permit tcp host 1.1.0.126 host 1.1.0.222 eq www
Router(config)#access-list 101 deny tcp host 1.1.0.2 host 1.1.0.222 eq www
Router(config)#access-list 101 permit ip any any
Router(config)#int g0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#


Router con0 is now available
```

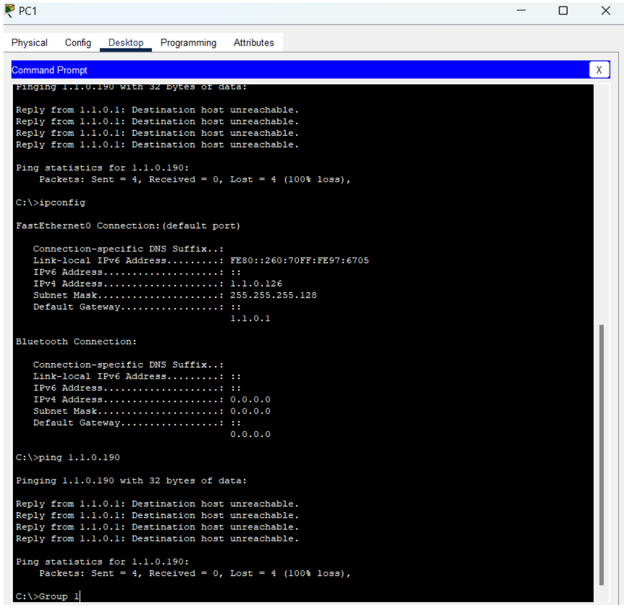
Fig5: Task2

Task3

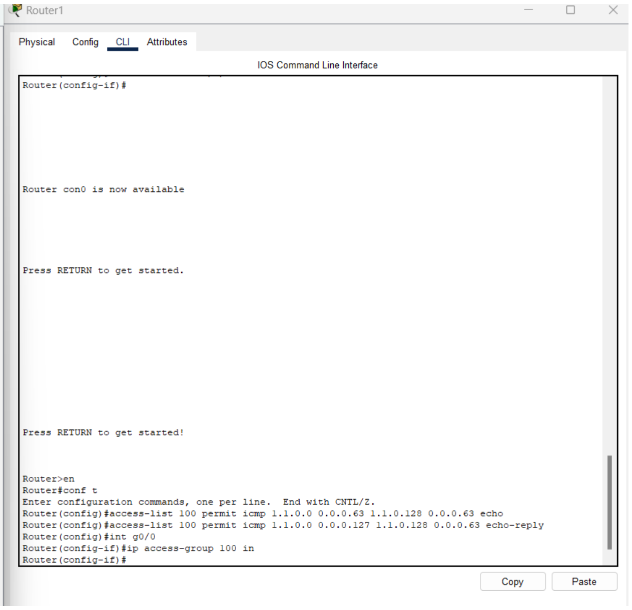
25. ***Allow*** only the ***first half*** of Subnet 1 to PING Subnet 0. All the PCs of Subnet 0 should be able to PING all PCs of Subnet 1.
26. Insert the necessary ACL statements as a note on your diagram.
27. Remove the previous ACL(s) from R2.
28. Check your work:
    a. Ping from PC1 to PC0 must 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]*

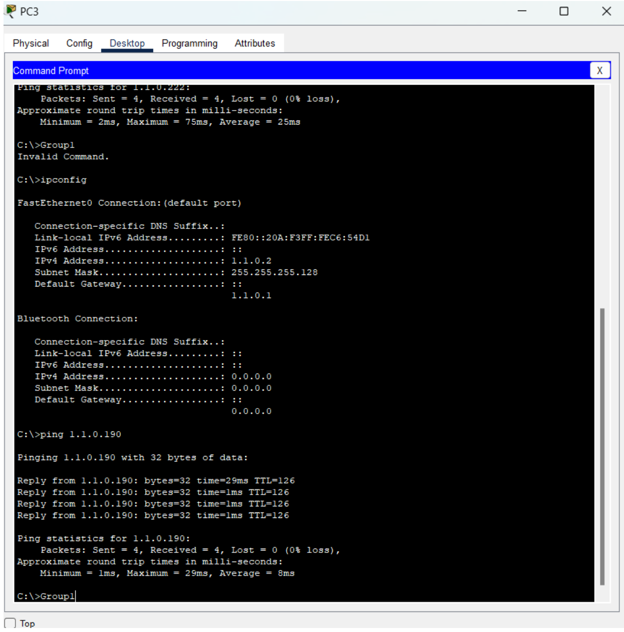
Insert your image here



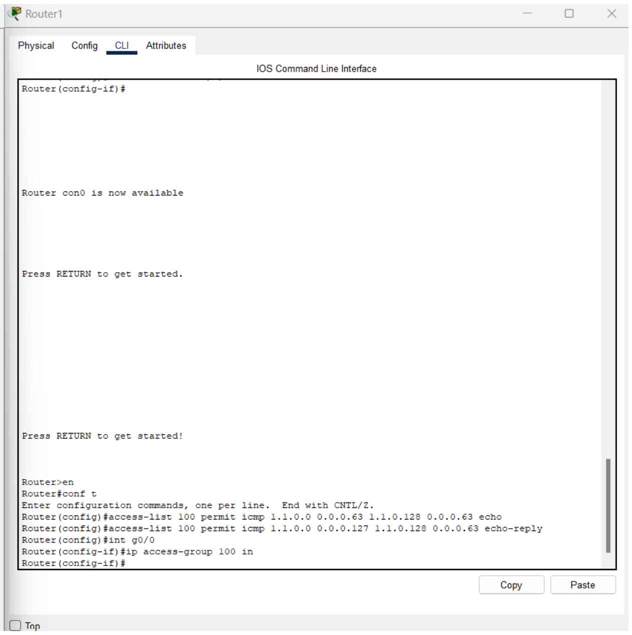
```
Pinging 1.1.0.190 with 32 bytes of data:

Reply from 1.1.0.1: Destination host unreachable.
Reply from 1.1.0.1: Destination host unreachable.
Reply from 1.1.0.1: Destination host unreachable.
Reply from 1.1.0.1: Destination host unreachable.

Ping statistics for 1.1.0.190:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:70FF:FE97:6705
   IPv6 Address....................: ::
   IPv4 Address....................: 1.1.0.126
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     1.1.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 1.1.0.190

Pinging 1.1.0.190 with 32 bytes of data:

Reply from 1.1.0.1: Destination host unreachable.
Reply from 1.1.0.1: Destination host unreachable.
Reply from 1.1.0.1: Destination host unreachable.
Reply from 1.1.0.1: Destination host unreachable.

Ping statistics for 1.1.0.190:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>Group 1
```



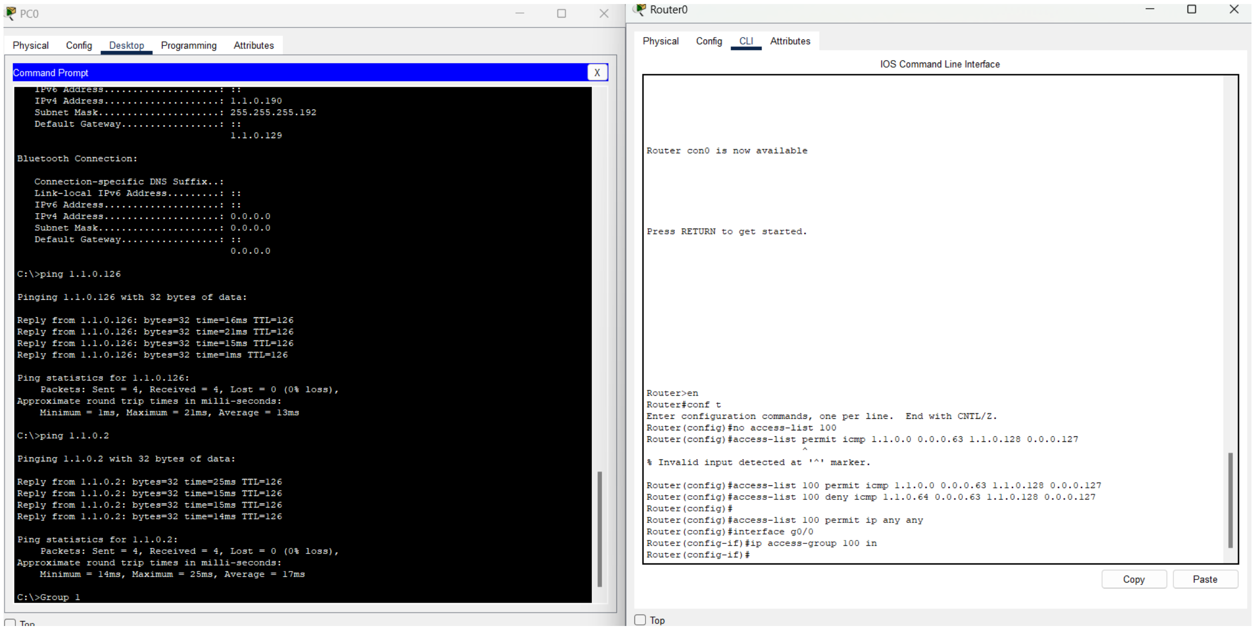
```
Router(config-if)#



Router con0 is now available



Press RETURN to get started.




Press RETURN to get started!


Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit icmp 1.1.0.0 0.0.0.63 1.1.0.128 0.0.0.63 echo
Router(config)#access-list 100 permit icmp 1.1.0.0 0.0.0.127 1.1.0.128 0.0.0.63 echo-reply
Router(config)#int g0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
```



```
Ping statistics for 1.1.0.222:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 75ms, Average = 25ms

C:\>Group1
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEC6:54D1
   IPv6 Address....................: ::
   IPv4 Address....................: 1.1.0.2
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     1.1.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 1.1.0.190

Pinging 1.1.0.190 with 32 bytes of data:

Reply from 1.1.0.190: bytes=32 time=29ms TTL=126
Reply from 1.1.0.190: bytes=32 time=1ms TTL=126
Reply from 1.1.0.190: bytes=32 time=1ms TTL=126
Reply from 1.1.0.190: bytes=32 time=1ms 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 = 1ms, Maximum = 29ms, Average = 8ms

C:\>Group1
```



```
Router(config-if)#



Router con0 is now available



Press RETURN to get started.




Press RETURN to get started!


Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit icmp 1.1.0.0 0.0.0.63 1.1.0.128 0.0.0.63 echo
Router(config)#access-list 100 permit icmp 1.1.0.0 0.0.0.127 1.1.0.128 0.0.0.63 echo-reply
Router(config)#int g0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
```



```
   IPv6 Address....................: ::
   IPv4 Address....................: 1.1.0.190
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: ::
                                     1.1.0.129

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 1.1.0.126

Pinging 1.1.0.126 with 32 bytes of data:

Reply from 1.1.0.126: bytes=32 time=16ms TTL=126
Reply from 1.1.0.126: bytes=32 time=21ms TTL=126
Reply from 1.1.0.126: bytes=32 time=15ms TTL=126
Reply from 1.1.0.126: bytes=32 time=1ms 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 = 1ms, Maximum = 21ms, Average = 13ms

C:\>ping 1.1.0.2

Pinging 1.1.0.2 with 32 bytes of data:

Reply from 1.1.0.2: bytes=32 time=25ms TTL=126
Reply from 1.1.0.2: bytes=32 time=15ms TTL=126
Reply from 1.1.0.2: bytes=32 time=15ms TTL=126
Reply from 1.1.0.2: bytes=32 time=14ms 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 = 14ms, Maximum = 25ms, Average = 17ms

C:\>Group 1
```

```
Router con0 is now available



Press RETURN to get started.



Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no access-list 100
Router(config)#access-list permit icmp 1.1.0.0 0.0.0.63 1.1.0.128 0.0.0.127
                           ^
% Invalid input detected at '^' marker.

Router(config)#access-list 100 permit icmp 1.1.0.0 0.0.0.63 1.1.0.128 0.0.0.127
Router(config)#access-list 100 deny icmp 1.1.0.64 0.0.0.63 1.1.0.128 0.0.0.127
Router(config)#
Router(config)#access-list 100 permit ip any any
Router(config)#interface g0/0
Router(config-if)#ip access-group 100 in
Router(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