Practical 7: Static and Dynamic NAT

Practical Title: Implement Static and Dynamic NAT using a router.

Aim: To configure and verify both Static and Dynamic NAT (Network Address Translation) on a Cisco router to allow devices on a private network to access the internet.

Objective:

- To understand the purpose of NAT.
- To configure Static NAT to map a private IP to a public IP.
- To configure Dynamic NAT to allow multiple private IPs to share a pool of public IPs.
- To verify the NAT translation using the show command.

Theory: **Network Address Translation (NAT)** is a process that translates private IP addresses into public IP addresses. This is essential for conserving public IP addresses and for security. **Static NAT** creates a one-to-one mapping between a private IP and a public IP, which is useful for servers. **Dynamic NAT** translates multiple private IP addresses to a pool of public IP addresses, allowing multiple devices to share a smaller number of public IPs.

Steps:

1. **Create the Network Topology:**
   - Open Cisco Packet Tracer.

   ○ Create a topology with a private LAN (PC, Switch, Router) and connect the router to a "Cloud" (representing the internet) and then to a web server. ○ The router will act as the NAT device.
2. **Assign IP Addresses:**
   - **Private LAN:**
     - PC: 192.168.1.10, Subnet Mask 255.255.255.0, Default Gateway 192.168.1.1
     - Router (FastEthernet0/0): 192.168.1.1, Subnet Mask 255.255.255.0
   - **Public Network (Cloud to Server):**
     - Router (FastEthernet0/1): 209.165.200.225, Subnet Mask 255.255.255.224
     - Server: 209.165.200.226, Subnet Mask 255.255.255.224
3. **Configure Static NAT:**
   - **On the Router:**
     - Set the inside and outside interfaces: interface fastethernet 0/0 > ip nat inside, interface fastethernet 0/1 > ip nat outside.
     - Create the static mapping: ip nat inside source static 192.168.1.10 209.165.200.227
4. **Configure Dynamic NAT (alternative to Static NAT):** ○ **On the Router:**

- ■ Define the private IP address range: access-list 1 permit 192.168.1.0 0.0.0.255
- ■ Define the public IP address pool: ip nat pool public-ips 209.165.200.228 209.165.200.229 netmask 255.255.255.224
- ■ Create the dynamic mapping: ip nat inside source list 1 pool public-ips overload

5. **Verify NAT:**
   - ○ From the PC, ping the public server (ping 209.165.200.226).
   - ○ On the router, use the command show ip nat translations to view the active NAT mappings.

Conclusion: This practical successfully demonstrated the implementation of both Static and Dynamic NAT. We were able to translate private IP addresses into public ones, allowing a device on a private network to communicate with a public server, showcasing the essential role of NAT in modern networks.

Viva / Oral Questions:

1. What is the primary function of NAT?
2. What is the difference between Static NAT and Dynamic NAT?
3. What is NAT Overload (PAT), and why is it important? 4. How does NAT help to conserve public IP addresses?

5. What are the inside and outside interfaces in NAT configuration?

CLI COMMANDS

On Router 0:

```
Router(config-if)#interface fa0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 20.20.20.1 255.0.0.0
Router(config-if)#ip nat outside
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip nat inside source static 10.1.1.10 203.0.113.100
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#ip nat pool PUB_POOL 203.0.113.110 203.0.113.111 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool PUB_POOL overload
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
```

On Router 1:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface se2/0
Router(config-if)#ip address 20.20.20.2 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fa0/0
Router(config-if)#ip address 203.0.113.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
```

VERIFY CONNECTIVITY:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.10

Pinging 10.1.1.10 with 32 bytes of data:


Reply from 10.1.1.10: bytes=32 time=21ms TTL=128
Reply from 10.1.1.10: bytes=32 time=4ms TTL=128
Reply from 10.1.1.10: bytes=32 time=5ms TTL=128
Reply from 10.1.1.10: bytes=32 time<1ms TTL=128


Ping statistics for 10.1.1.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 21ms, Average = 7ms


C:\>ping 10.1.1.11
```

```
Pinging 10.1.1.11 with 32 bytes of data:

Reply from 10.1.1.11: bytes=32 time<1ms TTL=128
Reply from 10.1.1.11: bytes=32 time<1ms TTL=128
Reply from 10.1.1.11: bytes=32 time<1ms TTL=128
Reply from 10.1.1.11: bytes=32 time=1ms TTL=128

Ping statistics for 10.1.1.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```