PRACTICAL-6

AIM:

Demonstrate the static and dynamic configuration of NAT using cisco packet tracer

THEORY:

- NAT stands for “Network Address Translation”.
- A Network Address Translation (NAT) is the process of mapping an internet protocol (IP) address to another by changing the header of IP packets while in transit via a router.
- This helps to improve security and decrease the number of IP addresses an organization needs.
- Usually a firewall, assigns a public address to a computer (or group of computers) inside a private network.
- The most common form of network translation involves a large private network using addresses in a private range
- The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers.
- Routers inside the private network can route traffic between private addresses with no trouble.

- However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.

- It is suitable only for small network.

- If a link fails it cannot reroute the traffic.

- There are three types of address translation.

    - Static NAT – translates one private IP address to a public one. The public IP address is always the same.

    - Dynamic NAT – private IP addresses are mapped to the pool of public IP addresses.

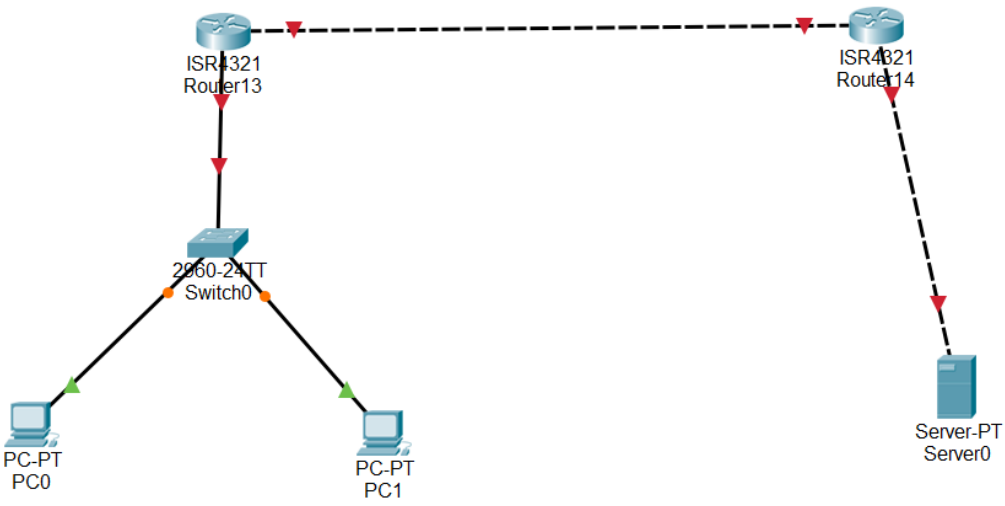
    - Port Address Translation (PAT)– one public IP address is used for all internal devices, but a different port is assigned to each private IP address. Also known as NAT Overload.

PRACTICAL IMPLEMENTATION:

STATIC NAT:

- Firstly, create a topology shown in the picture below by connecting the devices through appropriate connections.

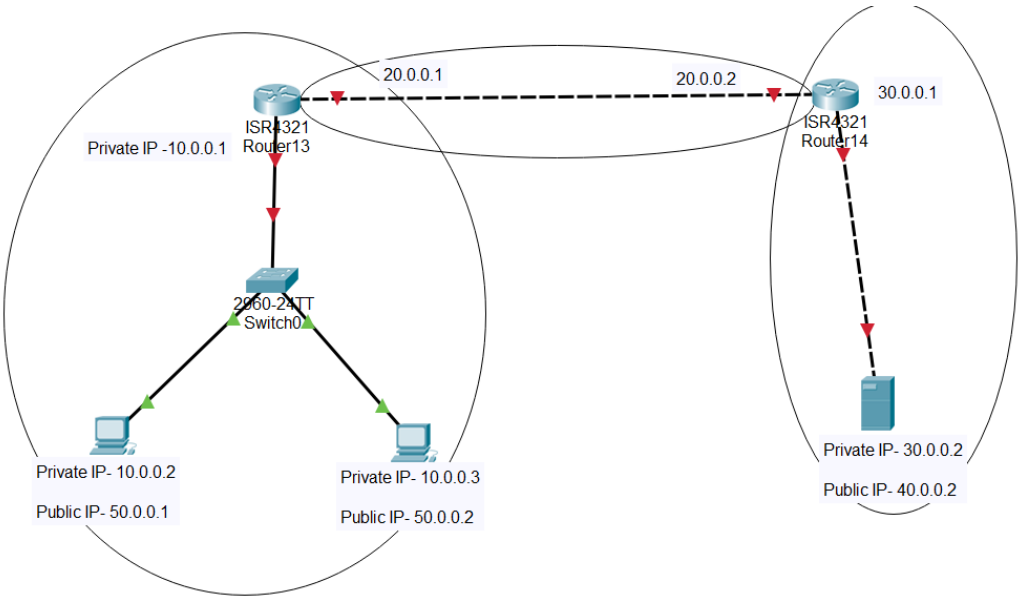
- For the topology, we will use 2 routers,2 PCs, 1 switch, and 1 server.



- Now, we will divide the topology into 3 networks.

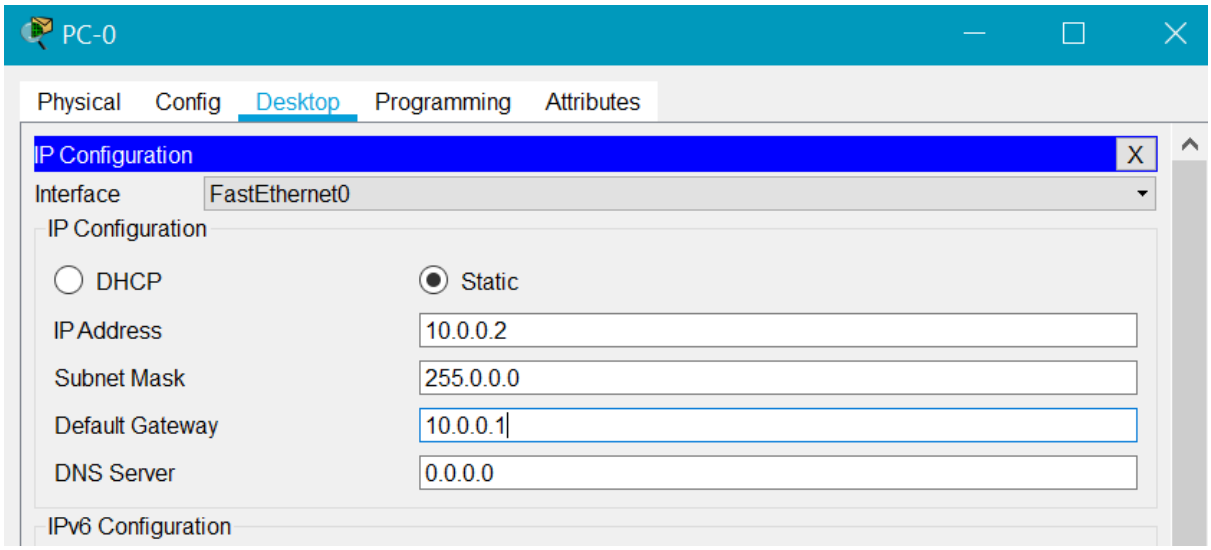
- Also, we will assign private and public IP addresses to each end devices and gateways.

- Topology will now look like the below image.



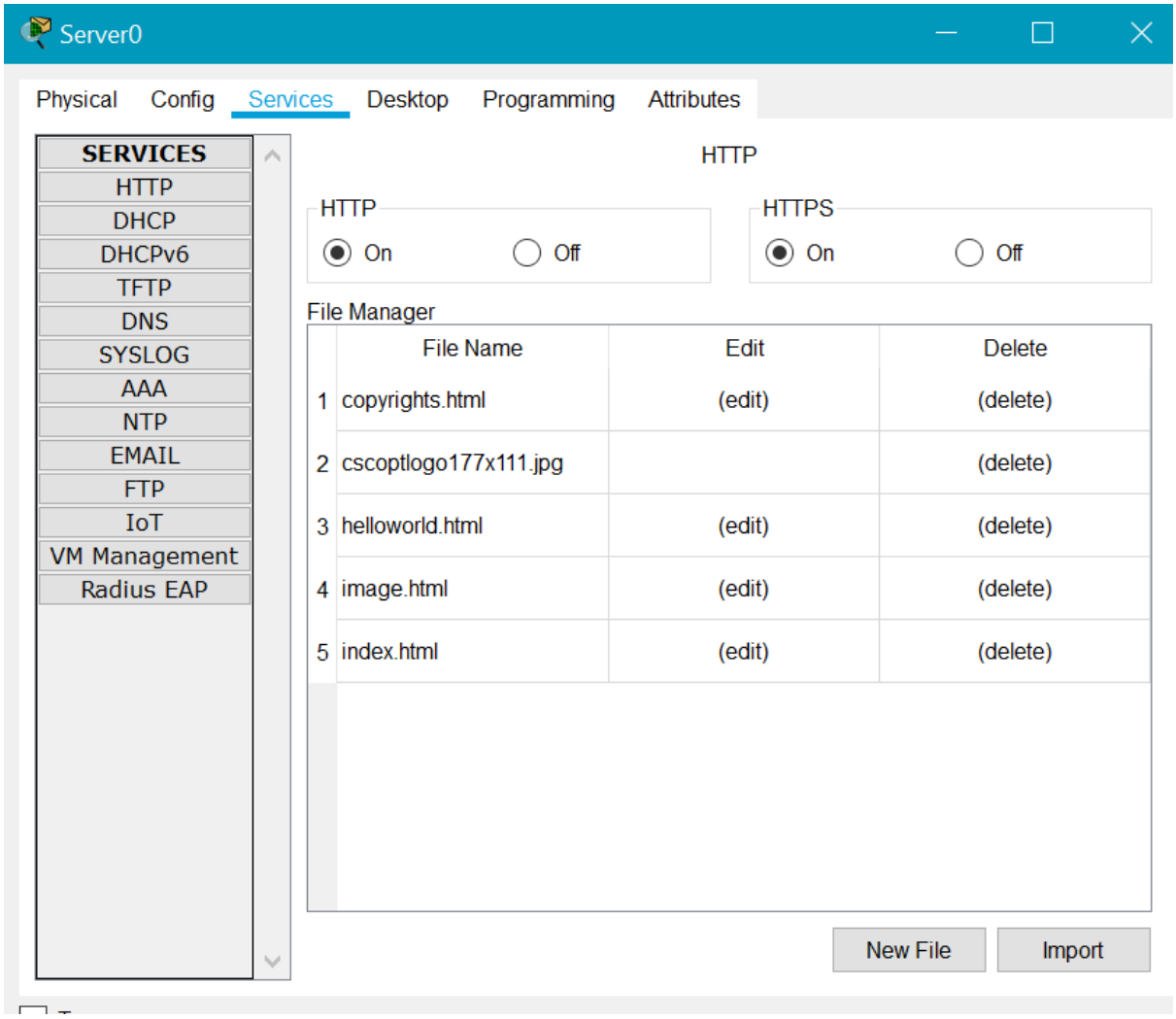
- Now, assign Private IP address to the end devices.

- Steps are: PC -> IP configuration -> Enter the IP address and Gateway.

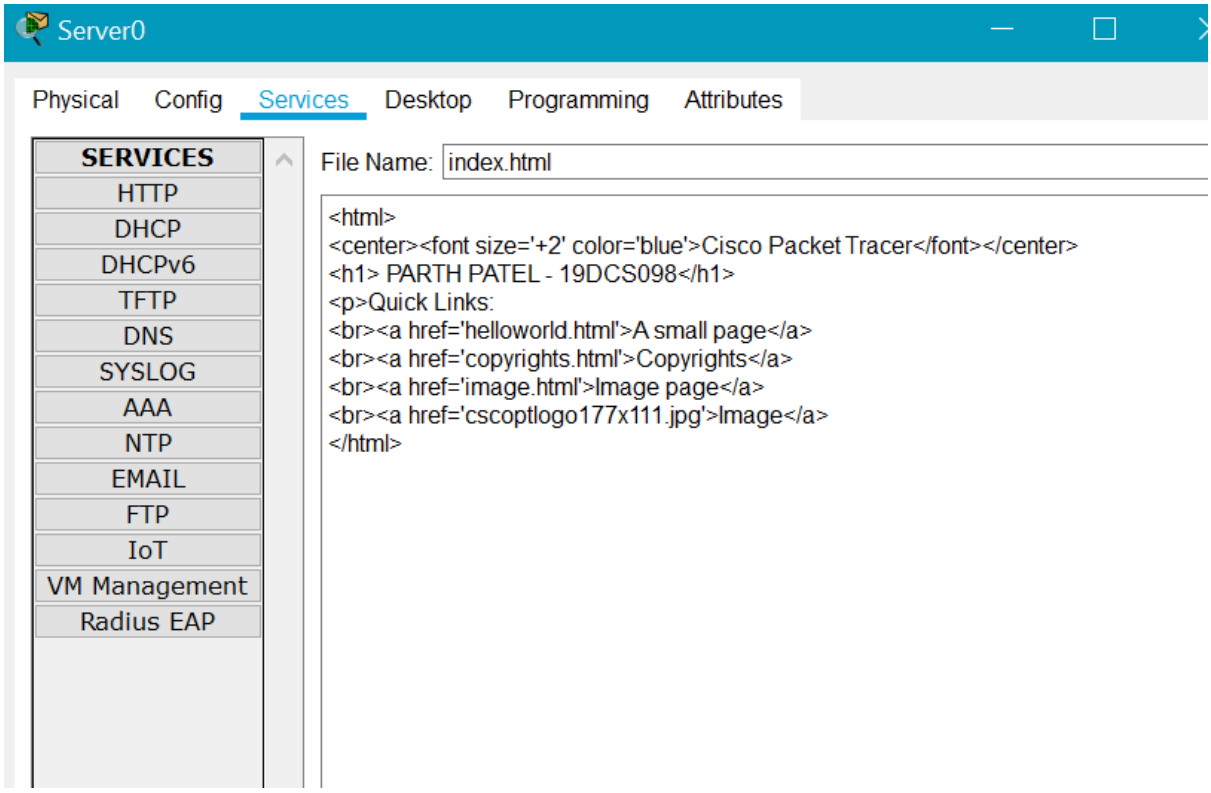


- Perform the same steps for all the PCs.

❖ In server services, we will select the HTTP option.



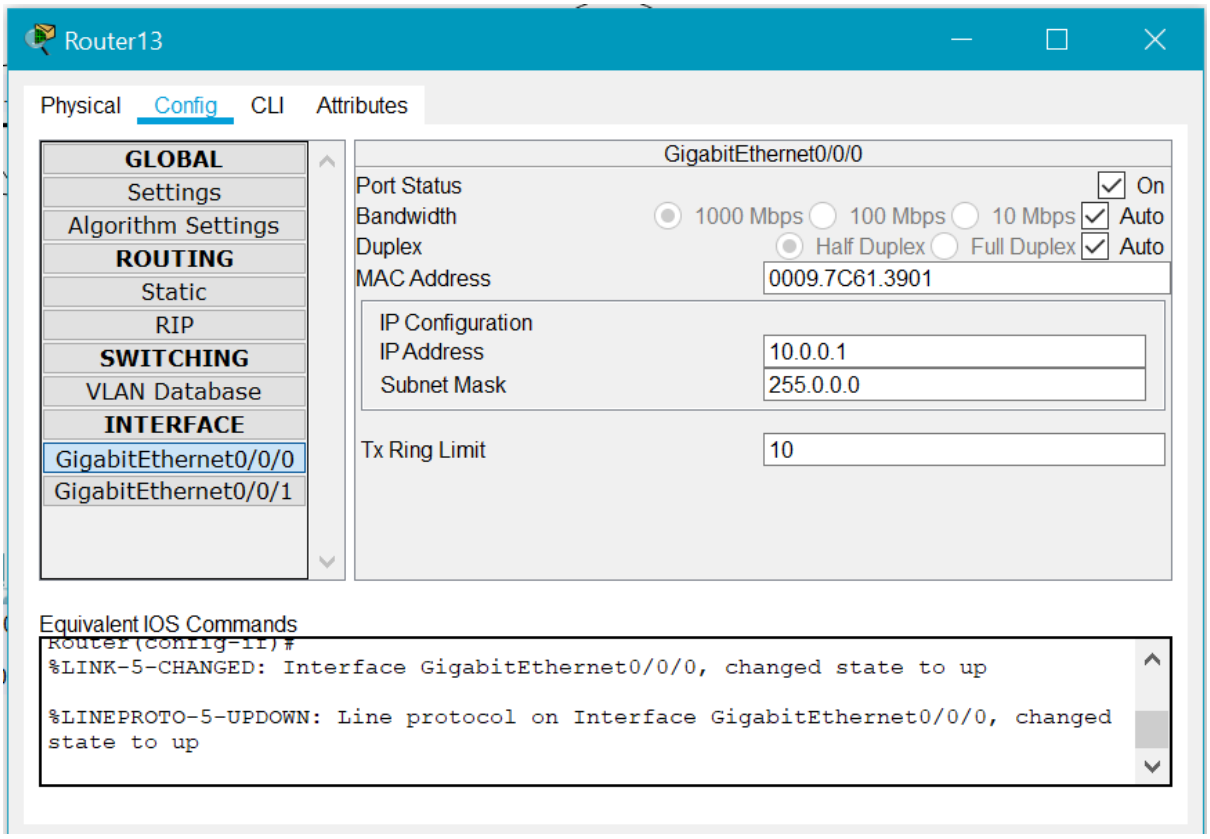
- Now, make some changes in index.html.



- Now, configure the router.

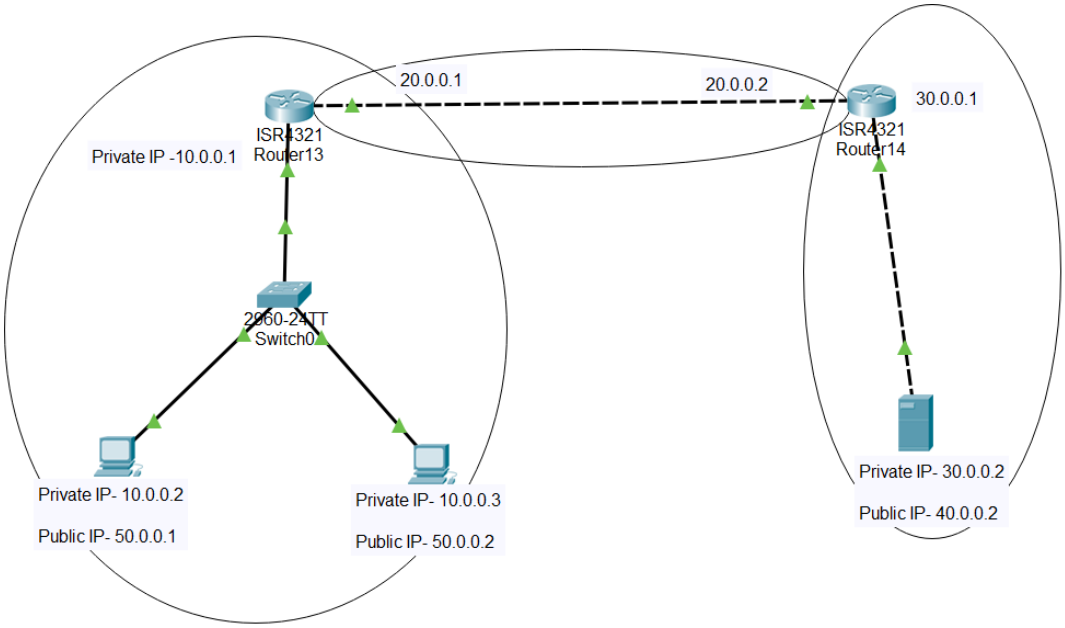
- This time, we will use config mode instead of CLI mode.

- For this method, Go to Config tab -> enter the IP address and check the On option.



- Perform the same steps for all the connections.

- Upon successful connection establishment, the Topology will look like the below image.



- Now, we will do the mapping of private and public IP address in Router.

- The above step will enable the router to know which public IP is mapped to its corresponding private IP.

```
Router(config-if)#exit
Router(config)#ip nat inside source static 10.0.0.2 50.0.0.1
Router(config)#ip nat inside source static 10.0.0.3 50.0.0.2
```

- This will let the router know the mappings of public and private IP.

```
Router(config)#int gigabitEthernet 0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
```

```
Router(config)#int gigabitEthernet 0/0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
```

- Follow the same steps for other router.

- Now we will do static routing configuration.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.2
```

- Perform the similar steps in other router.

NETWORK TESTING:

PING TEST:

```
Packet Tracer PC Command Line 1.0
C:\>ping 40.0.0.1

Pinging 40.0.0.1 with 32 bytes of data:

Reply from 40.0.0.1: bytes=32 time=14ms TTL=126
Reply from 40.0.0.1: bytes=32 time=27ms TTL=126
Reply from 40.0.0.1: bytes=32 time=14ms TTL=126
Reply from 40.0.0.1: bytes=32 time=27ms TTL=126

Ping statistics for 40.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 27ms, Average = 20ms
```

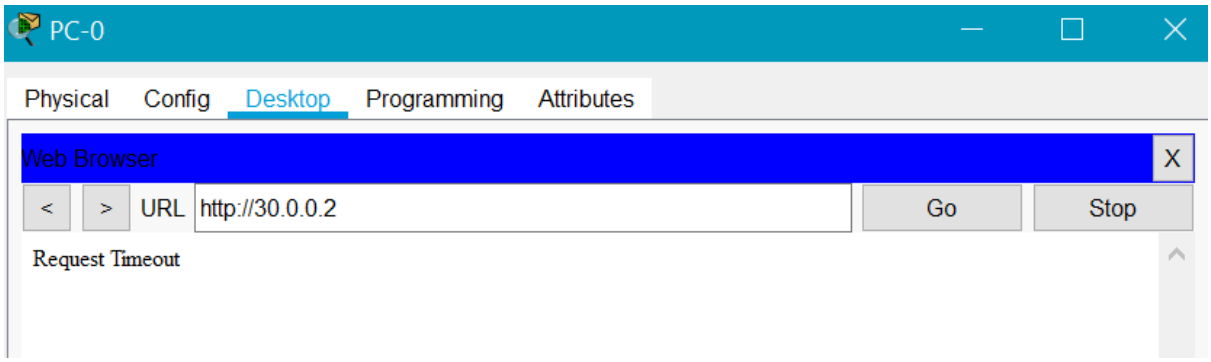
We can ping the server using public IP address

```
C:\>ping 30.0.0.2

Pinging 30.0.0.2 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Request timed out.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.

Ping statistics for 30.0.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

We cannot ping the server using private IP address.

TESTING USING BROWSER:

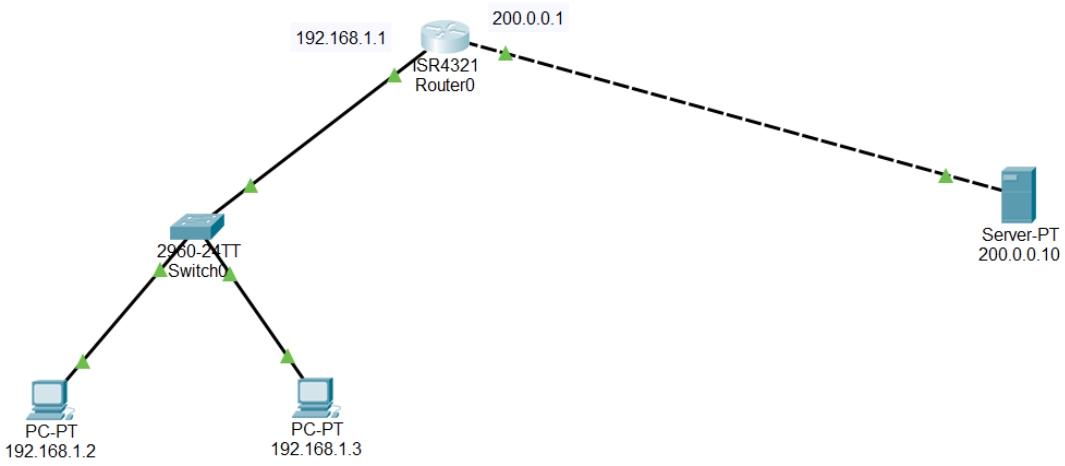
We can access index.html through public IP address



We cannot access index.html with private IP address.

DYNAMIC NAT:

- FOR DYNAMIC NAT, we will keep the same topology.
- So, first, we need to follow the same steps till the configuration of router.
- Now, after configuring the connection, the topology will be like the image below.



- Now, follow the below steps for Dynamic NAT configuration.

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

```
Router(config)#int GigabitEthernet0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
```

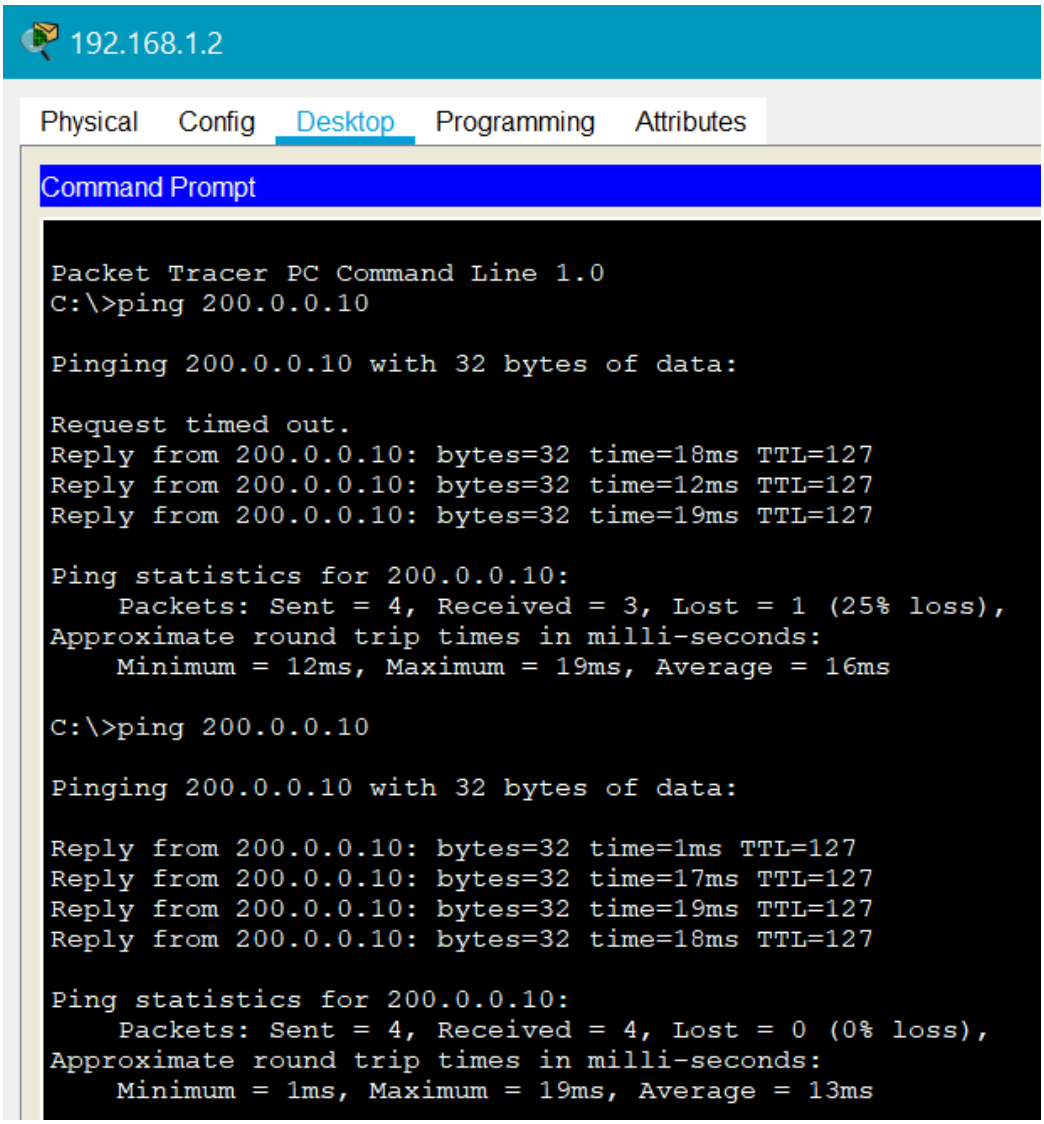
```
Router(config)#int GigabitEthernet0/0/1
Router(config-if)#ip nat pool parth 155.21.21.10 155.21.21.15 netmask 255.255.0.0
Router(config)#
Router(config)#ip nat inside source list 1 pool parth
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

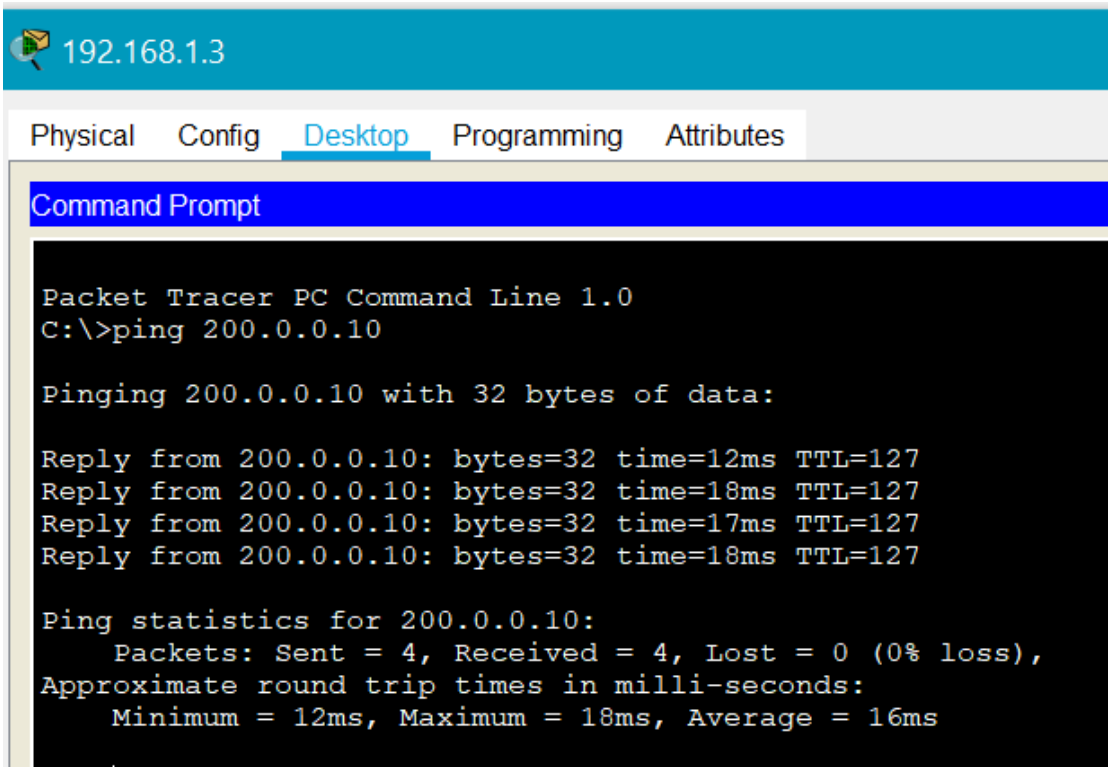
- To verify the configuration, perform the below mentioned steps

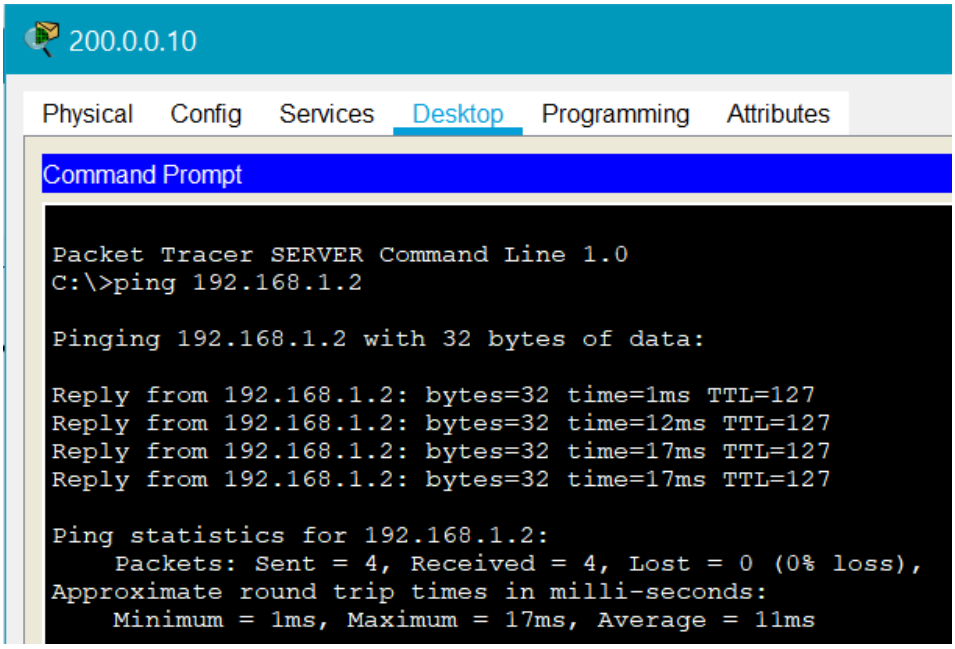
```
Router#show ip nat translations
Router#show access-list
Standard IP access list 1
    10 permit 192.168.1.0 0.0.0.255

Router#
```

NETWORK TESTING:

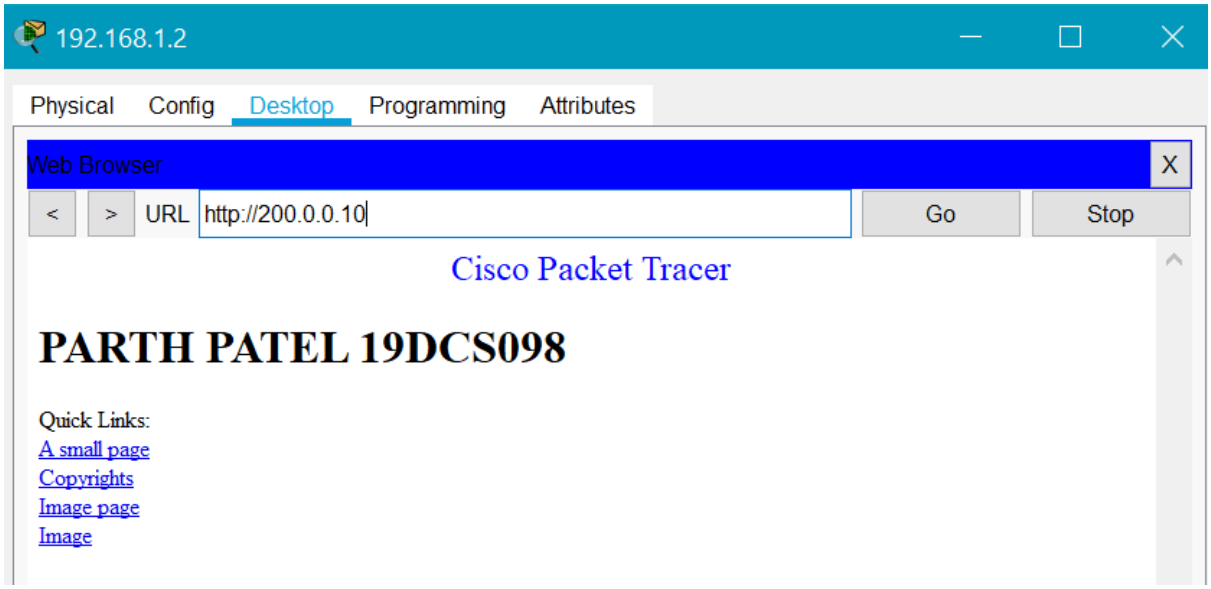
PING TEST:




192.168.1.3
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 200.0.0.10
Pinging 200.0.0.10 with 32 bytes of data:
Reply from 200.0.0.10: bytes=32 time=12ms TTL=127
Reply from 200.0.0.10: bytes=32 time=18ms TTL=127
Reply from 200.0.0.10: bytes=32 time=17ms TTL=127
Reply from 200.0.0.10: bytes=32 time=18ms TTL=127
Ping statistics for 200.0.0.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 18ms, Average = 16ms


200.0.0.10
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=12ms TTL=127
Reply from 192.168.1.2: bytes=32 time=17ms TTL=127
Reply from 192.168.1.2: bytes=32 time=17ms TTL=127
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 17ms, Average = 11ms

TESTING THROUGH WEB BROWSER:



CONCLUSION:

- By performing the above practical, we learned the concept of NAT.
- We also learned the types of NAT.
- We also learned how to configure the network using STATIC NAT and DYNAMIC NAT.