Lab 9: Configuration of Network address translation in Cisco packet tracer

Learning outcome:

- Learners will gain a solid understanding of Network Address Translation and its role in IP address translation between private and public networks.
- Learners will acquire hands-on experience in configuring different types of NAT in Cisco Packet Tracer.

Network Address Translation (NAT) is a technique used to translate private IP addresses to public IP addresses, allowing multiple devices on a local network to share a single public IP address for accessing the internet. Here's how to configure NAT on a Cisco router using Cisco Packet Tracer.

Step-by-Step Guide to Configuring NAT

Step 1: Set Up the Network Topology

1. **Add Devices**: Place a router, a switch, and multiple PCs in the workspace.
2. **Connect Devices**: Connect the PCs to the switch, and then connect the switch to the router's LAN interface. Connect the router's WAN interface to a simulated internet cloud or another router representing the ISP.

Step 2: Configure IP Addresses

1. **Assign IP Addresses to PCs**:
   - PC1: IP Address: 192.168.1.2, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.1
   - PC2: IP Address: 192.168.1.3, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.1
2. **Configure the Router's LAN Interface**:
   Router> enable
   Router# configure terminal
   Router(config)# interface gigabitEthernet 0/0
   Router(config-if)# ip address 192.168.1.1 255.255.255.0
   Router(config-if)# no shutdown
   Router(config-if)# exit
3. **Configure the Router's WAN Interface**:
   Router(config)# interface gigabitEthernet 0/1
   Router(config-if)# ip address 200.200.200.1 255.255.255.0
   Router(config-if)# no shutdown
   Router(config-if)# exit

Step 3: Configure the Default Route

Router(config)# ip route 0.0.0.0 0.0.0.0 200.200.200.2

.

Step 4: Configure NAT

1. **Define Inside and Outside Interfaces**:
   Router(config)# interface gigabitEthernet 0/0
   Router(config-if)# ip nat inside
   Router(config-if)# exit

   Router(config)# interface gigabitEthernet 0/1
   Router(config-if)# ip nat outside
   Router(config-if)# exit
2. **Configure the Access Control List (ACL)**:
   Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
3. **Configure NAT Overload (PAT)**:
   Router(config)# ip nat inside source list 1 interface gigabitEthernet 0/1 overload

Step 5: Verify Configuration

1. **Check NAT Translations**:
   Router# show ip nat translations
2. **Check NAT Statistics**:
   Router# show ip nat statistics

Testing the Configuration

1. **Ping an External IP Address from a PC**:
   - Open the command prompt on PC1.
   - Execute the following command to ping an external IP address (e.g., 8.8.8.8):

     ping 8.8.8.8
   - If NAT is configured correctly, you should receive replies.
2. **Check the NAT Translation Table on the Router**:
   Router# show ip nat translations

Example Configuration Summary

Here is a summarized version of the configurations:

Router Configuration:

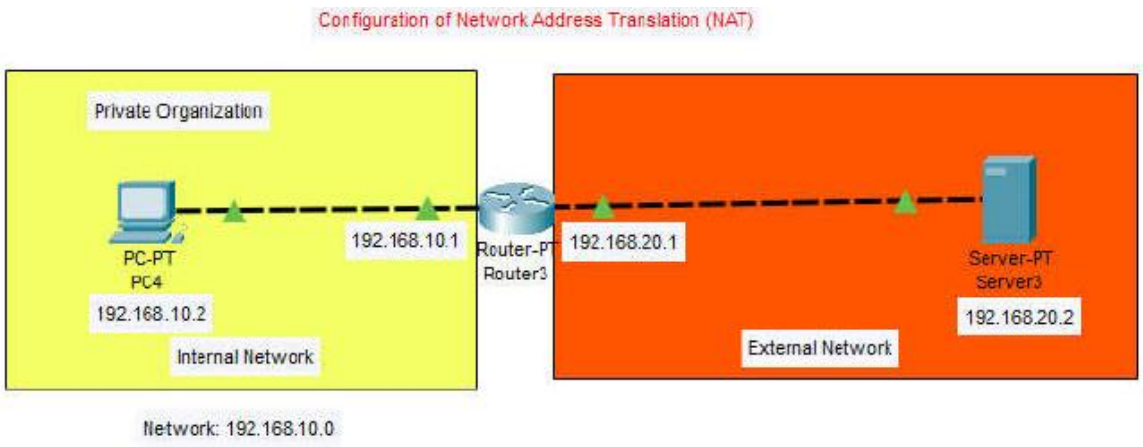
```
enable
configure terminal

interface gigabitEthernet 0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 no shutdown
 exit
interface gigabitEthernet 0/1
 ip address 200.200.200.1 255.255.255.0
 ip nat outside
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 200.200.200.2
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface gigabitEthernet 0/1 overload
end
write memory
```

PC Configuration:

- **PC1**:
  - IP Address: 192.168.1.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.1.1
- **PC2**:
  - IP Address: 192.168.1.3
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 192.168.1.1

By following these steps, you will have successfully configured NAT on a Cisco router using Cisco Packet Tracer, allowing devices on the local network to share a single public IP address for internet access.

Configuration of Static Network Address Translation (NAT)



Static NAT Configuration

```
Router(config)#int f0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int f1/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)# ip nat inside source static 192.168.10.2 100.100.100.100
Router(config)#exit
Router# debug ip nat
```

Configuration for PCs

PC4 IP Address: 192.168.10.2 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.10.1
Server3 IP Address: 192.168.20.2 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.20.1

Configuration for Routers

Fast Ethernet Port Configuration
Router 2 Router>en Router#config t Router(config)# int f0/0 Router(config-if)# ip address 192.168.10.1 255.255.255.0 Router(config-if)# no shut Router(config-if)#exit Router(config)# int f1/0 Router(config-if)# ip address 192.168.20.1 255.255.255.0 Router(config-if)# no shut
RIP Configuration
Router 2 Router#config t Router(config)# router rip Router(config-router)# network 192.168.10.0 Router(config-router)# network 192.168.20.0

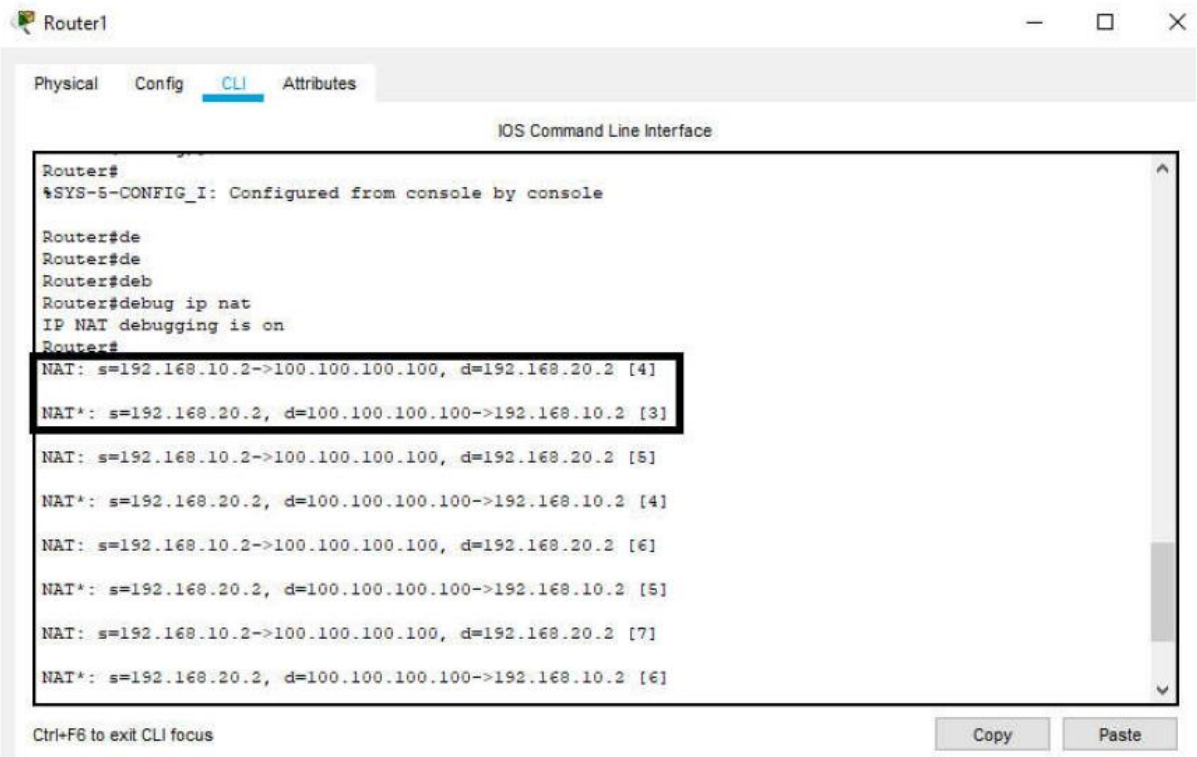
Output

To check whether the NAT configuration is running properly lets go to the Router and enable the NAT by giving the command "debug ip nat"

Then go to the command prompt of the PC4 and give the following command

C:\> ping 192.168.20.2

The output is as follows which means the conversion of private IP to public IP is successful.
The private IP -> 192.168.10.2 has been converted to the public IP -> 100.100.100.100



Conclusion

By following these steps, we successfully configured static NAT on a Cisco router using Cisco Packet Tracer. The process involved:

- Setting up the network topology with appropriate device connections.
- Assigning IP addresses to both LAN and WAN interfaces.
- Defining inside and outside NAT interfaces.
- Configuring static NAT to map a private internal IP to a specific public external IP.
- Verifying the configuration and testing connectivity to ensure proper operation.

Configuring static NAT is essential for scenarios where a device inside the private network needs to be accessible from the outside world using a fixed public IP address. This ensures that services such as web servers and other applications remain reachable and provide consistent service. Properly implemented static NAT enhances network functionality, enabling seamless communication between private internal networks and external public networks.

Lab 10: Configure the Standard and Extended Access Control List using cisco packet tracer and verify the configuration

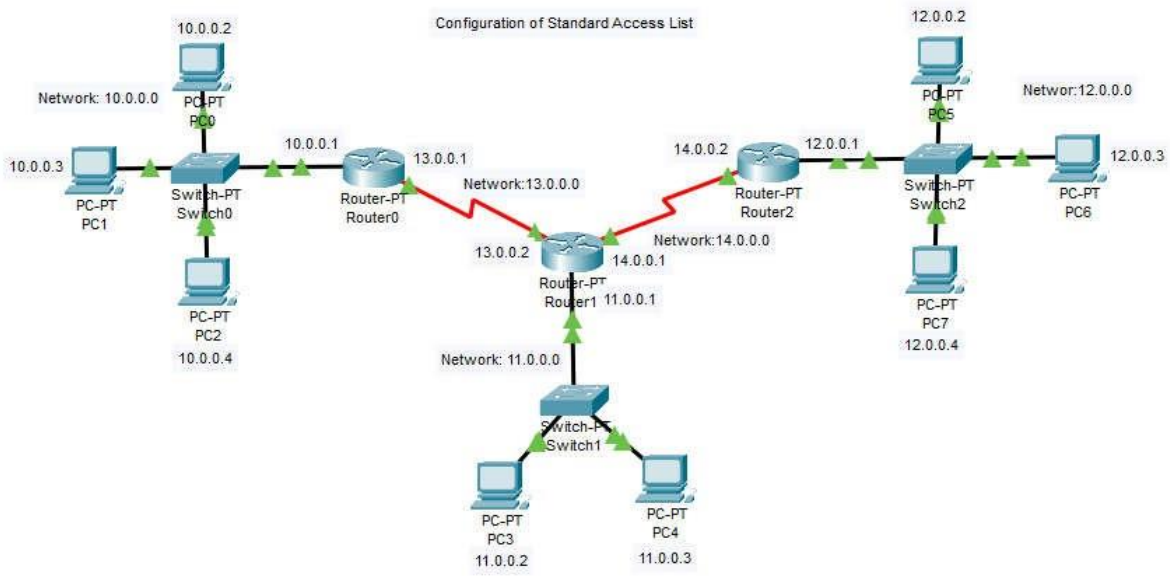
Learning outcome:

- Learn how to access and navigate Cisco Packet Tracer and Cisco IOS for configuration tasks.
- Gain hands-on experience in creating Standard ACLs using source IP addresses.
- Acquire skills in creating Extended ACLs with criteria including source and destination IP addresses, protocols, and port numbers.
- Apply Standard and Extended ACLs to network interfaces in both inbound and outbound directions.
- Understand the implications of applying ACLs in different directions on network traffic.

- **Configuration of Standard Access List**

- **PC0(10.0.0.2),**
- **PC1(10.0.0.3) and**
- **the network (12.0.0.0) from accessing the network**
- **11.0.0.0**

Network Topology



- **Configuration for PCs**

PC0	**PC1**	**PC2**
IP Address: 10.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1	IP Address: 10.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1	IP Address: 10.0.0.4 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1

PC3 IP Address: 11.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 11.0.0.1	**PC4** IP Address: 11.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 11.0.0.1	
PC5 IP Address: 12.0.0.2 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1	**PC6** IP Address: 12.0.0.3 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1	**PC7** IP Address: 12.0.0.4 Subnet Mask: 255.0.0.0 Default Gateway: 12.0.0.1

-
-
- **Configuration for Routers**

Fast Ethernet Port Configuration		
Router0 Router>en Router#hostname R1 R1#config t R1(config)# int f0/0 R1(config-if)# ip address 10.0.0.1 255.0.0.0 R1(config-if)# no shut	**Router1** Router>en Router#hostname R2 R2#config t R2(config)# int f0/0 R2(config-if)# ip address 11.0.0.1 255.0.0.0 R2(config-if)# no shut	**Router2** Router>en Router#hostname R3 R2#config t R2(config)# int f0/0 R2(config-if)# ip address 12.0.0.1 255.0.0.0 R2(config-if)# no shut
Serial Port Configuration		
Router0 R1#config t R1(config)# int s2/0 R1(config-if)# ip address 13.0.0.1 255.0.0.0 R1(config-if)# no shut	**Router1** R2#config t R2(config)# int s2/0 R2(config-if)# ip address 13.0.0.2 255.0.0.0 R2(config-if)# no shut R2(config-if)#exit R2(config)# int s3/0 R2(config-if)# ip address 14.0.0.1 255.0.0.0 R2(config-if)# no shut	**Router2** R2#config t R2(config)# int s2/0 R2(config-if)# ip address 14.0.0.2 255.0.0.0 R2(config-if)# no shut
Routing Protocol Configuration		
Router0 R1#config t R1(config)# router rip R1(config-router)# network 10.0.0.0 R1(config-router)# network 13.0.0.0	**Router1** R2#config t R2(config)# router rip R2(config-router)# network 11.0.0.0 R2(config-router)# network 13.0.0.0 R2(config-router)# network 14.0.0.0	**Router2** R2#config t R2(config)# router rip R2(config-router)# network 12.0.0.0 R2(config-router)# network 14.0.0.0
Standard Access List Configuration		

Router1

```
R1#config t
R1(config)# access-list 10 deny 10.0.0.2 0.0.0.0
R1(config)#  access-list 10 deny host 10.0.0.3
R1(config)#  access-list 10 deny 12.0.0.0 0.0.0.255
R1(config)#  access-list 10 permit any
R1(config)# int f0/0
R1(config-if)#  ip access-group 10 out
```

-
- **Output**
- To check whether the standard access list is working properly or not, we ping the PC3(11.0.0.2) from the PC0 (10.0.0.2) which had been blocked and we get the following result.
- **Pinging from 10.0.0.2(PC0)**

```
C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.
Reply from 13.0.0.2: Destination host unreachable.

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

-
- **Pinging from 10.0.0.2(PC2)**
- Again we ping the PC3(11.0.0.2) from the PC2 (10.0.0.4) which had not been blocked and we get the following result.
-

```
C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Reply from 11.0.0.2: bytes=32 time=1ms TTL=126
Reply from 11.0.0.2: bytes=32 time=12ms TTL=126
Reply from 11.0.0.2: bytes=32 time=4ms TTL=126
Reply from 11.0.0.2: bytes=32 time=13ms TTL=126

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 7ms
```

-
- **Pinging from 12.0.0.3(PC6)**
- Again we ping the PC3(11.0.0.2) from the PC5 (12.0.0.2) which had been blocked and we get the following result.

```
C:\>ping 11.0.0.2

Pinging 11.0.0.2 with 32 bytes of data:

Reply from 14.0.0.1: Destination host unreachable.
Reply from 14.0.0.1: Destination host unreachable.
Reply from 14.0.0.1: Destination host unreachable.
Reply from 14.0.0.1: Destination host unreachable.

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

-