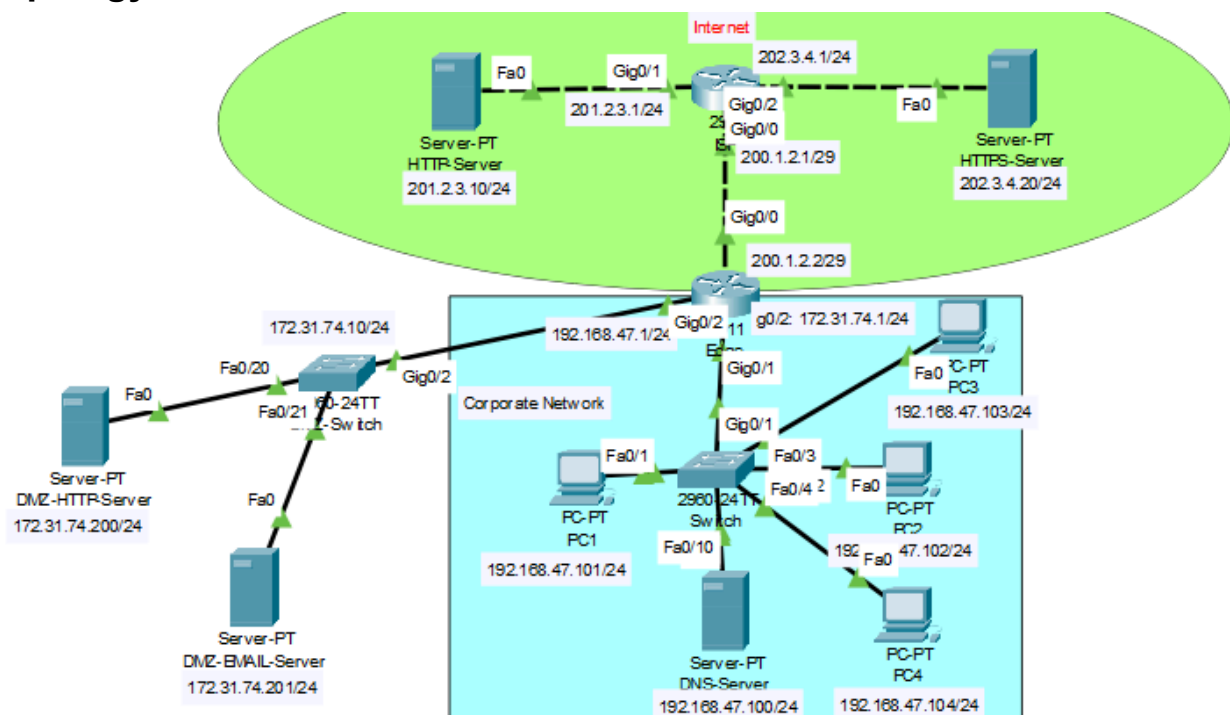


Lab 6

Description: In this lab we configured an access control list for our corporate network.

Topology:



Syntax:

Command	Description	IOS Mode
access-list 123 permit tcp any any eq 25	Permits SMTP traffic	Global Configuration Mode
ip access-group 123 in	Applies the ACL	Interface Configuration Mode
Clear access list counters	Resets all access list hit counter	Privileged Exec Mode

No access-list 123	Removes ACL 123	Global Configuration Mode
access-list 123 deny ip any any	Denies all traffic	Global Configuration Mode

Verification/Test Cases:

A. Initial connectivity -

These screenshots show that PC1 can ping everything in the topology.

```
C:\>ping 172.31.74.200

Pinging 172.31.74.200 with 32 bytes of data:

Reply from 172.31.74.200: bytes=32 time<1ms TTL=127
Reply from 172.31.74.200: bytes=32 time<1ms TTL=127
Reply from 172.31.74.200: bytes=32 time<1ms TTL=127
Reply from 172.31.74.200: bytes=32 time<1ms TTL=127

Ping statistics for 172.31.74.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.31.74.201

Pinging 172.31.74.201 with 32 bytes of data:

Reply from 172.31.74.201: bytes=32 time<1ms TTL=127
Reply from 172.31.74.201: bytes=32 time<1ms TTL=127
Reply from 172.31.74.201: bytes=32 time<1ms TTL=127
Reply from 172.31.74.201: bytes=32 time<1ms TTL=127

Ping statistics for 172.31.74.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 201.2.3.10

Pinging 201.2.3.10 with 32 bytes of data:

Reply from 201.2.3.10: bytes=32 time<1ms TTL=126
Reply from 201.2.3.10: bytes=32 time<1ms TTL=126
Reply from 201.2.3.10: bytes=32 time<1ms TTL=126
Reply from 201.2.3.10: bytes=32 time<1ms TTL=126

Ping statistics for 201.2.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
C:\>ping 202.3.4.20

Pinging 202.3.4.20 with 32 bytes of data:

Reply from 202.3.4.20: bytes=32 time<1ms TTL=126
Reply from 202.3.4.20: bytes=32 time<1ms TTL=126
Reply from 202.3.4.20: bytes=32 time<1ms TTL=126
Reply from 202.3.4.20: bytes=32 time<1ms TTL=126

Ping statistics for 202.3.4.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.47.103

Pinging 192.168.47.103 with 32 bytes of data:

Reply from 192.168.47.103: bytes=32 time<1ms TTL=128
Reply from 192.168.47.103: bytes=32 time<1ms TTL=128
Reply from 192.168.47.103: bytes=32 time=6ms TTL=128
Reply from 192.168.47.103: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.47.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>
```

B. This is a screenshot of the Edge routers IPv4 routing table.

```
Edge#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 200.1.2.1 to network 0.0.0.0

    172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.31.74.0/24 is directly connected, GigabitEthernet0/2
L       172.31.74.1/32 is directly connected, GigabitEthernet0/2
    192.168.47.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.47.0/24 is directly connected, GigabitEthernet0/1
L       192.168.47.1/32 is directly connected, GigabitEthernet0/1
    200.1.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.1.2.0/29 is directly connected, GigabitEthernet0/0
L       200.1.2.2/32 is directly connected, GigabitEthernet0/0
S*    0.0.0.0/0 [1/0] via 200.1.2.1
```

C. This screenshot shows all of the ACLs I made on the Edge router.

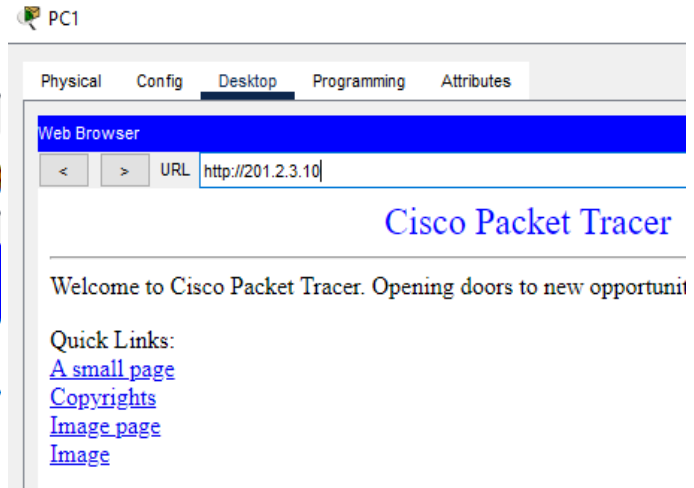
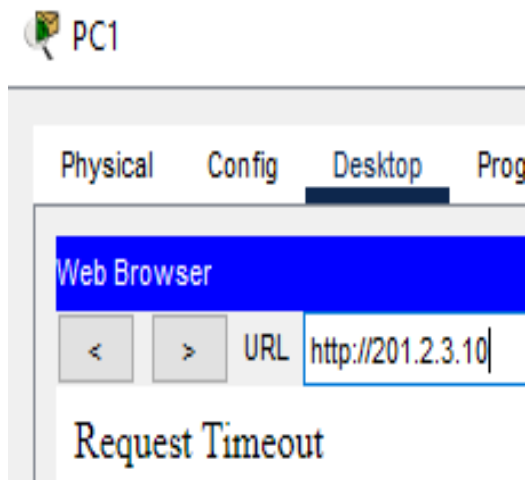
```
Edge#show access-lists
Extended IP access list 123
 10 permit tcp host 192.168.47.101 host 201.2.3.10 eq www
 20 permit tcp host 192.168.47.102 host 201.2.3.10 eq www
 30 permit tcp host 192.168.47.103 host 202.3.4.20 eq 443
 40 permit tcp host 192.168.47.104 host 202.3.4.20 eq 443
 50 permit tcp host 192.168.47.101 host 172.31.74.200 eq 443
 60 permit tcp host 192.168.47.102 host 172.31.74.200 eq 443
 70 permit tcp host 192.168.47.103 host 172.31.74.200 eq 443
 80 permit tcp host 192.168.47.104 host 172.31.74.200 eq 443
 90 permit tcp host 192.168.47.101 host 172.31.74.201 eq smtp
100 permit tcp host 192.168.47.102 host 172.31.74.201 eq smtp
110 permit tcp host 192.168.47.103 host 172.31.74.201 eq smtp
120 permit tcp host 192.168.47.104 host 172.31.74.201 eq smtp
130 permit tcp host 192.168.47.101 host 172.31.74.201 eq pop3
140 permit tcp host 192.168.47.102 host 172.31.74.201 eq pop3
150 permit tcp host 192.168.47.103 host 172.31.74.201 eq pop3
160 permit tcp host 192.168.47.104 host 172.31.74.201 eq pop3
170 permit icmp host 192.168.47.101 host 200.1.2.1
180 permit icmp host 192.168.47.102 host 200.1.2.1
190 permit icmp host 192.168.47.103 host 200.1.2.1
200 permit icmp host 192.168.47.104 host 200.1.2.1
210 deny ip any any
```

D. Test Cases -

- I used the commands “access-list 123 permit tcp 192.168.47.101 0.0.0.0 201.2.3.10 0.0.0.0 eq 80” to allow PC1 and 2 to access the Internet HTTP-Server via HTTP.

Before:

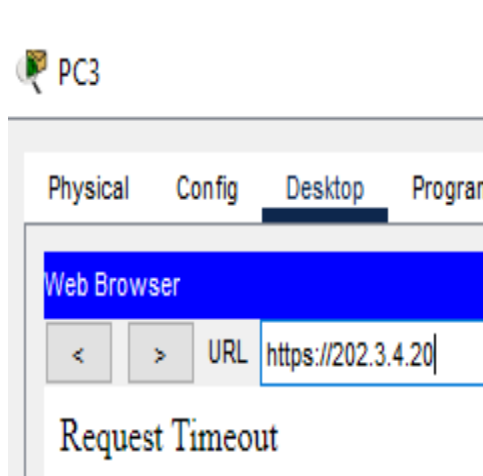
After:



- b. I used the commands “access-list 123 permit tcp 192.168.47.103 0.0.0.0 202.3.4.20 0.0.0.0 eq 443” to allow PC3 and 4 to access the Internet HTTPS-Server via HTTPS.

Before:

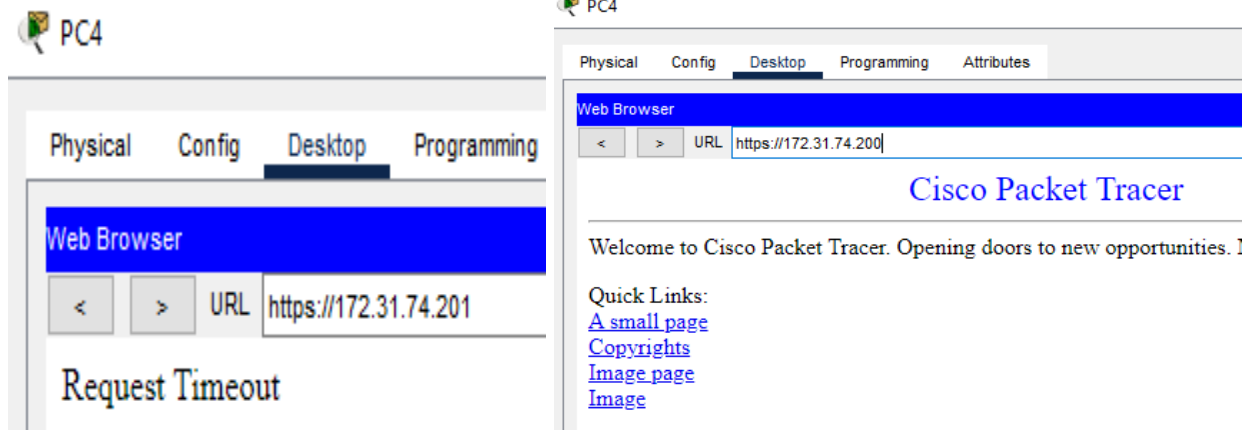
After:



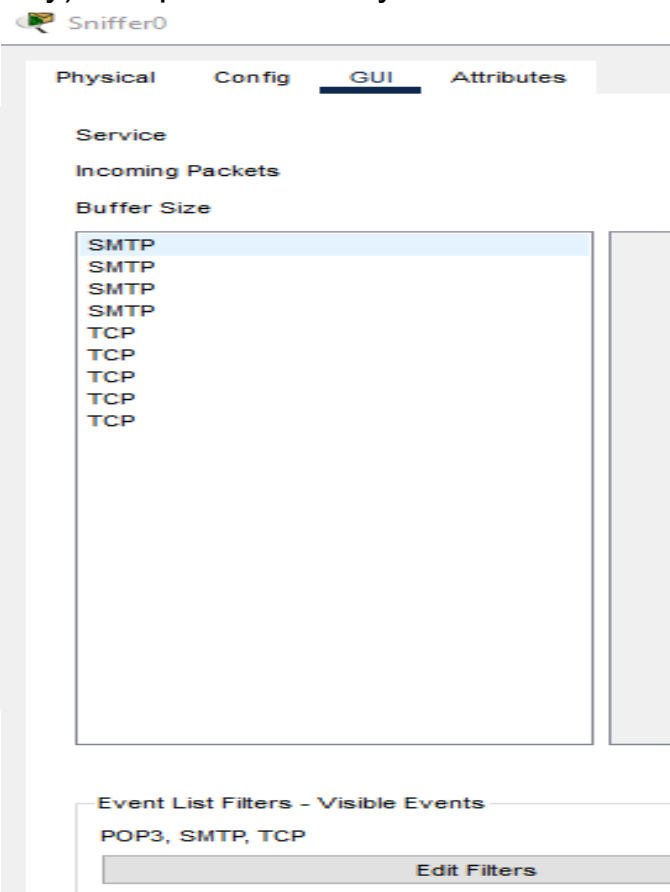
- c. I used the commands “access-list 123 permit tcp 192.168.47.104 0.0.0.0 172.31.74.200 0.0.0.0 eq 443” to allow every corporate PC to access the DMZ-HTTP-Server via HTTPS.

Before:

After:



- d. I used the commands “access-list 123 permit tcp 192.168.47.102 0.0.0.0 172.31.74.201 0.0.0.0 eq 25” and “access-list 123 permit tcp 192.168.47.102 0.0.0.0 172.31.74.201 0.0.0.0 eq 110” to allow all corporate PCs to access the DMZ-EMAIL-Server via SMTP and POP3. I did not know a good way to generate SMTP and POP3 traffic, so I put a sniffer in between the email server and the switch, proving that the packets were able to be sent through to the server even with the ACL. I used the traffic generator application on the PC to create the traffic (for some reason the POP3 traffic only came up as TCP on the sniffer and I am unsure why). I hope this is okay.



- e. I used the commands “access-list 123 permit icmp 192.168.47.102 0.0.0.0 200.1.2.1 0.0.0.0 “ to allow all corporate PCs to ping the ISP interface that is connected to the Edge router.

Before:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.1.2.1

Pinging 200.1.2.1 with 32 bytes of data:

Reply from 192.168.47.1: Destination host unreachable.
Reply from 192.168.47.1: Destination host unreachable.
Reply from 192.168.47.1: Destination host unreachable.
Reply from 192.168.47.1: Destination host unreachable.

Ping statistics for 200.1.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

After:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 200.1.2.1

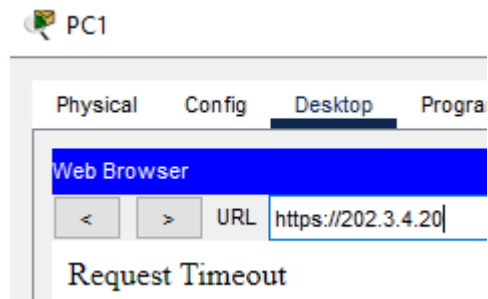
Pinging 200.1.2.1 with 32 bytes of data:

Reply from 200.1.2.1: bytes=32 time<1ms TTL=254
Reply from 200.1.2.1: bytes=32 time<1ms TTL=254
Reply from 200.1.2.1: bytes=32 time<1ms TTL=254
Reply from 200.1.2.1: bytes=32 time<1ms TTL=254

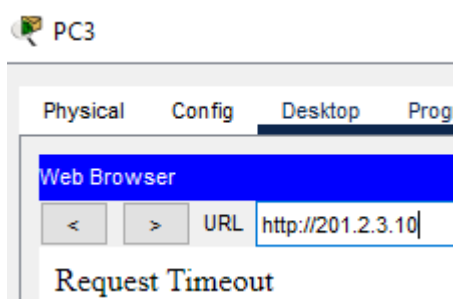
Ping statistics for 200.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

- f. I used the command “access-list 123 deny ip any any” to stop any other traffic from going through. Here I show that PC1 can not access the internet through the HTTPS server, PC3 can not access the internet through the HTTP server, and PC2 can not ping anything besides what it is allowed to.

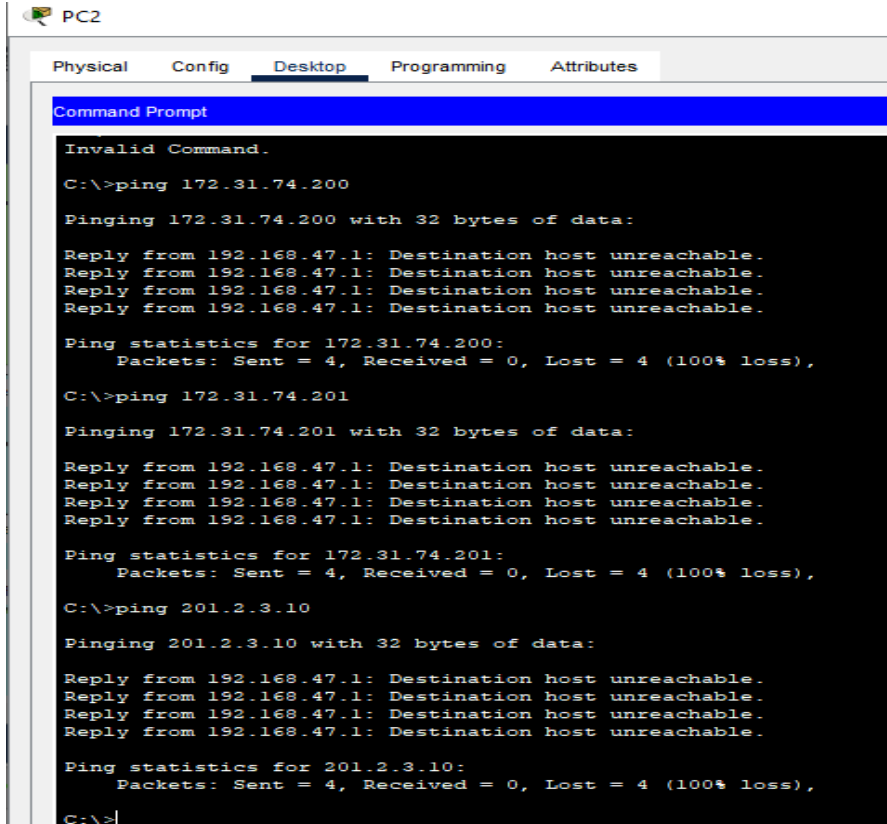
PC1:



PC3:



PC2:



The screenshot shows a PC2 desktop environment with a taskbar at the top containing icons for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, and a Command Prompt window is open. The Command Prompt displays the following text:

```
Invalid Command.  
C:\>ping 172.31.74.200  
  
Pinging 172.31.74.200 with 32 bytes of data:  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
  
Ping statistics for 172.31.74.200:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\>ping 172.31.74.201  
  
Pinging 172.31.74.201 with 32 bytes of data:  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
  
Ping statistics for 172.31.74.201:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\>ping 201.2.3.10  
  
Pinging 201.2.3.10 with 32 bytes of data:  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
Reply from 192.168.47.1: Destination host unreachable.  
  
Ping statistics for 201.2.3.10:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\>
```

Conclusion: In conclusion, access control lists are a little more complicated than I imagined. There is a lot of specific syntax that you need to know to be successful here. The videos that you had on this were very useful, so thank you. The only thing I would say I really struggled with was finding a way to create and capture the SMTP and POP3 traffic. I hope the method I used was able to verify that my configuration was successful and I apologize if there was a simpler method that I missed.