EXAMINE NETWORK ADDRESS TRANSLATION (NAT) USING CISCO PACKET TRACER

EXPT:12

INTRODUCTION

Network Address Translation (NAT) is a technique used in networking to modify network address information in IP packet headers while they are in transit. NAT allows multiple devices on a private network to access the internet using a single public IP address. It improves security by hiding internal IP addresses and helps conserve IPv4 addresses. In this experiment, Cisco Packet Tracer is used to simulate NAT and observe its behavior.
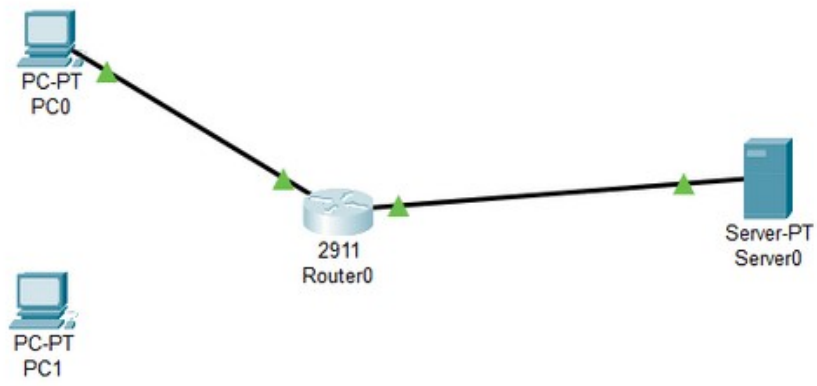
AIM

To configure and examine Network Address Translation (NAT) in a small network using Cisco Packet Tracer and observe how private IP addresses are translated to public IP addresses for internet communication.

PROCEDURE:

1. Open Cisco Packet Tracer and create a new project.

2. Set up the network topology:

    o   Add a Router, Switch, and PCs for the internal network.

    o   Add a Router simulating the ISP (public network).

3. Assign IP addresses:

    o   Configure private IP addresses for PCs (e.g., 192.168.1.2, 192.168.1.3).

    o   Assign a private IP to the internal interface of the router (e.g., 192.168.1.1).

    o   Assign a public IP to the router's external interface (e.g., 200.100.100.1).

4. Configure NAT on the Router:

    o   Go to the router CLI.

    o   Enable privileged mode:

    o   Router> enable

    o   Enter global configuration mode:

    o   Router# configure terminal

    o   Define the internal interface:

- o Router(config)# interface GigabitEthernet0/0

- o Router(config-if)# ip nat inside

- o Router(config-if)# exit

- o Define the external interface:

- o Router(config)# interface GigabitEthernet0/1

- o Router(config-if)# ip nat outside

- o Router(config-if)# exit

- o Create a NAT pool or configure PAT (Port Address Translation) / Overload:

- o Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

- o Router(config)# ip nat inside source list 1 interface GigabitEthernet0/1 overload

5. Configure default gateway on PCs pointing to the router's internal interface.

6. Test connectivity:

- o Ping the external/public IP from PCs.

- o Open the Command Prompt on a PC and ping external networks.

7. Observe NAT translation:

- o On the router, use:

- o Router# show ip nat translations

- o Router# show ip nat statistics

OUTPUT:

PC-PT
PC0

PC-PT
PC1

2911
Router0

Server-PT
Server0

```
NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [9]

NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [10]

NAT*: s=203.0.113.3, d=203.0.113.2->192.168.1.10 [1]

NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [11]

NAT*: s=203.0.113.3, d=203.0.113.2->192.168.1.10 [2]

NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [12]

NAT*: s=203.0.113.3, d=203.0.113.2->192.168.1.10 [3]

Router#show ip nat translations
Pro  Inside global     Inside local        Outside local       Outside global
icmp 203.0.113.2:10    192.168.1.10:10     203.0.113.3:10      203.0.113.3:10
icmp 203.0.113.2:11    192.168.1.10:11     203.0.113.3:11      203.0.113.3:11
icmp 203.0.113.2:12    192.168.1.10:12     203.0.113.3:12      203.0.113.3:12
icmp 203.0.113.2:9     192.168.1.10:9      203.0.113.3:9       203.0.113.3:9

Router#show ip nat statistics
NAT: expiring 203.0.113.2 (192.168.1.10) icmp 9 (9)|

NAT: expiring 203.0.113.2 (192.168.1.10) icmp 10 (10)

NAT: expiring 203.0.113.2 (192.168.1.10) icmp 11 (11)

NAT: expiring 203.0.113.2 (192.168.1.10) icmp 12 (12)

Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0 , GigabitEthernet0/2
Hits: 3  Misses: 12
Expired translations: 12
Dynamic mappings:
Router#write memory
Building configuration...
[OK]
```

```
NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [9]

NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [10]

NAT*: s=203.0.113.3, d=203.0.113.2->192.168.1.10 [1]

NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [11]

NAT*: s=203.0.113.3, d=203.0.113.2->192.168.1.10 [2]

NAT: s=192.168.1.10->203.0.113.2, d=203.0.113.3 [12]

NAT*: s=203.0.113.3, d=203.0.113.2->192.168.1.10 [3]

Router#show ip nat translations
Pro  Inside global     Inside local      Outside local      Outside global
icmp 203.0.113.2:10    192.168.1.10:10   203.0.113.3:10     203.0.113.3:10
icmp 203.0.113.2:11    192.168.1.10:11   203.0.113.3:11     203.0.113.3:11
icmp 203.0.113.2:12    192.168.1.10:12   203.0.113.3:12     203.0.113.3:12
icmp 203.0.113.2:9     192.168.1.10:9    203.0.113.3:9      203.0.113.3:9

Router#show ip nat statistics
NAT: expiring 203.0.113.2 (192.168.1.10) icmp 9 (9)|

NAT: expiring 203.0.113.2 (192.168.1.10) icmp 10 (10)

NAT: expiring 203.0.113.2 (192.168.1.10) icmp 11 (11)

NAT: expiring 203.0.113.2 (192.168.1.10) icmp 12 (12)

Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0 , GigabitEthernet0/2
Hits: 3  Misses: 12
Expired translations: 12
Dynamic mappings:
Router#write memory
Building configuration...
[OK]
```

RESULT

The experiment successfully demonstrated NAT in Cisco Packet Tracer. Internal private IP addresses were translated to a single public IP address, allowing multiple devices to access external networks while maintaining security and efficient IP address usage. The NAT translation table confirmed the correct mapping between internal and external addresses.