Ex.No:11	STUDY OF IPV6 ADDRESSING & SUBNETTING
Date:	

AIM:

To Study the IPV6 Addressing and Subnetting

What is IPv6:

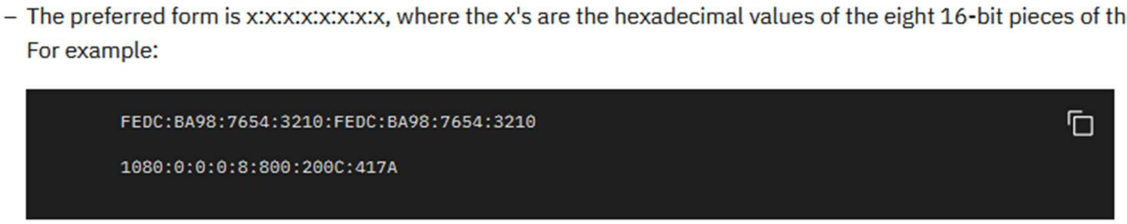
As the number of internet devices—also known as the Internet of Things (IoT)—increases around the world, more IP addresses are needed for these devices to communicate data. Consider smartphones, smartwatches, refrigerators, washing machines, smart TVs, and other electronic devices that require an IP address. All of these devices are now linked to the internet and have a unique IP address assigned to them. We'll focus on IPv6, its characteristics, and why it'll be the Internet Protocol standard in this quick overview.

Before we go into the technicalities, there are a few things to know about IPv6:

1. IPv6 addresses are 128-bit (2128) and allow for 3.4 x 1038 unique IP addresses.
2. IPv6 is written in hexadecimal notation, with the colons separating eight groups of 16 bits, for a total of 8 x 16 = 128, or bits. The following is an example of an IPv6 address:

➢ Syntax of IPv6 Addresses:

IPv4 addresses are represented in dotted-decimal format. The 32-bit address is divided along 8-bit boundaries. Each set of 8 bits is converted to its decimal equivalent and separated by periods. In contrast, IPv6 addresses are 128 bits divided along 16-bit boundaries. Each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons. The resulting representation is called colon-hexadecimal.



– The preferred form is x:x:x:x:x:x:x:x, where the x's are the hexadecimal values of the eight 16-bit pieces of the address.
For example:

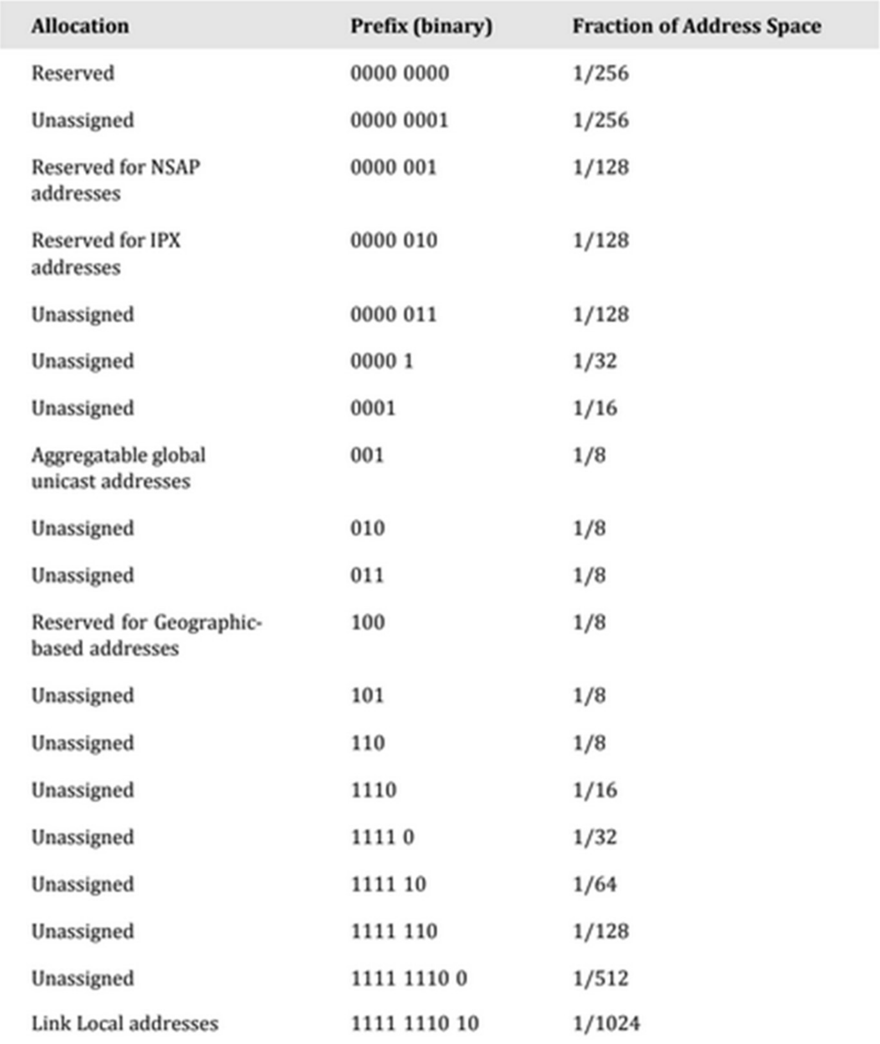
```
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A
```

➢ The Addressing Space:

The amount of memory dedicated to all potential addresses for a computational object, such as a device, a file, a server, or a networked computer, is known as address space. A range of physical or virtual addresses accessible to a processor or reserved for a process is referred to as address space. Each address defines an entity's location as a unique identifier of single entities (unit of memory that can be addressed separately). Each computer device and process is given address space on the computer, which is a piece of the processor's address space. The address space of a processor is always constrained by the width of its address bus and registers. Flat address space, in which addresses are expressed as continuously growing integers starting at zero, and segmented address space, in which addresses are written as discrete segments enhanced by offsets, are the two types of address space (values added to produce secondary addresses). Thunking is a procedure that allows address space to be changed from one format to another in some systems.

In terms of IP address space, there has been concern that IPv4 (Internet Protocol Version 4) had not anticipated the enormous growth of the Internet, and that its 32-bit address space would not be adequate. For that reason, IPv6 has been developed with 128-bit address space.

Allocation of the IPv6 addressing space:



Allocation	Prefix (binary)	Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP addresses	0000 001	1/128
Reserved for IPX addresses	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Aggregatable global unicast addresses	001	1/8
Unassigned	010	1/8
Unassigned	011	1/8
Reserved for Geographic-based addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link Local addresses	1111 1110 10	1/1024

- **Types of IPv6 Addresses:**

Generally, IPv6 addresses is classified into 3. They are:

1. Unicast: This type is the address of a single interface. A packet forwarded to a unicast address is delivered only to the interface identified by that address.
2. Anycast: This type is the address of a set of interfaces typically belonging to different nodes. A packet forwarded to an anycast address is delivered to only one interface of the set (the nearest to the source node, according to the routing metric).
3. Multicast: This type is the address of a set of interfaces that typically belong to different nodes. A packet forwarded to a multicast address is delivered to all interfaces belonging to the set.

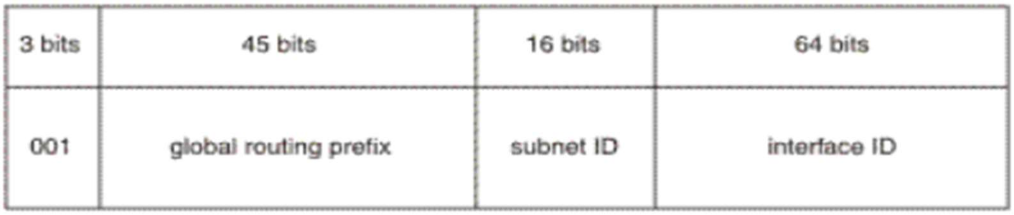
1. Unicast Addresses:

A unicast address identifies a single interface. When a network device sends a packet to a unicast address, the packet goes only to the specific interface identified by that address. Unicast addresses support a global address scope and two types of local address scopes.

A unicast address consists of *n* bits for the prefix, and 128 – *n* bits for the interface ID.

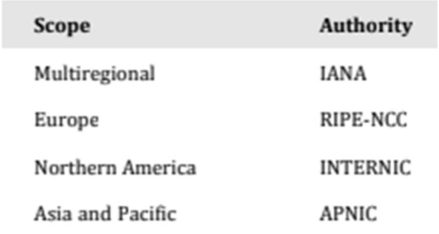
- Global unicast address—A unique IPv6 address assigned to a host interface. These addresses have a global scope and essentially the same purposes as IPv4 public addresses. Global unicast addresses are routable on the Internet.
- Link-local IPv6 address—An IPv6 address that allows communication between neighboring hosts that reside on the same link. Link-local addresses have a local scope, and cannot be used outside the link. They always have the prefix FE80::/10.
- Loopback IPv6 address—An IPv6 address used on a loopback interfaces. The IPv6 loopback address is 0:0:0:0:0:0:0:1, which can be notated as ::1/128.
- Unspecified address—An IPv6 unspecified address is 0:0:0:0:0:0:0:0, which can be notated as ::/128.

1. Aggregatable Global Unicast Addresses:
   Aggregate global unicast addresses are used for global communication. These addresses are similar in function to IPv4 addresses under classless interdomain routing (CIDR). The following table shows their format.



3 bits	45 bits	16 bits	64 bits
001	global routing prefix	subnet ID	interface ID

2. Geographic-Based Addresses:
   Geography addresses are those determined by country of origin. This type of address is only available in the IPv4 address category. The data address table includes a 'scope' and a 'authority'



Scope	Authority
Multiregional	IANA
Europe	RIPE-NCC
Northern America	INTERNIC
Asia and Pacific	APNIC

3. Link Local Addresses:
   A link-local address is a network address that is valid only for communications within the network segment or the broadcast domain that the host is connected to. Link-local addresses are most often assigned automatically with a process known as stateless address autoconfiguration or link-local address autoconfiguration,[1] also known as automatic private IP addressing (APIPA) or auto-IP.

4. Site Local Addresses:

Site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix. A site-local address cannot be reached from another site. A site-local address is not automatically assigned to a node. It must be assigned using automatic or manual configuration.

5. The Unspecified Address:
   The address 0:0:0:0:0:0:0:0 is called the unspecified address. It will not be assigned to any node. It indicates the absence of an address. One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.

6. The Loopback Address:
   The IP address 127.0.0.1 is called a loopback address. Packets sent to this address never reach the network but are looped through the network interface card only. This can be used for diagnostic purposes to verify that the internal path through the TCP/IP protocols is working.

7. NSAP Addresses:
   Short for Network Service Access Point, NSAP is an address consisting of up to 20 octets that identify a computer or network connected to an ATM network. NSAP is defined in ISO/IEC 8348.

8. IPX Addresses:
   Internetwork Packet Exchange (IPX) is the network layerprotocol in the IPX/SPXprotocol suite. IPX is derived from Xerox Network Systems' IDP. It may act as a transport layer protocol as well.

2. Anycast Address:

An anycast address identifies a set of interfaces that typically belong to different nodes. Anycast addresses are similar to multicast addresses, except that packets are sent only to one interface, not to all interfaces. The routing protocol used in the network usually determines which interface is physically closest within the set of anycast addresses and routes the packet along the shortest path to its destination.

There is no difference between anycast addresses and unicast addresses except for the subnet-router address. For an anycast subnet-router address, the low-order bits, typically 64 or more, are zero. Anycast addresses are taken from the unicast address space.

3. Multicast Addresses:

A multicast address identifies a set of interfaces that typically belong to different nodes. When a network device sends a packet to a multicast address, the device broadcasts the packet to all interfaces identified by that address. IPv6 does not support broadcast addresses, but instead uses multicast addresses in this role.

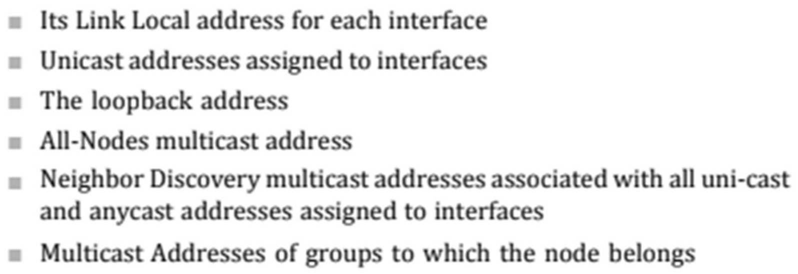
Multicast addresses support 16 different types of address scope, including node, link, site, organization, and global scope. A 4-bit field in the prefix identifies the address scope.

The following types of multicast addresses can be used in an IPv6 subscriber access network:

- Solicited-node multicast address—Neighbor Solicitation (NS) messages are sent to this address.
- All-nodes multicast address—Router Advertisement (RA) messages are sent to this address.
- All-routers multicast address—Router Solicitation (RS) messages are sent to this address.

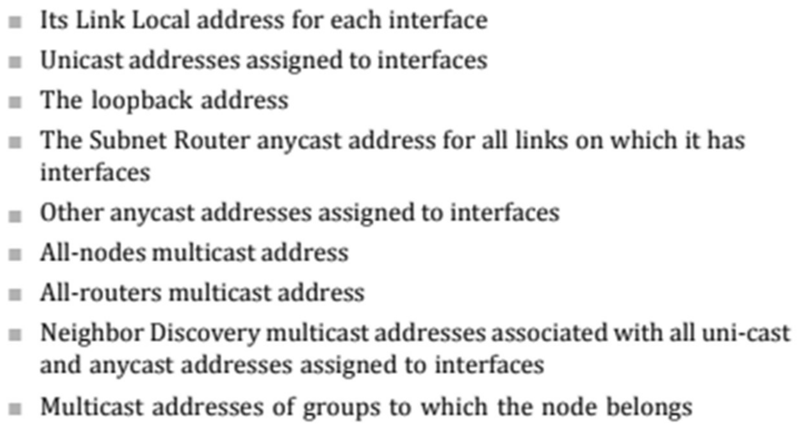
➢ **Which addresses are generally used for a node?**

1. **Addresses of a Host:**



- Its Link Local address for each interface
- Unicast addresses assigned to interfaces
- The loopback address
- All-Nodes multicast address
- Neighbor Discovery multicast addresses associated with all uni-cast and anycast addresses assigned to interfaces
- Multicast Addresses of groups to which the node belongs

2. **Addresses of a Router:**



- Its Link Local address for each interface
- Unicast addresses assigned to interfaces
- The loopback address
- The Subnet Router anycast address for all links on which it has interfaces
- Other anycast addresses assigned to interfaces
- All-nodes multicast address
- All-routers multicast address
- Neighbor Discovery multicast addresses associated with all uni-cast and anycast addresses assigned to interfaces
- Multicast addresses of groups to which the node belongs

Result :

Hence Study of IPV6 Addressing & Subnetting is completed sucessfully

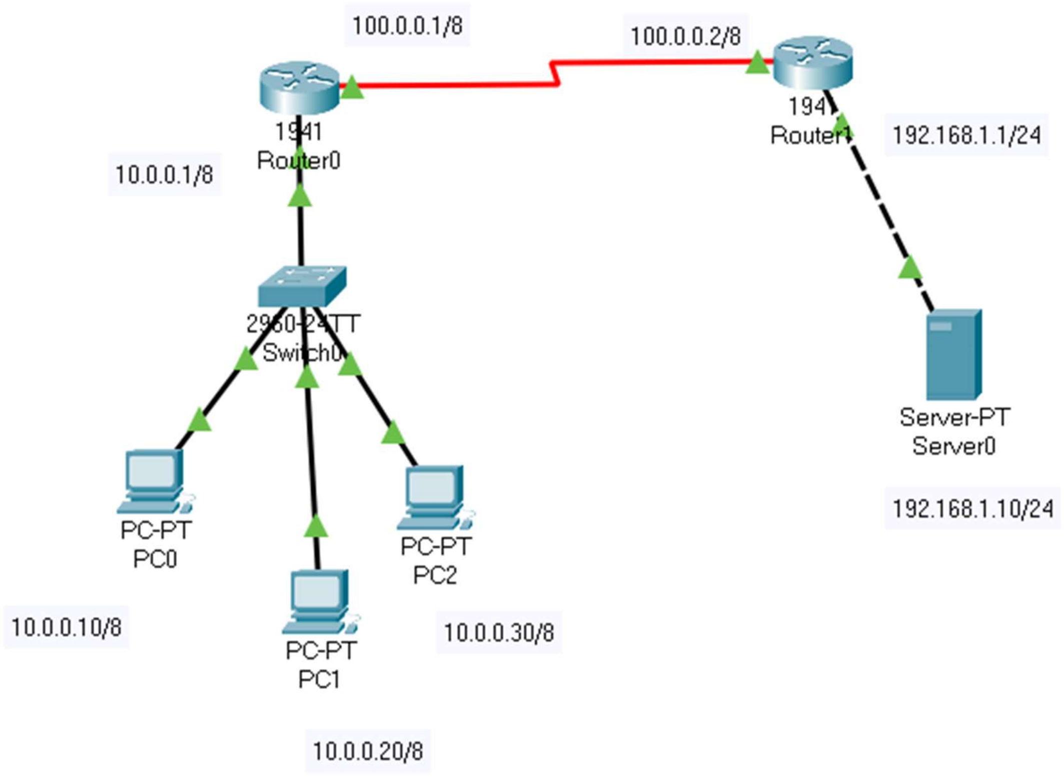
Ex.No:12	IMPLEMENTATION OF NETWORK ADDRESS TRANSLATION
Date:	

Aim:

To study and perform Network Address Translation (NAT) using cisco packet tracer.

Procedure:

1. Assign the following topology with respective IP addresses to pc, routers, servers and connection between them.



2. **Configure static NAT configuration**

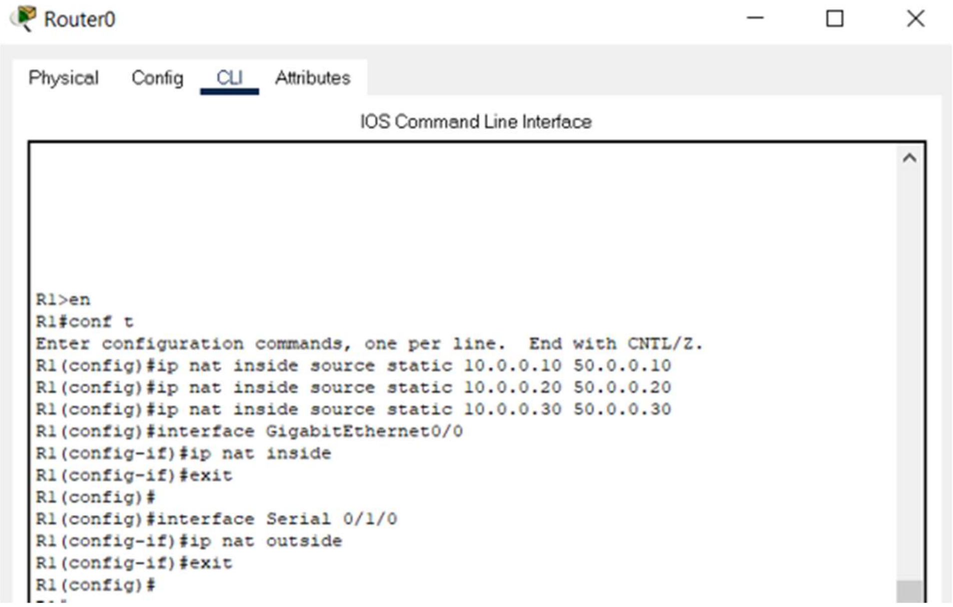
Since static NAT use manual translation, we have to map each inside local IP address (which needs a translation) with inside global IP address. Following command is used to map the inside local IP address with inside global IP address.

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

And use the following commands to define inside and outside network connection for your local and global IP addresses.

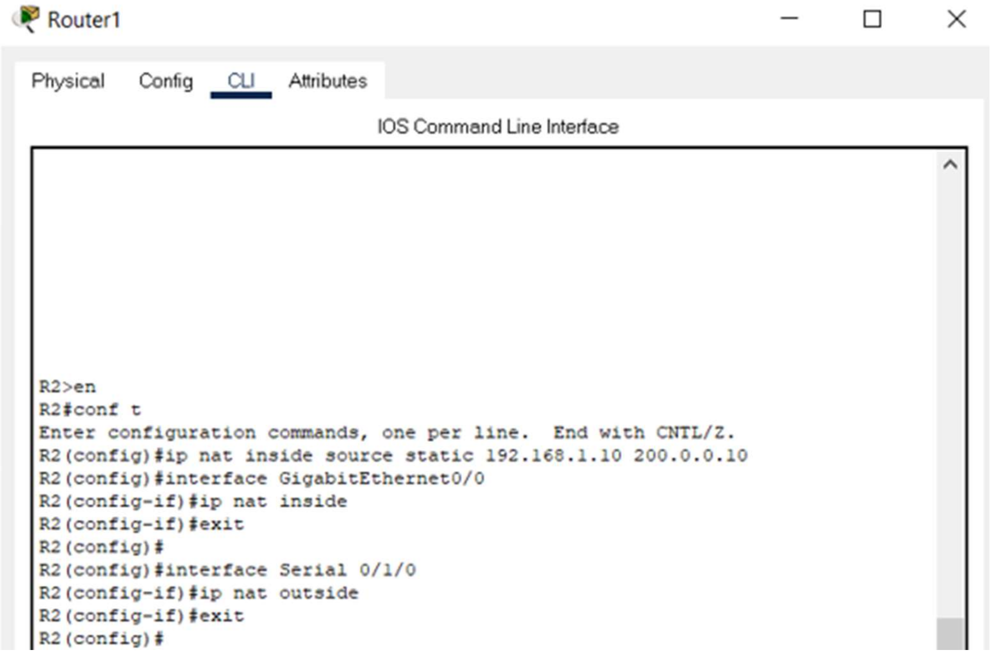
```
Router(config-if)#ip nat inside
Router(config-if)#ip nat outside
```

Static NAT configuration for Router0 connected with 3 pc's:



```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip nat inside source static 10.0.0.10 50.0.0.10
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
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#
R1(config)#interface Serial 0/1/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#
```

Static NAT configuration for Router0 connected with server:

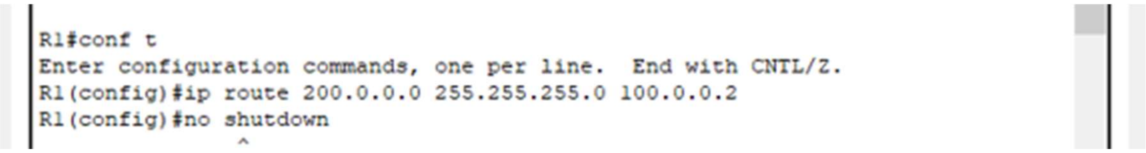


```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat inside source static 192.168.1.10 200.0.0.10
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
R2(config)#interface Serial 0/1/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#
```

3.Configure the IP routing

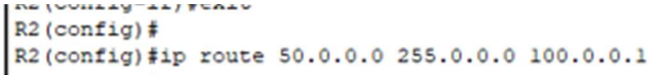
IP routing is the process which allows router to route the packet between different networks.

IP routing on router0:



```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 200.0.0.0 255.255.255.0 100.0.0.2
R1(config)#no shutdown
               ^
```

IP routing on router1:



```
R2(config-if)#exit
R2(config)#
R2(config)#ip route 50.0.0.0 255.0.0.0 100.0.0.1
```

4.Testing Static NAT Configuration

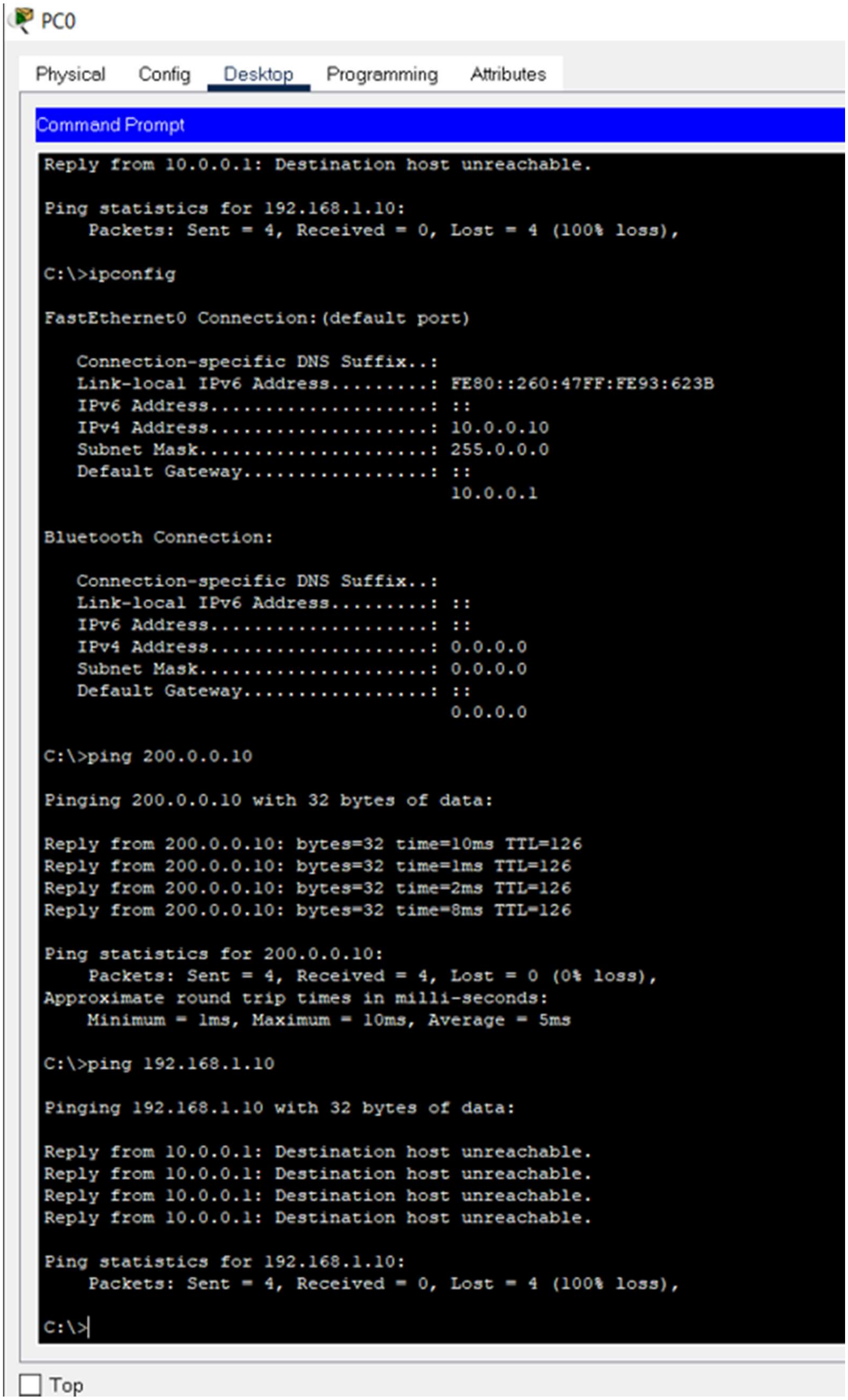
To test this setup click on any PC and Desktop and click Command Prompt.

- 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.

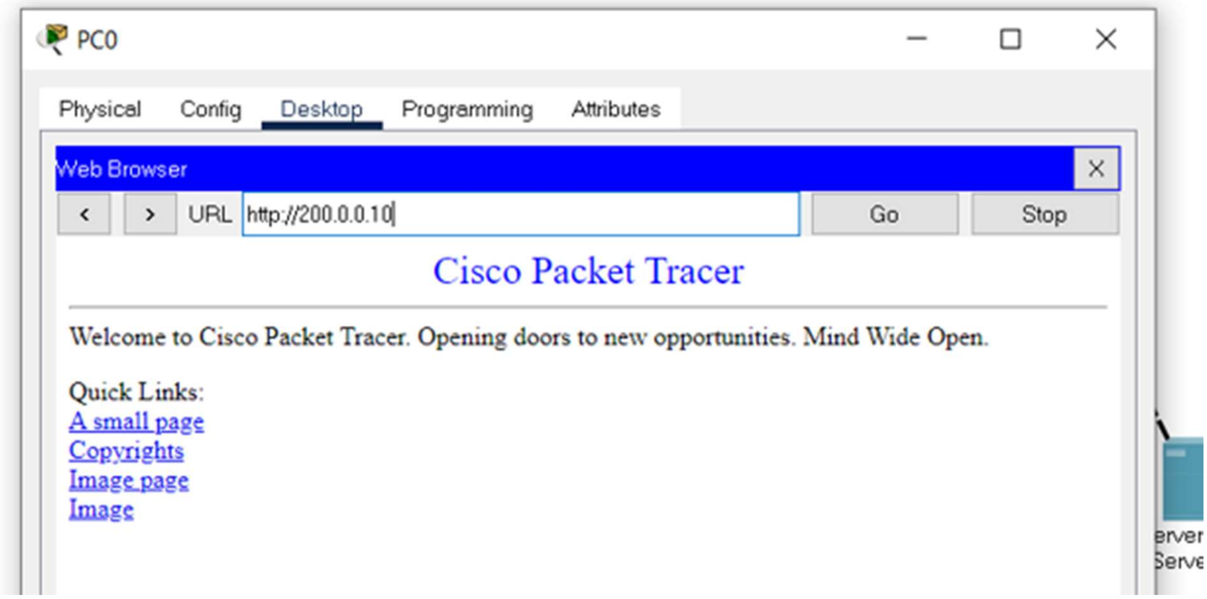
Second command checks whether we are able to access the remote device or not. A ping reply confirms that we are able to connect with remote device on this IP address.

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.



```
Reply from 10.0.0.1: Destination host unreachable.

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

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::260:47FF:FE93:623B
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.10
   Subnet Mask.....................: 255.0.0.0
   Default Gateway.................: ::
                                     10.0.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

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=10ms TTL=126
Reply from 200.0.0.10: bytes=32 time=1ms TTL=126
Reply from 200.0.0.10: bytes=32 time=2ms TTL=126
Reply from 200.0.0.10: bytes=32 time=8ms TTL=126

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 5ms

C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.

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

C:\>
```

Another way of testing is via browser:



URL http://200.0.0.10

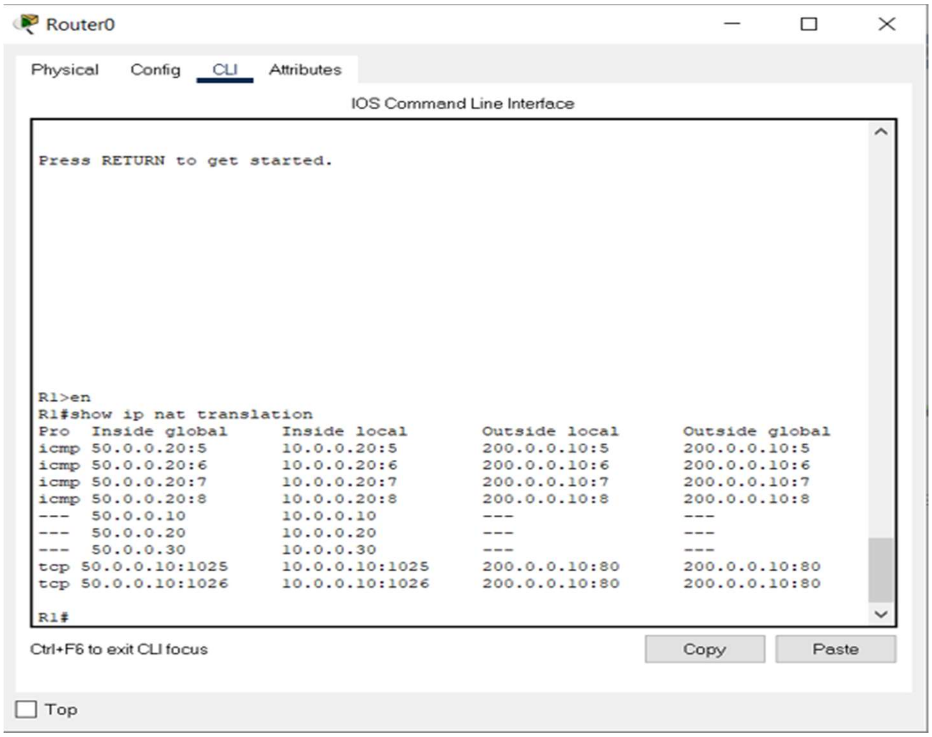
Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

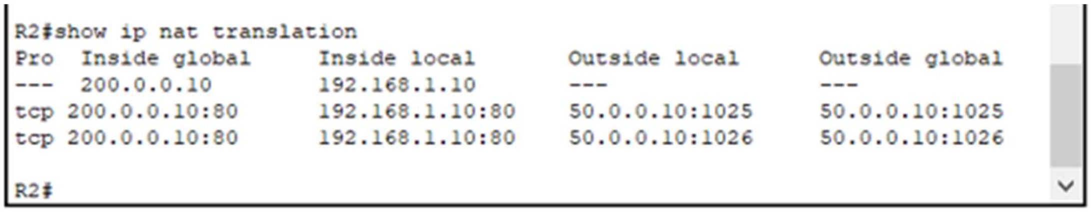
We can also verify this translation on router with ***show ipnat translation*** command.

For router0:



```
Press RETURN to get started.








R1>en
R1#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 50.0.0.20:5       10.0.0.20:5        200.0.0.10:5       200.0.0.10:5
icmp 50.0.0.20:6       10.0.0.20:6        200.0.0.10:6       200.0.0.10:6
icmp 50.0.0.20:7       10.0.0.20:7        200.0.0.10:7       200.0.0.10:7
icmp 50.0.0.20:8       10.0.0.20:8        200.0.0.10:8       200.0.0.10:8
---  50.0.0.10         10.0.0.10          ---                ---
---  50.0.0.20         10.0.0.20          ---                ---
---  50.0.0.30         10.0.0.30          ---                ---
tcp 50.0.0.10:1025     10.0.0.10:1025     200.0.0.10:80      200.0.0.10:80
tcp 50.0.0.10:1026     10.0.0.10:1026     200.0.0.10:80      200.0.0.10:80

R1#
```

For router1:



```
R2#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  200.0.0.10        192.168.1.10       ---                ---
tcp 200.0.0.10:80      192.168.1.10:80    50.0.0.10:1025     50.0.0.10:1025
tcp 200.0.0.10:80      192.168.1.10:80    50.0.0.10:1026     50.0.0.10:1026

R2#
```

Result:

Henceforth, Network Address Translation (NAT) using cisco packet tracer implemented and verified.