



Academic Year: 2023-24

Class/Branch: TE/DS

Semester: V

Subject: WCN

Experiment No. 09

1. **Aim:** To design and simulate NAT on router using Cisco packet tracer/ GNS3.

2. **Software used:** CISCO Packet Tracer

3. **Theory:** -

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.

These addresses are within the range of:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.255.255.255
- 192.168.0.0 to 192.168.255.255

Network Address Translation

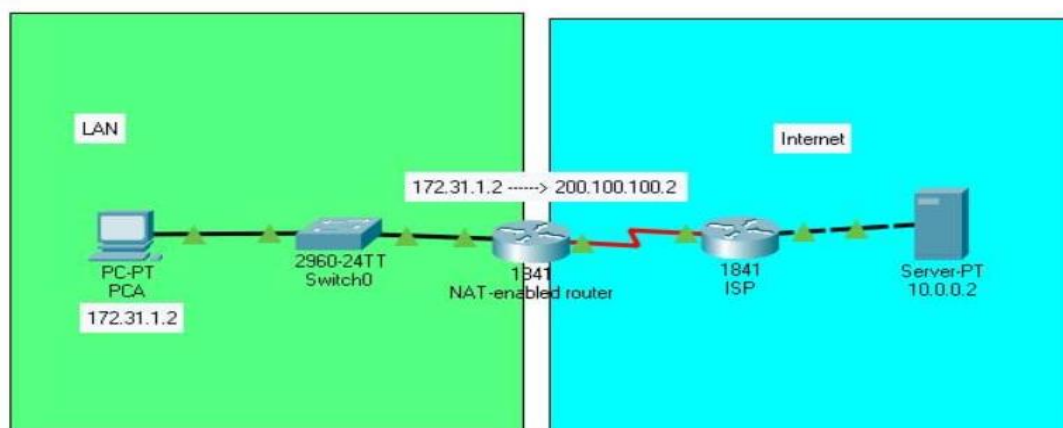


To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Working of 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.

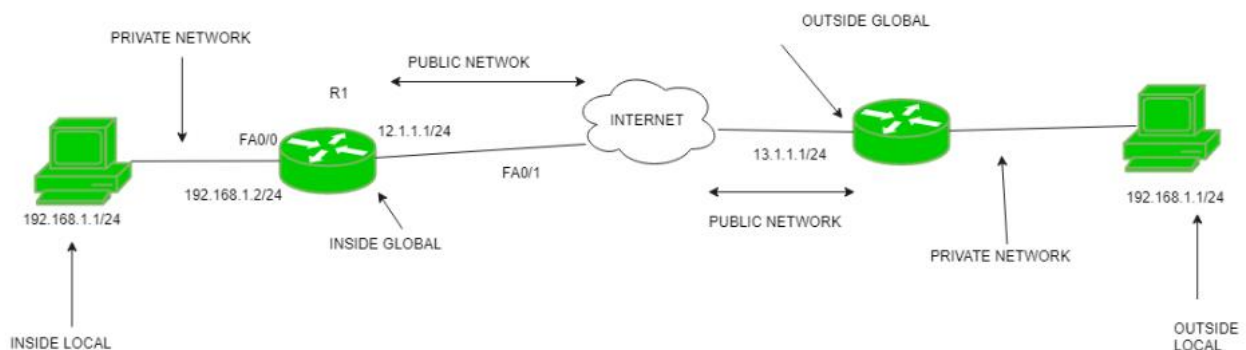


From the server's perspective, it sees this address as the source address. Suppose the server wants to send data to the PC, it will use the same source address as its destination address.

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.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address** – An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.
- **Inside global address** – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside local address** – This is the actual IP address of the destination host in the local network after translation.
- **Outside global address** – This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:



1. **Static NAT** – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT** – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.

Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT)** – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

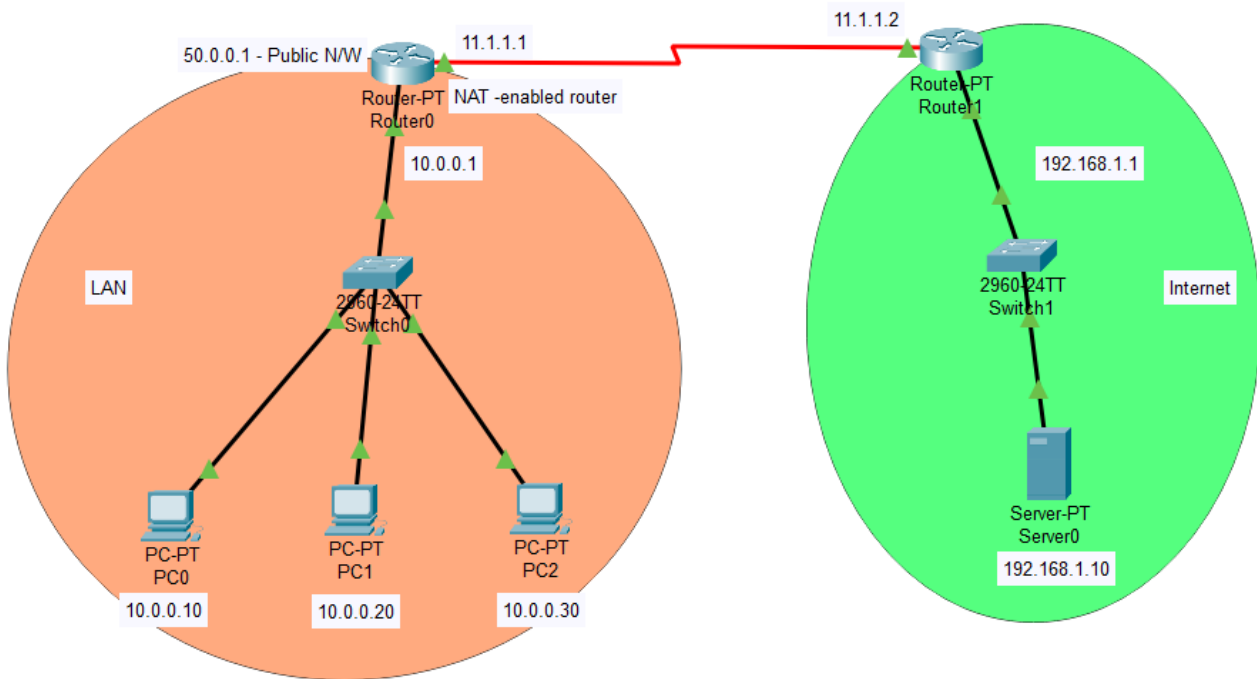
- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.



Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunnelling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

Procedure:



In the above network diagram, we have 3 PCs assigned with private network addresses as 10.0.0.10, 10.0.0.20, 10.0.0.30, respectively .

In this topology, a Cisco switch is connected with 3 Cisco PCs and a router0 Component, and that router0 is connected with another router (router1) which is again connected with a switch that connects Server with IP address 192.168.1.10.

PC 0 to PC 3 are computers (end devices) and a Switch in this network.

Black strong lines are Copper Straight-Through cables which use to connect different types of devices.

Red color lines are Serial DCE cables which are building the connection between two routers.

We will configure the devices such that PC0, PC1 (and deny PC2) will communicate with Server using only one public IP address (50.0.0.1/50.0.0.2) which is R0's Se2/0 interface's IP address.

STEP 1: NETWORK CONFIGURATION



Assign IP address to PCs

Double click **PC0** and click **Desktop** menu item and click **IP Configuration**. Assign IP address 10.0.0.10/8 to PC0.

Device	Interface	IP Configuration	Gateway	Switch	Connected with
PC0	Fast Ethernet0/0	10.0.0.10/8	10.0.0.1	Switch0	Router0's Fa0/0
PC1	Fast Ethernet0/0	10.0.0.20/8	10.0.0.1	Switch0	Router0's Fa0/0
PC2	Fast Ethernet0/0	10.0.0.30/8	10.0.0.1	Switch0	Router0's Fa0/0
Server	Fast Ethernet0/0	192.168.1.10/24	12.168.1.1	Switch1	Router1's Fa0/0

STEP 2: ROUTER CONFIGURATION

Router 0

Device	Interface	IP Configuration	Switch	Connected with
Router0	Fa0/0	10.0.0.1/8	Switch0	Client N/W Fa0/0
Router0	Se2/0	11.1.1.1/8	--	Router1's Se2/0

Device Name: Router0
Device Model: Router-PT
Hostname: Router

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	10.0.0.1/8	<not set>	0010.116A.AD61
FastEthernet1/0	Down	<not set>	<not set>	0003.E4D8.50D9
Serial2/0	Up	11.1.1.1/8	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0007.ECE0.48C8
FastEthernet5/0	Down	<not set>	<not set>	0005.5EB7.7946

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0

Router0

Physical Config CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

INTERFACE

- FastEthernet0/0
- FastEthernet1/0
- Serial2/0
- Serial3/0
- FastEthernet4/0
- FastEthernet5/0

FastEthernet0/0

Port Status ☒ On
Bandwidth 100 Mbps 10 Mbps ☒ Auto
Duplex Half Duplex Full Duplex ☒ Auto
MAC Address 0010.116A.AD61

IP Configuration

IPv4 Address 10.0.0.1
Subnet Mask 255.0.0.0

Tx Ring Limit 10



Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

INTERFACE

FastEthernet0/0

FastEthernet1/0

Serial2/0

Serial3/0

FastEthernet4/0

FastEthernet5/0

Serial2/0

Port Status ☒ On

Duplex ☐ Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 11.1.1.1

Subnet Mask 255.0.0.0

Tx Ring Limit 10

Router 1

Device	Interface	IP Configuration	Switch	Connected with
Router1	Fa0/0	192.168.1.1/24	Switch1	Server N/W Fa0/0
Router1	Se2/0	11.1.1.2/8	--	Router0's Se2/0

Device Name: Router1

Device Model: Router-PT

Hostname: Router

Port	Link	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	192.168.1.1/24	<not set>	000C.CF1E.7EC0
FastEthernet1/0	Down	<not set>	<not set>	0003.E453.8D69
Serial2/0	Up	11.1.1.2/8	<not set>	<not set>
Serial3/0	Down	<not set>	<not set>	<not set>
FastEthernet4/0	Down	<not set>	<not set>	0002.1724.5179
FastEthernet5/0	Down	<not set>	<not set>	0001.C921.40C9

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1

Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

INTERFACE

FastEthernet0/0

FastEthernet1/0

Serial2/0

Serial3/0

FastEthernet4/0

FastEthernet5/0

FastEthernet0/0

Port Status ☒ On

Bandwidth ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

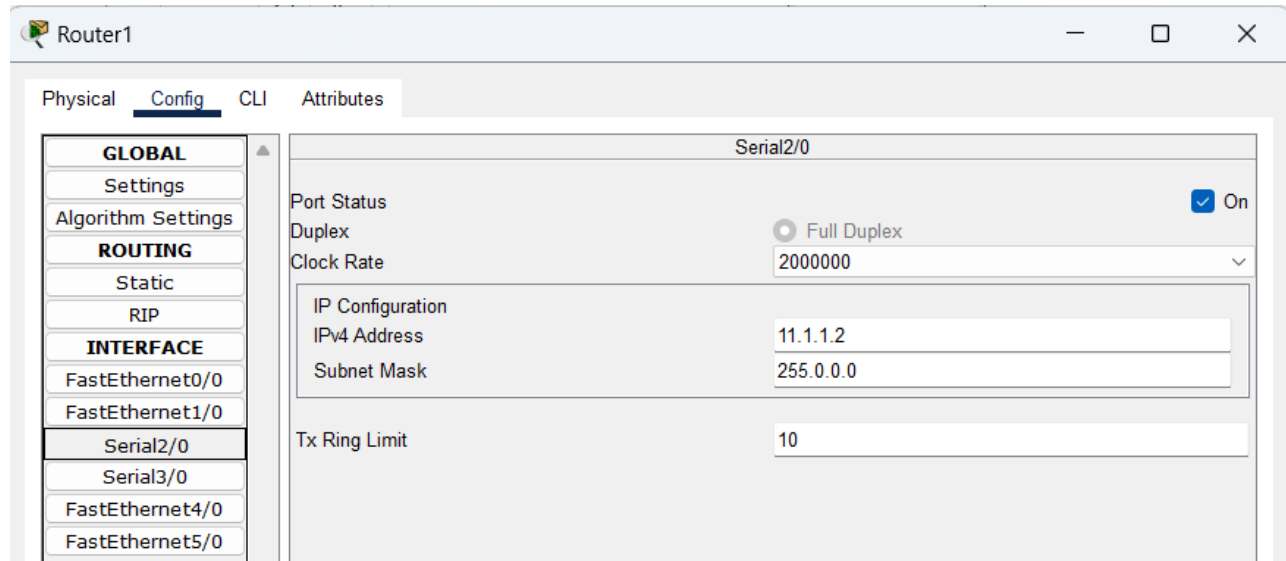
MAC Address 000C.CF1E.7EC0

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

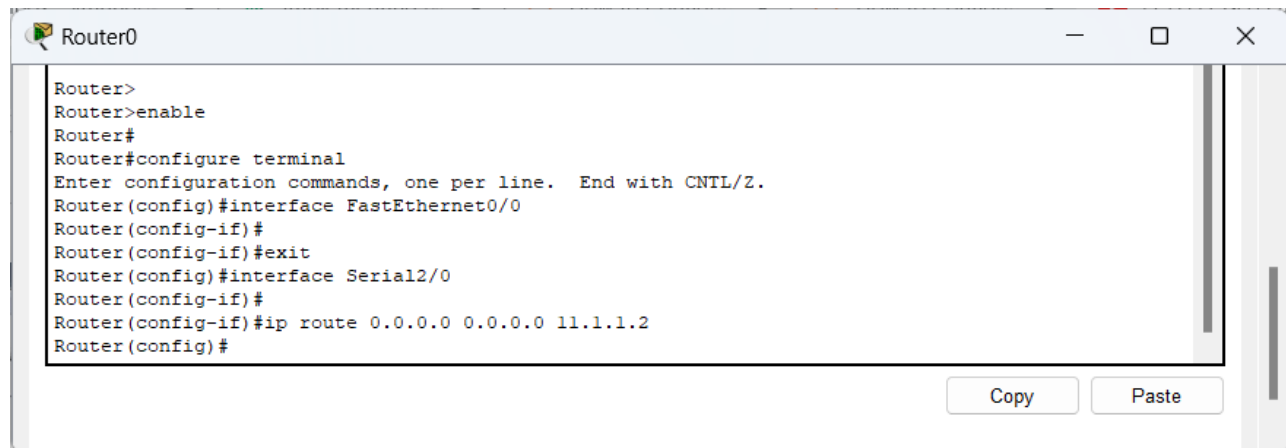


STEP 3: IP ROUTING-CONFIGURING DEFAULT ROUTE TO INTERNET

IP routing is the process which allows router to route the packet between different networks.

Double click **router0** and click **CLI** menu item and click Enter.

Router 0 to Server



STEP 4: IP ROUTING-CONFIGURING STATIC ROUTE TO PRIVATE NETWORK ROUTER

Router 1 to LAN's Router 0



The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. On the left sidebar, the 'ROUTING' section is expanded, and 'Static' is selected. The main area is titled 'Static Routes' and contains the following fields: 'Network' (50.0.0.0), 'Mask' (255.0.0.0), and 'Next Hop' (11.1.1.1). Below these fields is an 'Add' button. At the bottom, a summary box shows 'Network Address' as '50.0.0.0/8 via 11.1.1.1'.

STEP 5: 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

1. Create an access list of IP addresses which need translation

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 grouping the conditions under a single ACL. This number is also a unique identifier for this ACL in router.

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

- **Any**

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

- **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.

- **A.B.C.D**

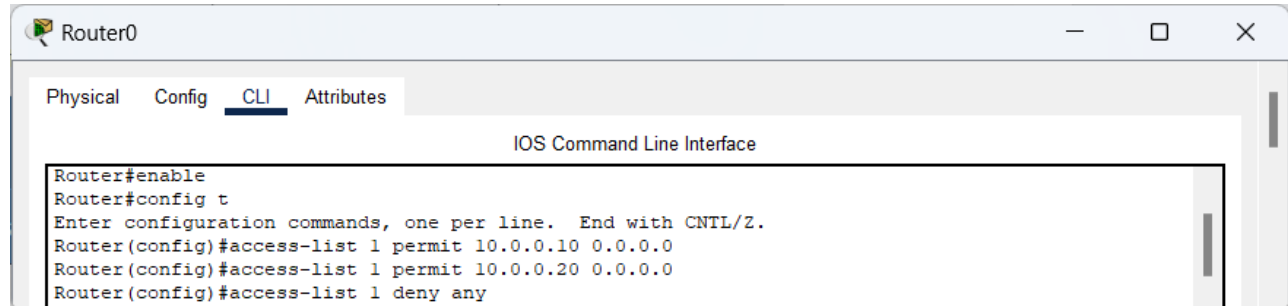
Through this option we can match a single address or a range of addresses. To match a single address, simply type its address. To match a range of addresses, we need to use wildcard mask.

- **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 two hosts* and *denies one host*.



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router#enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 10.0.0.10 0.0.0.0
Router(config)#access-list 1 permit 10.0.0.20 0.0.0.0
Router(config)#access-list 1 deny any
```

2. Create a pool of all IP address which are available for translation

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.

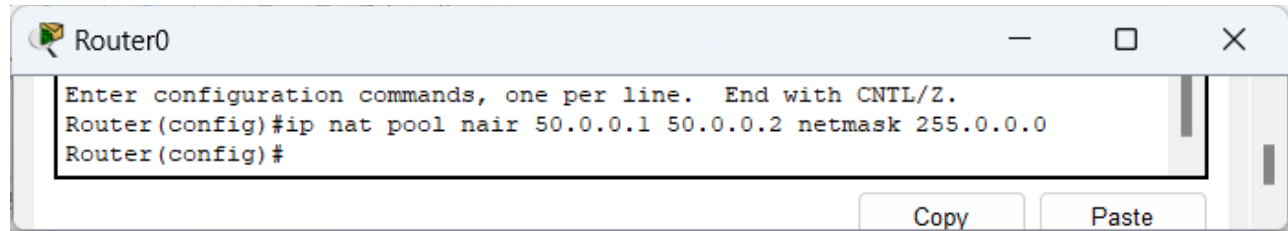
End IP Address: - Last IP address from the IP range which is available for translation. There is no minimum or maximum criteria for IP range for example we can have a range of single IP address or we can have a range of all IP address from a subnet.

Subnet Mask: - Subnet mask of IP range.

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

```
Router(config)#ip nat pool nair 50.0.0.1 50.0.0.2 netmask 255.0.0.0
```

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



3. Map access list with pool

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]
```

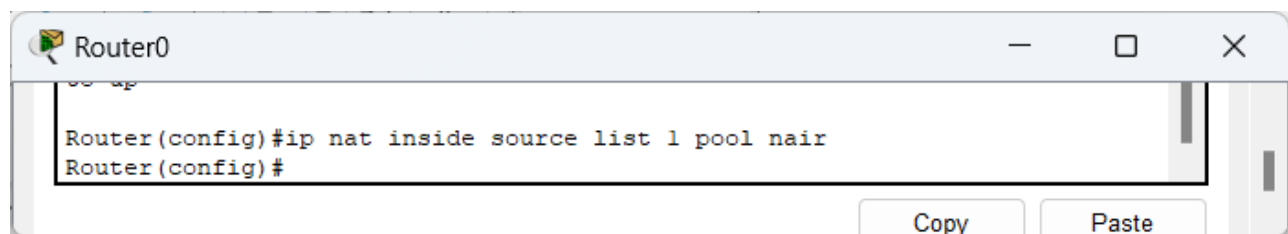
This command accepts two options.

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 **nair**. To configure a dynamic NAT with these options we will use following command.

```
Router(config)#ip nat inside source list 1 pool nair
```



4. Define inside and outside interfaces

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

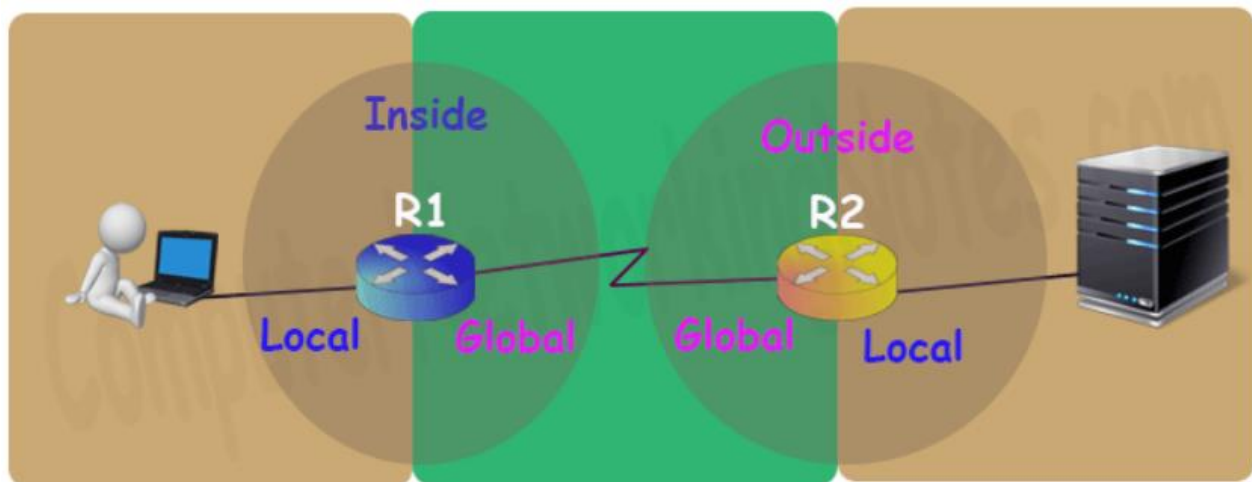
To define an inside local we use following command.

Double click **router0** and click **CLI** menu item and click Enter.



On Router 0

```
Router0
Router#enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial 2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```



DYNAMIC NAT TABLE

In this lab we configured dynamic NAT on R0 for 10.0.0.10 and 10.0.0.20.

Device	Inside Local IP Address	Inside Global IP Address
PC0	10.0.0.10	50.0.0.1
PC1	10.0.0.20	50.0.0.2

STEP 6: DATA TRANSMISSION

To test this setup, click **PC0/PC1** and **Desktop** and click **Command Prompt**.

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



The screenshot shows a window titled 'PC1' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of a 'ping 192.168.1.10' command, indicating a successful connection with 0% loss.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>
```

As the pool is not created for PC2, ping fails to connect the server.

The screenshot shows a window titled 'PC2' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of a 'ping 192.168.1.10' command, indicating a failed connection with 100% loss due to 'Request timed out'.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.10

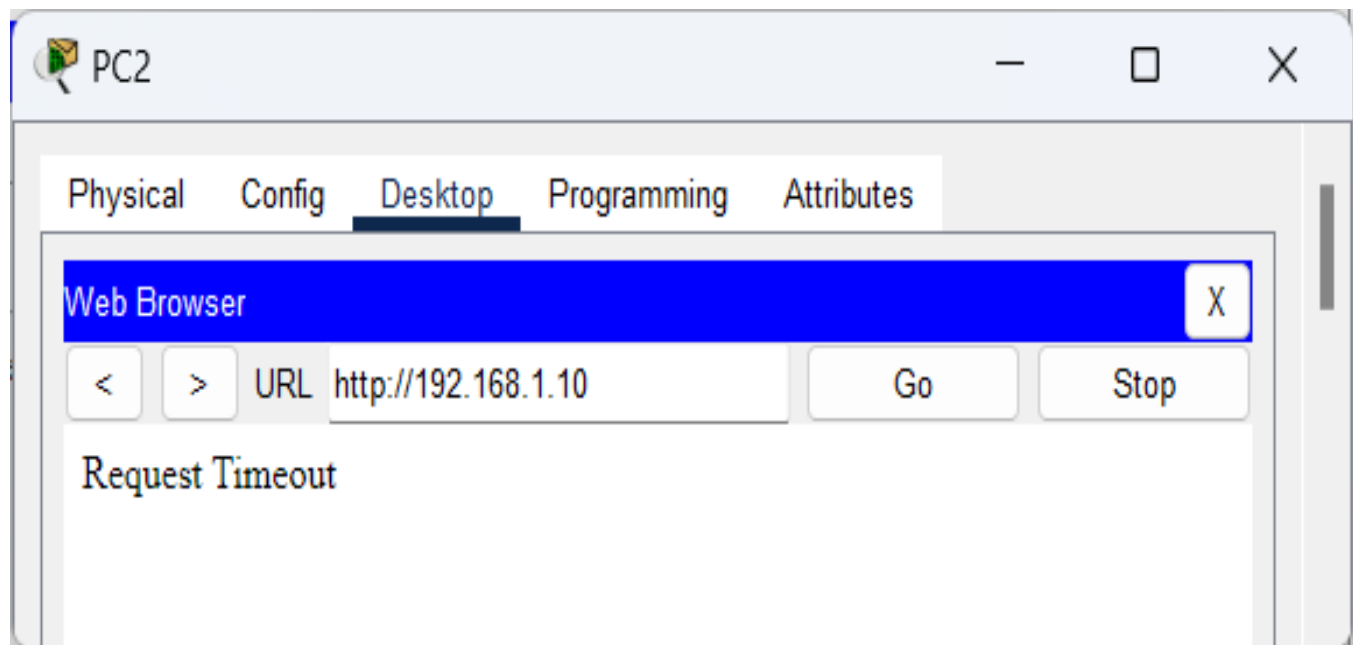
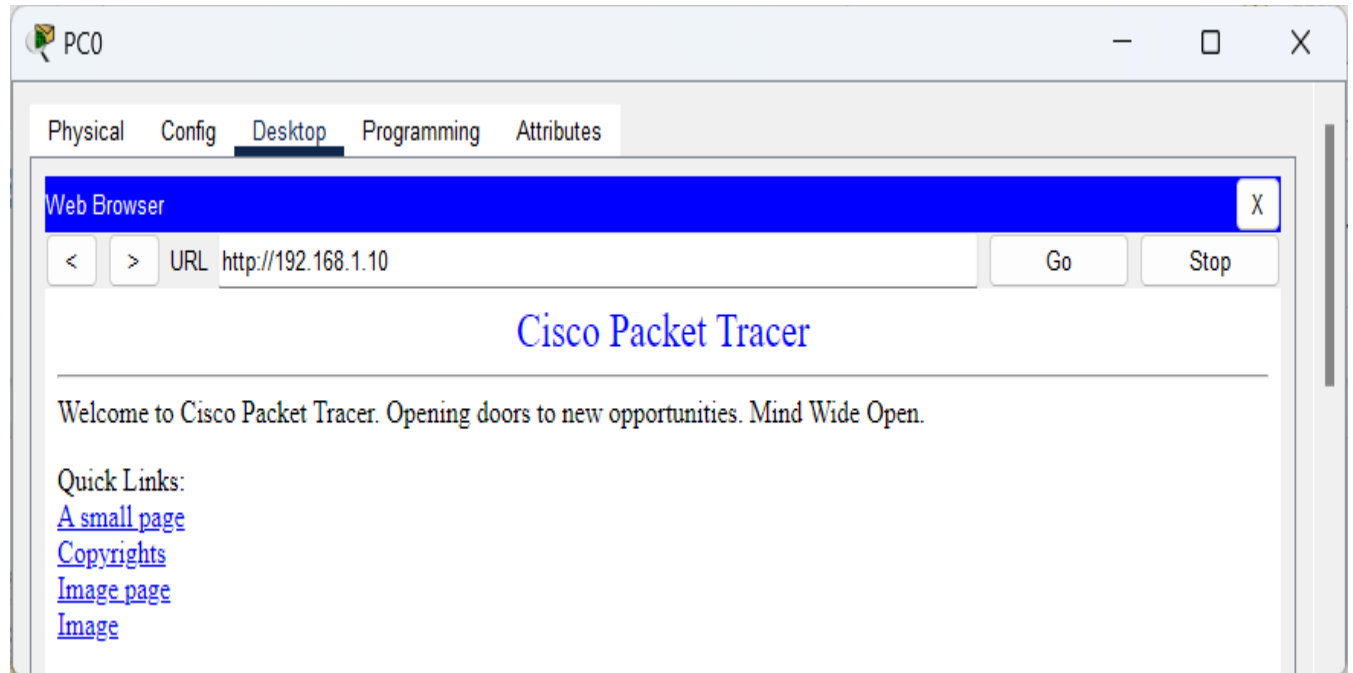
Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Other way to test this setup, click PC0/PC1 and Web Browser and enter <http://192.168.1.10> in URL.



OUTPUT:

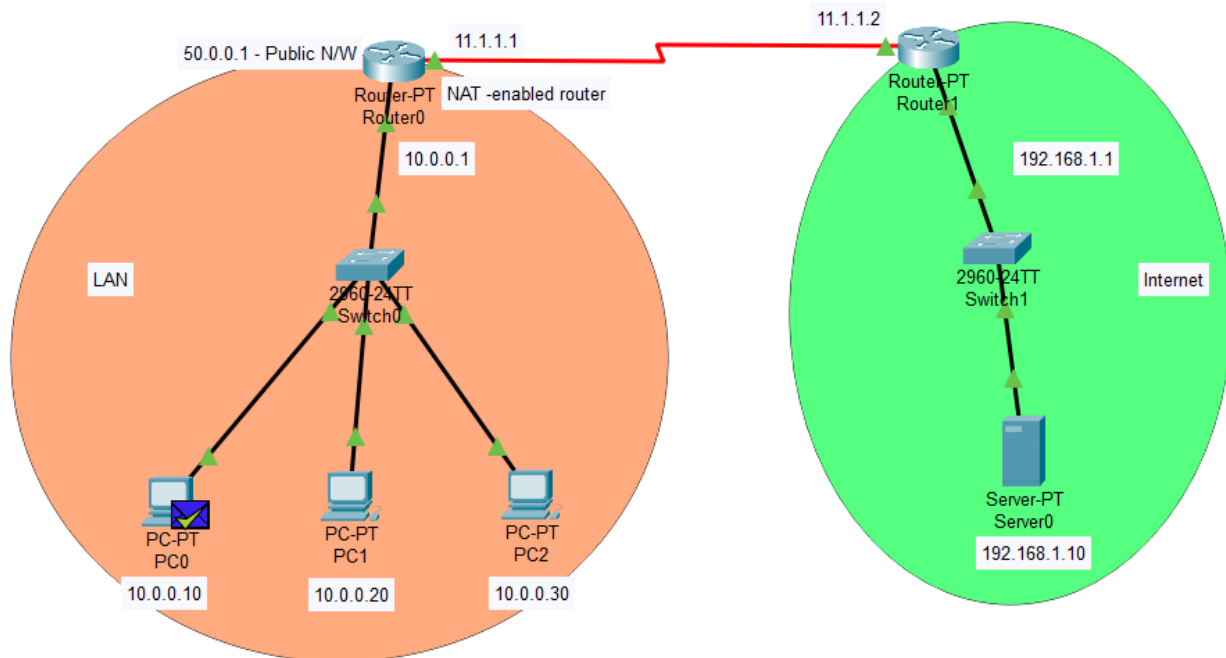


Fig: Simulation output from PC0 to Server

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	Router0	ICMP
	0.003	Router0	Router1	ICMP
	0.004	Router1	Switch1	ICMP
	0.005	Switch1	Server0	ICMP
	0.006	Server0	Switch1	ICMP
	0.007	Switch1	Router1	ICMP
	0.008	Router1	Router0	ICMP
	0.009	Router0	Switch0	ICMP
	0.010	Switch0	PC0	ICMP
Reset Simulation <input checked="" type="checkbox"/> Constant Delay Captured to: 0.010 s				
Play Controls				
Event List Filters - Visible Events ICMP Edit Filters Show All/None				



PDU Information at Device: Router0

At Device: Router0
Source: PC0
Destination: Server0

OSI Model Inbound PDU Details Outbound PDU Details

In Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IP Header Src. IP: 10.0.0.10, Dest. IP: 192.168.1.10 ICMP Message Type: 8
- Layer 2: Ethernet II Header 0001.C76C.3E78 >> 0010.116A.AD61
- Layer 1: Port FastEthernet0/0

Out Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IP Header Src. IP: 50.0.0.2, Dest. IP: 192.168.1.10 ICMP Message Type: 8
- Layer 2: HDLC Frame HDLC
- Layer 1: Port(s): Serial2/0

1. The routing table finds a routing entry to the destination IP address.
2. The device decrements the TTL on the packet.

Challenge Me << Previous Layer Next Layer >>

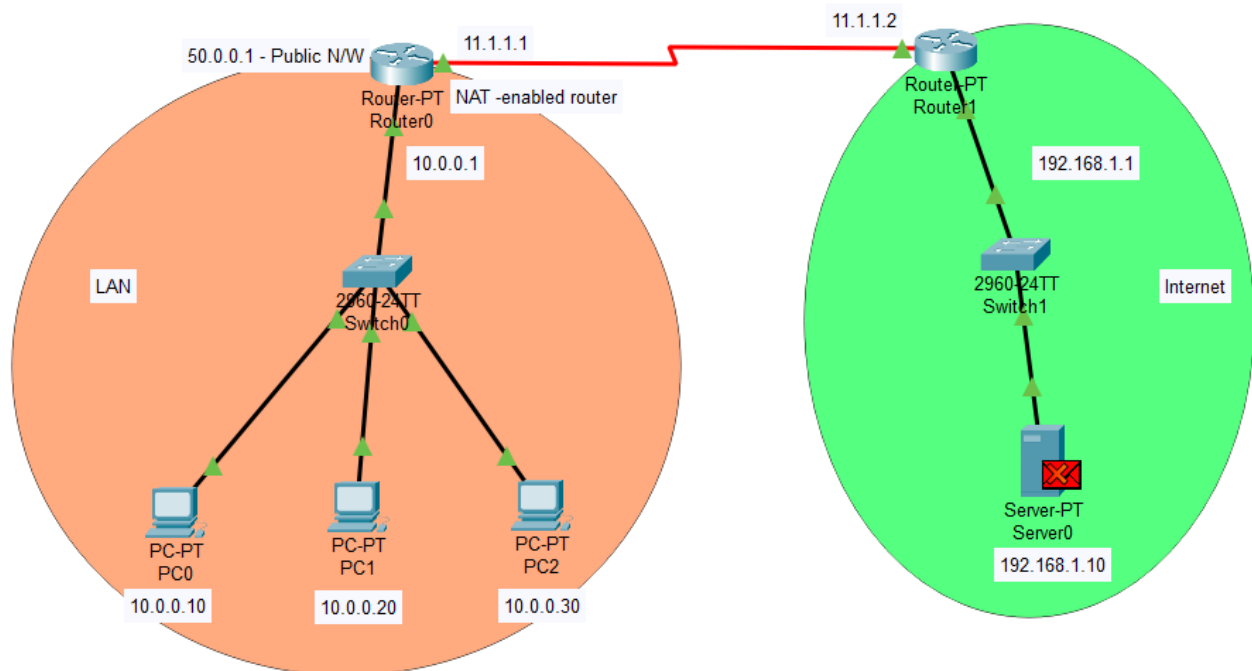


Fig: Simulation output from PC2 to Server

CONCLUSION:

We have successfully designed and simulated NAT on router using Cisco packet tracer.