Data Communication and Computer Networks

EEE314

Lab # 12

Name	**Muhammad Haris Irfan**
Registration Number	FA18-BCE-090
Class	BCE-6B
Instructor's Name	Sir Asad Ali Malik.

Lab #12 NAT Configuration

Network Address Translation (NAT)

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

Advantages of Network Address Translation (NAT)

- NAT allows the local addressing to be independent of any external constraints.

- NAT saves the IP addresses in two levels first by not using the global IP address in the local addressing and second local addresses are also not used in the global addressing mainly in IPv4 system.

- NAT also brings safety to your networking environment by not exposing the internal addressing structure to the outsider.

- Nat also provides an extra level of privacy by not reveling the device IP address or the sending ad receiving of traffic.

- NAT increases network flexibility in term of establishing any network.

Disadvantages of Network Address Translation (NAT)

- NAT is a memory consuming technology as it converts the local and global IP addresses so it saves hose translation in the memory.

- There are some applications that tend to have some compatibility issues with NAT.

- It sometimes restricts some incoming connections which are important.

- NAT doesn't perform well at a higher scale.

- NAT was a temporary technology and face several issues to work with new technologies.

- Nat basically changes the address which makes the troubleshooting complex

Commands used:

1. ip nat inside source static

Statically translates the destination IP address of packets that travel from outside to inside.

2. ip nat inside/ ip nat outside

Translates the source **IP** address of packets that travel from **inside** to outside and vice versa in the later.

3. ip nat pool

A NAT pool is a set of IP addresses that you can define and use for address translation.

4. ip access-list extended

Extended Access Control **Lists** (ACLs) allow you to permit or deny traffic from specific **IP** addresses to a specific destination **IP** address and port.

5. ip nat inside source list

Translates the destination of the **IP** packets that are traveling **outside** to **inside**

6. show ip nat translations

To **display** active Network Address **Translation** (**NAT**) **translations**, use the **show ip nat translations** EXEC command.

7. show ip nat statistics

Information about which interfaces use **NAT**, how many entries are in the **NAT** table, how often they have been used, and, most importantly, how often packets have bypassed **NAT**.

8. <u>debug ip nat</u>

Used to verify the operation of **NAT** displaying information about each packet the router translates.

9. <u>clear ip nat translation *</u>

To clear dynamic NAT translations from the translation table.

10. <u>show run</u>

shows detailed configurations of a router.

Lab Implementation:

IP Address: 192.168.90.0/24 (roll number 90)

Subnet Mask: 255.255.255.240/28

No of hosts: 16

No of subnets: 16

#	Subnet	First host address	Last host address	Broadcast Address
1	192.168.90.0	192.168.90.1	192.168.90.14	192.168.90.15
2	192.168.90.16	192.168.90.17	192.168.90.30	192.168.90.31
3	192.168.90.32	192.168.90.33	192.168.90.46	192.168.90.47
Last	192.168.90.240	192.168.90.241	192.168.90.254	192.168.90.255

Addressing table

Device	Interface	IP Address	Subnet Mask
R1	Se2/0	192.168.90.1	255.255.255.240
	Fa0/0	192.168.90.17	255.255.255.240
	Fa1/0	192.168.90.33	255.255.255.240
R2	Se2/0	192.168.90.2	255.255.255.240
	Se3/0	192.168.90.49	255.255.255.240
	Fa0/0	192.168.90.65	255.255.255.240
ISP	Se3/0	192.168.90.50	255.255.255.240
Server	Fa0/0	192.168.90.66	255.255.255.240
	Global	192.168.90.254	255.255.255.240

➢ Scenario 1: Before NAT Implementation
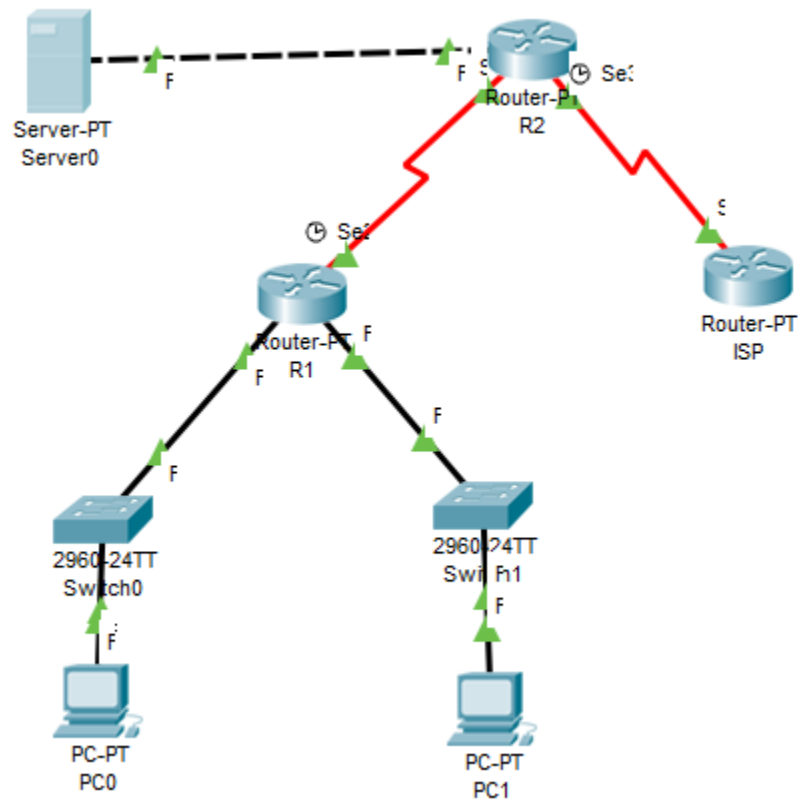
Topology:

Packets sent:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Peri
●	Successful	PC0	Server0	ICMP		0.000	
●	Failed	PC0	ISP	ICMP		0.000	
●	Successful	PC0	PC1	ICMP		0.000	
●	Failed	PC1	ISP	ICMP		0.000	
●	Successful	PC1	PC0	ICMP		0.000	
●	Successful	PC1	Server0	ICMP		0.000	

Pinging server from ISP before NAT:
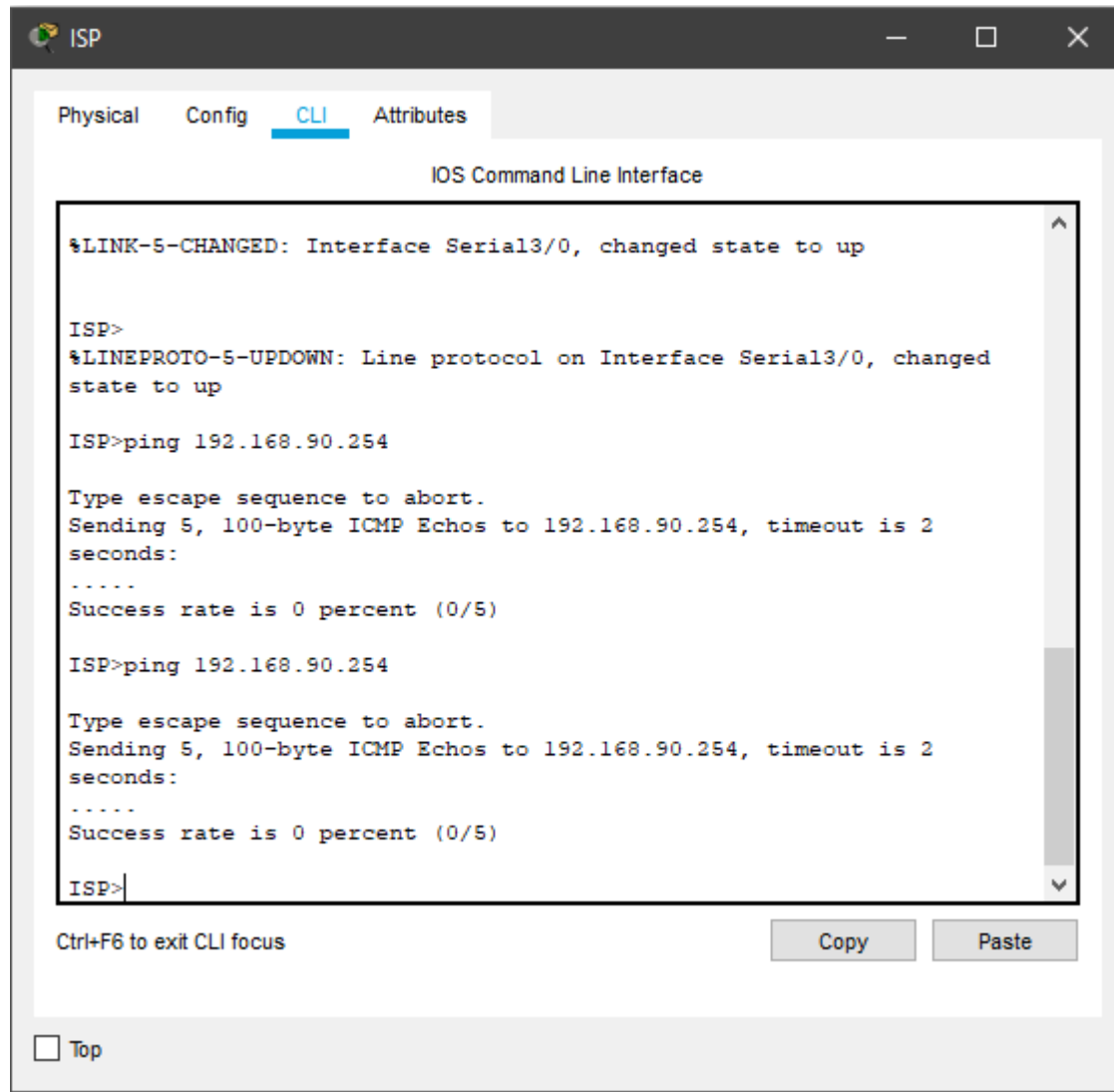
➤ Scenario 2: After NAT Implementation

Topology:
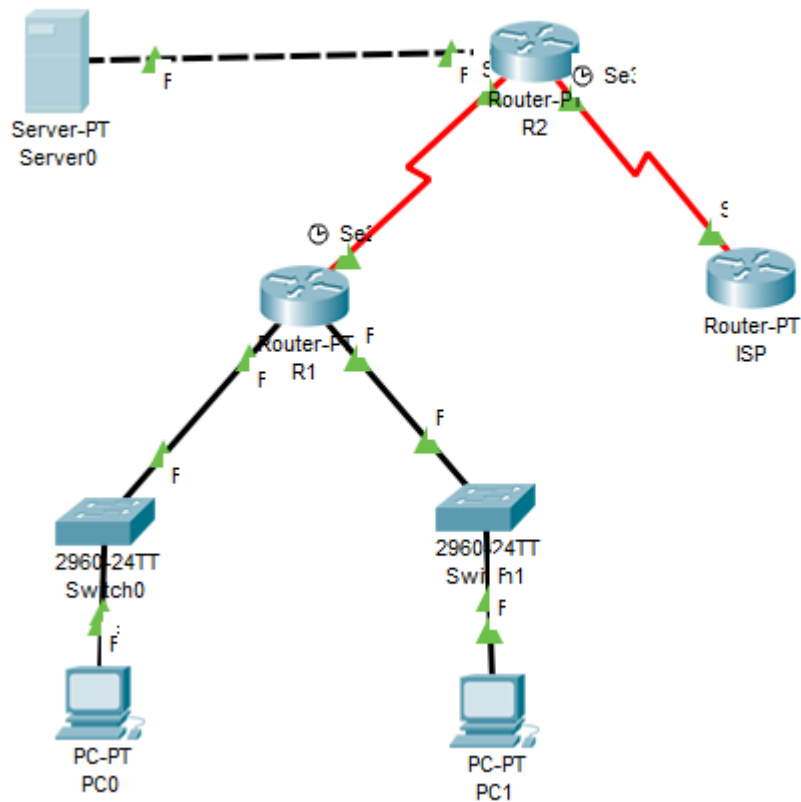
Packets sent:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
●	Successful	PC0	Server0	ICMP		0.000	N
●	Successful	PC0	ISP	ICMP		0.000	N
●	Successful	PC0	PC1	ICMP		0.000	N
●	Successful	PC1	Server0	ICMP		0.000	N
●	Successful	PC1	ISP	ICMP		0.000	N
●	Successful	PC1	PC0	ICMP		0.000	N

PDU List Window

Pinging server from ISP after NAT:
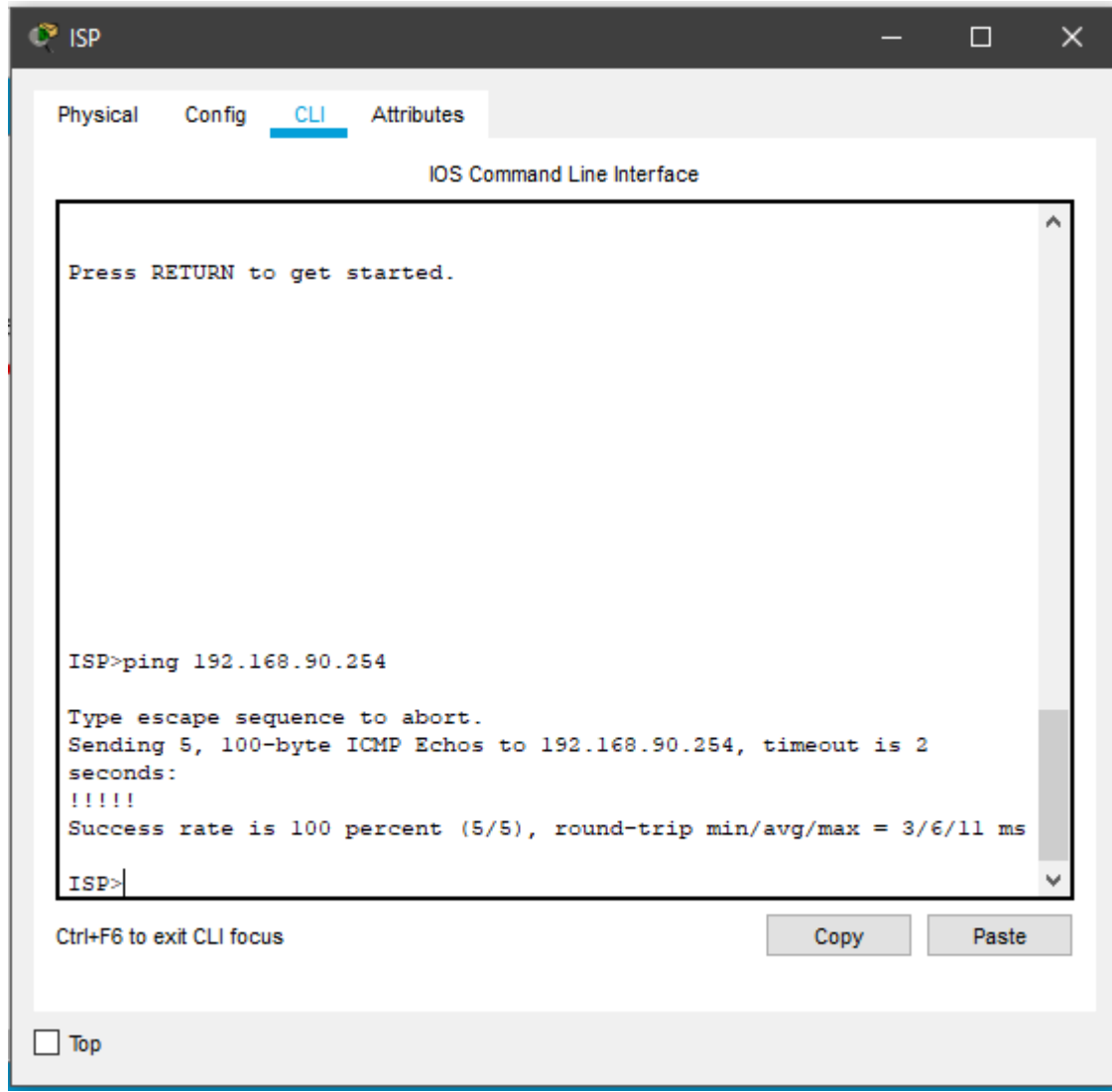
Critical Analysis / Conclusion

In this lab we learnt about Network Address Translation (NAT) configuration. It is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

Moreover, we showed two implementations on the topology, one before implementing NAT and one after implementing lab.

Lab Assessment		
Pre Lab	**/5**	
Performance	**/5**	
Results	**/5**	**/25**
Viva	**/5**	
Critical Analysis	**/5**	
Instructor Signature and Comments		