Computer Network

LABORATORY PROJECT

ON

Network Address Translation

Submitted

In partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology in

Computer Science Engineering (Artificial Intelligence & Machine Learning)

by

GUGULAVATH NAVEEN 23261A6615

KHYATI CHINTHA 23261A6620

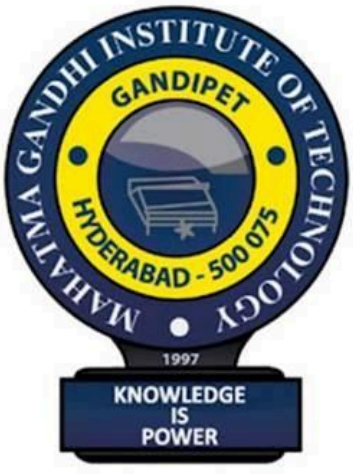
Under the guidance of

Mrs. A. Swapna

ASSISTANT PROFESSOR

DEPARTMENT OF EMERGING TECHNOLOGIES

MAHATMA GANDHI INSTITUTE OF TECHNOLOGY



Department of Emerging Technologies

MAHATMA GANDHI INSTITUTE OF TECHNOLOGY

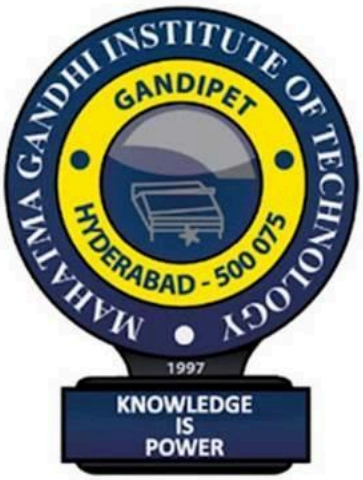
GANDIPET, HYDERABAD-500075, INDIA

October 2025

MAHATMA GANDHI INSTITUTE OF TECHNOLOGY

(Affiliated To Jawaharlal Nehru Technological University Hyderabad)
GANDIPET, HYDERABAD-500075, Telangana

CERTIFICATE



This is to certify that the project entitled "**Network Address Translation**" is being submitted by GUGULAVATH NAVEEN 23261A6615 and KHYATI CHINTHA 23261A6620 in partial fulfilment of the requirement for the **Laboratory Project** in **EMERGING TECHNOLOGIES** is a record of bonafide work carried out by them. The results of the investigations enclosed in this report have been verified and found satisfactory.

Mrs. A. Swapna
Assistant Professor
ET Department
MGIT

Network Address Translation (NAT)

Introduction

Network Address Translation (NAT) is a process used in intermediate network devices (typically routers or firewalls) to modify IP address and port information in packet headers. NAT allows communication between private networks and the public Internet even when the devices inside the private network do not have globally unique IP addresses.

It acts as a translator, ensuring that private IP addresses (not routable on the Internet) can still send and receive data via a public IP address.

Why NAT Became Essential

1. IPv4 Address Exhaustion: Before NAT, every device needed a unique public IPv4 address. This became impossible due to the explosion of devices (phones, PCs, IoT, servers). NAT allows organizations to use limitless private IPs internally.

2. Simplified Network Management: Organizations can redesign internal networks without changing their public IPs.

3. Privacy & Security: Since internal private addresses are not exposed on the Internet, attackers cannot directly target internal devices without NAT rules.

4. Controlled Internet Access: Network admins can define what internal hosts can access outside, and what external traffic can reach inside.

Private IP Ranges (Used by NAT)

According to RFC 1918:

Class	Private IP Range
A	10.0.0.0 – 10.255.255.255
B	172.16.0.0 – 172.31.255.255
C	192.168.0.0 – 192.168.255.255

These addresses cannot exist on the public Internet. NAT converts them before sending traffic out.

How NAT Works Internally

When a device inside a private network sends a packet to the Internet:

1. Source IP = Private IP (e.g., 192.168.1.10)

2. Packet reaches router.

3. Router changes it to: Source IP = Public IP (e.g., 203.0.113.5)

4. Router records this mapping in the NAT Translation Table.

5. When a reply returns, NAT uses this table to map the packet back to the correct internal device.

NAT Table Example

Inside Local	Inside Global	Outside Local	Outside Global
192.168.1.5:1025	203.0.113.5:50000	142.250.1.2:80	142.250.1.2:80

The port numbers help distinguish multiple internal connections.

Types of NAT

1. Static NAT (One-to-One Mapping)

Static NAT establishes a permanent, manual, and fixed mapping between a private IP address and a public IP address.

This mapping can be unidirectional (inside → outside) or bidirectional (inside ↔ outside), depending on the configuration.

Key Characteristics

The mapping is manually created by the network administrator.

The same public IP is always used for the same internal device.

Provides predictable, consistent translation — essential for devices that need to be reachable from outside.

Mapping remains constant, regardless of the number of sessions or traffic conditions.

Works at the Network Layer (Layer 3) by modifying the IP header.

How Static NAT Works

Static NAT performs a permanent, one-to-one translation between a private IP address and a public IP address. Here is the detailed sequence of operations:

1. Internal Device Sends a Packet

A device inside the private network (example: 10.10.10.2) wants to communicate with an external host (example: 8.8.8.8).

It creates an IP packet with:

Source IP: 10.10.10.2 (private IP)

Destination IP: 8.8.8.8 (public Internet server)

This packet is forwarded to the NAT-enabled router because the router is the default gateway.

2. Packet Arrives at the NAT Router

The NAT router receives the packet on its inside interface (marked with ip nat inside).

The router checks:

“Is there a static NAT rule for this private IP?”

Example static mapping:

10.10.10.2 ↔ 50.50.50.2

Since the mapping exists, the router knows exactly which public IP must replace the private one.

3. Router Replaces the Source Private IP

The NAT router modifies the IP header:

Old Source IP: 10.10.10.2

New Source IP: 50.50.50.2

Nothing else changes.

The destination IP, ports, payload remain the same.

This process is called source NAT (SNAT).

4. NAT Router Creates (or Confirms) Translation Table Entry

Since this is static NAT, the entry already exists by configuration.

The router maintains a translation table such as:

Private IP	Public IP	Direction
10.10.10.2	50.50.50.2	Static

Static entries do not time out or expire.

They remain permanently stored in the NAT table.

5. Packet Goes to the Internet

Because the packet now has a public source IP, it can travel through the Internet.

To the outside world, the internal device now appears as:

50.50.50.2

This hides internal addresses and ensures private IPs are never exposed.

6. External Server Sends a Reply

The external server (8.8.8.8) processes the request and sends back a response.

Reply packet fields:

Source IP: 8.8.8.8

Destination IP: 50.50.50.2 (public IP of the NAT router)

7. Reply Packet Reaches NAT Router

When the reply hits the NAT router's outside interface (ip nat outside), the router checks:

"Is this destination public IP mapped to an internal private IP?"

It finds:

50.50.50.2 → 10.10.10.2

8. Router Performs Reverse Translation

The router modifies the destination IP in the reply packet:

Old Destination IP: 50.50.50.2

New Destination IP: 10.10.10.2

This is called destination NAT (DNAT).

The router keeps ports and payload unchanged.

9. Packet Delivered to Internal Device

The packet is forwarded inside the private network and reaches the internal host that originally made the request.

The internal device sees the reply as if it communicated directly with 8.8.8.8 — but in reality, NAT was translating IPs the whole time.

Key Points Strengthening the Explanation

1) NAT Hides Internal IPs

External users can never see 10.10.10.2.

They always see only the mapped public IP.

2) Static NAT Mapping Is Permanent

Unlike Dynamic NAT or PAT, the mapping:

does not time out

does not depend on sessions

does not change with traffic load

3) Routing and NAT Are Both Required

NAT handles translation.

Routing handles forwarding.

4) The Public IP Must Be Reachable

Proper routing must exist so the static public IP can return traffic to the NAT router.

Real-World Use Cases

Static NAT is commonly used when internal systems must be reachable from the Internet:

Hosting Internal Servers Externally

Web Server (HTTP/HTTPS)

DNS Server

Email Server / FTP Server

Surveillance and Security

CCTV cameras accessible from outside

DVR/NVR remote access

Remote Access

Remote Desktop (RDP) to a dedicated internal PC

Access to application servers, IoT devices, gateways

Business Use

When a company needs to expose any internal service publicly

When vendors or partners need a fixed endpoint

When firewall policies require static public IP bindings

Advantages

Predictable and stable communication because the public IP never changes.

Enables incoming external connections — suitable for hosting services.

Simplifies firewall rules and access control since IPs are fixed.

Easy to configure and troubleshoot.

Disadvantages

Consumes public IP addresses — one public IP per internal device.

Not scalable for large networks with many servers.

Provides no inherent security (must be paired with firewall or ACLs).

Manual configuration increases administrative overhead.

Static NAT Configuration

Network Setup:

Private Network: 10.10.10.0/24
Public Network: 50.50.50.0/24
External Network: 60.60.60.0/24
Router1 performs Static NAT
Router2 connects to the external network

Steps:

1. Assign IP addresses to all devices and router interfaces.
2. Configure inside and outside interfaces:

Router(config)# interface fastEthernet0/0

Router(config-if)# ip address 10.10.10.1 255.255.255.0

Router(config-if)# ip nat inside

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface fastEthernet0/1

Router(config-if)# ip address 192.162.10.1 255.255.255.0

Router(config-if)# ip nat outside

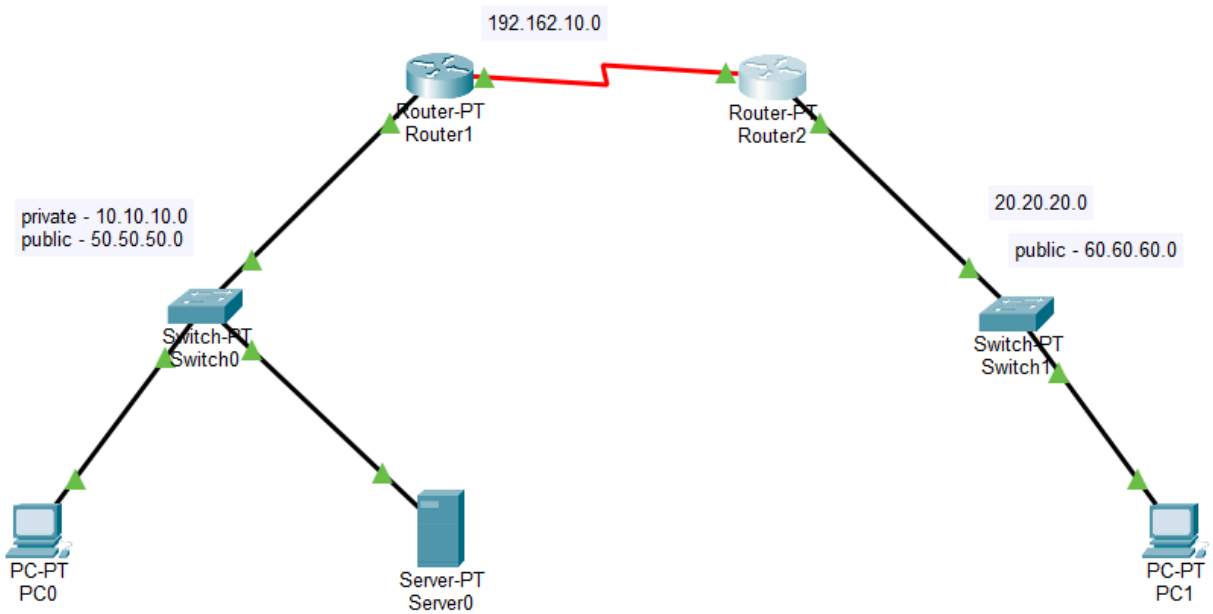
Router(config-if)# no shutdown

Router(config-if)# exit

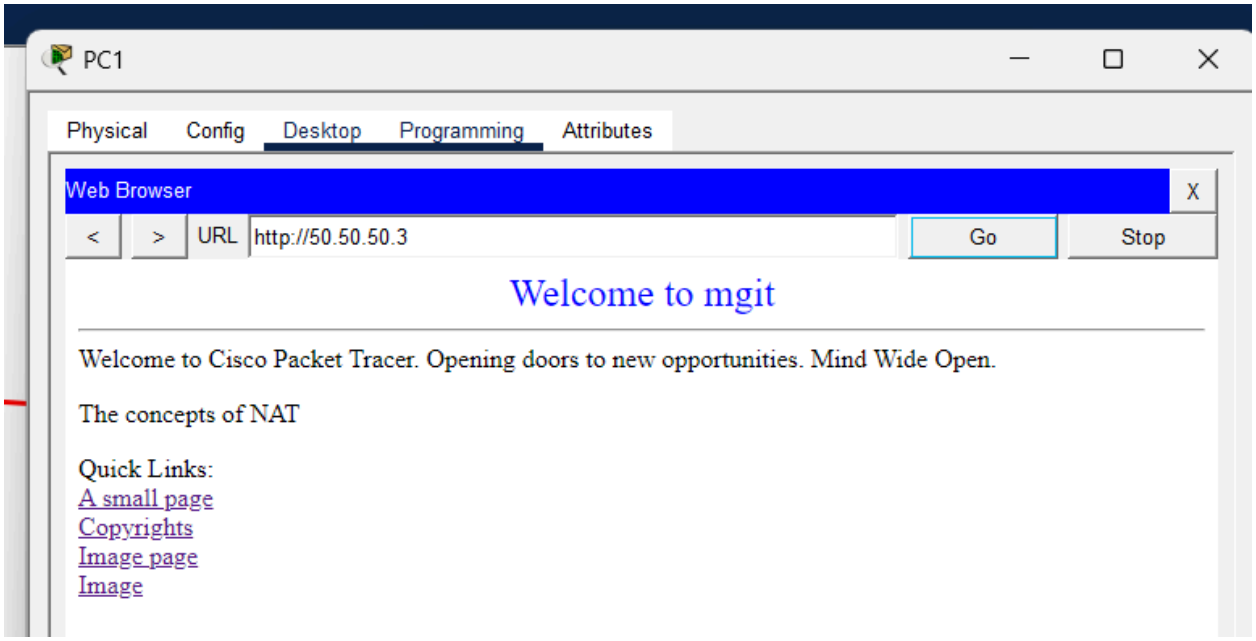
Create a Static NAT mapping:

Router(config)# ip nat inside source static 10.10.10.2 50.50.50.2

Router(config)# ip nat inside source static 10.10.10.3 50.50.50.3



Output:



2) Dynamic NAT (Many-to-Many Mapping)

Dynamic NAT provides on-demand translation between internal private IP addresses and a pool of public IP addresses.

Unlike Static NAT, where each internal device has a fixed public IP, Dynamic NAT assigns a temporary public IP only when needed.

Key Characteristics

Uses a pool (range) of public IP addresses.

Example: 50.50.50.10 – 50.50.50.20

Mapping is not permanent; it only exists when a session is active.

Each internal private IP is assigned a public IP from the pool randomly or sequentially.

When the session ends, the mapping expires and the public IP becomes available for others.

No two internal hosts can share the same public IP at the same time (unlike PAT).

How Dynamic NAT Works

1. Internal Host Initiates Traffic

A private device (e.g., 10.10.10.5) sends a packet to the Internet.

Packet details:

Source IP: 10.10.10.5

Destination IP: 8.8.8.8

Since the destination is outside the local network, packets go to the NAT router.

2. Router Receives Packet and Checks NAT Pool

The router looks at its configured NAT pool:

Example Pool: 50.50.50.10 – 50.50.50.20

The router checks:

“Is there a public IP available in the pool?”

If yes, it assigns one.

If no, the packet is dropped (pool exhausted).

3. Router Assigns a Temporary Public IP

Suppose the router assigns 50.50.50.11 to 10.10.10.5.

The router updates its NAT table:

Private IP	Public IP	Type
10.10.10.5	50.50.50.11	Dynamic

This mapping is temporary and tied to the session.

4. Packet Source IP Is Replaced

The router changes:

Old Source IP: 10.10.10.5

New Source IP: 50.50.50.11

Then it forwards the packet to the Internet.

5. External Server Sends a Reply

The server replies back to:

Destination IP: 50.50.50.11

6. Router Performs Reverse Translation

The router checks its NAT table and finds:

50.50.50.11 → 10.10.10.5

It replaces the destination address:

Old Destination IP: 50.50.50.11

New Destination IP: 10.10.10.5

Then it forwards the packet to the internal host.

7. Mapping Expires After Session Ends

When the internal host finishes communication:

Idle timeout expires

Session ends

The NAT mapping is removed

Public IP returns to the pool

This ensures efficient use of public addresses.

Use Cases of Dynamic NAT

Enterprise Environments

Companies that purchased multiple public IPs

Want outbound Internet access for many internal users

Scenarios Where Inbound Traffic Is Not Required

Internal systems only need to initiate connections

Services inside the network do not need to be accessed from outside

Temporary Access Needs

Employees accessing external cloud applications

Testing labs needing external access without permanent mapping

Advantages of Dynamic NAT

1) More efficient than Static NAT

Public IPs are reused when sessions end

No fixed one-to-one mapping required

2) Provides privacy and security

Internal IPs remain hidden from external networks

Attackers cannot see private addressing schemes

3) Reduces administrative overhead

No need to manually configure a public IP for every internal device

Disadvantages of Dynamic NAT

1) Still requires multiple public IPs

You must have a pool of public addresses

Not suitable when you only have 1 IP (PAT is better)

2) No inbound connections allowed

External hosts cannot reach internal devices

Mapping is not predictable or permanent

Not suitable for hosting websites or servers

3) Mapping fails if pool runs out

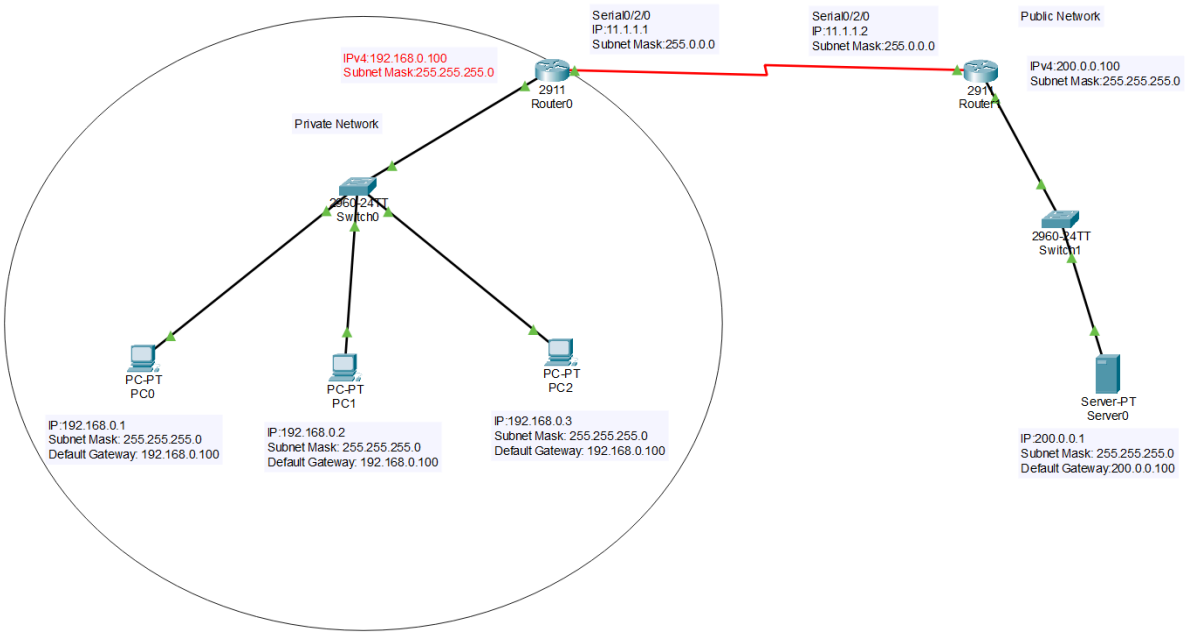
When all public IPs are used, new connections fail

Users may experience connection drops under high load

Dynamic NAT Configuration

Network Setup:

Inside Network: 192.168.0.0/24
Public Network: 11.1.1.0/24
Outside Network: 200.0.0.0/24
Router0 performs Dynamic NAT
Router1 connects to the public/outer network

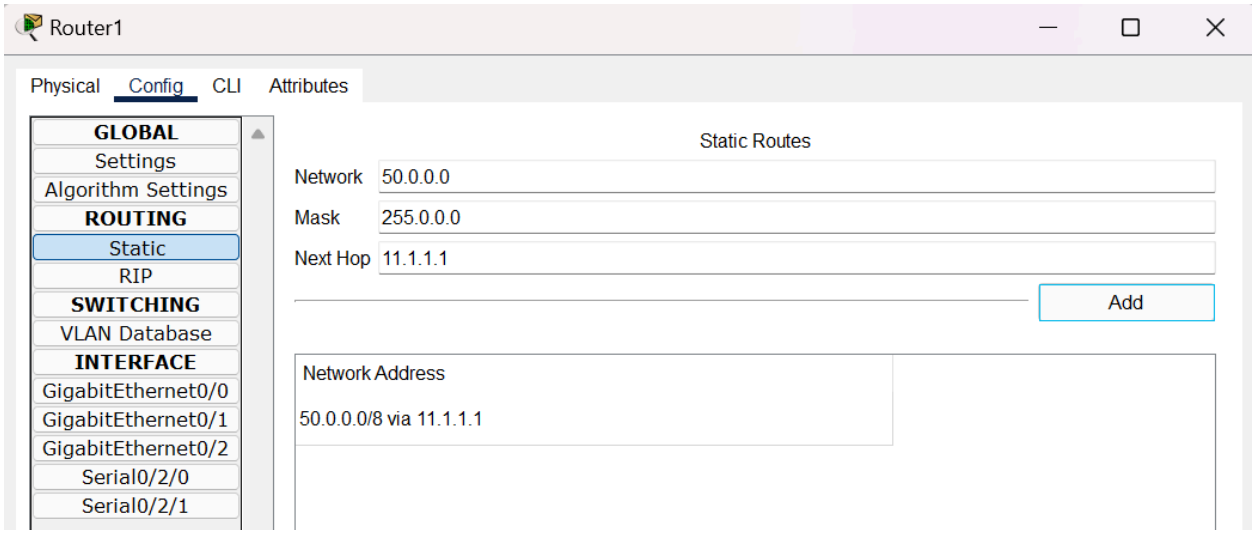


Define default routes

Router0

```
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 11.1.1.2
Router(config)#
```

Define static route



Configure Router0 interfaces

Define nat

```
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 11.1.1.2
Router(config)#int g0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int se0/2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

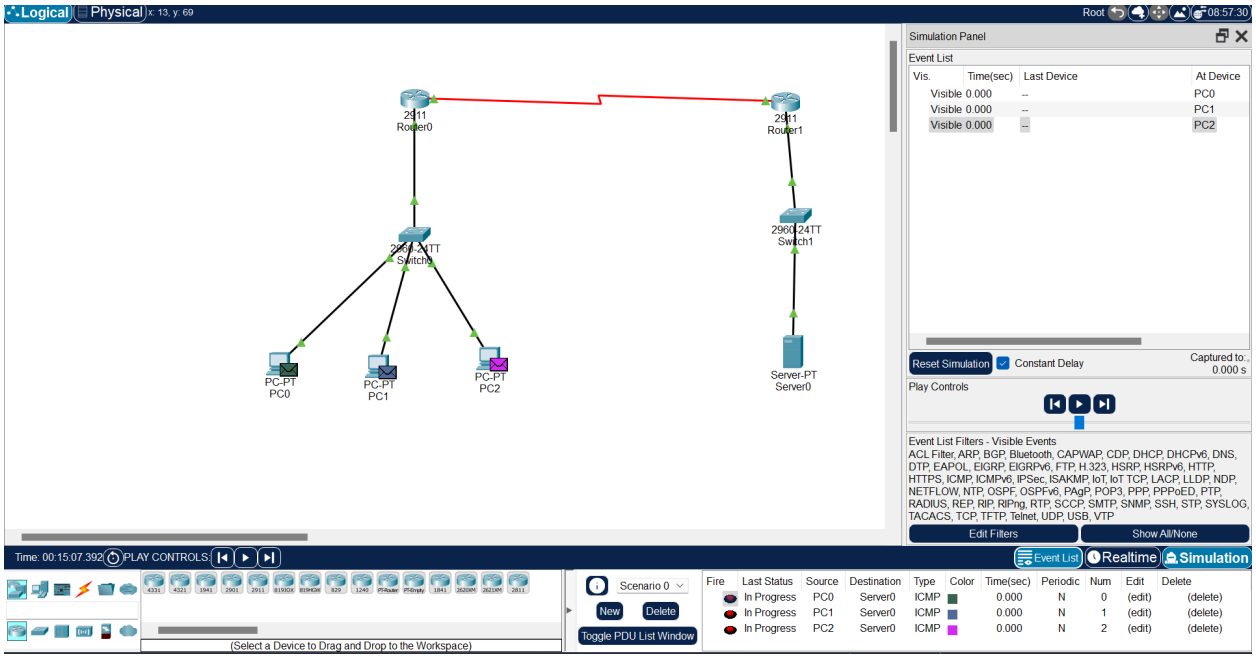
Dynamic nat process

Create an access list to define the inside local network: Define access list (a list of private IPs)

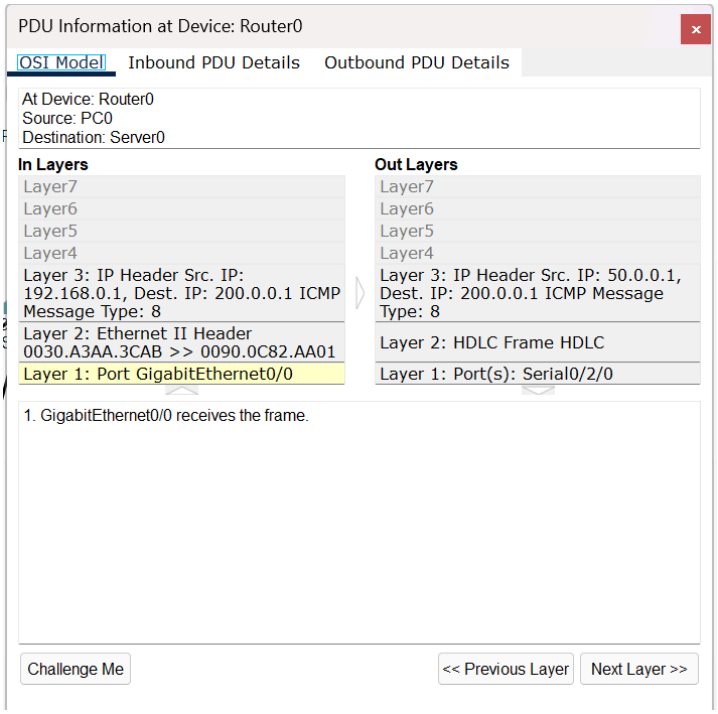
Create a NAT pool for public IPs

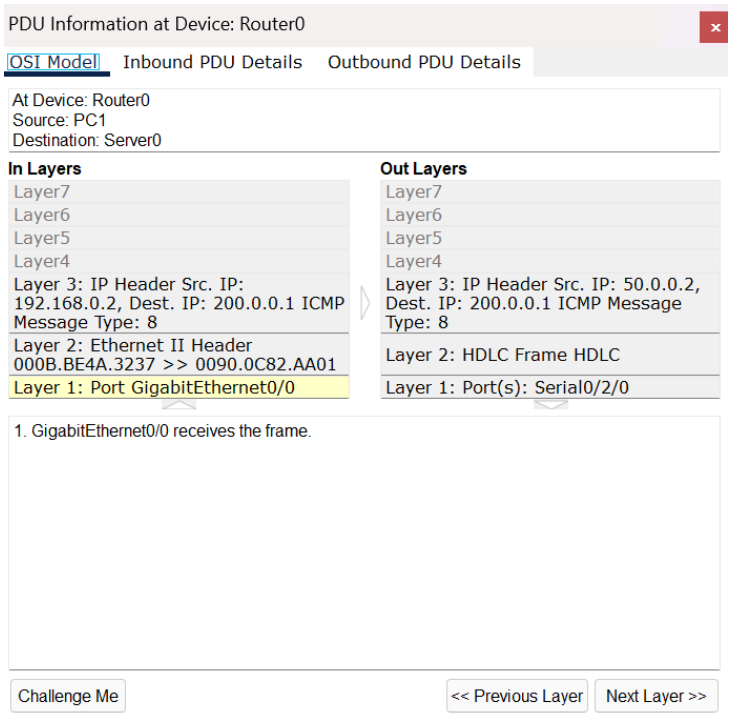
Link the access list to the NAT pool: define pool of public IP addresses

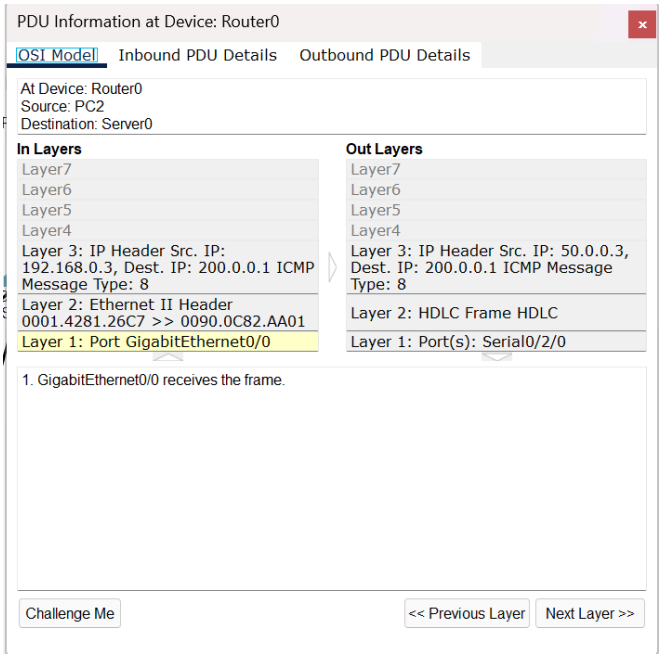
```
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 11.1.1.2
Router(config)#int g0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int se0/2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#access-list 50 permit 192.168.0.0 0.0.0.255
Router(config)#ip nat pool publicip 50.0.0.1 50.0.0.50 netmask 255.255.255.0
Router(config)#ip nat inside source list 50 pool publicip
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC2	Server0	ICMP		0.000	N	2	(edit)	(delete)


PDU Information at Device: Router0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Router0
Source: PC0
Destination: Server0
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.0.1, Dest. IP: 200.0.0.1 ICMP Message Type: 8
Layer 3: IP Header Src. IP: 50.0.0.1, Dest. IP: 200.0.0.1 ICMP Message Type: 8
Layer 2: Ethernet II Header 0030.A3AA.3CAB >> 0090.0C82.AA01
Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0
Layer 1: Port(s): Serial0/2/0
1. GigabitEthernet0/0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>


PDU Information at Device: Router0
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Router0
Source: PC1
Destination: Server0
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.0.2, Dest. IP: 200.0.0.1 ICMP Message Type: 8
Layer 3: IP Header Src. IP: 50.0.0.2, Dest. IP: 200.0.0.1 ICMP Message Type: 8
Layer 2: Ethernet II Header 000B.BE4A.3237 >> 0090.0C82.AA01
Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0
Layer 1: Port(s): Serial0/2/0
1. GigabitEthernet0/0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>



Conclusion

Static NAT and Dynamic NAT both play important roles in modern network design, but they serve different needs.

Static NAT provides a permanent one-to-one mapping between a private and public IP address. This makes it ideal for systems that must always be reachable—such as web servers, email servers, or remote-access machines. Its predictability ensures stable communication, but it requires dedicating a public IP for every internal device, which limits scalability.

Dynamic NAT, in contrast, is more flexible. It uses a pool of public IP addresses and assigns them only when internal devices initiate traffic. This makes much more efficient use of available public IP space, while still hiding private IP addresses from the outside world. However, it cannot support inbound connections, since mappings change and exist only during active sessions.

Together, both NAT types enhance network security, conserve public IPs, and ensure smooth communication between private networks and the wider internet. Choosing the right type depends on whether a system must be reachable from outside (Static NAT) or only requires outbound access (Dynamic NAT).