Computer Networks-Lab 12

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 12

OBJECTIVES

After these Lab students shall be able to perform

- **Network Layer.**
- **Understanding of Public and Private IPs**
- **Understanding of NAT (S-NAT, D-NAT, P-NAT).**
- **Implementation of Static NAT in cisco packet Tracer**

PRE-LAB READING ASSIGNMENT

Remember the delivered lecture carefully.

Table of Contents

Layer #	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc…	Messages	n/a
4	Transport	TCP/UDP	Segments/ Datagrams	Port #s
3	Network or Internet	IP	Packets	IP Address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

Network Address Translation (NAT)

Internet Protocol

Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

The IP address can be classified as:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)

IPv4 defines an IP address as a 32-bit number, while IPv6 defines an IP address as a 128-bit number.

Public and private IP address

- All IPv4 addresses can be divided further into public (global) and private (local) addresses.

- Public addresses are routable addresses that are used on the internet, these addresses allow the users to access resources on a computer network located anywhere in the world.

- While, private addresses are not routable and no traffic can be sent to them or by them over the internet.

Private Address Ranges

The Internet Assigned Numbers Authority (IANA) has assigned several address ranges to be used by private networks.

Address ranges to be use by private networks are:

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

An IP address within these ranges is therefore considered non-routable, as it is not unique. Any private network that needs to use IP addresses internally can use any address within these ranges

without any coordination with IANA or an Internet registry. Addresses within this private address space are only unique within a given private network.

All addresses outside these ranges are considered public.

Private Addressing

- The major limitation of Internet Protocol version 4 (IPv4) is its address exhaustion issue.
- As a short-term solution, various protocols such as private addressing and Network Address Translation (NAT) were introduced.
- These two standards work closely together, allowing organizations to assign private addresses to their internal network, while translating them to public addresses and allowing them to connect to the internet.
- Some devices in an organization's network may not need to connect to the internet when building such a network. So, an administrator is expected to use private IP addresses as defined in RFC 1918 documentation.
- The documentation defines a set of network addresses assigned to an organization's internal network so that devices can communicate locally. If there is a need for such devices to connect to the internet, their private addresses must be translated to public addresses using Network Address Translation (NAT).

Network Address Translation

For a device configured with a private address to access the internet or a remote network, the address must be translated into a public routable address.

This translation takes place on a NAT-enabled router which typically operates on the border of a stub network.
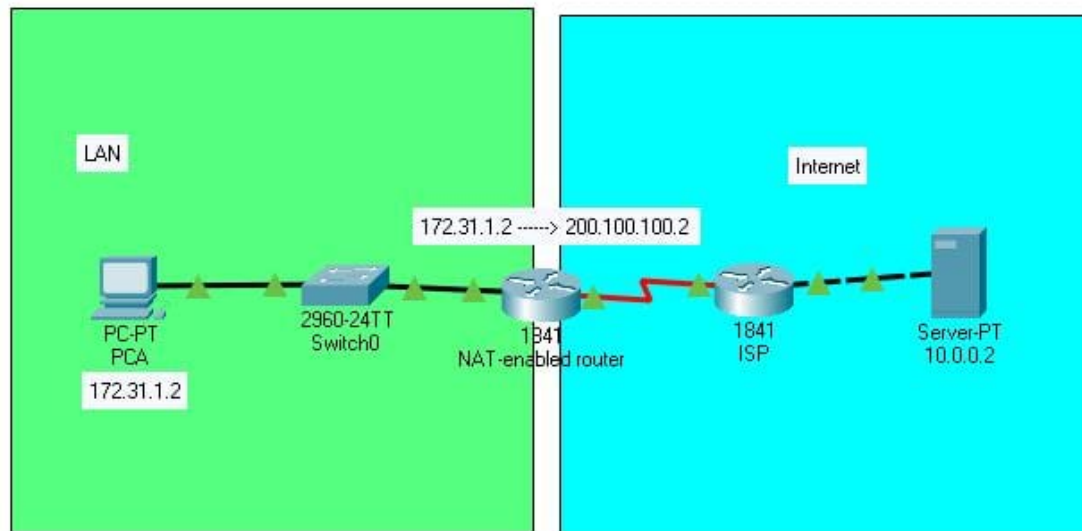
Network Address Translation - Client-Server connection

In the figure above, PCA with an IP address of 172.31.1.2 wants to reach the webserver, but because PCA's address is not routable, it cannot access the webserver directly.

Instead, the NAT-enabled router translates the PC's private address of 172.31.1.2 to a public address of 200.100.100.2, which is routable over the internet.

From the server's perspective, it sees this address as the source address. Suppose the server wants to send data to the PC, it will use the same source address as its destination address.

When the data reaches the NAT-enabled router, the public address is then translated back to its original private address, and the data is forwarded back to the PC.

Types of NAT

Network address translation can be classified into three types. They are:

1. Static Network Translation (Static NAT)
2. Dynamic Network Address Translation (Dynamic NAT)
3. Port Address Translation (PAT)

Static NAT

Static NAT creates a one-to-one mapping between private and public addresses. Static NAT is usually configured by a network administrator, and this configuration remains constant.
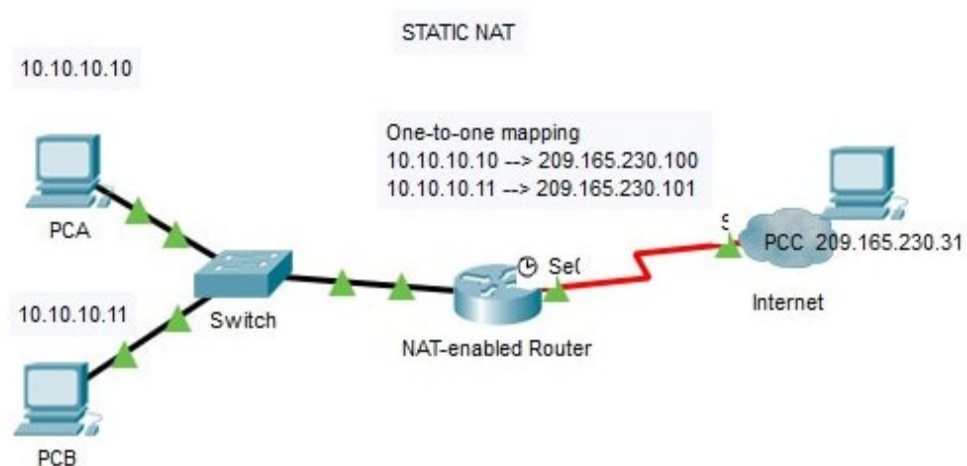
In the figure above, PCA and PCB wants to reach PCC, which is a remote network.

But because both are configured with private addresses, they cannot access PCC directly.

To access PCC, a NAT-enabled router is configured with static NAT, that maps their private addresses to public addresses using one-to-one relationship, thus allowing them to communicate with PCC.

Therefore, static NAT is useful for a device that needs a dedicated address, such as a web server. But, it requires an equal number of public addresses for users using them simultaneously.

Dynamic NAT

Similar to static NAT, the dynamic NAT gives a one-to-one mapping between private and public addresses. But, the mapping is done dynamically.

Dynamic NAT makes a pool of public addresses and assigns them to private addresses on a first-come-first-served (FCFS) basis to determine which private addresses ought to be translated.
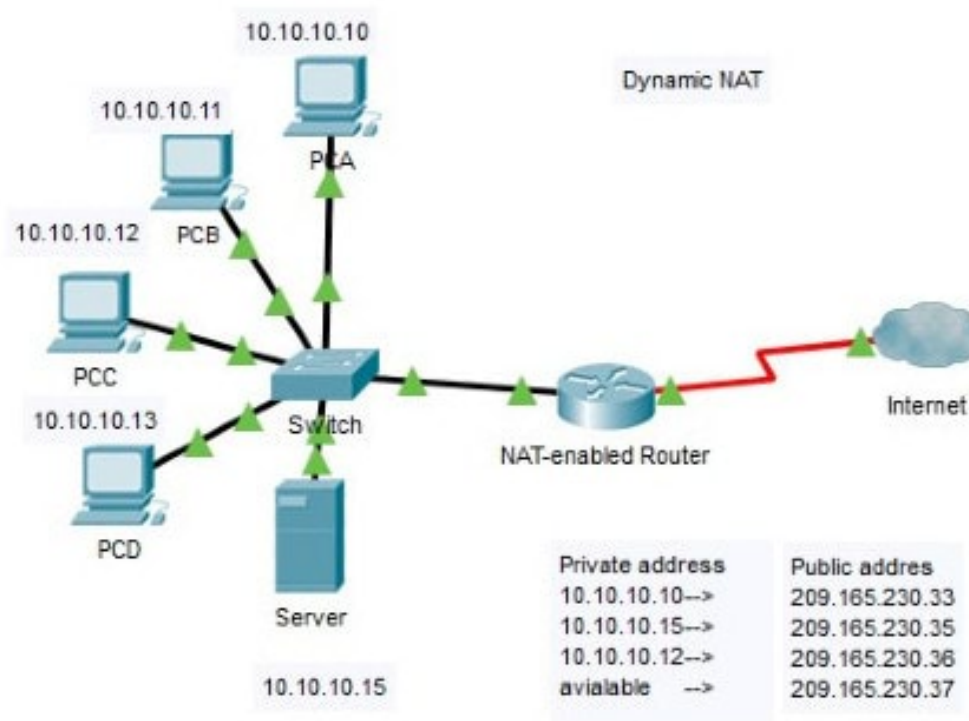
In the figure above, an organization is assigned to four different public addresses, but the organization can have more than four internal devices that require access to the internet.

To resolve this problem, the network administrator decides to configure dynamic NAT to allow these devices to access the internet.

If all the internal devices have been assigned to all the available global addresses, then the device requesting for a public address will have to wait until one is made available.

Port Address Translation (PAT)

Dynamic NAT is more commonly used by organizations, to connect their devices to the internet. If their network is large, it requires a huge set of registered public addresses. Thus, it completely defeats NAT's goal.

Dynamic NAT reduces this problem to some degree. However, if a large percentage of internal hosts need access to the internet then, we must use Port Address Translation, also called NAT overload.

To understand how PAT works, it is important to recall how the host uses the Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and port numbers to transmit data.

With these protocols, PAT can map multiple private addresses to one or more public addresses by ensuring that devices use different TCP and UDP port numbers for each session.
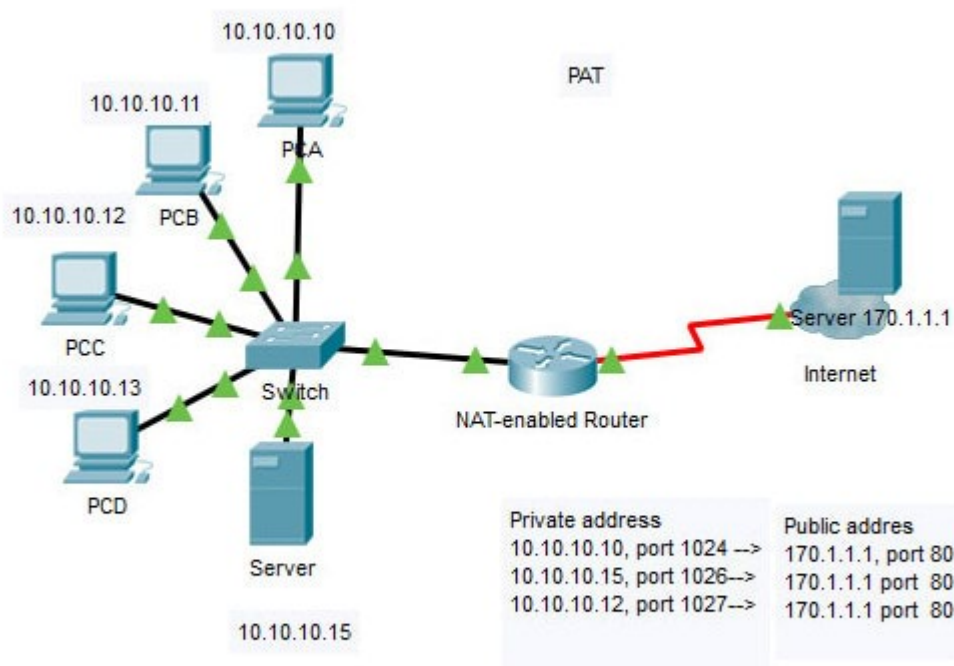
NAT configuration

How to Configure Static NAT in Cisco Router?

This tutorial explains Static NAT configuration in detail. Learn how configure static NAT, map address (inside local address, outside local address, inside global address and outside global address), debug and verify Static NAT translation step by step with practical examples in packet tracer.

In order to configure NAT we have to understand four basic terms; inside local, inside global, outside local and outside global. These terms define which address will be mapped with which address.

Term	Description
Inside Local IP Address	Before translation source IP address located inside the local network.
Inside Global IP Address	After translation source IP address located outside the local network.
Outside Global IP Address	Before translation destination IP address located outside the remote network.
Outside Local IP Address	After translation destination IP address located inside the remote network.

Static NAT Practice LAB Setup

To explain Static NAT Configuration, I will use packet tracer network simulator software.
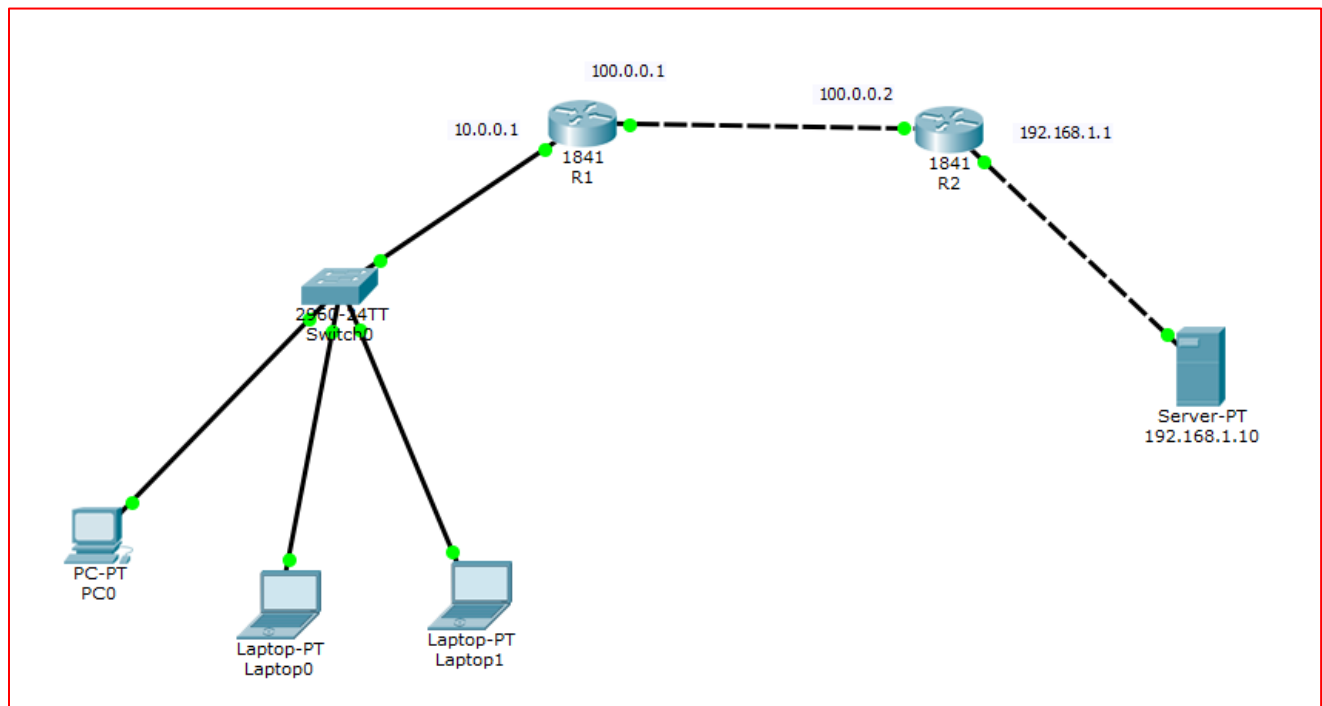

Figure 1 Static Nat Topology

Initial IP Configuration

Device / Interface	IP Address	Connected With
PC0	10.0.0.10/8	Fa0/0 of R1
Laptop0	10.0.0.20/8	Fa0/0 of R1
Laptop1	10.0.0.30/8	Fa0/0 of R1
Server0	192.168.1.10/24	Fa0/0 of R2
F0/1 of R1	100.0.0.1/8	Fa0/1of R2
F 0/1of R2	100.0.0.2/8	Fa0/1 of R1

To assign IP address in Laptop click **Laptop** and click **Desktop** and **IP configuration** and Select **Static** and **set IP address** as given in above table.
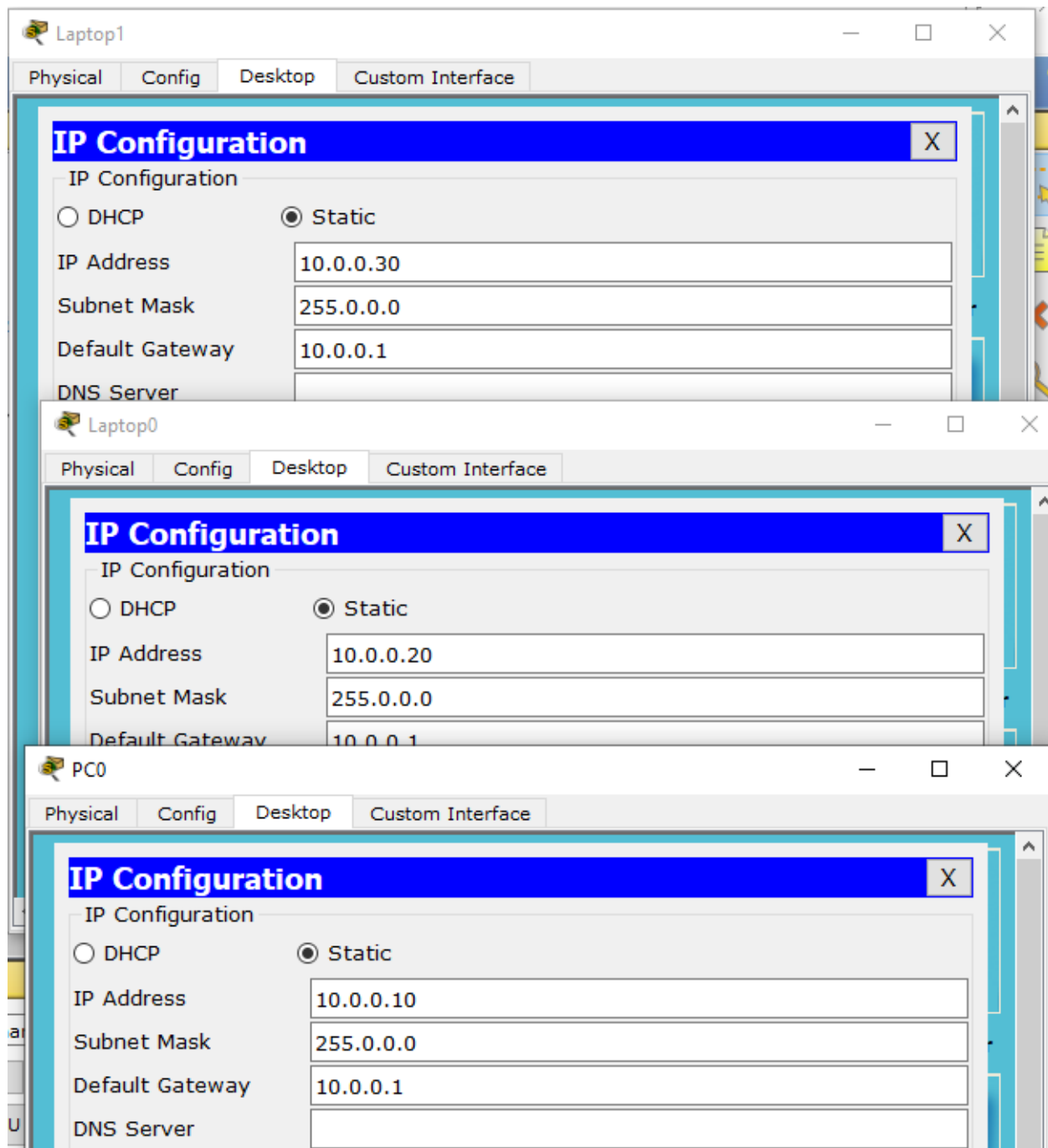
Following same way configure IP address in Server.
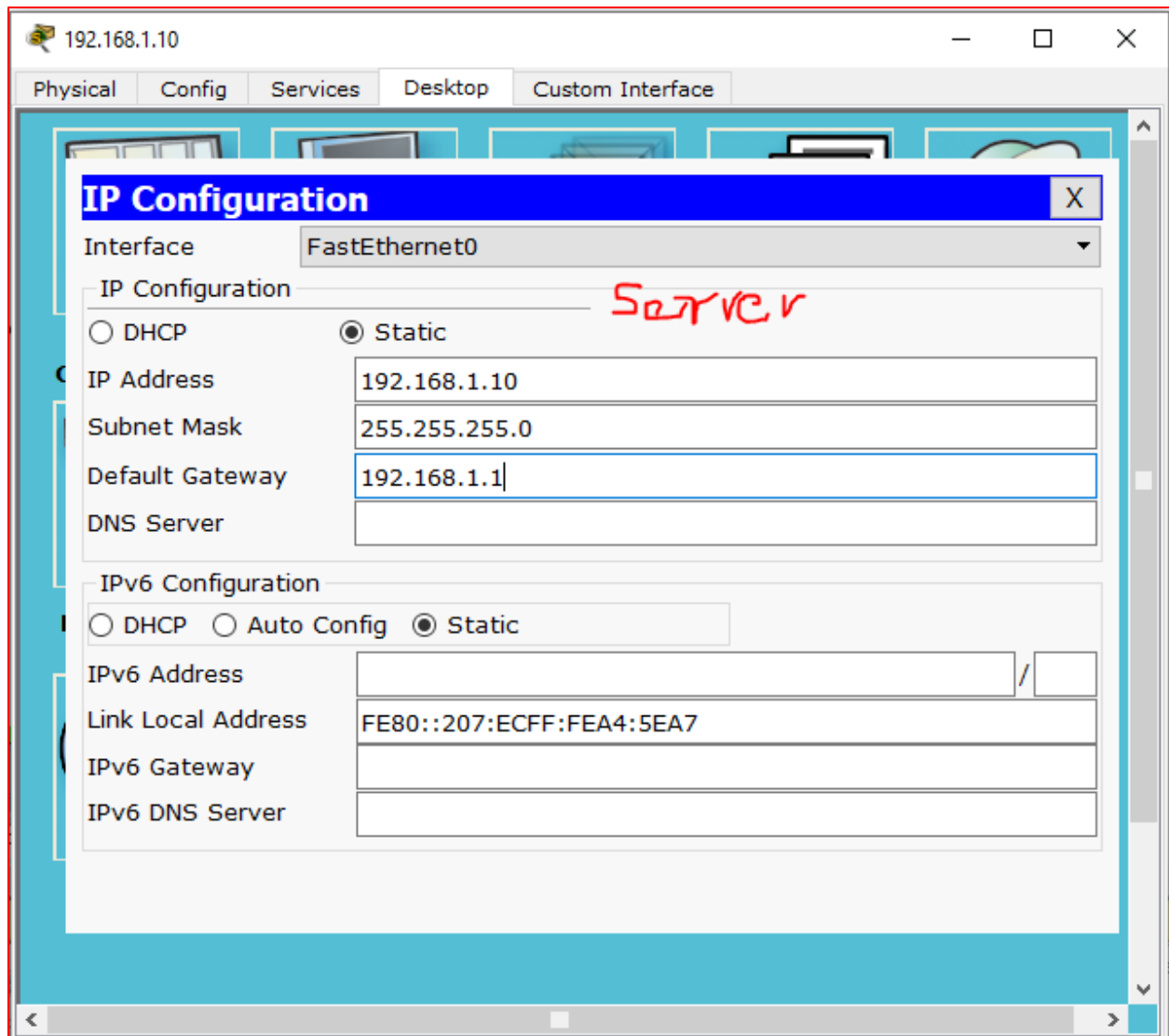
To configure IP address in Router1 click **Router1** and select **CLI** and press **Enter key**.

Two interfaces of Router1 are used in topology; FastEthernet0/0 and FastEthernet0/1.

By default interfaces on router are remain administratively down during the start up. We need to configure IP address and other parameters on interfaces before we could actually use them for routing. Interface mode is used to assign the IP address and other parameters. Interface mode can be accessed from global configuration mode. Following commands are used to access the global configuration mode.

```
Router>enable

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#
```

Before we configure IP address in interfaces let's assign a unique descriptive name to router.

```
Router(config)#hostname R1

R1#
```

Now execute the following commands to set IP address in FastEthernet 0/0 interface.

```
R1(config)#interface FastEthernet0/0

R1(config-if)#ip address 10.0.0.1 255.0.0.0

R1(config-if)#no shutdown

R1(config-if)#exit
```

interface FastEthernet 0/0 command is used to enter in interface mode.

ip address 10.0.0.1 255.0.0.0 command assigns IP address to interface.

no shutdown command is used to bring the interface up.

exit command is used to return in global configuration mode.

Now we have necessary information let's assign IP address to interface f0/1.

```
R1#configure terminal

R1(config)#interface f0/1

R1(config-if)#ip address 100.0.0.1 255.0.0.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#
```

Router# configure terminal Command is used to enter in global configuration mode.

Router(config)#interface f0/1 Command is used to enter in interface mode.

Router(config-if)#ip address 100.0.0.1 255.0.0.0 Command assigns IP address to interface.

Router(config-if)#no shutdown Command brings interface up.

Router(config-if)#exit Command is used to return in global configuration mode.

We will use same commands to assign IP addresses on interfaces of Router2. We need to provided clock rate and bandwidth only on DCE side of serial interface. Following command will assign IP addresses on interface of Router2.

Initial IP configuration in R2

```
Router>enable

Router# configure terminal

Router(config)#hostname R2

R2(config)#interface FastEthernet0/0

R2(config-if)#ip address 192.168.1.1 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface FastEthernet0/1

R2(config-if)#ip address 100.0.0.2 255.0.0.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#
```

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

Configure Static NAT

Static NAT configuration requires three steps: -

1. Define IP address mapping
2. Define inside local interface
3. Define inside global interface

Since static NAT use manual translation, we have to map each inside local IP address (which needs a translation) with inside global IP address. Following command is used to map the inside local IP address with inside global IP address.

```
Router(config)#ip nat inside source static [inside local ip
address] [inside global IP address]
```

For example in our lab Laptop1 is configured with IP address 10.0.0.10. To map it with 50.0.0.10 IP address we will use following command

```
Router(config)#ip nat inside source static 10.0.0.10 50.0.0.10
```

In second step we have to define which interface is connected with local the network. On both routers interface Fa0/0 is connected with the local network which need IP translation.

Following command will define interface Fa0/0 as inside local.

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

In third step we have to define which interface is connected with the global network. On both routers serial 0/0/0 interface is connected with the global network. Following command will define interface Serial0/0/0 as inside global.

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

Following figure illustrates these terms.
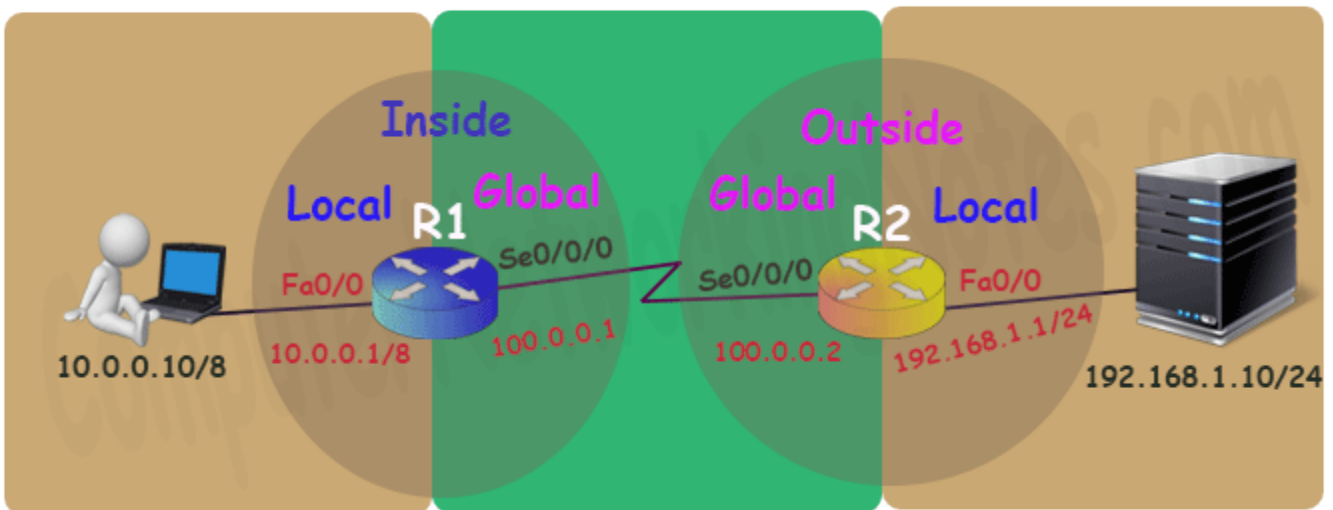
Let's implement all these commands together and configure the static NAT.

R1 Static NAT Configuration

```
R1(config)#ip nat inside source static 10.0.0.10 50.0.0.10

R1(config)#interface FastEthernet 0/0

R1(config-if)#ip nat inside
```

```
R1(config-if)#exit

R1(config)#

R1(config)#interface FastEthernet 0/1

R1(config-if)#ip nat outside

R1(config-if)#exit
```

For testing purpose I configured only one static translation. You may use following commands to configure the translation for remaining address.

```
R1(config)#ip nat inside source static 10.0.0.20 50.0.0.20

R1(config)#ip nat inside source static 10.0.0.30 50.0.0.30
```

R2 Static NAT Configuration

```
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10

R2(config)#interface FastEthernet 0/1

R2(config-if)#ip nat inside

R2(config-if)#exit

R2(config)#

R2(config)#interface FastEthernet 0/0

R2(config-if)#ip nat outside

R2(config-if)#exit
```

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
```

Configure static routing in R2

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

Testing Static NAT Configuration

In this lab we configured static NAT on R1 and R2. On R1 we mapped inside local IP address 10.0.0.10 with inside global address 50.0.0.10 while on R2 we mapped inside local IP address 192.168.1.10 with inside global IP address 200.0.0.10.

Device	Inside Local IP Address	Inside Global IP Address
PC0	10.0.0.10	50.0.0.10
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 200.0.0.10** command.
- Run **ping 192.168.1.10** 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. Click **PC0** and click **Desktop** and click **Web Browser** and access 200.0.0.10.
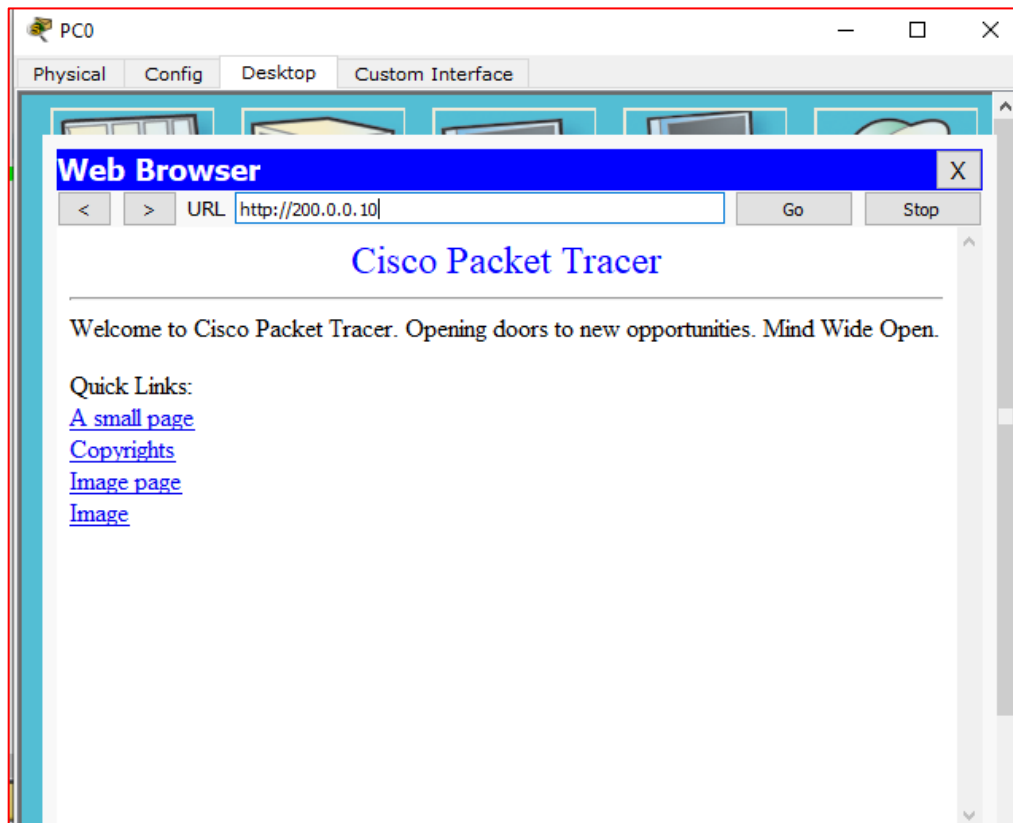
Above figure confirms that host 10.0.0.10 is able to access the 200.0.0.10.

Lab Task:

- **Implement the S-NAT for web server of (flex and slate) in a single topology.**