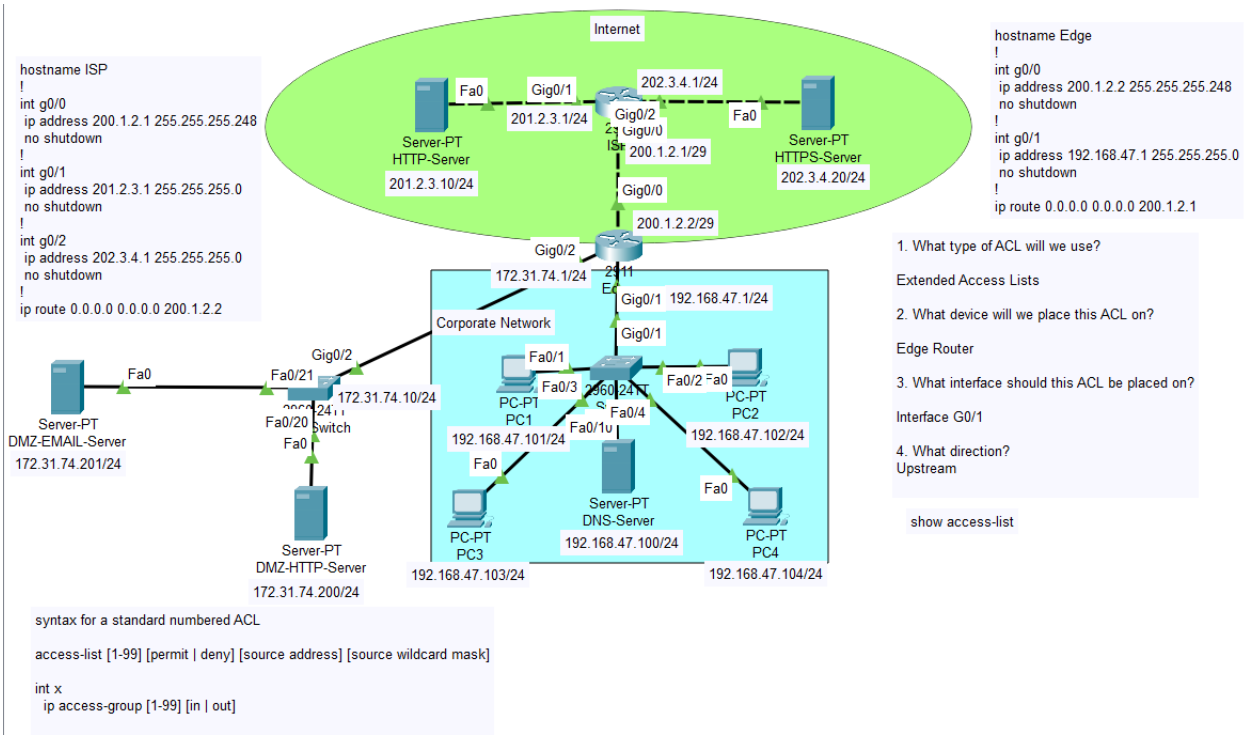
Justin Sterlacci
Internetworking
Professor Cannistra
April 16th, 2023

Lab 9 Lab Report

Lab Description:
Set up Access Control lists in a network to prevent or allow certain communications.

Topography:



Syntax:

CLI Command	Description	Mode of Cisco OIS
ping	Used to ping ip addresses from a PC. You can ping other PC's or switches with this.	Windows CMD
Logging synchronous	Forces error messages to be on its own line, rather than interrupt a line that you're typing on.	Console Line
Enable	Enter Privileged Mode	User Mode
Conf t	Enter Global Configurator Mode	Privileged Mode
Line con 0	Enter the Console Line	Global Configurator Mode
Hostname	Used to name a switch or PC	Privileged Mode

Password	Used to set a password	Privileged Mode
Login	Used to require the password to utilize User Mode	Global Configurator Mode
Enable password	Used to set an unencrypted Privileged Password	Global Configurator Mode
Show ip interface brief (sh ip int brief)	Displays a brief list of all interfaces	Privileged Mode
vtp domain INETLAB	Renames the VTP domain from NULL to INETLAB	Global Configurator Mode
Vtp password cisco	Set a password within the VTP Domain	Global Configurator Mode
Vtp mode server/client	Sets the vtp mode between server or client, in the case of this lab.	Global Configurator Mode
Switchport mode access	Changes the mode of a switchport to access mode	Line configuration Mode (within a vlan)
Switchport trunk encapsulation dot1q	Sets up the switch to switch connect to use IEEE 802.1Q encapsulation	Within a vlan with a multi-Connection switch
Switchport mode trunk	Sets the mode for the switchport to trunk	Within a vlan
Spanning-tree vlan xx root primary	Setting up a spanning tree within a vlan, and setting it to root primary	Privileged mode
Encapsulation dot1q xx	Sets up a VLAN in IEEE 802.1Q within a router	ROUTER Line Configuration Mode(within a sub interface)
Ip route (ip) (SM) (ip)	Sets up a static IP Route	Interface Mode
Router rip	Sets the Router into RIP mode	Global Configuration
Version 2	Sets the RIP version to version 2	Global Configuration
Network (ip address)	Sets the Network for RIPv2 networking	Global Configuration
Ipv6 router ospf 1	Sets the router to have OSPFv3 enabled	Global Configuration
Passive-interface (interface)	Will set the selected interface as a passive interface in OSPFv3	Router Line Configuration mode
Ipv6 ospf 1 area 0	Sets the passive interface in area 0	Interface Configuration
access-list # permit/deny (protocol) ip wildcard ip wildcard eq (port)	Sets up an extended access list to allow or deny the flow of a packet depending on the protocol and destination it is getting sent to	Global Configuration Mode

int x ip access-group [1-99] [in | out]	Sets up the flow for the specified port when it comes to access groups	Interface Mode

Test Cases:

Test Case 1: Verify that PC1 and PC2 can reach the HTTP-Server

1. Configure the ACL to allow traffic from PC1's or PC2's IP address
2. Send a packet from PC1 or PC2 to the HTTP-Server
3. Verify that the packet is received, and communication occurs.

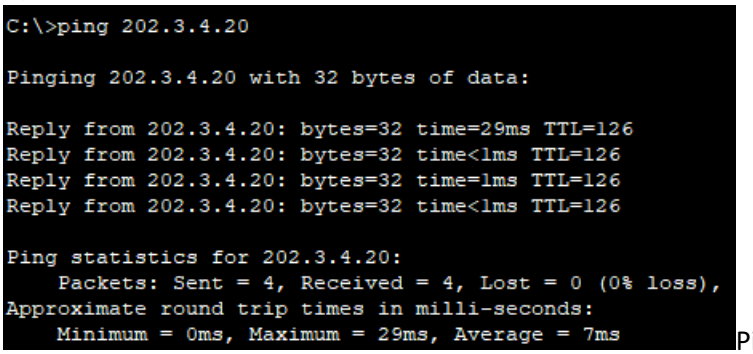
Test Case 2: Verify that PC3 and PC4 can reach the HTTPS-Server
1. Configure the ACL to allow traffic from PC3s or PC4s IP address
2. Send a packet from PC3 or PC4 to the HTTPS-Server
3. Verify that the packet is received, and communication occurs.

Test case 3: Verify that all Corporate PC's can access the DMZ-HTTP-Server via HTTPS
1. Configure the ACL to allow traffic from any of the Corporate PCs IP addresses
2. Send a packet from any of the corporate PCs to the DMZ-HTTP-Server
3. Verify that the packet is received, and communication occurs.

Test Case 4: Verify that all Corporate PCs can "ping" the ISP interface connected to the Edge Router
1. Configure the ACL to allow traffic from any of the Corporate PCs IP addresses
2. Send a packet from any of the Corporate PCs to the ISP interface connected to the Edge router, which is int g0/0 in this case.
3. Verify that the packet is received, and communication occurs.

Verification:

A)



Ping from PC1 to HTTPS-Server

```
C:\>ping 192.168.47.104

Pinging 192.168.47.104 with 32 bytes of data:

Reply from 192.168.47.104: bytes=32 time=36ms TTL=128
Reply from 192.168.47.104: bytes=32 time<1ms TTL=128
Reply from 192.168.47.104: bytes=32 time<1ms TTL=128
Reply from 192.168.47.104: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.47.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms
```

Ping from PC1 to PC4

```
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=29ms 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 = 29ms, Average = 7ms
```

Ping from PC1 to DMZ-HTTP-Server

B)

```
Edge(config-if)#do sh 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
```

Edge Router's IP Route table

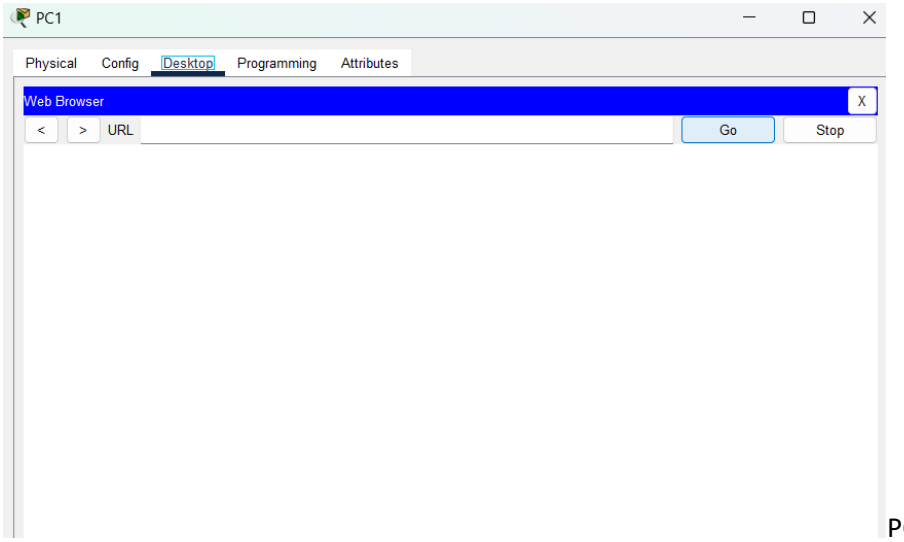
C)

```
Edge(config-if)#do sh access-list
Extended IP access list 100
    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 pop3
    100 permit tcp host 192.168.47.102 host 172.31.74.201 eq pop3
    110 permit tcp host 192.168.47.103 host 172.31.74.201 eq pop3
    120 permit tcp host 192.168.47.104 host 172.31.74.201 eq pop3
    130 permit tcp host 192.168.47.104 host 172.31.74.201 eq smtp
    140 permit tcp host 192.168.47.103 host 172.31.74.201 eq smtp
    150 permit tcp host 192.168.47.102 host 172.31.74.201 eq smtp
    160 permit tcp host 192.168.47.101 host 172.31.74.201 eq smtp
    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
```

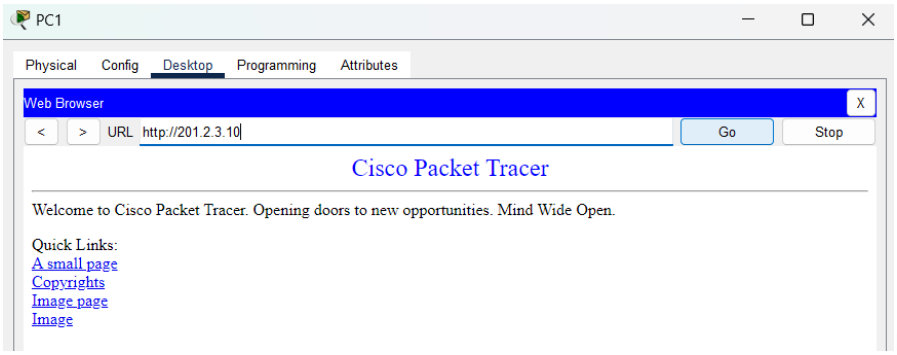
Edge Router's Access List after implementation

D)

Test Case 1:

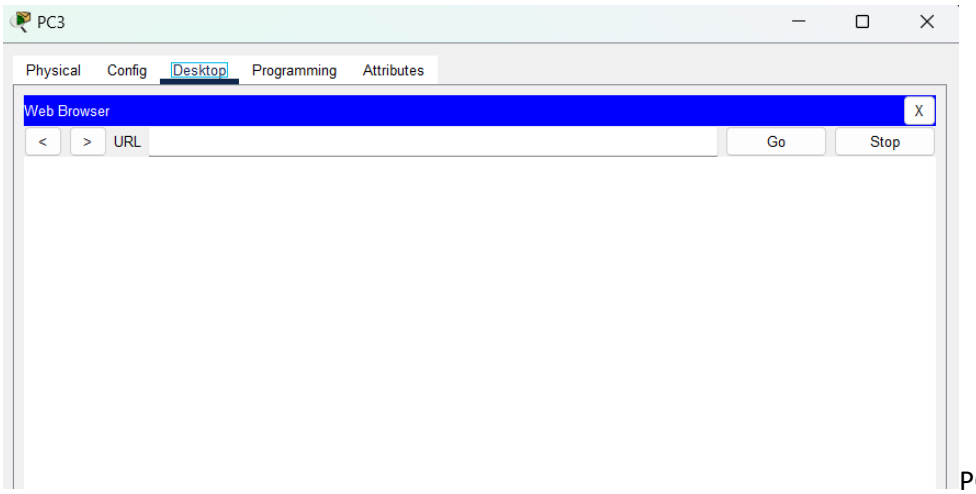


PC1 before Test Case

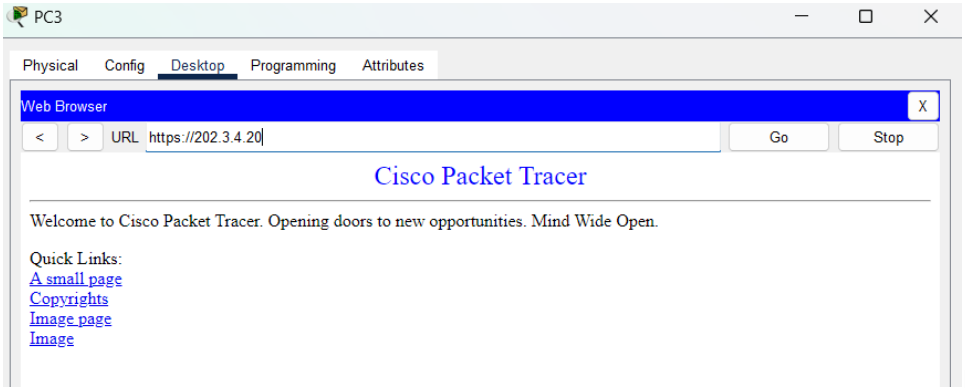


PC1 after Test Case

Test case 2:

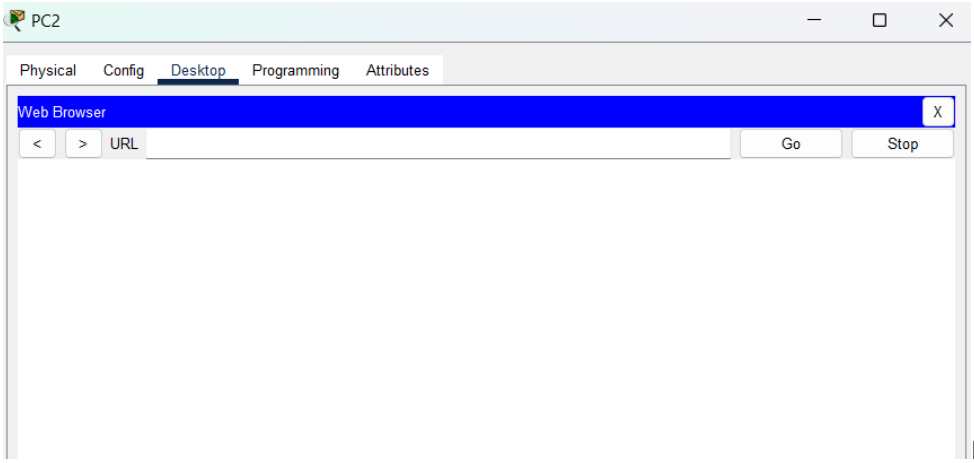


PC3 before Test Case

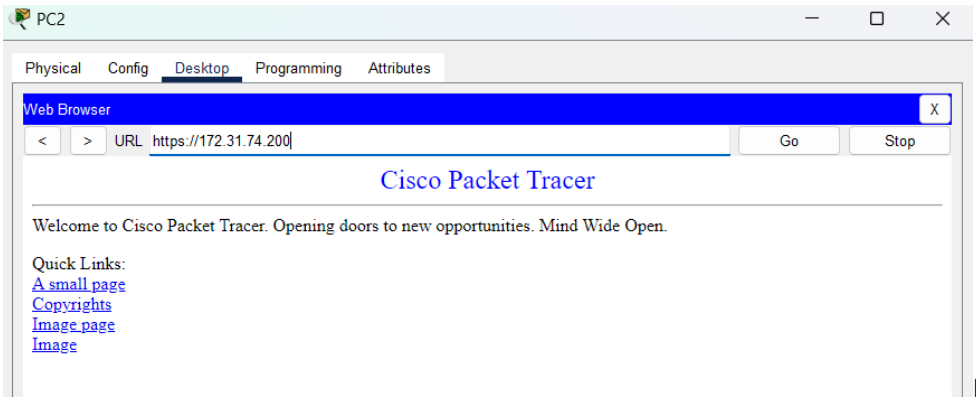


PC3 after Test Case

Test Case 3:

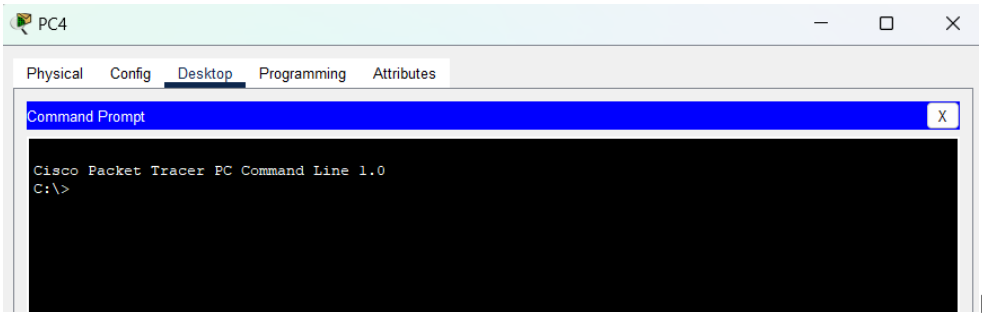


PC2 before Test Case

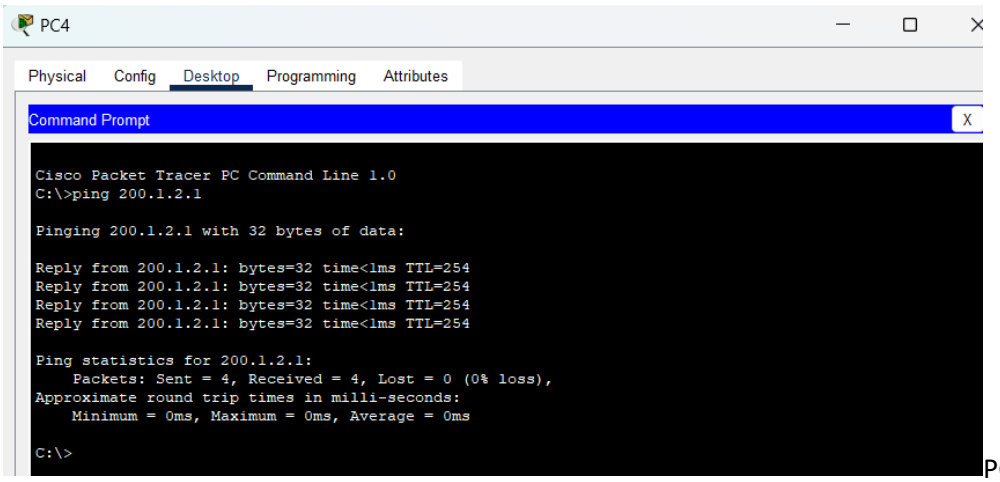


PC2 after Test Case

Test Case 4:



PC4 before Test Case



PC4 after Test Case

Conclusion:

This lab's initial set up was quite easy due to the partially completed network being configured, however I struggled to implement the Access Lists, since at first it allowed all packets to travel through regardless of me setting it to deny all other packets that wasn't specified, then I had an issue where it didn't allow any packets to get sent at all. What fixed this was making sure I didn't set anything on int g0/1 and int g0/2 with ip access-group 100 [in | out]. When I set this, it allowed the proper communication with the PCs to the HTTP and HTTPS server, as well as allowing the Corporate PCs to ping the ISP interface connected to the Edge Router. The only thing left unresolved is allowing all the Corporate PCs to access the DMZ-EMAIL-Server. I believe I set the proper access list commands; however, I am unsure how to set up the email function on both the PC and the DMZ-EMAIL-Server.