Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4412 : Data Communication and Networking Lab

Name	**: Mirza Mohammad Azwad**
Student ID	**: 200042121**
Section	**: BSc in SWE(Group A)**
Semester	**: 4th Semester**
Academic Year	**: 2022-23**
Date	**: 11/04/2023**
Lab No	**: 10**

Title: Understanding the concept of NAT and configuration of NAT.

Objective:

1. Understand NAT
2. Configuration of NAT

Devices Used In the Experiment:

1. Switch-PT
2. Router-PT
3. PC-PT
4. Server-PT
5. Copper Straight-Through Cables
6. Copper Cross-Over Cables
7. DCE/DTE Serial Connectors

Theory:

NAT Definition

Several devices on a private network can share one public IP address due to the router technique known as NAT. This is accomplished by translating the private IP addresses of local network devices to the router's public IP address for internet data transmission, and vice versa for data receiving. By using a single public IP address, this enables several devices on a private network to access the internet.

Usage of NAT:

NAT serves a variety of common objectives, such as:

IP address conservation: NAT allows numerous devices on a private network to share a single public IP address, which helps preserve IPv4 addresses.

Network Administration: Administration is made easier by NAT, which enables private network devices to use unregistered private IP addresses.

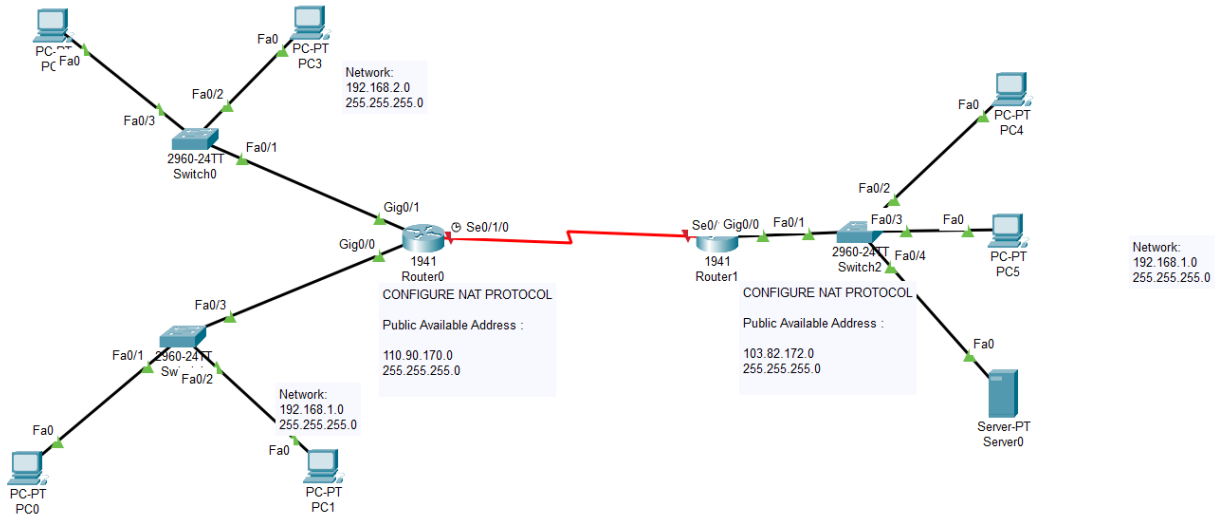
Security: By concealing the private IP addresses of devices on the local network from the internet, NAT offers a fundamental level of security.

Explain the usage of NAT with an example.

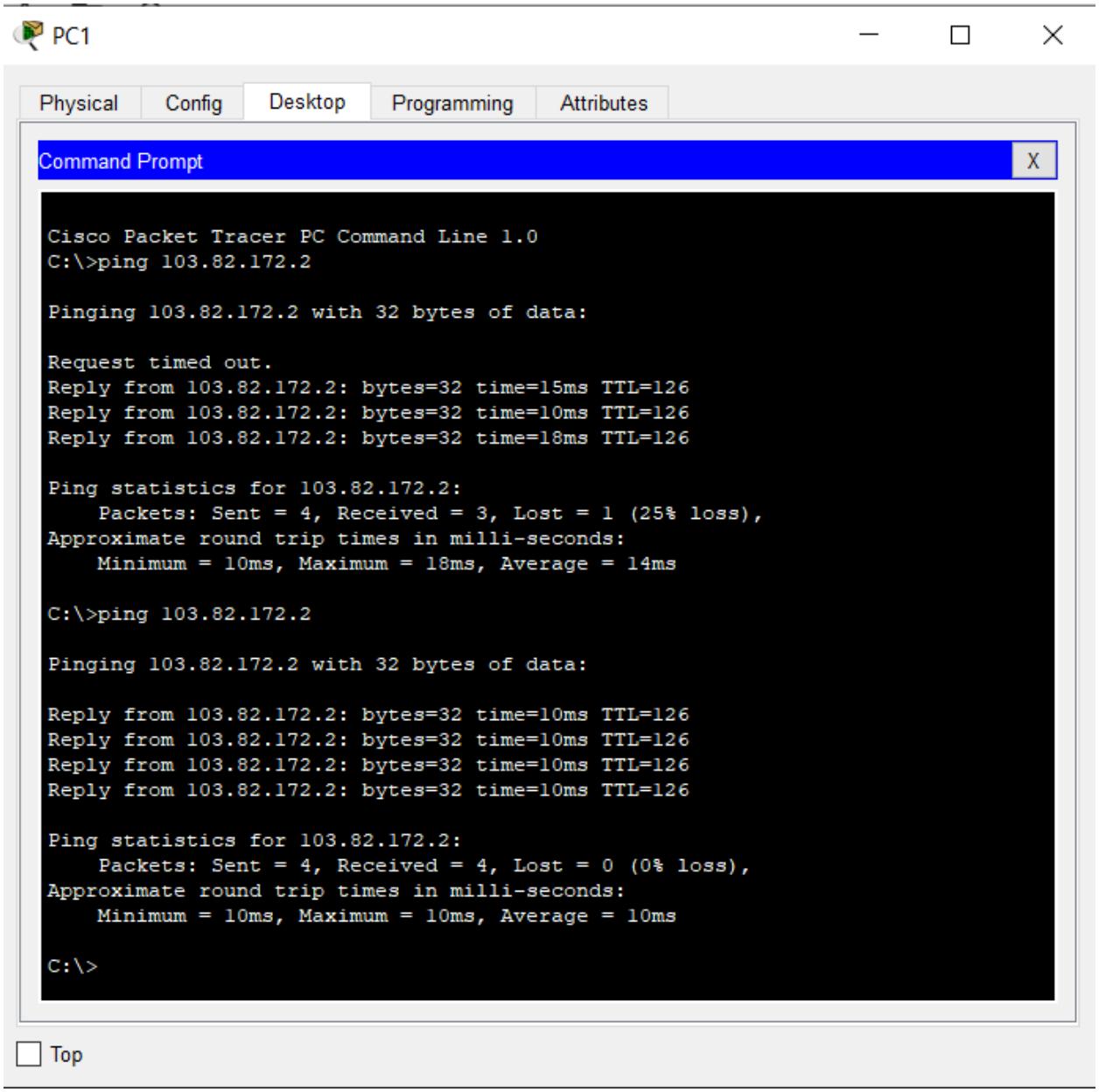
Computers in the CSE department, for instance, each have a unique private IP address that can only be used on the network. However, in order to access the internet, we would require a public IP address that would allow others to recognize us as part of the CSE department subnetwork. Therefore, instead of assigning the private IP address that is only used internally, a NAT box in the router that connects to the internet assigns a public IP address.

Diagram of the experiment:

(Take a screenshot of your lab task from packet tracer and paste here)



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch1	ICMP
	0.002	Switch1	Router0	ICMP
	0.003	Router0	Router1	ICMP
	0.004	Router1	Switch2	ICMP
	0.005	Switch2	PC4	ICMP
	0.005	Switch2	PC5	ICMP
	0.005	Switch2	Server0	ICMP
	0.006	PC4	Switch2	ICMP
	0.007	Switch2	Router1	ICMP
	0.008	Router1	Router0	ICMP
	0.009	Router0	Switch1	ICMP
	0.010	Switch1	PC1	ICMP


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 103.82.172.2
Pinging 103.82.172.2 with 32 bytes of data:
Request timed out.
Reply from 103.82.172.2: bytes=32 time=15ms TTL=126
Reply from 103.82.172.2: bytes=32 time=10ms TTL=126
Reply from 103.82.172.2: bytes=32 time=18ms TTL=126
Ping statistics for 103.82.172.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 18ms, Average = 14ms
C:\>ping 103.82.172.2
Pinging 103.82.172.2 with 32 bytes of data:
Reply from 103.82.172.2: bytes=32 time=10ms TTL=126
Reply from 103.82.172.2: bytes=32 time=10ms TTL=126
Reply from 103.82.172.2: bytes=32 time=10ms TTL=126
Reply from 103.82.172.2: bytes=32 time=10ms TTL=126
Ping statistics for 103.82.172.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 10ms, Maximum = 10ms, Average = 10ms
C:\>
Top

Configuration of NAT in Router:

Commands for configuring NAT

In router 0

```
interface GigabitEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 50.0.0.1 255.0.0.0
 ip nat outside
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
!
```

```
ip nat pool pool1 110.90.170.1 110.90.170.5 netmask 255.255.255.0
ip nat inside source list 1 pool pool1
ip classless
ip route 103.82.172.0 255.255.255.0 50.0.0.2
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 deny any
```

In router 1

```
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 50.0.0.2 255.0.0.0
 ip nat outside
!
```

```
ip nat inside source static 192.168.1.2 103.82.172.2
ip nat inside source static 192.168.1.3 103.82.172.3
ip nat inside source static 192.168.1.4 103.82.172.4
ip classless
ip route 110.90.170.0 255.255.255.0 50.0.0.1
```

Observation:

The screenshots of ***show nat*** command in two switches are shown below:

In router 0(Dynamic NAT)

```
Router#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 110.90.170.1:4    192.168.1.2:4      103.82.172.2:4     103.82.172.2:4
icmp 110.90.170.1:5    192.168.1.2:5      103.82.172.2:5     103.82.172.2:5
icmp 110.90.170.1:6    192.168.1.2:6      103.82.172.2:6     103.82.172.2:6
icmp 110.90.170.1:7    192.168.1.2:7      103.82.172.2:7     103.82.172.2:7
```

This was the outcome of pinging 103.82.172.2 from PC1
It resulted in entries to the NAT table showing the IP address mapping from the pool provided
In router 1(Static NAT)

```
Router#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  103.82.172.2      192.168.1.2        ---                ---
---  103.82.172.3      192.168.1.3        ---                ---
---  103.82.172.4      192.168.1.4        ---                ---
```

Challenges:

Firstly I initially could not comprehend where I should provide the NAT instructions upon configuring the routers. Later although, I understood the basics of how it worked with static NAT, I had a really difficult time figuring out how to work with dynamic NAT. Later I figured out that dynamic NAT should be applied to one end and static on the other for testing purposes otherwise it wasn't really possible to test and this was what was shown in the classroom, sir also configured dynamic on one end and static on the other and upon pinging from the dynamic end to the static end we could find the required results as shown in this lab report.

Another place I struggled greatly add was setting the access-list although sir clearly mentioned the difference between the netmask and the wildcard but I forgot so after various experimental tries I saw why upon entering the netmask instead of wildcard the access-list gets a whitelist IP entry, upon seeing that I could configure accordingly and figured out the difference between netmask and wildcards respectively.