Name:	Yash Nilesh Kasare
Roll No:	27
Class/Sem:	TE/V
Experiment No.:	9
Title:	Perform to simulate NAT on the router using Cisco packet tracer/GNS3.
Date of Performance:	24/9/25
Date of Submission:	4/10/25
Marks:	
Sign of Faculty:	

Aim: Perform to simulate NAT on the router using Cisco packet tracer/GNS3.

Objective: Developing the understanding of NAT on the switch/router.

Theory:

Network Address Translation (NAT) is a vital network function that allows private IP addresses to be translated into public IP addresses. This process enables devices within a private network to communicate with external networks, such as the internet, while conserving global IP address space and providing a layer of security. Tools like Cisco Packet Tracer and GNS3 are excellent for simulating NAT configurations, providing a practical environment to understand and apply NAT in network scenarios.

Understanding NAT

NAT modifies the IP address information in the headers of IP packets while they are in transit across a traffic routing device. The primary functions of NAT include:

1. **IP Address Conservation**: By allowing multiple devices on a local network to be mapped to a single public IP address, NAT conserves the limited number of available IP addresses.
2. **Security**: NAT helps protect the internal network by hiding internal IP addresses from external networks.
3. **Flexibility**: NAT allows for internal network restructuring without needing changes to the external IP address scheme.

There are several types of NAT, including Static NAT, Dynamic NAT, and Port Address Translation (PAT), also known as Overloading.

Tools for Simulation

Cisco Packet Tracer: Cisco Packet Tracer is a network simulation tool developed by Cisco. It is widely used for learning networking concepts and practicing configurations in a controlled, virtual environment.

GNS3 (Graphical Network Simulator-3): GNS3 is an open-source network software emulator that provides a more realistic and advanced simulation environment. It allows for the use of real Cisco IOS images, making it suitable for professional network engineers preparing for certifications or managing complex network designs. **Setting Up NAT Using Cisco Packet Tracer**

1. **Create a New Project**:

- Open Cisco Packet Tracer and start a new project.
- Add the necessary devices to the workspace, including routers, switches, and end devices (e.g., PCs).

2. **Design the Network Topology**:

- Connect the devices using appropriate network cables.
- Configure IP addressing schemes for the internal network and the external network (e.g., the internet).

3. **Configure Router Interfaces**:
   - Access the router's configuration interface.
   - Assign IP addresses to the router interfaces. Typically, one interface will be connected to the internal network (inside) and another to the external network (outside).
4. **Configure NAT on the Router**:
   - Define the inside and outside interfaces on the router.
   - Configure the NAT rules. For example, for PAT, you would specify the range of internal IP addresses that will be translated and the single public IP address they will be translated to.
   - Set up any necessary access control lists (ACLs) to permit traffic that will be translated.
5. **Verify Configuration**:
   - Use tools within Packet Tracer to test connectivity. Ensure that devices in the internal network can communicate with external networks.
   - Verify the NAT translations using appropriate commands to ensure the internal addresses are being translated correctly. **Setting Up NAT Using GNS3**

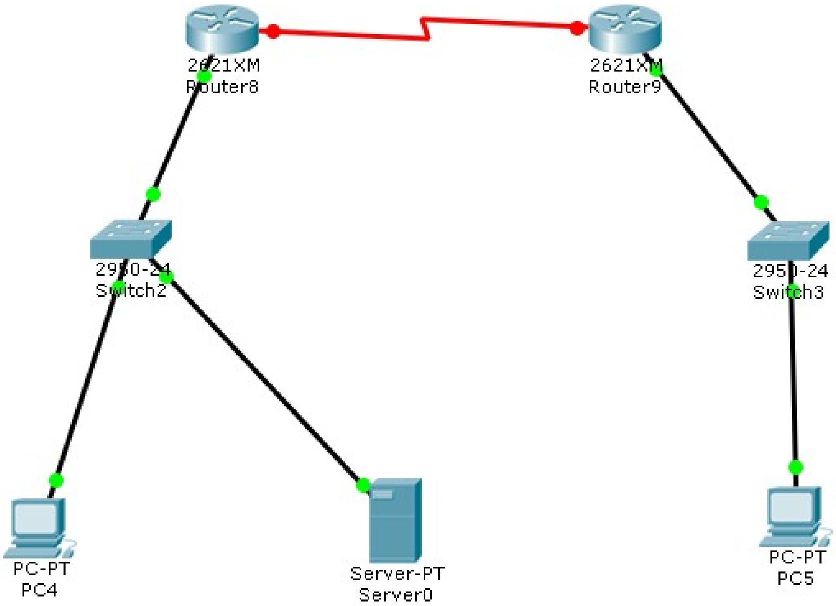
1. **Create a New Project**:
   - Open GNS3 and start a new project.
   - Add routers, switches, and other necessary devices to the workspace.
2. **Design the Network Topology**:
   - Connect the devices using virtual network cables.
   - Plan the IP addressing schemes for both the internal network and the external network.
3. **Import Cisco IOS Images**:
   - Use real Cisco IOS images to ensure a realistic simulation environment.
   - Assign these images to the virtual routers in your topology.
4. **Configure Router Interfaces**:
   - Start each router and access its CLI.
   - Assign IP addresses to the router interfaces, designating one as the inside interface and another as the outside interface.

5. **Configure NAT on the Router**:
   - Define the inside and outside interfaces.
   - Set up NAT rules, such as dynamic NAT, static NAT, or PAT.
   - Configure ACLs if necessary to control which traffic is subject to NAT.
6. **Verify Configuration**:
   - Use diagnostic tools and commands to test connectivity and ensure proper translation.
   - Verify that internal devices can access external networks and that NAT translations are occurring as expected.

Practical Applications and Benefits

1. **Address Conservation**:
   - NAT allows multiple devices on a private network to share a single public IP address, reducing the need for a large number of public IP addresses.
2. **Security**:
   - By hiding internal IP addresses, NAT adds a layer of security, making it more difficult for external attackers to target internal network devices.
3. **Network Flexibility**:
   - NAT allows internal network configurations to change without affecting the external IP addressing scheme. This flexibility is crucial for network scalability and management.
4. **Connectivity**:
   - NAT enables devices within a private network to communicate with external networks, facilitating internet access and external communications.

Output:


2621XM
Router8
2621XM
Router9
2950-24
Switch2
2950-24
Switch3
PC-PT
PC4
Server-PT
Server0
PC-PT
PC5

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.5: bytes=32 time=1ms TTL=126
Reply from 192.168.3.5: bytes=32 time=0ms TTL=126
Reply from 192.168.3.5: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.3.7

Pinging 192.168.3.7 with 32 bytes of data:

Reply from 192.168.3.7: bytes=32 time=0ms TTL=126
Reply from 192.168.3.7: bytes=32 time=0ms TTL=126
Reply from 192.168.3.7: bytes=32 time=0ms TTL=126
Reply from 192.168.3.7: bytes=32 time=0ms TTL=126

Ping statistics for 192.168.3.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

```
Router(config-if)#exit
Router(config)#interface Serial0/2
Router(config-if)#ip address 192.162.10.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/2, changed state to down
Router(config-if)#exit
Router(config)#ip nat inside source static 10.10.10.2 50.50.50.2
Router(config)#ip nat inside source static 10.10.10.3 50.50.50.3
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 0/2
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip route 60.0.0.0 255.0.0.0 192.162.10.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
Router#
```

```
Router(config-if)#exit
Router(config)#interface Serial0/2
Router(config-if)#ip address 192.162.10.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/2, changed state to down
Router(config-if)#exit
Router(config)#ip nat inside source static 10.10.10.2 50.50.50.2
Router(config)#ip nat inside source static 10.10.10.3 50.50.50.3
Router(config)#interface FastEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 0/2
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip route 60.0.0.0 255.0.0.0 192.162.10.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    10.0.0.0/8 is directly connected, FastEthernet0/0
Router#
```

Conclusion

Simulating NAT using Cisco Packet Tracer and GNS3 provides invaluable practical experience for network engineers and students. These tools offer a realistic environment to study and apply NAT configurations, ensuring that users can design, configure, and troubleshoot NAT implementations effectively. Mastering NAT in these simulated environments enhances one's ability to manage and secure real-world networks, providing a strong foundation for efficient and scalable network design.