Department of Computer Science and Engineering
Islamic University of Technology (IUT)
A subsidiary organ of OIC

Laboratory Report

CSE 4512: Computer Networks Lab

Name: Hasin Mahtab Alvee
Student ID: 210042174
Section: SWE – Even (B)
Semester: 4th
Academic Year: 2023-24

Date of Submission: April 7th, 2024

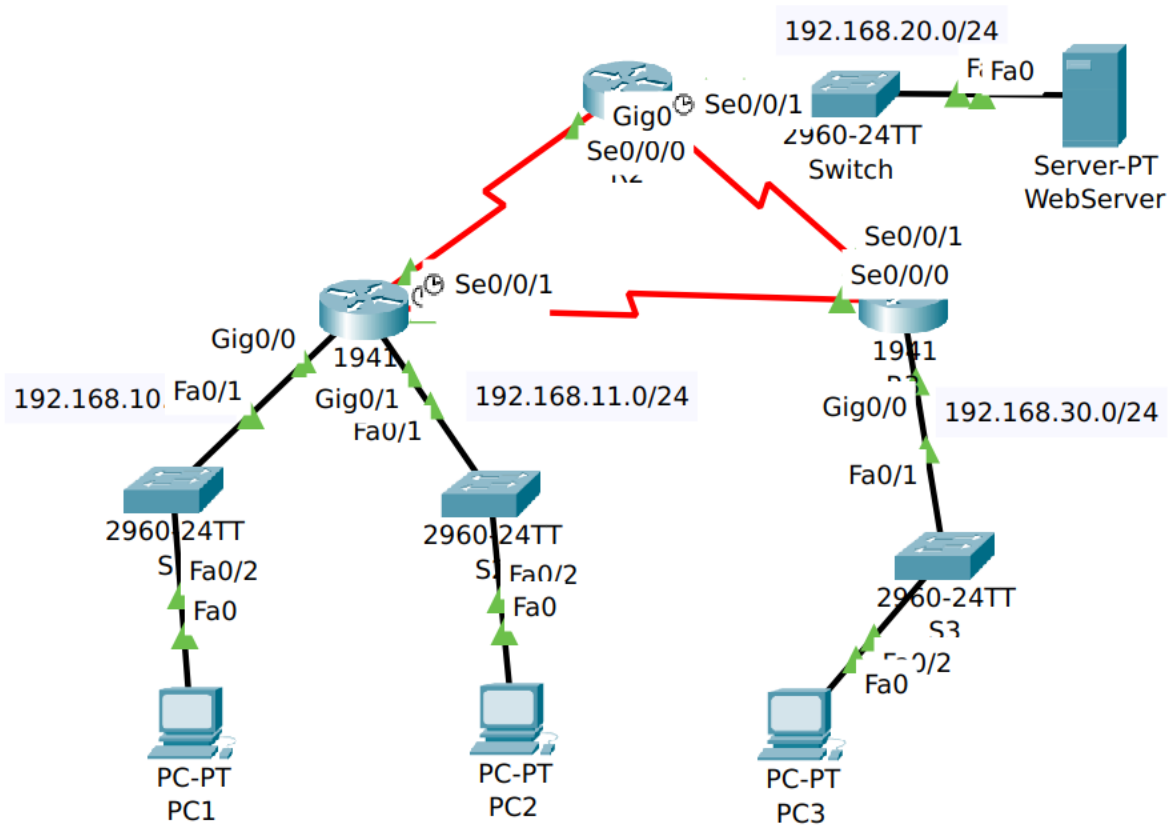**Title:** Configuring ACL and NAT in Cisco Devices

Objective:

1. Configure and understand ACL
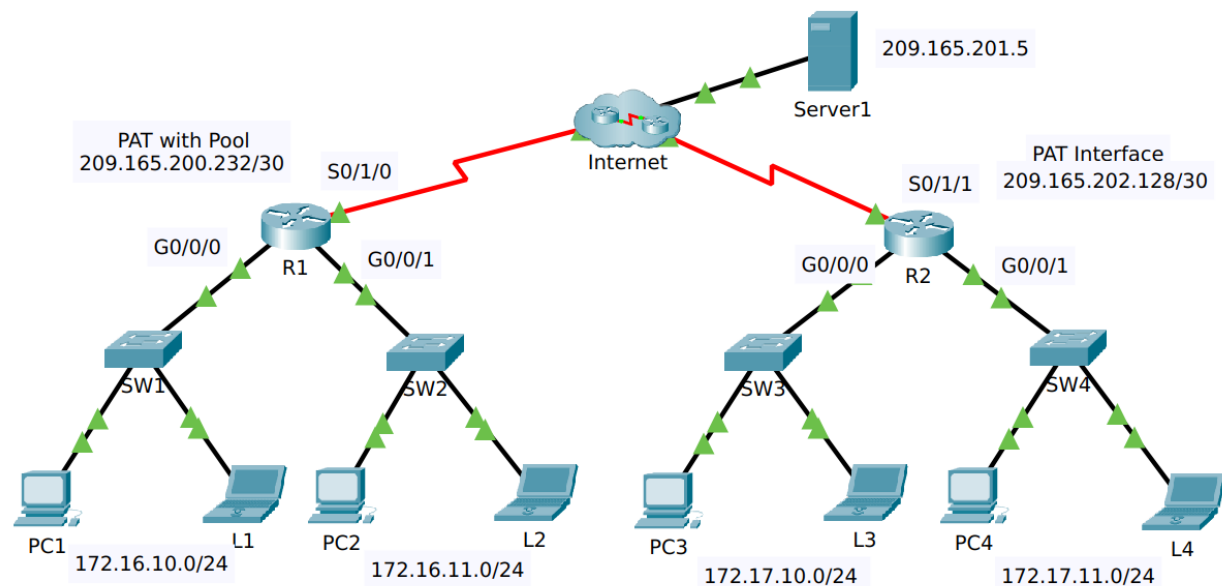2. Configure and understand NAT

Devices/ software Used:

1. Cisco Packet Tracer

Diagram of the experiment(s):

TASK 01

TASK 02

209.165.201.5

Server1

PAT with Pool
209.165.200.232/30   S0/1/0   Internet   S0/1/1   PAT Interface
209.165.202.128/30

G0/0/0   G0/0/1   G0/0/0   R2   G0/0/1
R1

SW1   SW2   SW3   SW4

PC1   L1   PC2   L2   PC3   L3   PC4   L4
172.16.10.0/24   172.16.11.0/24   172.17.10.0/24   172.17.11.0/24

Working Procedure:

TASK 01

- At first, I created a ACL for the access list 1 on Router 2, where I denied access permission to network 192.168.11.0. By default, if I deny permission to a network, ACL denies to all networks, so I need to permit all other networks using "permit any" on access list 1.
- Next, I need to set the access list to a specific interface, which I did the network of PC 1.
- I did the same for the next router, and configured ACL.

```
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#
R2(config)#access-list 1 den
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#acc
R2(config)#access-list 1 per
R2(config)#access-list 1 permit any
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show acc
R2#show access-lists
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255
    20 permit any

R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int
R2(config)#interface gi
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip acc
R2(config-if)#ip access-group 1 o
R2(config-if)#ip access-group 1 out
R2(config-if)#
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#acc
R3(config)#access-list 1 de
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#access-list 1 permit any
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show access-lists
Standard IP access list 1
    10 deny 192.168.10.0 0.0.0.255
    20 permit any

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface gi
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#
R3(config-if)#exit
R3(config)#show ru
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- Later, I performed some tests to verify the connection and found the the number of packets that matched with each line of access list.

```
R2#
R2#show ac
R2#show access-lists
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255
    20 permit any

R2#show access-lists
Standard IP access list 1
    10 deny 192.168.11.0 0.0.0.255 (3 match(es))
    20 permit any (3 match(es))
```

TASK 02

- On Router 1, we configured ACL on 172.16.0.0 to permit any connections.
- Then we used NAT pool to add two networks to the pool, which are 209.165.200.233 and 209.165.200.234, with the netmask of 255.255.255.252.
- Then I configured the NAT with the interfaces.

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#acce
R1(config)#access-list 1 per
R1(config)#access-list 1 permit 172.16.0.0 0.0.255.255
R1(config)#ip nat pool overload_nat_pool 209.165.200.233 209.165.200.234 netmask 255.255.255.252
R1(config)#ip nat inside source list 1 overload_nat_pool overload
                                         ^
% Invalid input detected at '^' marker.

R1(config)#ip nat inside source list 1 pool overload_nat_pool overload
R1(config)#int
R1(config)#interface s0/1/0
R1(config-if)#ip nat outside
R1(config-if)#interface g0/0/0
R1(config-if)#ip nat inside
R1(config-if)#interface g0/0/1
R1(config-if)#ip nat inside
```

- Then I check the NAT translations on Router 1.

```
R1#
R1#show ip nat trans
R1#show ip nat translations
Pro  Inside global      Inside local        Outside local      Outside global
icmp 209.165.200.233:1024172.16.10.11:1    209.165.201.5:1    209.165.201.5:1024
icmp 209.165.200.233:1025172.16.11.10:1    209.165.201.5:1    209.165.201.5:1025
icmp 209.165.200.233:1026172.16.11.11:1    209.165.201.5:1    209.165.201.5:1026
icmp 209.165.200.233:1 172.16.10.10:1      209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.233:2 172.16.10.10:2      209.165.201.5:2    209.165.201.5:2

R1#
```

- For router 2, we need to configure a PAT connection. We use ACL on access list 2 for the PAT.
- Then I checked the PAT translations.

```
R2#
R2#show ip nat tra
R2#show ip nat translations
Pro  Inside global      Inside local        Outside local      Outside global
icmp 209.165.202.130:1024172.17.10.11:1    209.165.201.5:1    209.165.201.5:1024
icmp 209.165.202.130:1025172.17.11.10:1    209.165.201.5:1    209.165.201.5:1025
icmp 209.165.202.130:1026172.17.11.11:1    209.165.201.5:1    209.165.201.5:1026
icmp 209.165.202.130:1 172.17.10.10:1      209.165.201.5:1    209.165.201.5:1
```

Questions:

Task # 01:

1. The ping from 192.168.10.10 to 192.168.11.10 is successful or not? Explain.
   Ans: It was successful as we did not deny ACL between these networks.

2. The ping from 192.168.10.10 to 192.168.20.254 is successful or not? Explain.

Ans: It was successful as we did not deny ACL between these networks.

3. The ping from 192.168.11.10 to 192.168.20.254 failed or not? Explain.
   Ans: It was not successful. AS we denied ACL between these networks.

Task # 02:

1. From the web browser of each of the PCs that use R1 as their gateway (PC1, L1, PC2, and L2), access the web page for Server1.
   Question:
   Were all connections successful?

   Ans: Yes all the connections were successful.

2. From the web browser of each of the PCs that use R2 as their gateway (PC3, L3, PC4, and L4), access the web page for Server1.
   Question:
   Were all connections successful?

   Ans: Yes all the connections were successful.

3. Compare the NAT statistics on the two devices.
   Question:
   Why doesn't R2 list any dynamic mappings?

   Ans: In R1, there are multiple NAT translations; in R2, there is just one. Because PAT only generates one-to-many translations utilising a single public IP address and various source port numbers, R2 doesn't display any dynamic mappings when using PAT.

Observation:

- The task defines how we can use ACL to allow and deny connections over the internet. We can also implement NAT and PAT to have control over our internal and external connections with hosts and servers.

Challenges (if any):

- I could not add the extra PC in the task 1 according to my Student ID.