NETWORK ADDRESS TRANSLATION (NAT)

1. Network Address Translation (NAT) is a technique used in networking to allow multiple devices on a local network (private IP addresses) to communicate with external networks (like internet) using a single public IP address.
2. NAT is typically implemented in routers or firewalls.
3. NAT operates at Layer 3 (Network Layer) of the OSI model and modifies IP headers as packets pass through a router.
4. During router configuration , each of its interface should be explicitly mentioned either as inside or outside the Private Network.
5. Each interface marked as inside should be given a mapping for all possible private IP’s there to public IP for external communication. This can be achieved in many ways. Those are discussed below:

* Static NAT – a technique by which one to one mapping between each unique private and public IPs are made during router configuration

ip nat source static <private> <public>

access-list 1 permit <network id> <wild card mask>

* Dynamic NAT - a technique by which based on availability of public IP in the pool maintained, private to public IP mapping is done by router. For this, during router configuration, pool to be made with all possible public IP and its netmask.

ip nat pool <pool name> <comma separated public IPs > netmask <common netmask>

ip nat inside source <acl> pool <pool name> overload

* Port Address based translation (NAPT / NAT overload) – an advanced and modern day technique for doing NAT along with conserving the available IPv4 public addresses by mapping many private ip to one public IP and distinguish each instances using client port

1. Uses of NAT

* Multiple devices (in home or enterprise networks) can share less number of public IP for more private IP in accessing internet.
* Helps in hiding the private network from internet
* Helps in creating access control list (important for firewall) leading to enhanced security.
* Offers better isolation between private and public network.

1. Disadvantages of NAT

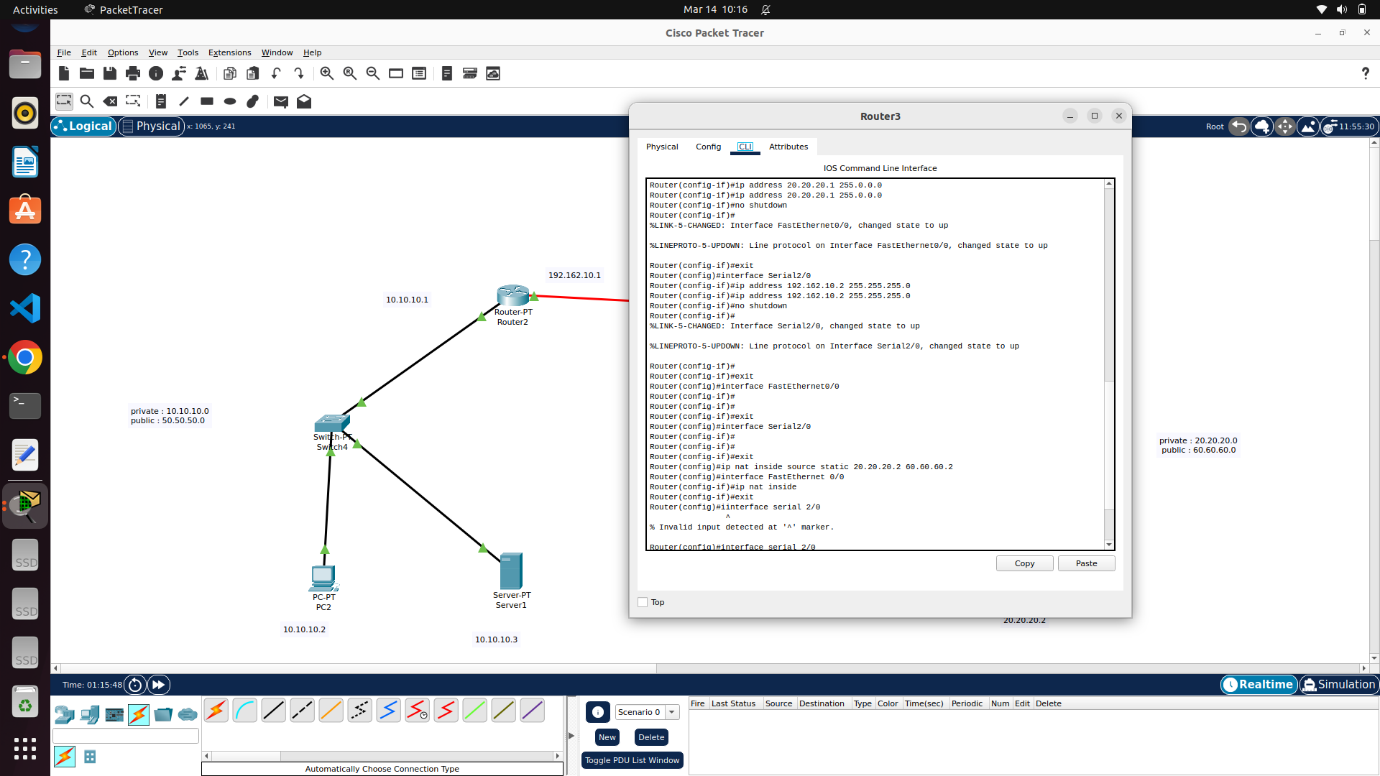
* Introduces overhead to router in editing packet’s information before routing
* May disrupt VPN or direct communication protocols.

SCENARIO CONSIDERED :

Two different networks are made to communicate with each other in this setup:

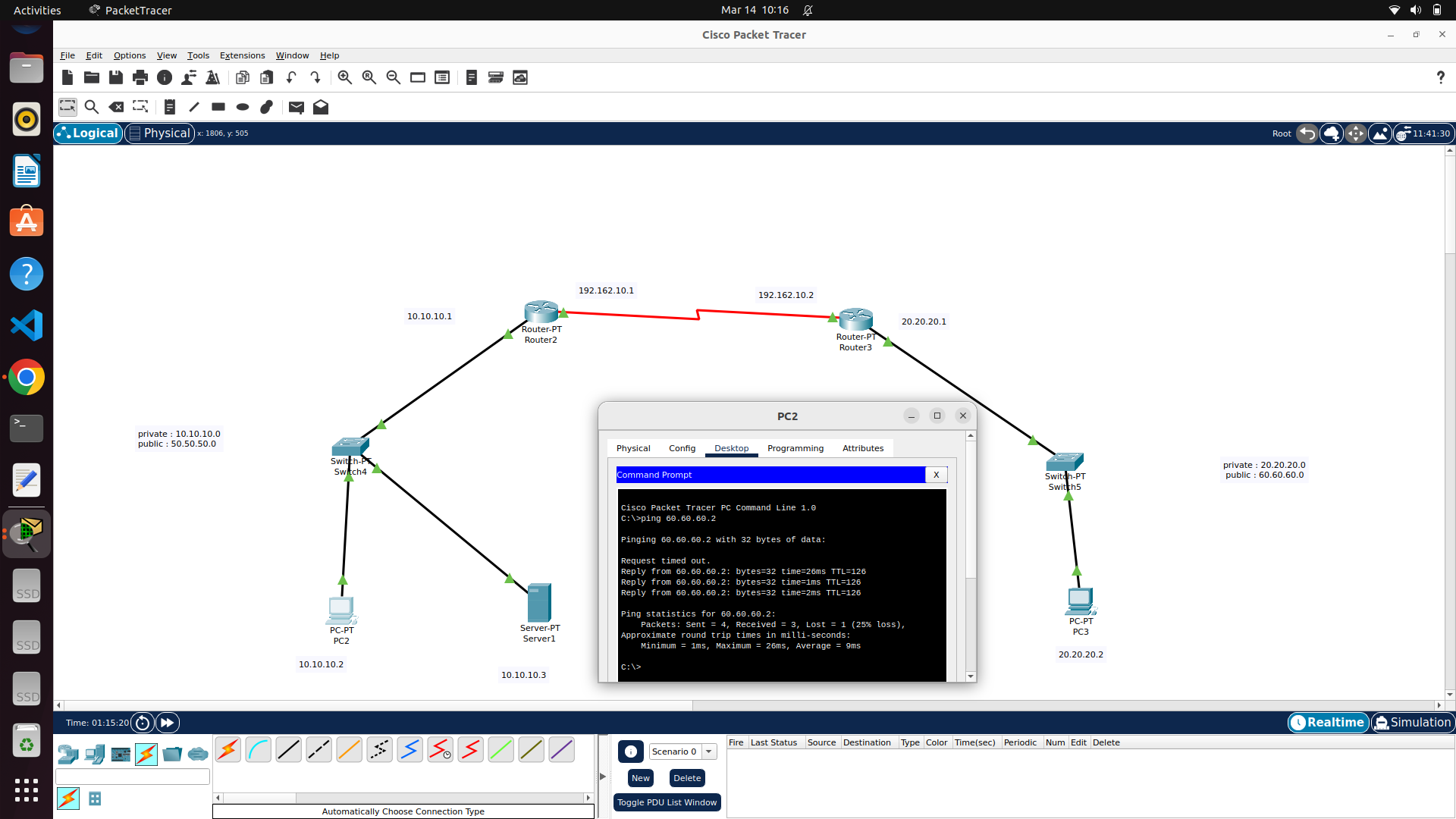
1. Private network with network address – 10.10.10.0/8 with PC of IP – 10.10.10.2/8 and Server of IP – 10.10.10.3/8 [this network is translated to 50.50.50.0/8 by NAT accordingly PC will be represented as 50.50.50.2/8 and Server as 50.50.50.3/8]

Sample router configuration is shown below with constructed network.

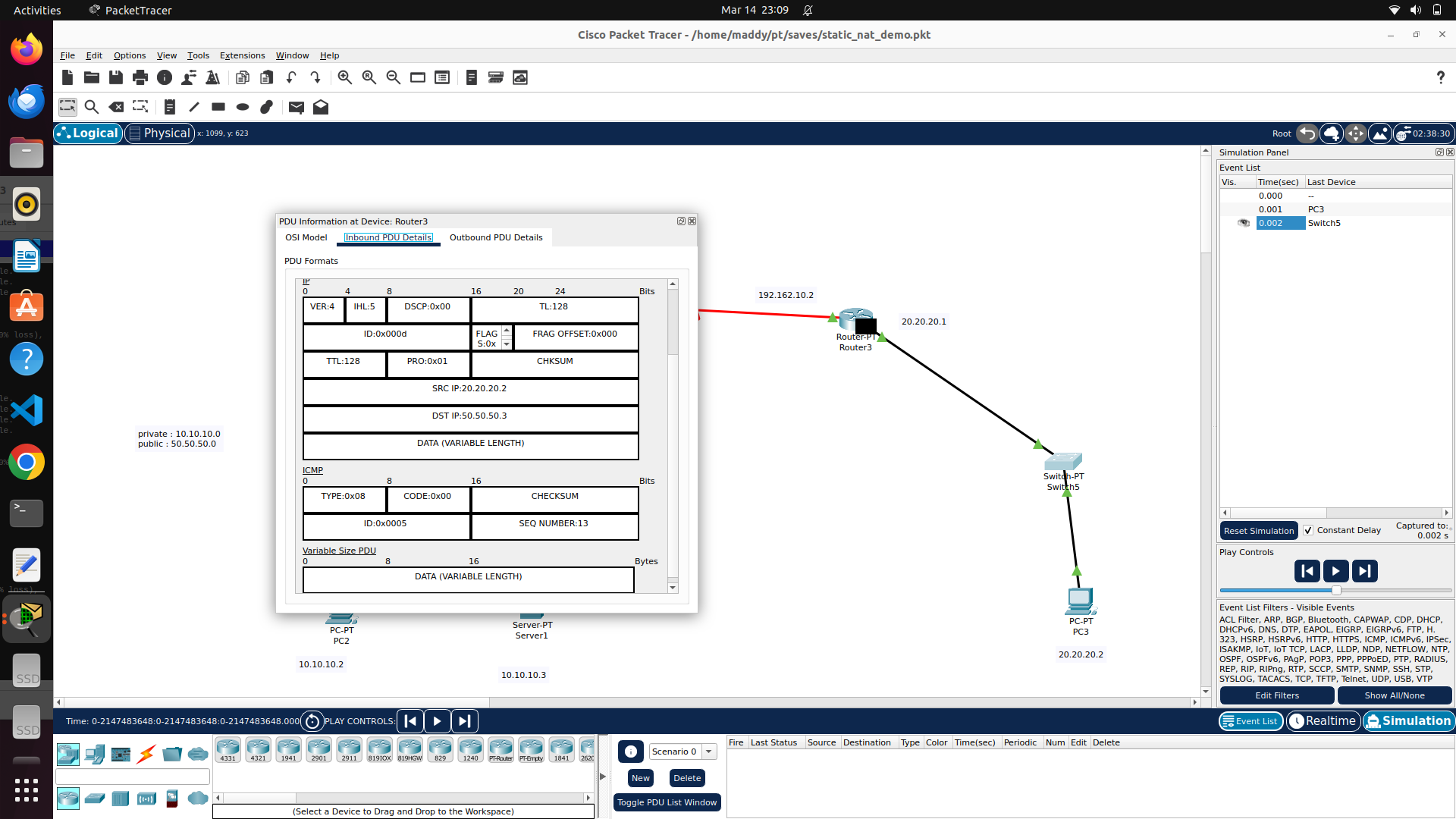


(Here, in right side network, consisting of single PC, though 20.20.20.0/8 is not coming under private IP, just for security reasons or to isolate, it also got translated to other public IP – 60.60.60.0/8)

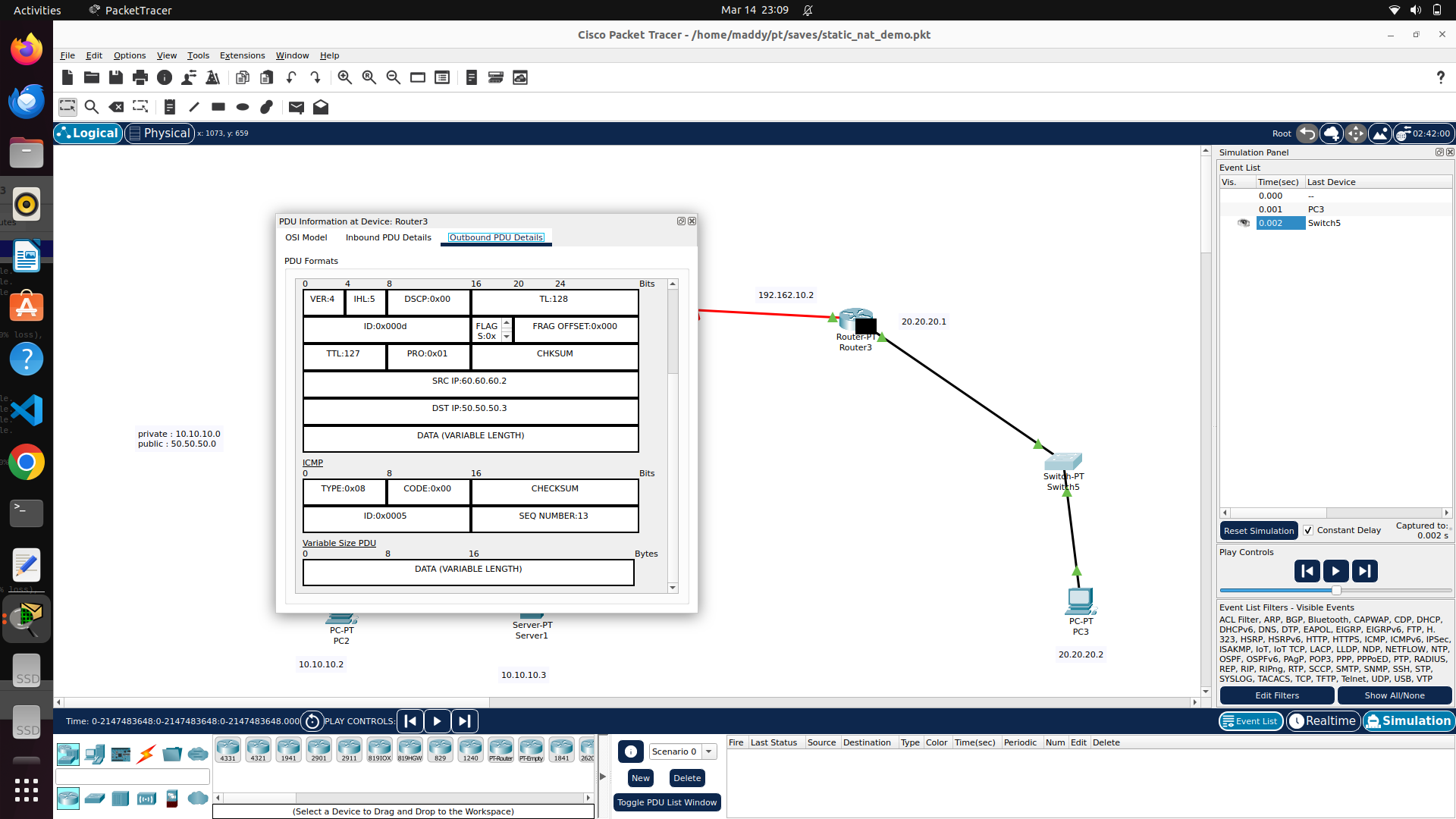
RESULT :



SOURCE IP (FROM 20.20.20.2/8) BEFORE NAT :



SOURCE IP (FROM 20.20.20.2/8) AFTER NAT -> TO 60.60.60.2/8:



ABOVE PACKETS ARE CAPTURED USING BUILT-IN PACKET CAPTURE AND FILTER OPTIONS IN CISCO PACKET TRACER