



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

Laboratory Report

CSE 4512: Computer Networks Lab

Name: Adid-Al-Mahamud Shazid

Student ID: 210042172

Section: SWE (B)

Semester: 4th

Academic Year: 2022-23

Date of Submission: 7th April 2024

Title: Configuring ACL and NAT in Cisco Devices

Objective:

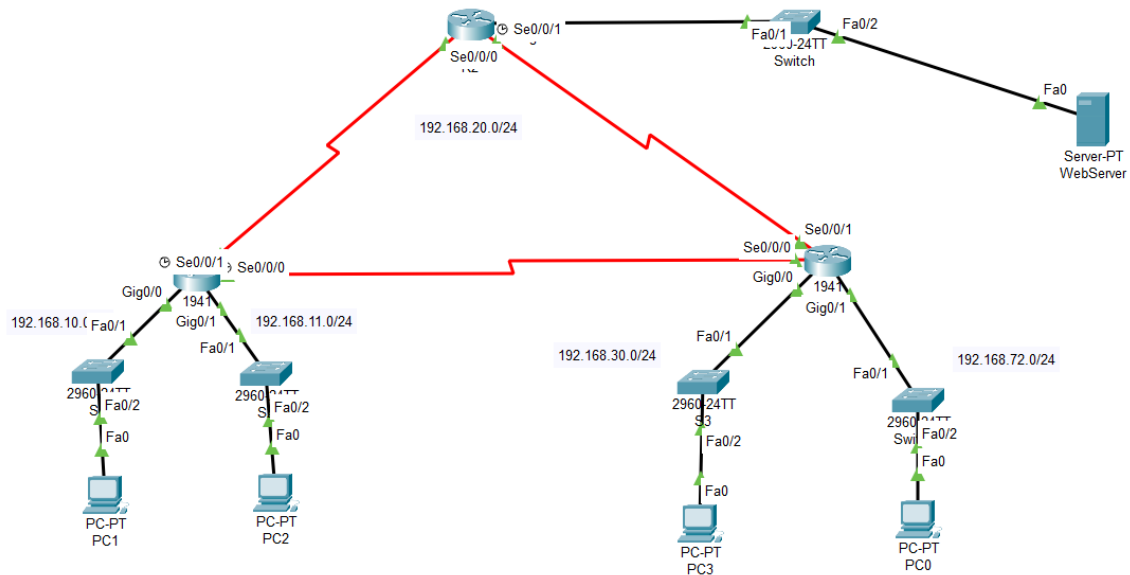
1. Describe the concept of Access Control List (ACL)
2. Implement standard numbered ACL
3. Describe the concept of Network Address Translation (NAT)
4. Explain different types of NAT configuration
5. Implement NAT in a given topology

Devices/ software Used:

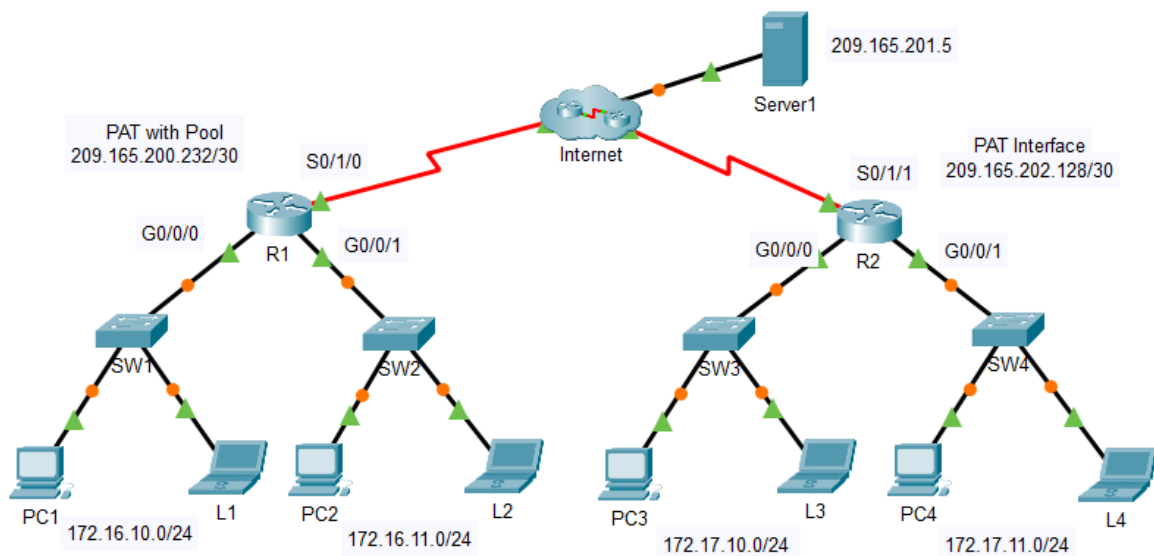
- Cisco Packet Tracer

Diagram of the experiments:

Task 01:



Task 02:



Working Procedure:

Task 01:













1. Investigated the current network configuration given in classroom and found that it is working correctly.
2. First, I Created an ACL using the number 1 on R2.
3. Then I denied access to the 192.168.20.0/24 (server) network from the 192.168.11.0/24 (PC2) network and permitted access from any other network across the topology.

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

4. Then I applied ACL1 to g0/0 of Router2 which made the interface restrict to receive any data from 192.168.11.0/24 network.
5. Then I created another ACL using the number 1 on R3 with a statement that denies access to the 192.168.30.0/24 (PC3) network from the 192.168.10.0/24 (PC1) network.

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

6. Then I applied ACL1 to g0/0 of Router3 which made the interface restrict to receive any data from 192.168.10.0/24 network.
7. Then I went through some tests to verify the ACL implementations.

	Successful	PC1	PC2	ICMP		0.000	N	0	(edit)
	Successful	PC1	WebServer	ICMP		0.000	N	1	(edit)
	Failed	PC2	WebServer	ICMP		0.000	N	2	(edit)
	Failed	PC1	PC3	ICMP		0.000	N	3	(edit)
	Successful	PC2	PC3	ICMP		0.000	N	4	(edit)
	Successful	PC3	WebServer	ICMP		0.000	N	5	(edit)

8. Then I issued the show access-lists command again on routers R2 and R3 and got output that indicates the number of packets that have matched each line of the access list.

```
R2# show access-lists
Standard IP access list 1
 10 deny 192.168.11.0 0.0.0.255 (2 match(es))
 20 permit any (4 match(es))

R3# show access-lists
Standard IP access list 1
 10 deny 192.168.10.0 0.0.0.255 (3 match(es))
 20 permit any (5 match(es))
```

9. Then I created a new file and copied the whole topology and added a PC with a switch on R3 assigning IP address 192.168.172.2 for the network 192.168.172.0.

10. Then I created an ACL using the number 2 on R3 with a statement that permits access to the 192.168.11.0/24 (PC2) network from the 192.168.172.0/24 (PC0) network and applied ACL1 to g0/1 of Router3.

```
R3(config)# access-list 2 permit 192.168.11.0 0.0.0.255
R3(config)# access-list 2 deny any
R3(config)# exit







R3(config)# int g0/1
R3(config-if)# ip ac
R3(config-if)# ip access-group 2 out
```

11. PC0 is denying any response from PC3. However, it rejects any response from PC2 as well though it was permitted while configuring ACL.

12. So, I applied static routing on R1 and R2 to connect my new network with other networks of the topology.

```
R1(config)# ip route 192.168.172.0 255.255.255.0 10.3.3.2
R2(config)# ip route 192.168.172.0 255.255.255.0 10.2.2.2
R2(config)# exit
```

13. Finally, I pinged to PC 0 from all other PC's. Only PC2 was successful to communicate.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	PC1	PC0	ICMP		0.000	N	0	(edit)
	Successful	PC2	PC0	ICMP		0.000	N	1	(edit)
	Failed	PC3	PC0	ICMP		0.000	N	2	(edit)

```
R3# show access-list 2
Standard IP access list 2
  permit 192.168.11.0 0.0.0.255 (3 match(es))
  deny any (6 match(es))
```









Task 2:

NAT Configuration

1. First, On R1, I configured one statement for ACL 1 to permit any address belonging to 172.16.0.0/16.
2. Then I Configured R1 with a NAT pool that uses the two useable addresses in the 209.165.200.232/30 address space.
3. Then I associated ACL 1 with the NAT pool and allow addresses to be reused.
4. I completed the NAT configuration by configuring the NAT interfaces.

```
R1(config)#  
R1(config)# access-list 1 permit 172.16.0.0 0.0.255.255  
R1(config)# ip nat pool Pool1 209.165.200.233 209.165.200.234 netmask 255.255.255.252  
R1(config)# ip nat inside source list 1 pool Pool1 overload  
R1(config)# int s0/1/0  
R1(config-if)# ip nat outside  
R1(config-if)# int g0/0/0  
R1(config-if)# ip nat inside  
R1(config-if)# int g0/0/1  
R1(config-if)# ip nat inside  
R1(config-if)# exit  
R1(config)#exit
```

5. From the web browser of each of the PCs that use R1 as their gateway (PC1, L1, PC2, and L2), I accessed the web page for Server1 and found that all the connection were successful.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	L1	Server1	ICMP		0.000	N	0	(edit)	
	Successful	PC2	Server1	ICMP		0.000	N	1	(edit)	
	Successful	L2	Server1	ICMP		0.000	N	2	(edit)	
	Successful	PC1	Server1	ICMP		0.000	N	3	(edit)	

6. Then I Viewed the NAT translations on R1.









```
R1# show ip nat translations  
Pro Inside global      Inside local          Outside local          Outside global  
icmp 209.165.200.233:1024 172.16.10.11:1       209.165.201.5:1       209.165.201.5:1024  
icmp 209.165.200.233:1025 172.16.11.10:1       209.165.201.5:1       209.165.201.5:1025  
icmp 209.165.200.233:1026 172.16.11.11:1       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
```

PAT Configuration

1. First, on **R2**, I configure another statement for ACL 2 to permit any address belonging to 172.17.0.0/16.
2. Then I Entered the **R2** NAT statement to use the interface connected to the internet and provide translations for all internal devices.
3. Then I Configured **R2** interfaces with the appropriate inside and outside NAT commands.

```
R2(config)# access-list 2 permit 172.17.0.0 0.0.255.255
R2(config)# ip nat pool Pool2 209.165.202.129 209.165.201.130 netmask 255.255.255.252
%Pool Pool2 mask 255.255.255.252 too small; should be at least 0.0.0.0
%Start and end addresses on different subnets
R2(config)# ip nat pool Pool2 209.165.202.129 209.165.202.130 netmask 255.255.255.252
R2(config)# ip nat inside source list 2 interface s0/1/1 overload
R2(config)#
R2(config)# int g0/0/0
R2(config-if)# ip nat inside
R2(config-if)# int g0/0/1
R2(config-if)# int g0/0/1
R2(config-if)# ip nat inside
R2(config-if)# int s0/1/1
R2(config-if)# ip nat outside
R2(config-if)# exit
R2(config)# exit
```

4. From the web browser of each of the PCs that use R2 as their gateway (PC3, L3, PC4, and L4), I accessed the web page for Server1 and found that all the connection were successful.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	Server1	ICMP		0.000	N	0	(edit)	
	Successful	L3	Server1	ICMP		0.000	N	1	(edit)	
	Successful	PC4	Server1	ICMP		0.000	N	2	(edit)	
	Successful	L4	Server1	ICMP		0.000	N	3	(edit)	

5. Then I Viewed the NAT translations on R2.

```
R2# show ip nat tr
R2# show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.202.130:1026172.17.11.11:1      209.165.201.5:1      209.165.201.5:1026
```


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. Because no ACL was applied between the networks.

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

Ans: It was successful. Because no ACL was applied between the networks.

3. The ping from 192.168.11.10 to 192.168.20.254 failed or not? Explain.
Ans: It failed. Because the 192.168.20.0 network denied access for network 192.168.11.0 using ACL.

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. Were all connections successful?

Ans: Yes.

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. Were all connections successful?

Ans: Yes.

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

Ans: There are several NAT translations in R1, however, only 1 in R2. The reason that R2 doesn't list any dynamic mappings while using PAT is because PAT only creates one-to-many translations by using a single public IP address and different source port numbers. When a device from the internal network initiates a connection to the outside network, R2's PAT function assigns a unique source port number to each internal IP address to differentiate between multiple internal hosts accessing external resources. These translations are dynamic, as they are created on-demand and are maintained in a translation table.

Observation:

Throughout the task, I learnt how to implement Access Control list and limit users to communicate a network. Also, I learnt to implement NAT and PAT. Both NAT and Port Address Translation (PAT) were configured to enable communication between internal hosts and external servers. NAT translations were successfully established, allowing internal hosts to access external resources via translated IP addresses.

Challenges (if any):

- The main challenge I faced is that I added a new PC in Task 1 and configured everything correctly. But it was not working correctly. Then I observed that the new PC is sending message to the network connected under the same router but not to the networks outside. So, I realized that internetworking isn't happening here. So, I applied static routing on the other routers for the new network I added and then it was successfully working.
- In task-2, After opening the pka file while I was writing the report, I tried to view the NAT translations again for verification. But I couldn't get any output. However, I had screenshot taken before. Thus, I didn't have to do the task again :3