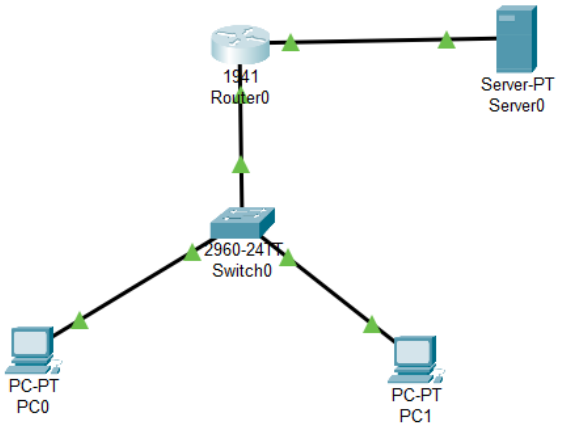
7. In Cisco Packet Tracer, create a small network with multiple devices (e.g., 2 PCs and a router). Use private IP addresses (e.g., 192.168.1.x) on the PCs and configure the router to perform NAT to allow the PCs to access the internet.

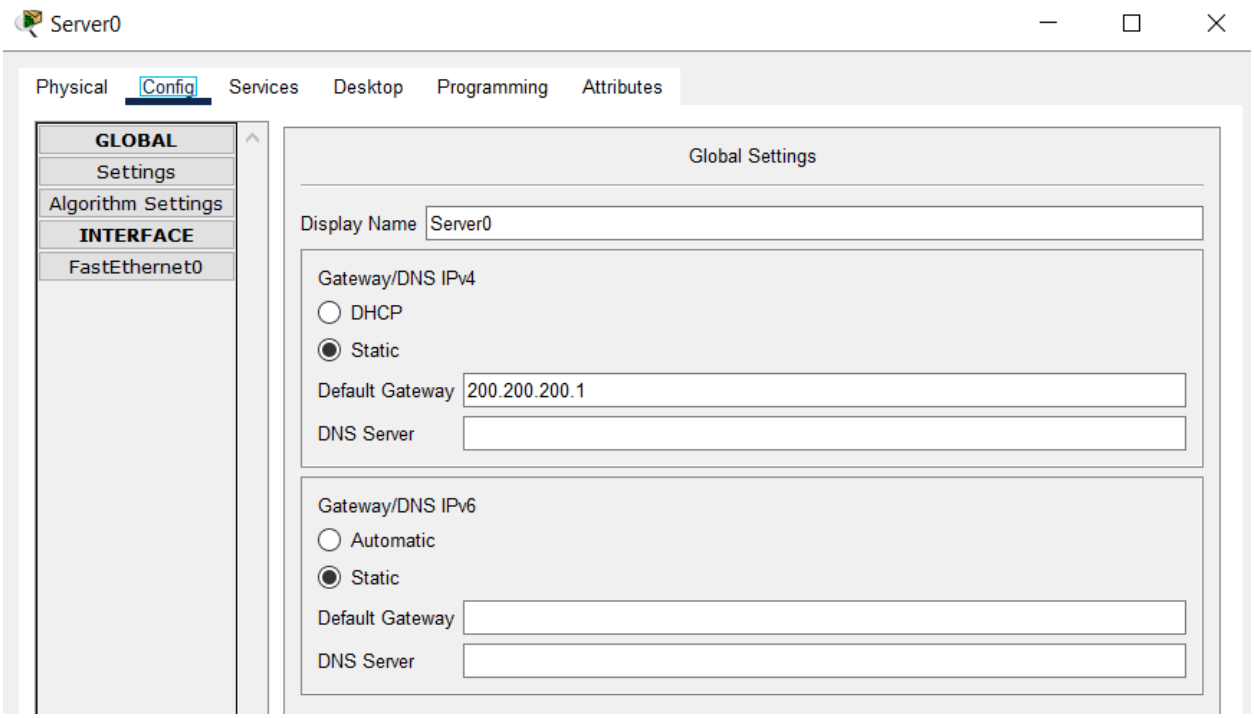
Task: Test the NAT configuration by pinging an external IP address from the PCs and capture the traffic using Wireshark.

What is the source IP address before and after NAT?

Setup:



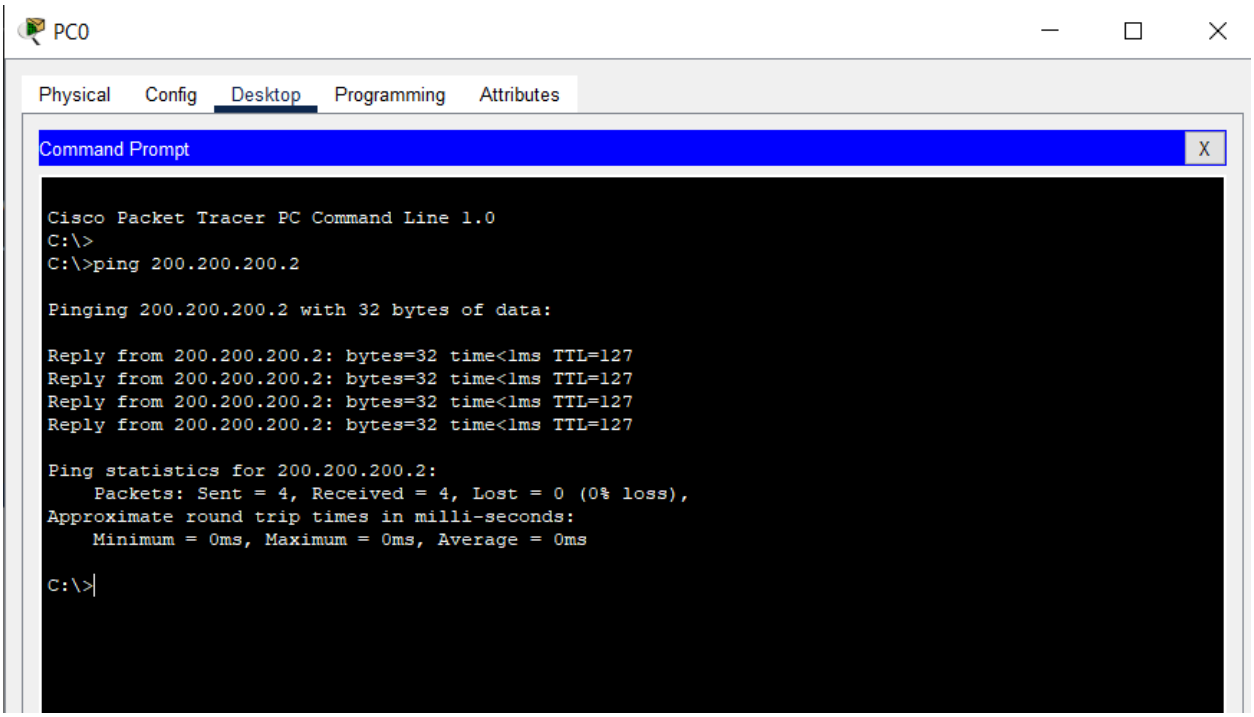
In this setup, we configured **Network Address Translation (NAT)** on a Cisco router to allow internal devices with private IPs to access the internet using a public IP.




```
Router#ping 200.200.200.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.200.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.200.200.1:13  192.168.1.2:13     8.8.8.8:13         8.8.8.8:13
icmp 200.200.200.1:14  192.168.1.2:14     8.8.8.8:14         8.8.8.8:14
```



Network Address Translation (NAT) is a technique used in routers to modify IP addresses in packets as they pass through. It allows multiple devices on a private network to access the internet using a single public IP address.

How NAT Works

When a private device (e.g., PC) wants to access the internet:

Packet is Sent – A device in a private network sends a packet to an internet server (e.g., 8.8.8.8).

Router Modifies IP – The NAT router replaces the private IP (e.g., 192.168.1.2) with its public IP (e.g., 200.200.200.1).

Packet Reaches Destination – The packet reaches the server (8.8.8.8).

Server Responds – The server replies to the public IP (200.200.200.1).

Router Translates Back – The router maps the response back to the original private IP (192.168.1.2) and forwards it.