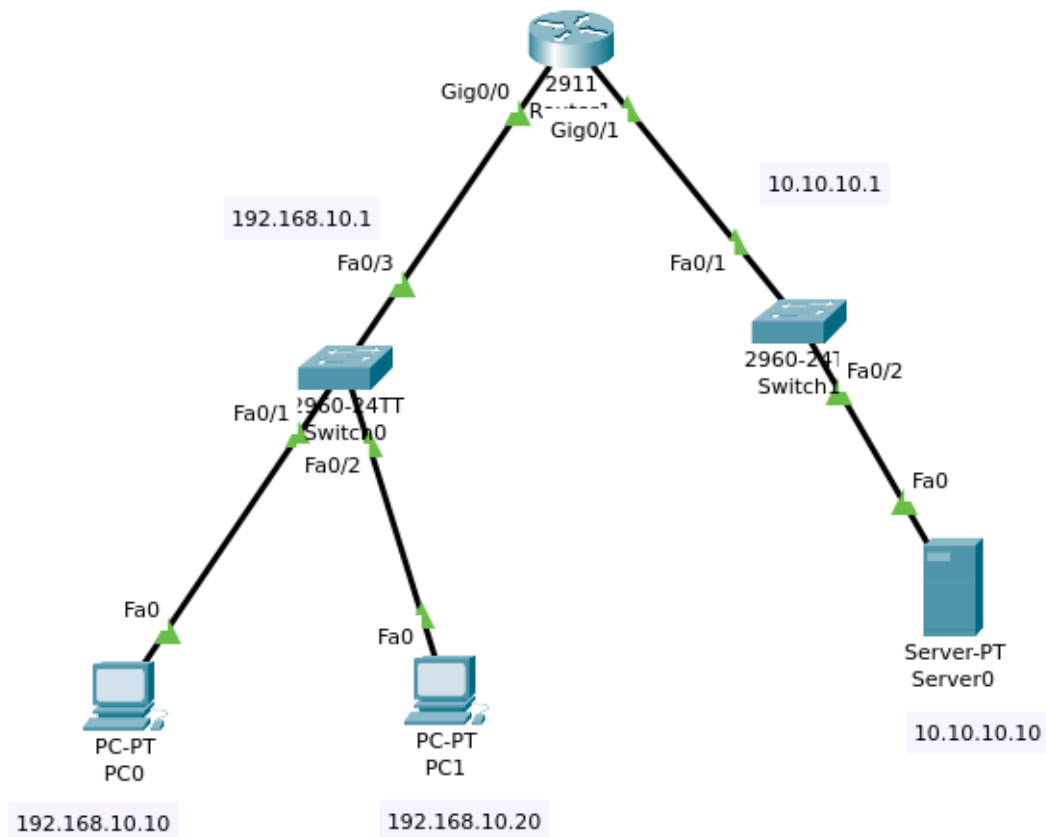


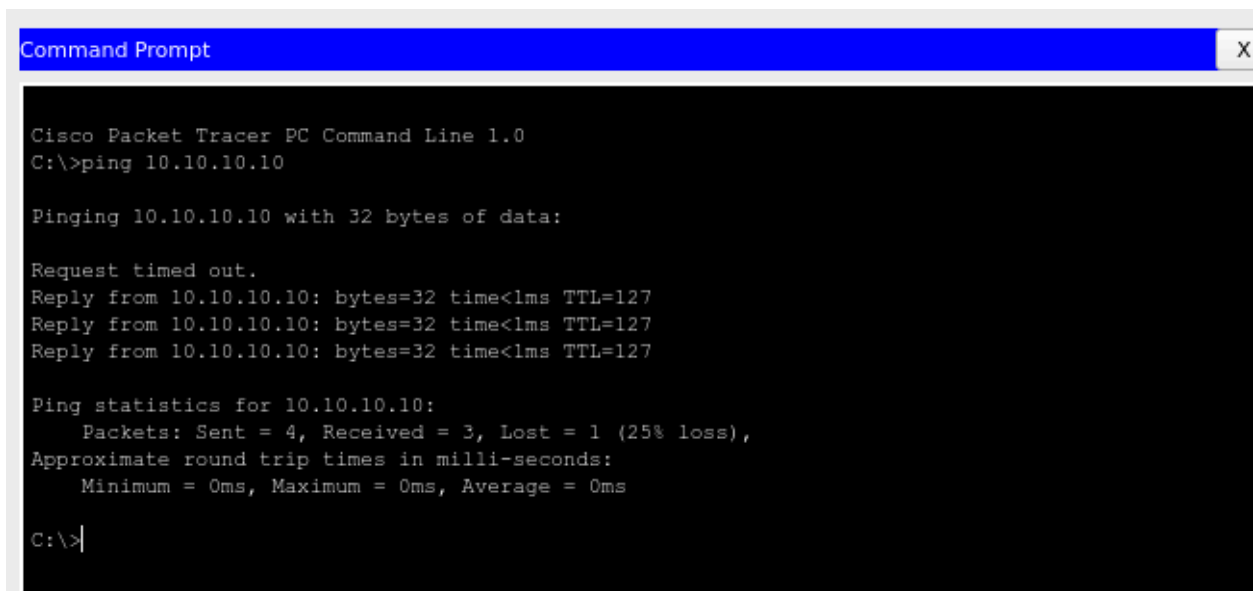
Name: J Kevin Immanuel
College: VIT Chennai



We will be implementing ACL to block 192.168.10.10 from accessing 10.10.10.10

Ping Test Before ACL:

192.168.10.10:



```
Command Prompt X

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

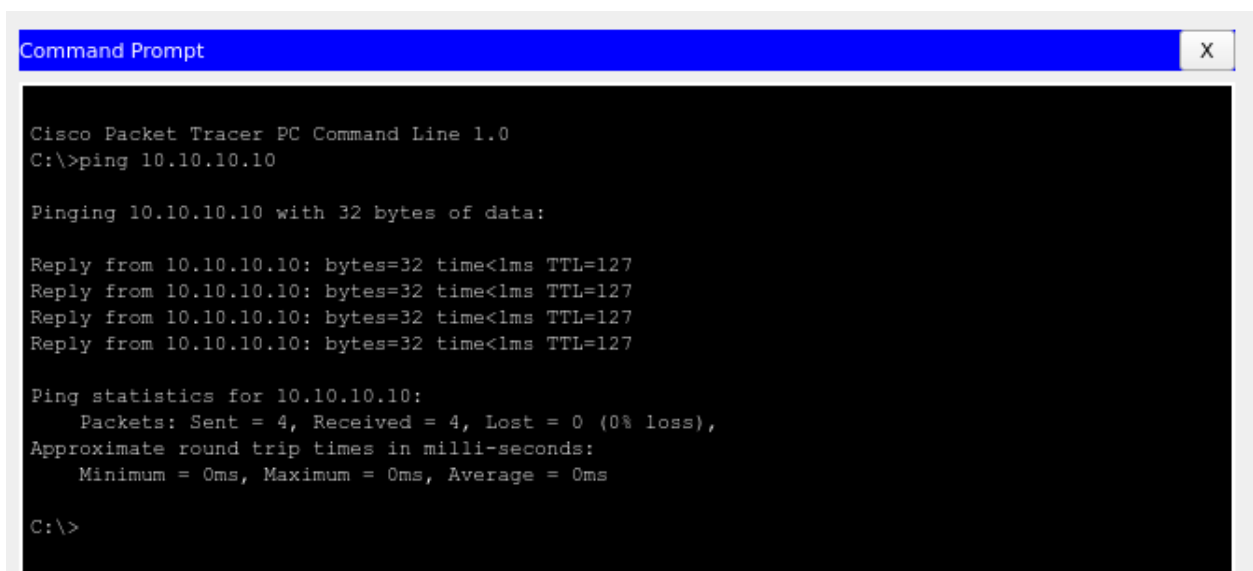
Pinging 10.10.10.10 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

192.168.10.20:



```
Command Prompt X

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

As we can see both pcs can access the server, we will now implement an ACL to block 192.168.10.10

Access List:

We will be creating an access list that allows only 192.168.10.20 and deny anything else. We will then bind the access list to the interface between Router and PC.

```
Router(config)#
Router(config)#access
Router(config)#access-list 10 permit ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
Router(config)#access-list 10 permit host 192.168.10.20 ?
<cr>
Router(config)#access-list 10 permit host 192.168.10.20
Router(config)#access
Router(config)#access-list 10 den
Router(config)#access-list 10 deny ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
Router(config)#access-list 10 deny any
Router(config)#
Router(config)#
Router(config)#int gig
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip acce
Router(config-if)#ip access-group 10 in
Router(config-if)#ex
Router(config)#int gig
Router(config)#do wr
Building configuration...
[OK]
Router(config)#sh acce
Router(config)#do show access-list
Standard IP access list 10
  10 permit host 192.168.10.20
  20 deny any
```

Ping Check:

192.168.10.20:

```
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=13ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>
```

192.168.10.10:

```
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

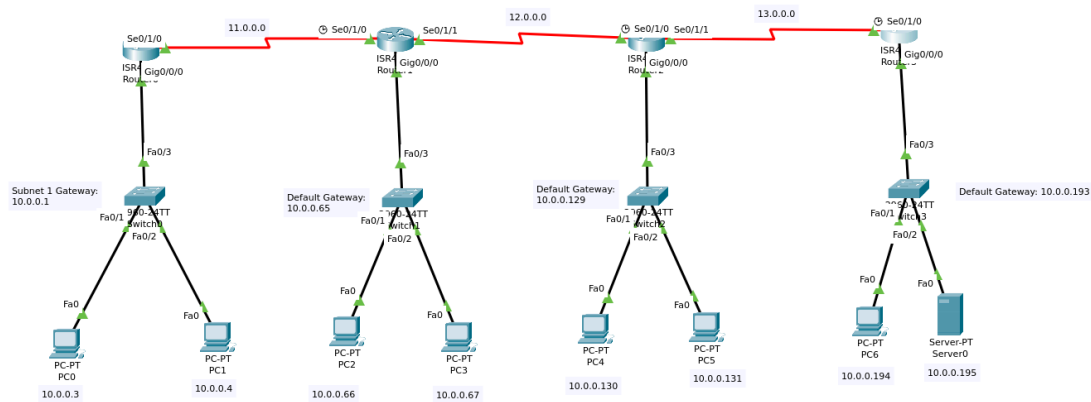
Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

We can see that 192.168.10.10 returns Destination host unreachable when pinging to 10.10.10.10. Thus, we have successfully blocked the IP address.

Q12) Standard ACL to permit a specific range.

We will be using the subnet network used in Module 6 Q3 as an example.



Here, it is decided to permit any incoming traffic from the subnet 10.0.0.0, while denying any others. This access-list will be bound to the interface between router and 10.0.0.192. The subnet mask for this question is 255.255.255.192 and the wildcard mask is 0.0.0.63.

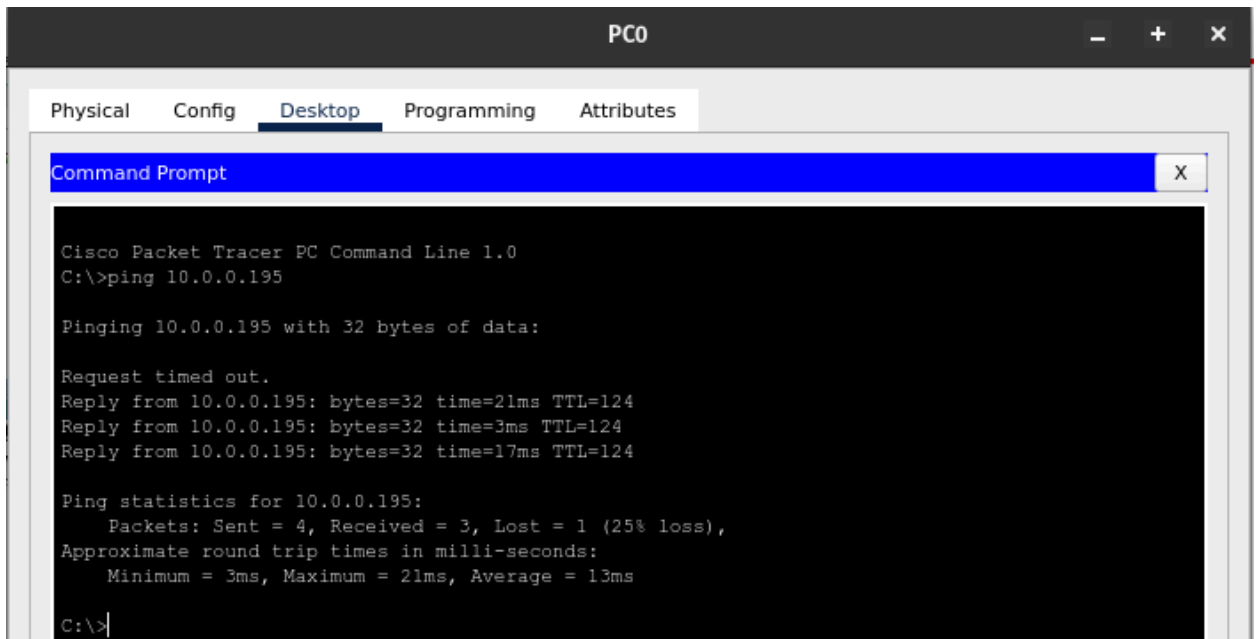
Access list assigning:

```
Router(config)#access
Router(config)#access-list 10 permit 10.0.0.0 0.0.0.63
Router(config)#access-list 10 deny any
Router(config)#do show access
Router(config)#do show access?
LINE
Router(config)#do show access-list
Standard IP access list 10
  10 permit 10.0.0.0 0.0.0.63
  20 deny any

Router(config)#int gig0
Router(config)#int gig
Router(config)#int gigabitEthernet 0/0/0
Router(config-if)#ip acce
Router(config-if)#ip access-group ?
  <1-199> IP access list (standard or extended)
  WORD   Access-list name
Router(config-if)#ip access-group 10 out
Router(config-if)#
```

PING CHECK:

1. Pinging from 10.0.0.2 to 10.0.0.195:



The screenshot shows a Cisco Packet Tracer window for PC0. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 10.0.0.195'. The output indicates that the ping failed with a 25% loss (1 out of 4 packets received). The round trip times for the received packets are 21ms, 3ms, and 17ms, with an average of 13ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.195

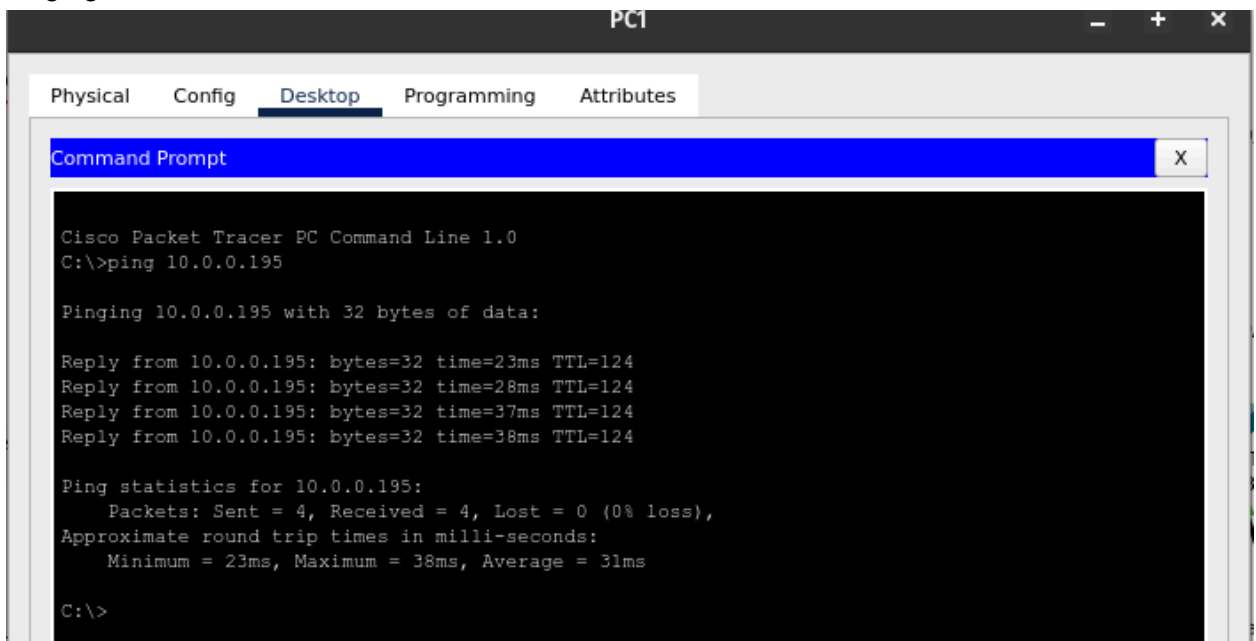
Pinging 10.0.0.195 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.195: bytes=32 time=21ms TTL=124
Reply from 10.0.0.195: bytes=32 time=3ms TTL=124
Reply from 10.0.0.195: bytes=32 time=17ms TTL=124

Ping statistics for 10.0.0.195:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 21ms, Average = 13ms

C:\>
```

2. Pinging from 10.0.0.3 to 10.0.0.195:



The screenshot shows a Cisco Packet Tracer window for PC1. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 10.0.0.195'. The output indicates that the ping was successful with 0% loss (4 out of 4 packets received). The round trip times for the received packets are 23ms, 28ms, 37ms, and 38ms, with an average of 31ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.195

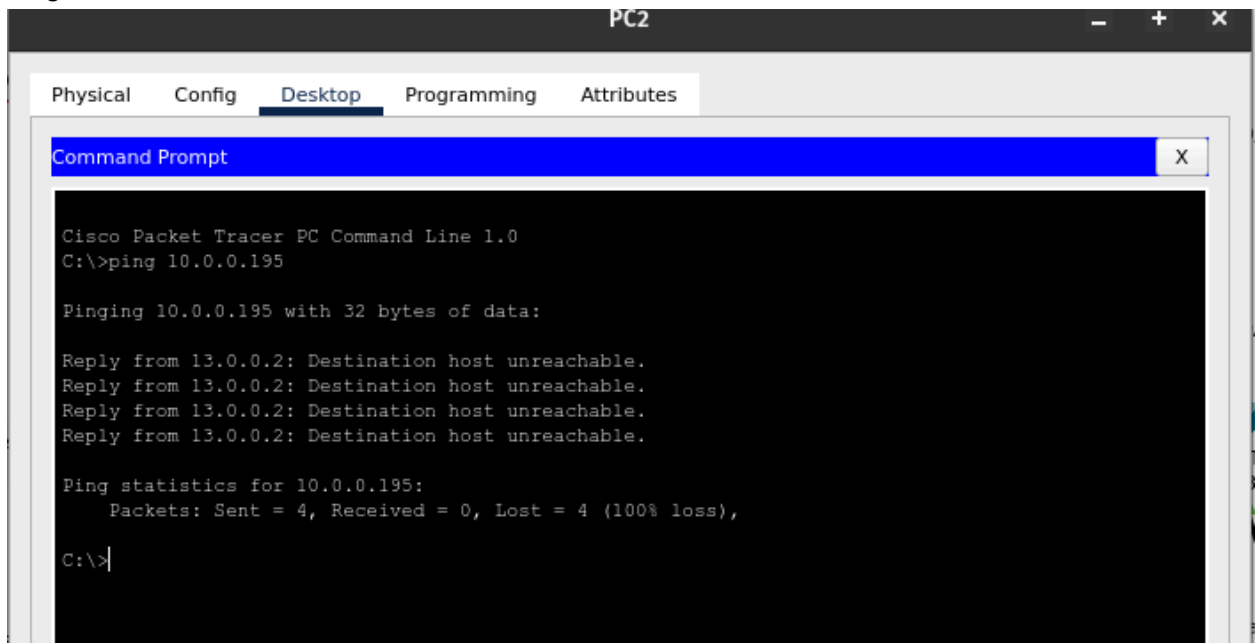
Pinging 10.0.0.195 with 32 bytes of data:

Reply from 10.0.0.195: bytes=32 time=23ms TTL=124
Reply from 10.0.0.195: bytes=32 time=28ms TTL=124
Reply from 10.0.0.195: bytes=32 time=37ms TTL=124
Reply from 10.0.0.195: bytes=32 time=38ms TTL=124

Ping statistics for 10.0.0.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 38ms, Average = 31ms

C:\>
```

3. Ping from 10.0.0.66 to 10.0.0.195:



The screenshot shows a Cisco Packet Tracer PC window for PC2. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 10.0.0.195'. The output indicates that the destination host is unreachable for all four attempts, resulting in a 100% loss of packets.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.195

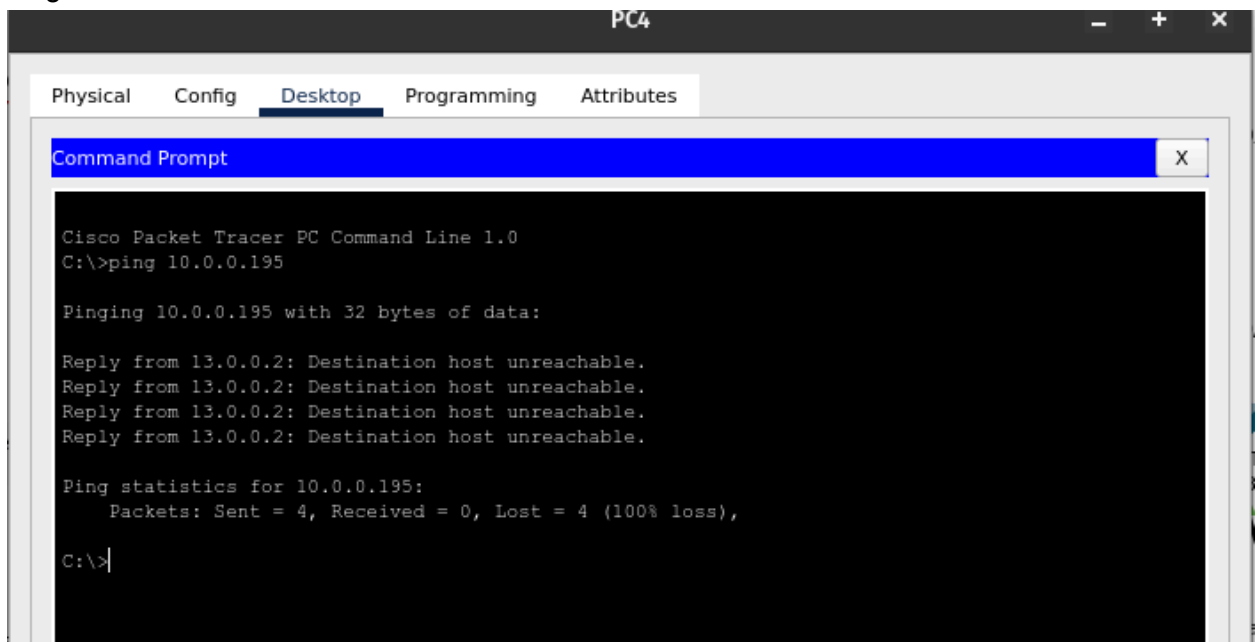
Pinging 10.0.0.195 with 32 bytes of data:

Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.

Ping statistics for 10.0.0.195:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

4. Ping from 10.0.0.130 to 10.0.0.195:



The screenshot shows a Cisco Packet Tracer PC window for PC4. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 10.0.0.195'. The output indicates that the destination host is unreachable for all four attempts, resulting in a 100% loss of packets.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.195

Pinging 10.0.0.195 with 32 bytes of data:

Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.

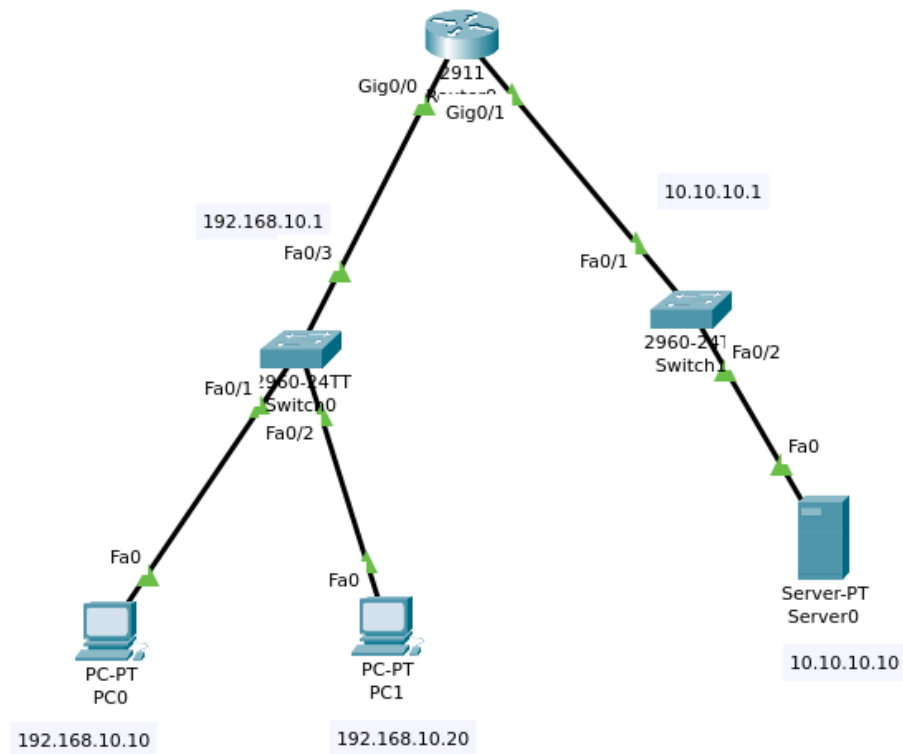
Ping statistics for 10.0.0.195:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

As we can see, any network other than 10.0.0.0 cannot reach the server. This ensures that our access list has been successfully implemented.

Q13) Extended ACL to deny HTTP or FTP:

We will be using the same network used in Q11.



We will be denying any TCP packets inbound from 192.168.10.10 to 10.10.10.10, and allowing any other packets.

Same configurations used as q11.

Access list assigning:

```
Router(config)#
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#deny tcp host 192.168.10.10 host 10.10.10.10 ?
    eq          Match only packets on a given port number
    established established
    gt          Match only packets with a greater port number
    lt          Match only packets with a lower port number
    neq         Match only packets not on a given port number
    range       Match only packets in the range of port numbers
    <cr>
Router(config-ext-nacl)#deny tcp host 192.168.10.10 host 10.10.10.10 eq www
Router(config-ext-nacl)#deny tcp host 192.168.10.10. host 10.10.10.10 eq ftp
    ^
% Invalid input detected at '^' marker.

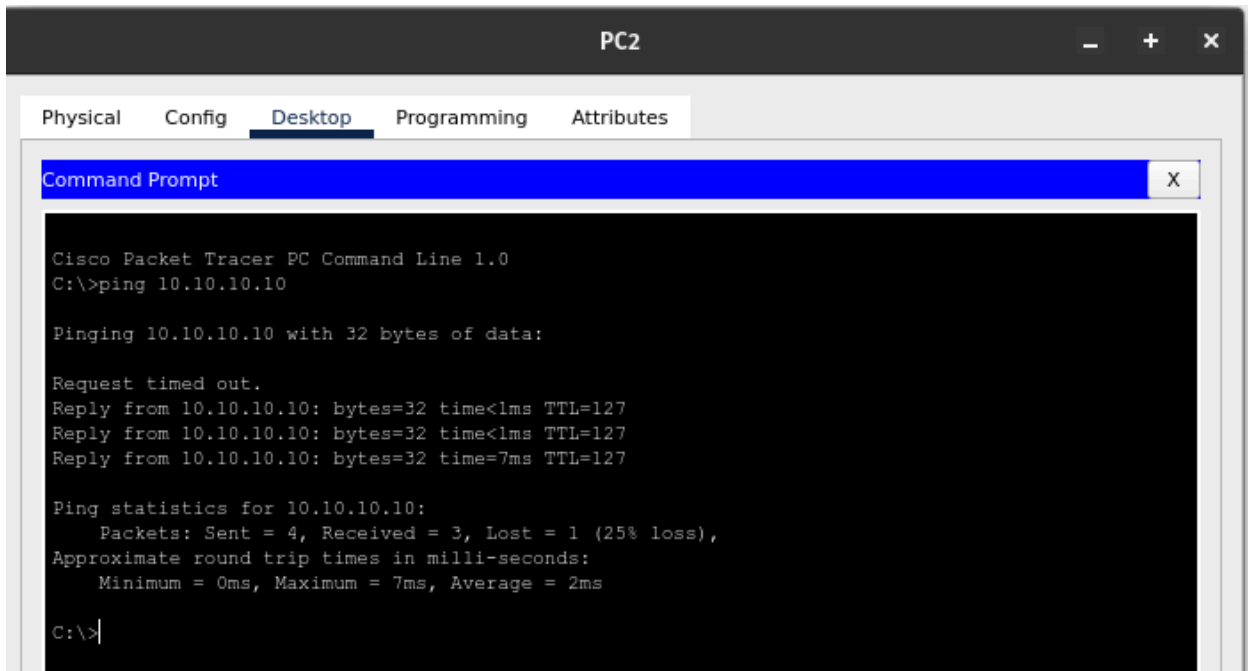
Router(config-ext-nacl)#deny tcp host 192.168.10.10 host 10.10.10.10 eq ftp
Router(config-ext-nacl)#permit icmp any any
Router(config-ext-nacl)#permit tcp any
% Incomplete command.
Router(config-ext-nacl)#permit tcp any any
Router(config-ext-nacl)#ex
Router(config)#
Router(config)#ip access-grou
Router(config)#do show access-list
Extended IP access list 101
    10 deny tcp host 192.168.10.10 host 10.10.10.10 eq www
    20 deny tcp host 192.168.10.10 host 10.10.10.10 eq ftp
    30 permit icmp any any
    40 permit tcp any any

Router(config)#

Router(config)#int gig0/0
Router(config-if)#ip access
Router(config-if)#ip access-group 101
Router(config-if)#ip access-group 101 in
Router(config-if)#ip access-group 101 in
Router(config-if)#ex
Router(config-if)#
```

Testing:

1. Ping from 192.168.10.30 to 10.10.10.10:



The screenshot shows a Cisco Packet Tracer PC window for PC2. The 'Desktop' tab is active, displaying a Command Prompt. The user has entered the command 'ping 10.10.10.10'. The output shows that the first ping request timed out, while the subsequent three replies were successful. The ping statistics indicate a 25% loss (1 out of 4 packets lost).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

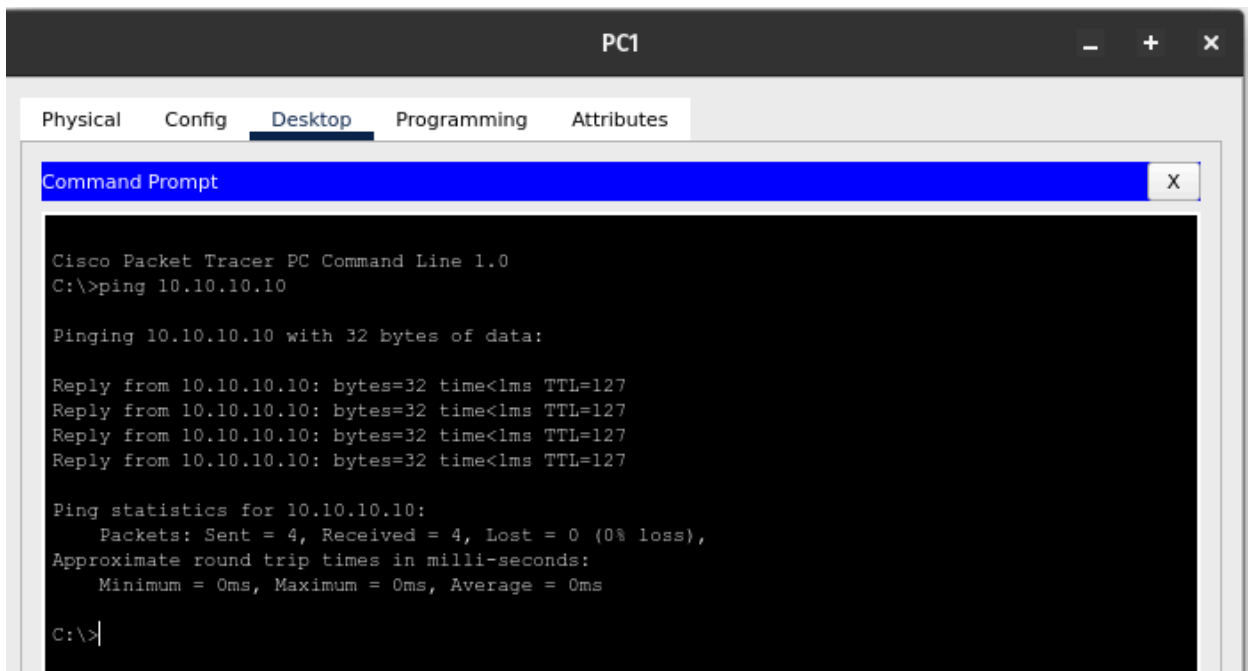
Pinging 10.10.10.10 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time=7ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\>
```

2. Ping from 192.168.10.20 to 10.10.10.10



The screenshot shows a Cisco Packet Tracer PC window for PC1. The 'Desktop' tab is active, displaying a Command Prompt. The user has entered the command 'ping 10.10.10.10'. The output shows four successful replies from 10.10.10.10. The ping statistics indicate 0% loss (0 out of 4 packets lost).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

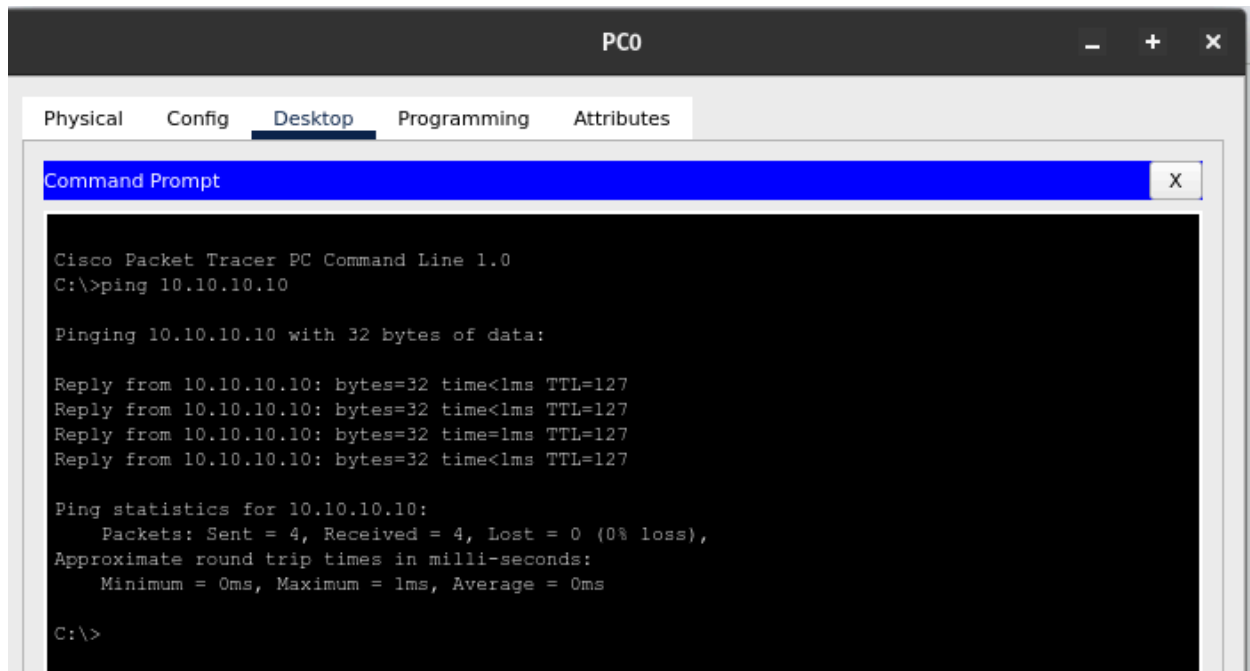
Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127
Reply from 10.10.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

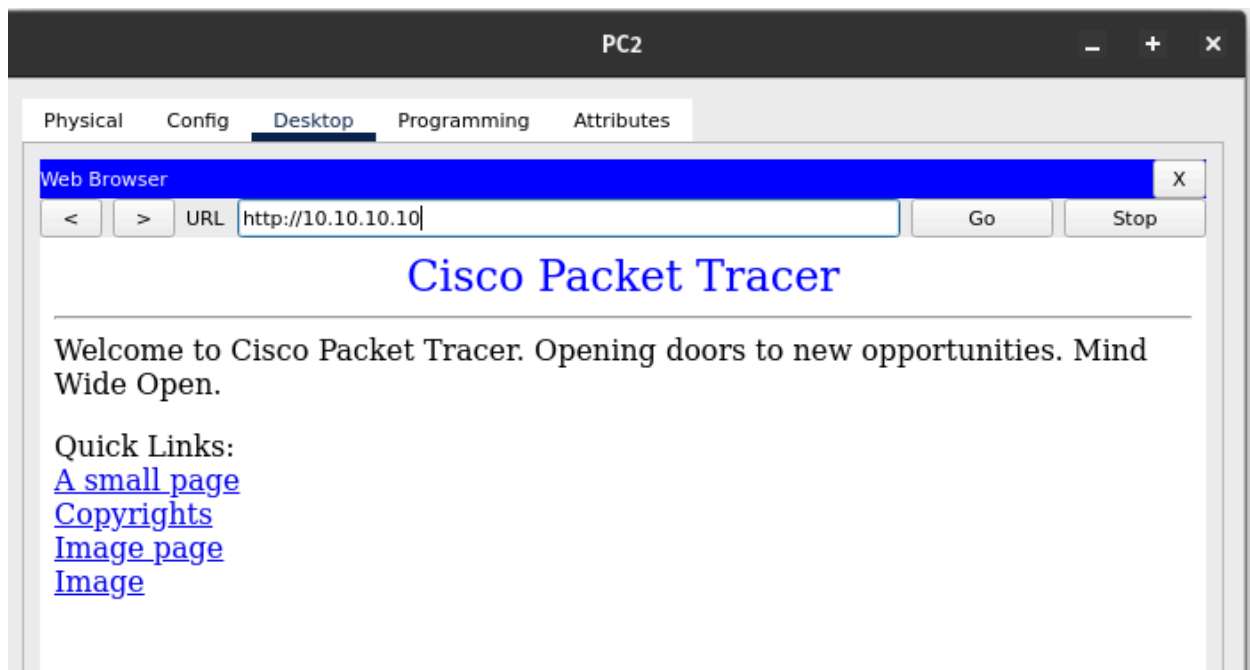
C:\>
```

3. Ping from 192.168.10.10 to 10.10.10.10:

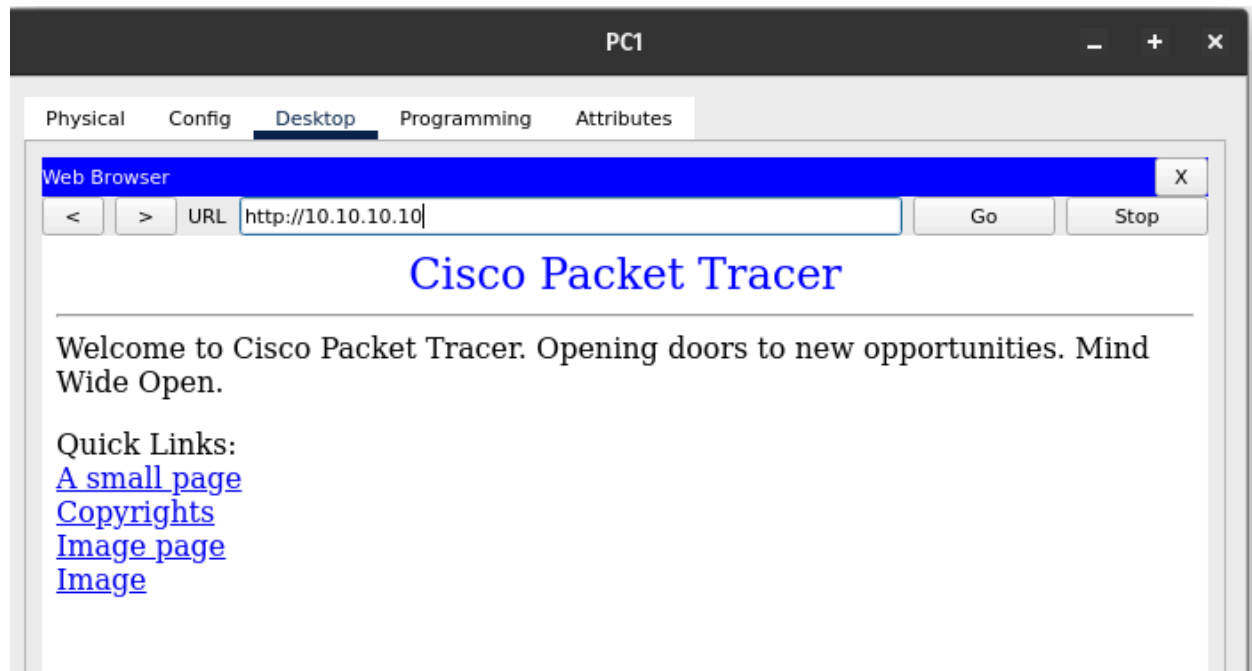


HTTP check:

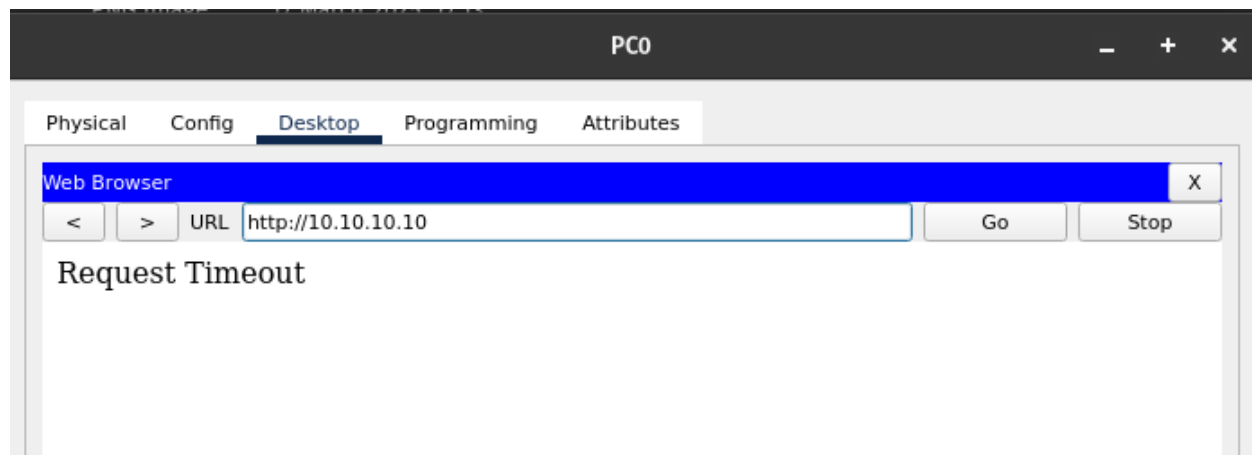
1. From 192.168.10.30 to 10.10.10.10:



2. From 192.168.10.20. to 10.10.10.10:



3. From 192.168.10.10 to 10.10.10.10:



FTP Check:

1. 192.168.10.30 to 10.10.10.10:

```
C:\>ftp 10.10.10.10
Trying to connect...10.10.10.10
Connected to 10.10.10.10
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

2. 192.168.10.10 to 10.10.10.10:

```
C:\>ftp 10.10.10.10
Trying to connect...10.10.10.10

%Error opening ftp://10.10.10.10/ (Timed out)
.

(Disconnecting from ftp server)

|
```

Thus, we have verified that the Extended ACL works.