Computer Networks-Lab 13

Instructor: Hurmat Hidayat

CL30001 – Computer Networks-Lab

SEMESTER Fall 2022

NATIONAL UNIVERSTIY OF COMPUTER AND EMERGING SCIENCES, FAST- PESHAWAR CAMPUS
Department of Computer Science & Software Engineering

Computer Networks - Lab 13

OBJECTIVES

After these Lab students shall be able to perform

- **Implementation of D-NAT in cisco packet Tracer**

PRE-LAB READING ASSIGNMENT

Remember the delivered lecture carefully.

Table of Contents

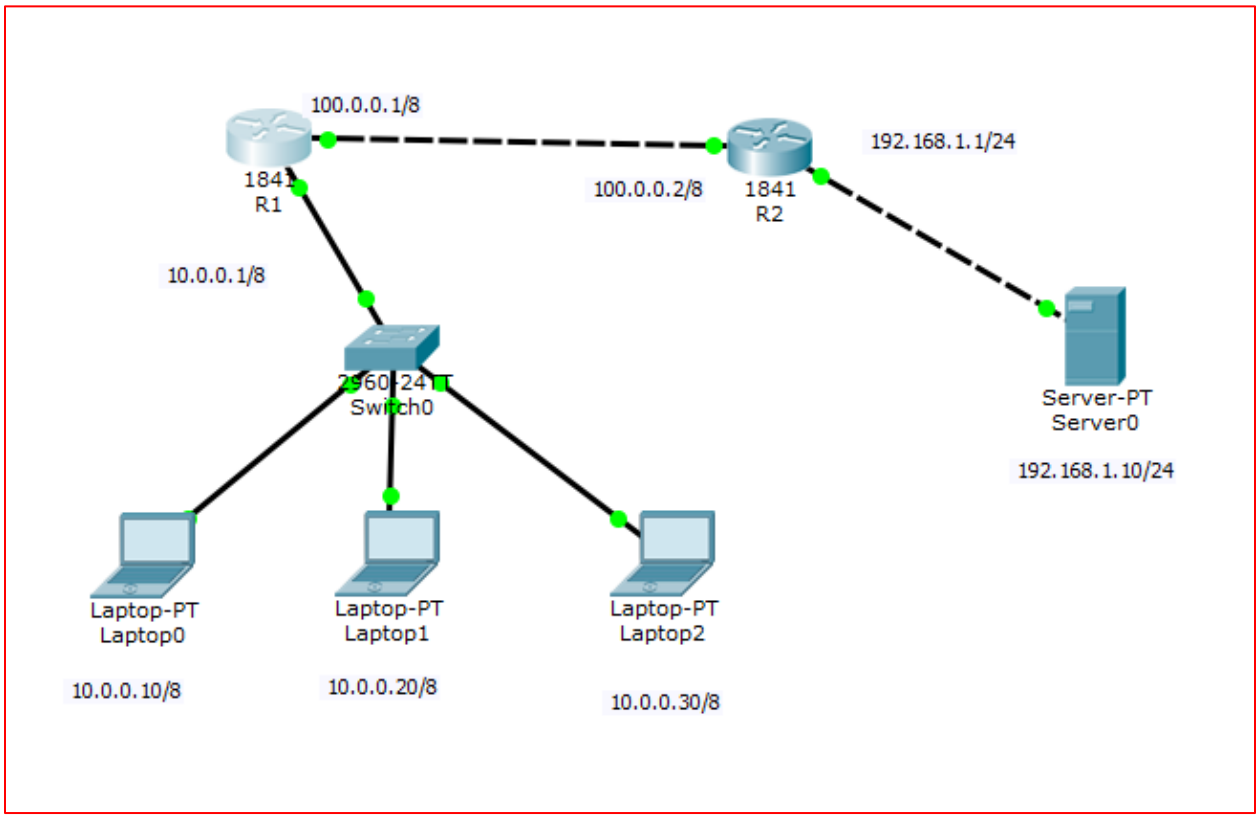
Dynamic NAT Configuration

How to Configure Dynamic NAT in Cisco Router

Dynamic NAT maps a private IP address to a public IP address from a pool of public IP addresses. This is unlike static NAT in which one private IP address is translated into one public IP address.

In dynamic NAT, the router will dynamically pick a public address from the pool. The dynamic mapping entry will stay in the NAT translations as long as the traffic is being exchanged. Otherwise, after a period of no traffic flow, the global IP address will be reused for new translations.

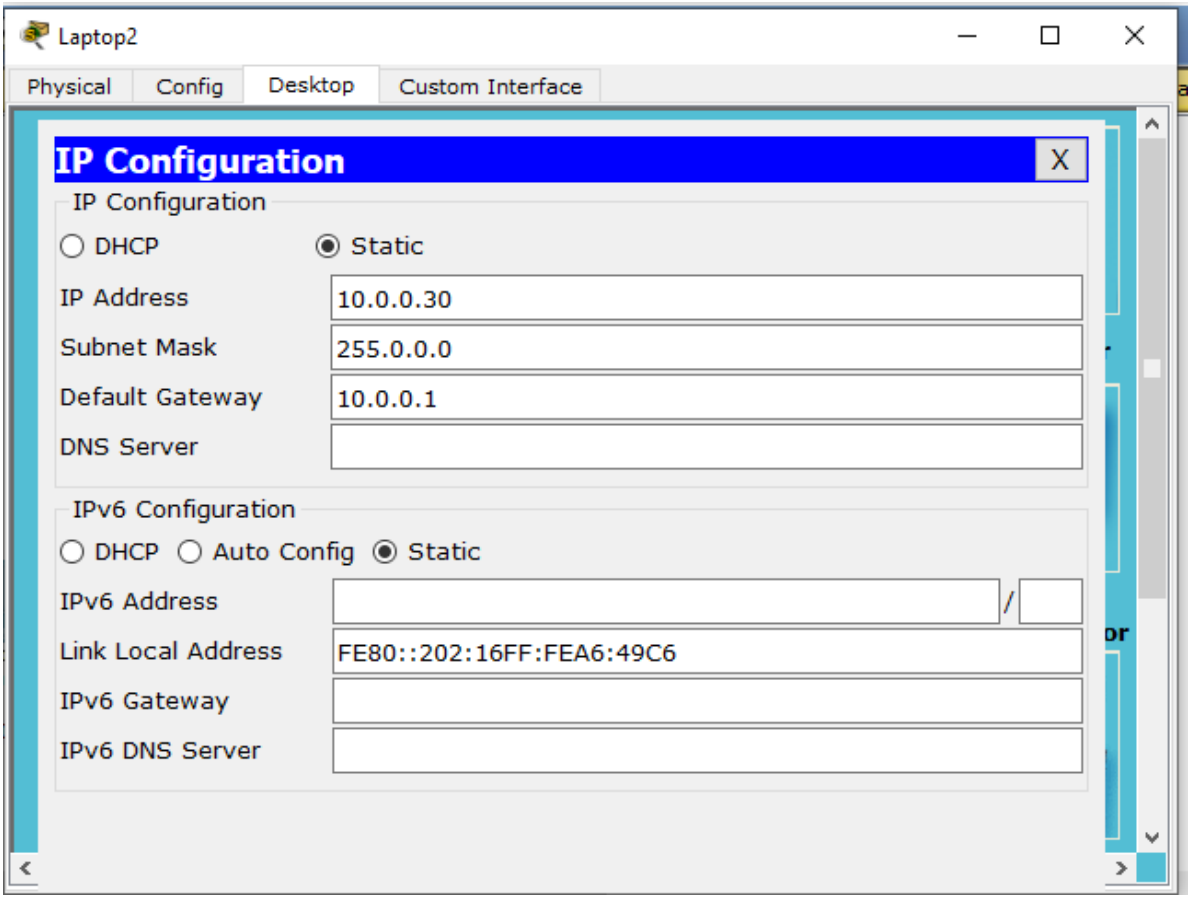
To explain Dynamic NAT configuration, I will use packet tracer network simulator software.

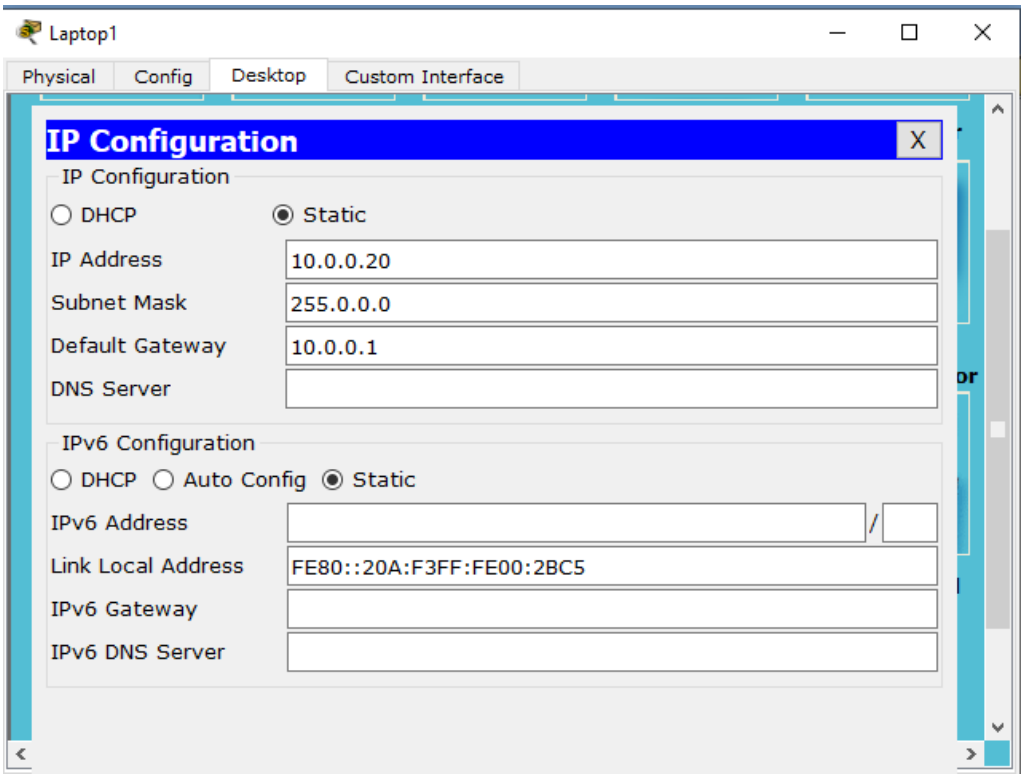


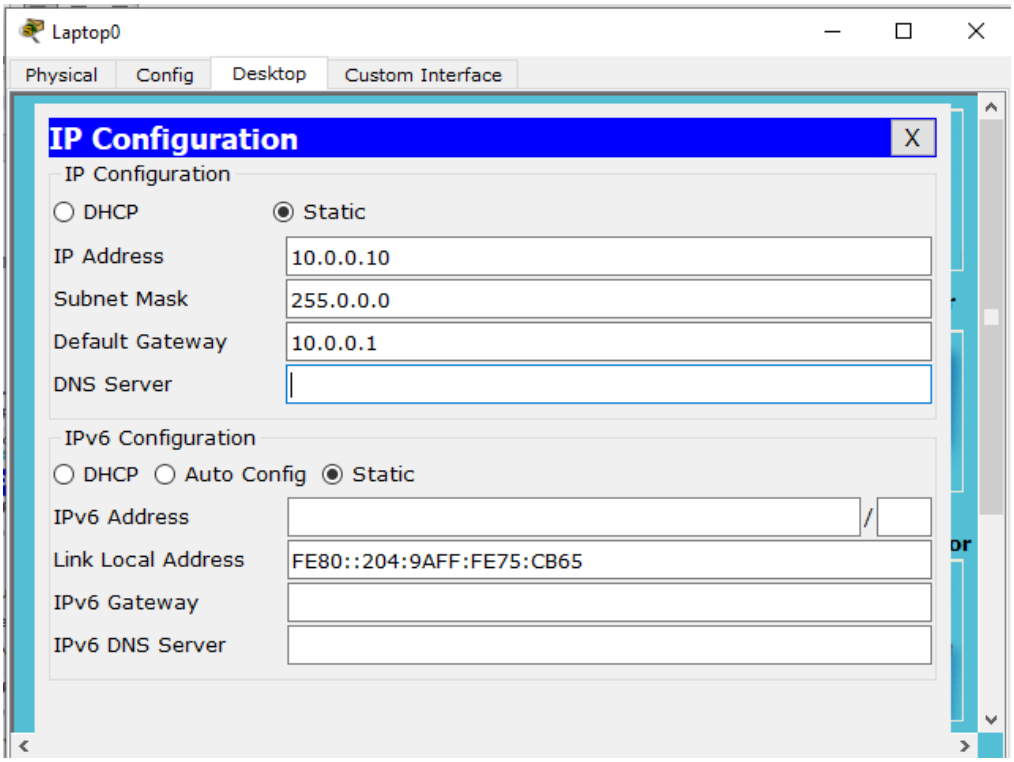
Initial IP Configuration

Device / Interface	IP Address	Connected With
Laotop0	10.0.0.10/8	Fa0/1 of R0
Laptop1	**10.0.0.20/8**	**Fa0/1 of R0**
Laptop2	10.0.0.30/8	Fa0/1 of R0
Server0	**192.168.1.10/24**	**Fa0/1 of R2**
F0/0 of R1	100.0.0.1/8	F0/0 of R2
F0/0 of R2	100.0.0.2/8	F0/0 of R1

To assign IP address in Laptop click **Laptop** and click **Desktop** and click **IP configuration** and Select **Static** and set **IP address** as given in above table.

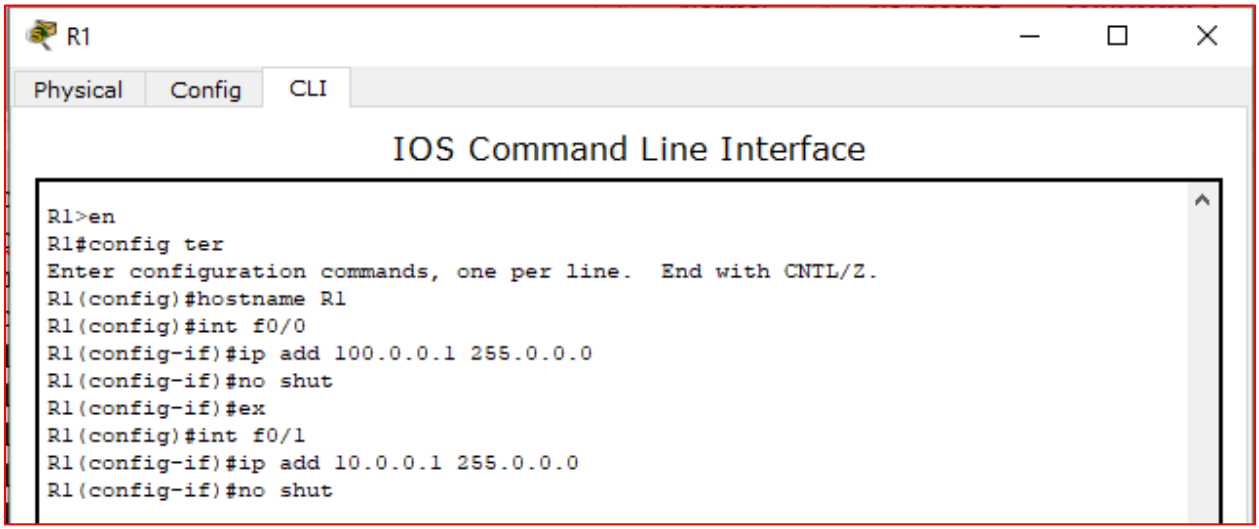



Laptop1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.0.0.20
Subnet Mask
255.0.0.0
Default Gateway
10.0.0.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20A:F3FF:FE00:2BC5
IPv6 Gateway
IPv6 DNS Server


Laptop0
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.0.0.10
Subnet Mask
255.0.0.0
Default Gateway
10.0.0.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::204:9AFF:FE75:CB65
IPv6 Gateway
IPv6 DNS Server

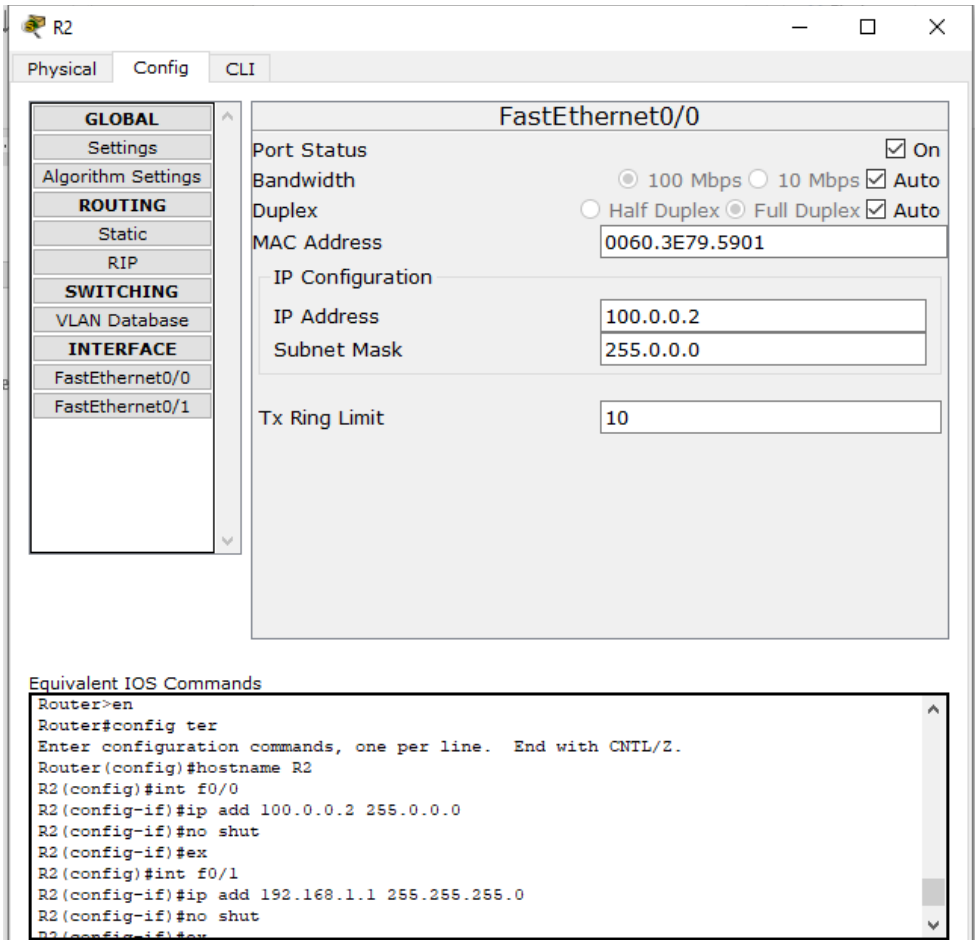
To configure IP address in Router1 click **Router1** and select **CLI** and press **Enter key**.

```
Router>en
Router#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int f0/0
R1(config-if)#ip add 100.0.0.1 255.0.0.0
R1(config-if)#no shut
```



Same way access the command prompt of R2 and run following commands to set IP address and hostname.

```
Router>en
Router#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int f0/0
R2(config-if)#ip add 100.0.0.2 255.0.0.0
R2(config-if)#no shut
R2(config-if)#ex
R2(config)#int f0/1
```



That's all initial IP configuration we need. Now this topology is ready for the practice of dynamic nat.

Configure Dynamic NAT

Dynamic NAT configuration requires four steps: -

1. Create an access list of IP addresses which need translation
2. Create a pool of all IP address which are available for translation
3. Map access list with pool
4. Define inside and outside interfaces

In first step we will create a standard access list which defines which inside local addresses are permitted to map with inside global address.

To create a standard numbered ACL following global configuration mode command is used:-

```
Router(config)# access-list ACL_Identifier_number permit/deny
matching-parameters
```

Let's understand this command and its options in detail.

Router(config)#

This command prompt indicates that we are in global configuration mode.

access-list

Through this parameter we tell router that we are creating or accessing an access list.

ACL_Identifier_number

With this parameter we specify the type of access list. We have two types of access list; standard and extended. Both lists have their own unique identifier numbers. Standard ACL uses numbers range 1 to 99 and 1300 to 1999. We can pick any number from this range to tell the router that we are working with standard ACL. This number is used in groping the conditions under a single ACL. This number is also a unique identifier for this ACL in router.

An Access Control List (ACL) is a set of rules that is usually used to filter network traffic. ACLs can be configured on network devices with packet filtering compatibilities, such as routers and firewalls.

permit/deny

An ACL condition has two actions; permit and deny. If we use permit keyword, ACL will allow all packets from the source address specified in next parameter. If we use deny keyword, ACL will drop all packets from the source address specified in next parameter.

matching-parameters

This parameter allows us to specify the contents of packet that we want to match. In a standard ACL condition it could be a single source address or a range of addresses. We have three options to specify the source address.

- Any
- host
- A.B.C.D

1 Any

Any keyword is used to match all sources. Every packet compared against this condition would be matched.

2 Host

Host keyword is used to match a specific host. To match a particular host, type the keyword host and then the IP address of host.

3 A.B.C.D

Through this option we can match a single address or a range of addresses. To match a single address, simply type its address. To match a range of addresses, we need to use wildcard mask.

4 Wildcard mask

Just like subnet mask, wildcard mask is also used to draw a boundary in IP address. Where subnet mask is used to separate network address from host address, wildcard mask is used to distinguish the matching portion from the rest. Wildcard mask is the invert of Subnet mask. Wildcard can be calculated in decimal or in binary from subnet mask.

We have three hosts in lab. Let's create a standard access list which allows any hosts.

```
R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255
```

In second step we define a pool of inside global addresses which are available for translation.

Following command is used to define the NAT pool.

```
Router(config)#ip nat pool [Pool Name] [Start IP address] [End
IP address] netmask [Subnet mask]
```

This command accepts four options pool name, start IP address, end IP address and Subnet mask.

Pool Name: - This is the name of pool. We can choose any descriptive name here.

Start IP Address: - First IP address from the IP range which is available for translation.

End IP Address: - Last IP address from the IP range which is available for translation. There is no minimum or maximum criteria for IP range for example we can have a range of single IP address or we can have a range of all IP address from a subnet.

Subnet Mask: - Subnet mask of IP range.

Let's create a pool named ccna with an IP range of two addresses.

```
R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.2 netmask 255.0.0.0
```

This pool consist two class A IP address 50.0.0.1 and 50.0.0.2.

In third step we map access list with pool. Following command will map the access list with pool and configure the dynamic NAT.

```
Router(config)#ip nat inside source list [access list name or
number] pool [pool name]
```

This command accepts two options.

Access list name or number: - Name or number the access list which we created in first step.

Pool Name: - Name of pool which we created in second step.

In first step we created a standard access list with number **1** and in second step we created a pool named **ccna**. To configure a dynamic NAT with these options we will use following command.

```
R1(config)#ip nat inside source list 1 pool ccna
```

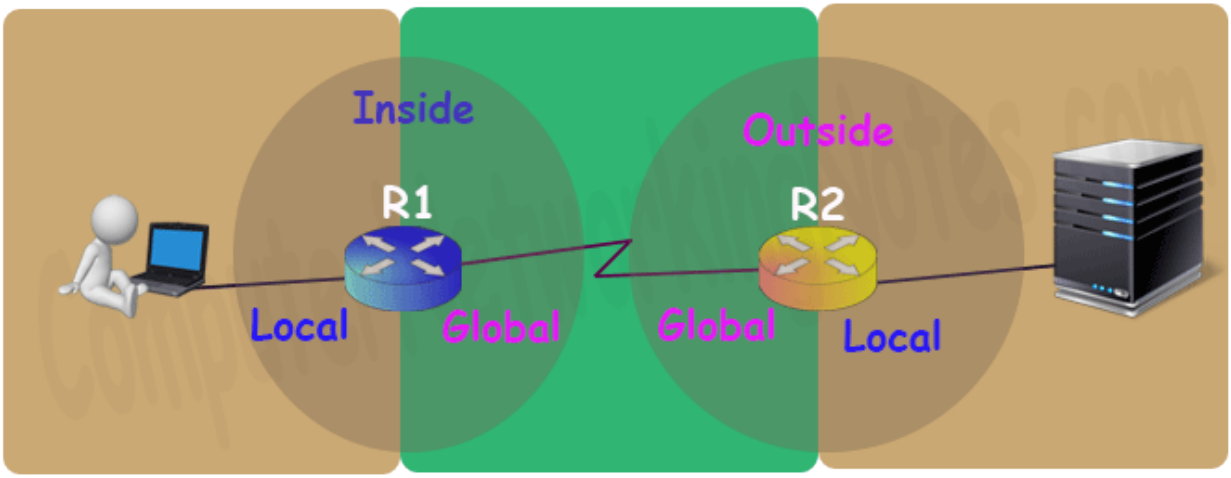
Finally we have to define which interface is connected with local network and which interface is connected with global network.

To define an inside local we use following command

```
Router(config-if)#ip nat inside
```

Following command defines inside global

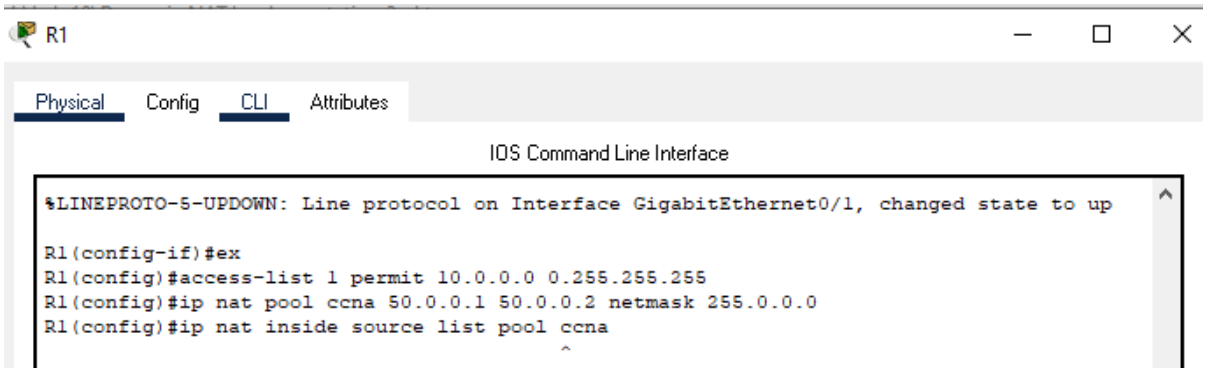
```
Router(config-if)#ip nat outside
```

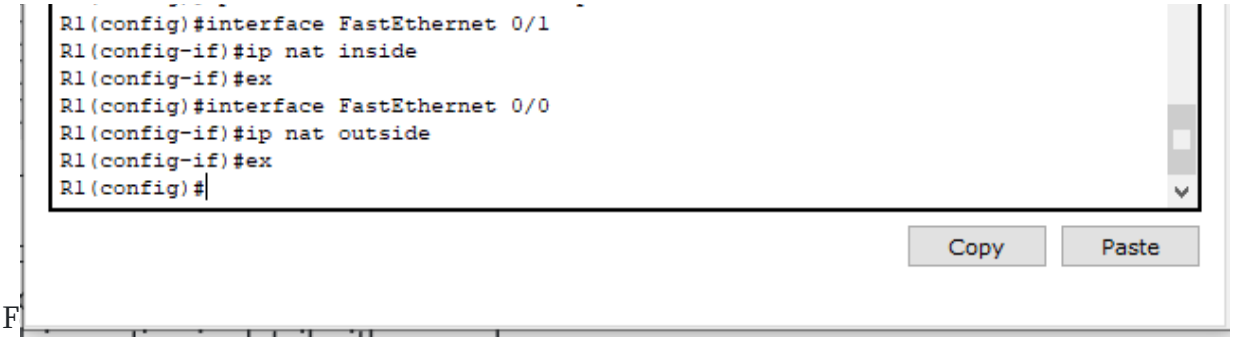


Let's implement all these commands together and configure the dynamic NAT.

R1 Dynamic NAT Configuration

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255
R1(config)#ip nat pool ccna 50.0.0.1 50.0.0.2 netmask 255.0.0.0
R1(config)#ip nat inside source list 1 pool ccna
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
```



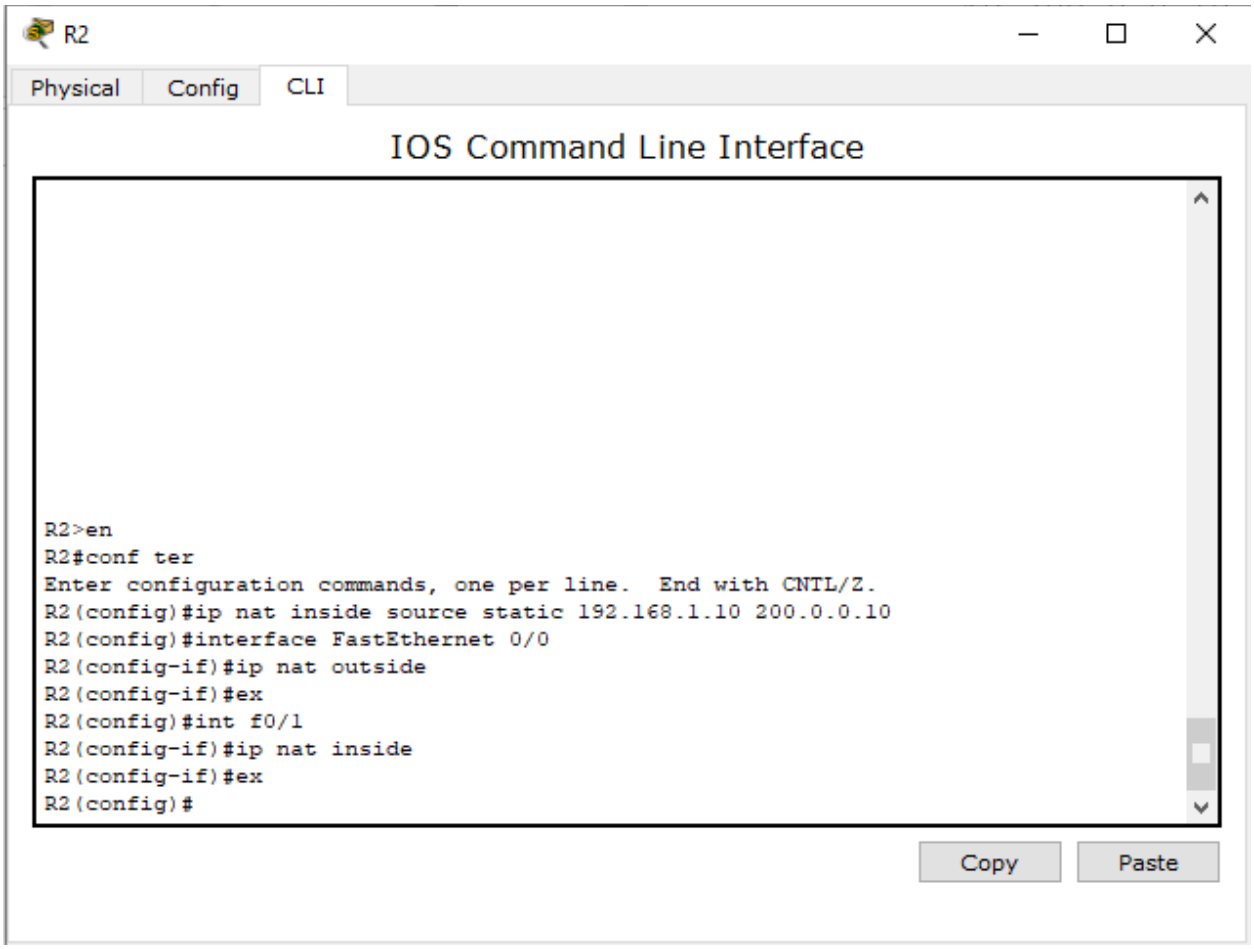


F

On R2 we can keep standard configuration or can configure dynamic NAT as we just did in R1 or can configure static NAT as we learnt in pervious Lab.

Let's do a quick recap of what we learnt in previous part and configure static NAT on R2.

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface FastEthernet 0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```



Before we test this lab we need to configure the IP routing. IP routing is the process which allows router to route the packet between different networks.

Configure static routing in R1

```
R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2
R1(config)# ip route 200.0.0.0 255.255.255.252 100.0.0.2
```

Configure static routing in R2

```
R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1
```

R1#show ip nat statistics

show ip nat translations

clear ip nat translation *

config terminal

no ip nat pool *old pool name*

ip nat pool *new pool*

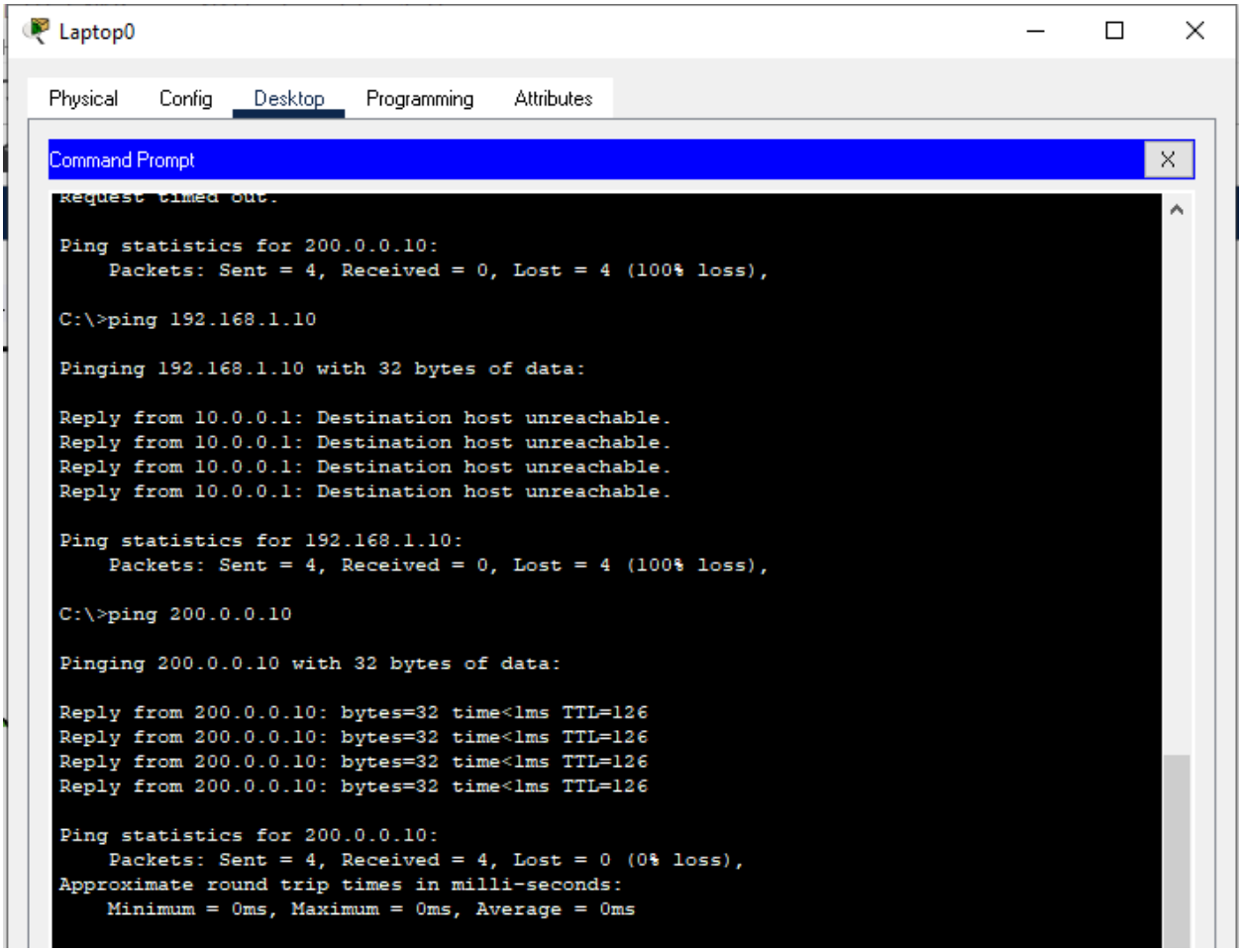
Testing Dynamic NAT Configuration

In this lab we configured dynamic NAT on R1for 10.0.0.10 and 10.0.0.20 and static NAT on R2 for 192.168.1.10.

Device	Inside Local IP Address	Inside Global IP Address
Laptop0	10.0.0.10	50.0.0.1
Laptop1	10.0.0.20	50.0.0.2
Server	192.168.1.10	200.0.0.10

To test this setup click **Laptop0** and **Desktop** and click **Command Prompt**.

- Run **ipconfig** command.
- Run **ping 192.168.1.10** command.
- Run **ping 200.0.0.10** command.

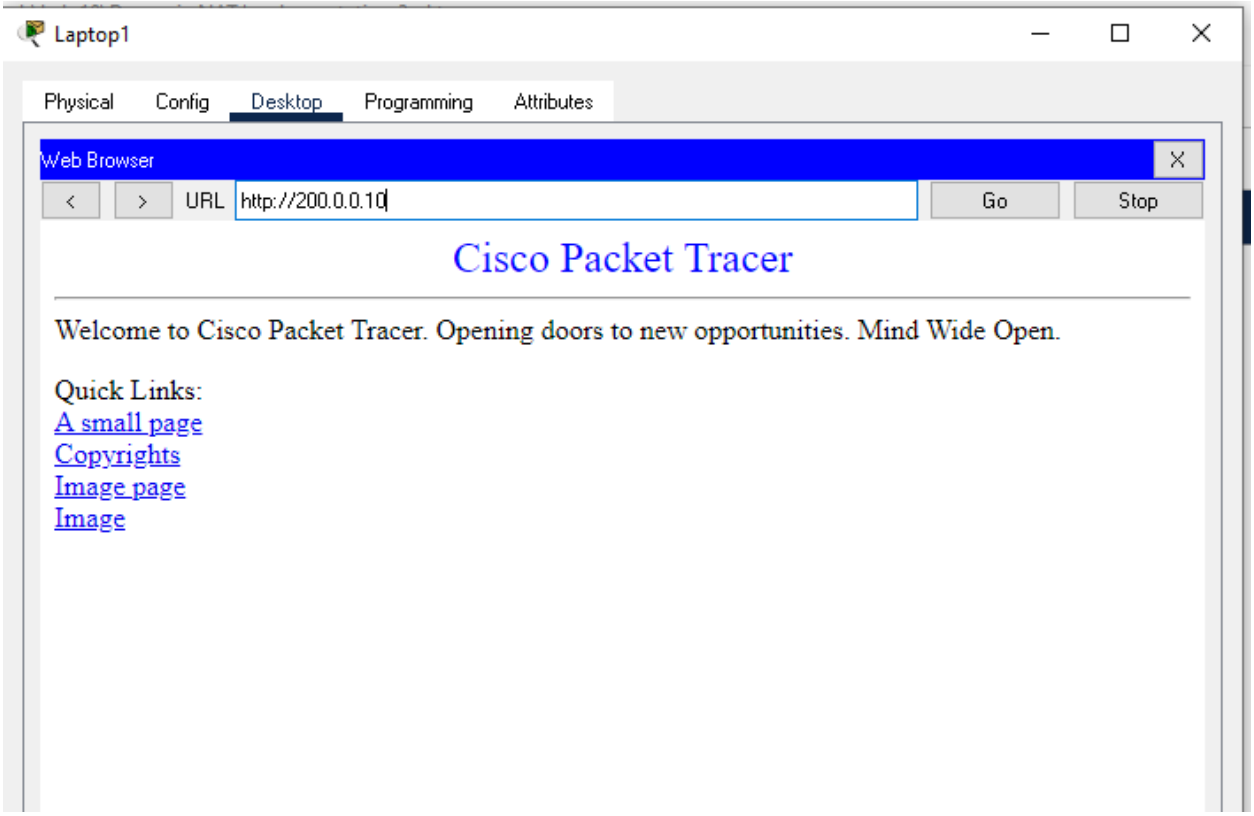


First command verifies that we are testing from correct NAT device.

Second command checks whether we are able to access the remote device or not. A ping reply confirms that we are able to connect with remote device on this IP address.

Third command checks whether we are able to access the remote device on its actual IP address or not. A ping error confirms that we are not able to connect with remote device on this IP address.

Let's do one more testing. Close the command prompt and click web server and access 200.0.0.10.




```
R1#show ip access-lists
```

Lab 13 Task:

- **Implement the S-NAT for web server of (flex and slate) and Dynamic-NAT for Client Systems in a single topology.(Use routers and switches).**
- **Create a pdf file of each step.**
- **Upload .pkt and pdf file in google class room**