**Static Network Address Translation (NAT)**

**Intended Learning Outcome:**a. To understand the properties of NAT router.  
b. To analyze how statically NAT router is configured for translating the private addresses to public addresses.

**Expected skills:**The basic concepts of Private and Public IP address and Subnet mask.   
  
**Tools Required :**Packet Tracer  
  
**Session Detail:**

A web server connected with Router 1. Web server is using the IP address 10.0.0.2. But company wants to use 50.0.0.1 IP address for this server. Now the task is to configure NAT on Router 1 which translate 10.0.0.2 [inside local web server address] to 50.0.0.1 [inside global ip address].

**Router 1:**

Router>enable

Router#configure terminal

Router(config)#hostname R1

R1(config)#interface fastethernet 0/0

R1(config-if)#ip address 10.0.0.1 255.0.0.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#interface serial 2/0

R1(config-if)#ip address 20.0.0.2 255.0.0.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.1

R1(config)#ip nat inside source static 10.0.0.2 50.0.0.1

R1(config)#interface fastEthernet 0/0

R1(config-if)#ip nat inside

R1(config-if)#exit

R1(config)#interface serial 2/0

R1(config-if)#ip nat outside

R1(config-if)#exit

**Router 0:**

Router>enable

Router#configure terminal

Router(config)#hostname R0

R0(config)#interface fastethernet 0/0

R0(config-if)#ip address 30.0.0.1 255.0.0.0

R0(config-if)#no shutdown

R0(config-if)#exit

R0(config)#interface serial 2/0

R0(config-if)#ip address 20.0.0.1 255.0.0.0

R0(config-if)#clock rate 64000

R0(config-if)#bandwidth 64

R0(config-if)#no shutdown

R0(config-if)#exit

R0(config)#ip route 50.0.0.0 255.0.0.0 20.0.0.2

R0(config)#

As you have seen in configuration there is not direct route for 10.0.0.2. So PC from network of 30.0.0.0 will never know about it. They will access 50.0.0.1 as the web server IP. To test it double click on any computer and ping from 50.0.0.1 and you will get replay.

Packet Tracer PC Command Line 1.0

PC>ping 50.0.0.1

Pinging 50.0.0.1 with 32 bytes of data:

Reply from 50.0.0.1: bytes=32 time=141ms TTL=126

Reply from 50.0.0.1: bytes=32 time=80ms TTL=126

Reply from 50.0.0.1: bytes=32 time=109ms TTL=126

Reply from 50.0.0.1: bytes=32 time=125ms TTL=126

Ping statistics for 50.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 80ms, Maximum = 141ms, Average = 113ms

Now ping from 10.0.0.2 and you will get destination host unreachable error.

PC>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 30.0.0.1: Destination host unreachable.

Reply from 30.0.0.1: Destination host unreachable.

Reply from 30.0.0.1: Destination host unreachable.

Reply from 30.0.0.1: Destination host unreachable.

Ping statistics for 10.0.0.2:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

This demonstration show how the companies use NAT to hide their internal network from the outside of the world. Now open web browser from any PC in 30.0.0.0 network and brows the 50.0.0.1 site.

As you can see in image you can easily access the 50.0.0.1



**Post Lab Exercise:** Configuration of Dynamic NAT for the same topology.