EX.NO:11

EXAMINE NETWORK ADDRESS TRANSLATION(NAT) USING CISCO PACKET

AIM:

The aim of NAT is to enable multiple devices on a private network to access the internet using a single public IP address while enhancing security by masking internal IPs.

Design of NAT in Cisco Packet Tracer:

Network Topology

1. **Internal Network (Private)**:
    - Hosts with private IP addresses (e.g., 192.168.1.0/24) behind a router.
2. **External Network (Public)**:
    - Router connects to the internet with a public IP address assigned to its interface (e.g., 203.0.113.1/24).
3. **Router**:
    - This router will perform the NAT operation. One interface will connect to the internal network (Private) and the other to the external network (Internet).

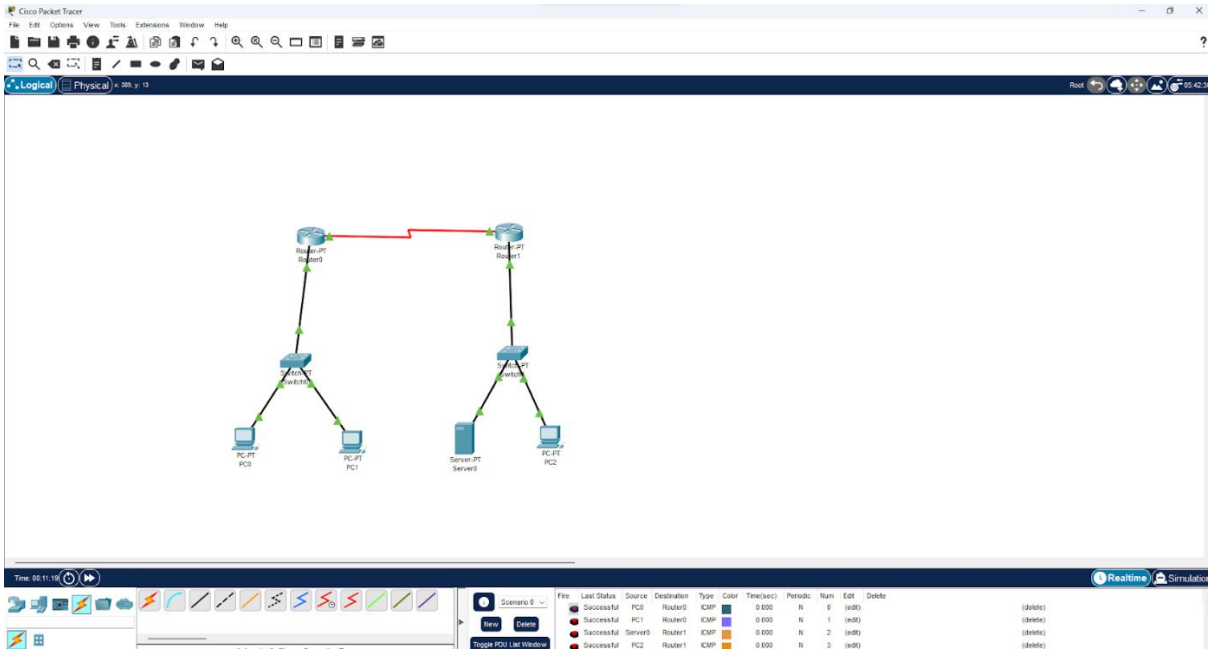
Steps to Design NAT in Cisco Packet Tracer (Short Version):

1. **Create Network Topology**:
    - Connect a router to two networks: internal (e.g., 192.168.1.0/24) and external (e.g., 203.0.113.0/24).
2. **Assign IP Addresses**:

- Set static IPs for router interfaces (e.g., 192.168.1.1 for internal, 203.0.113.1 for external).
- Assign IPs to hosts in the private network (e.g., 192.168.1.2, 192.168.1.3).

3. **Enable NAT**:
   - Configure NAT on the router to translate internal IPs to public IP.
4. **Configure Static or Dynamic NAT**:
   - Static NAT: One-to-one mapping (e.g., 192.168.1.2 to 203.0.113.2).
   - Dynamic NAT: Map multiple internal IPs to a pool of public IPs.
5. **Configure ACLs**:
   - Create an ACL to allow internal IP range (e.g., 192.168.1.0/24) for NAT translation

OUTPUT:



RESULT:

NAT (PAT) configuration successfully allowed internal devices to access the internet using the router's public IP .

NAME:K.DHARANI

ROLL NO:241901025

DEPARTMENT:CSE-CYBER SECURITY