**5. In Cisco Packet Tracer, configure NAT on a router to allow internal devices (192.168.1.x) to access the internet.**

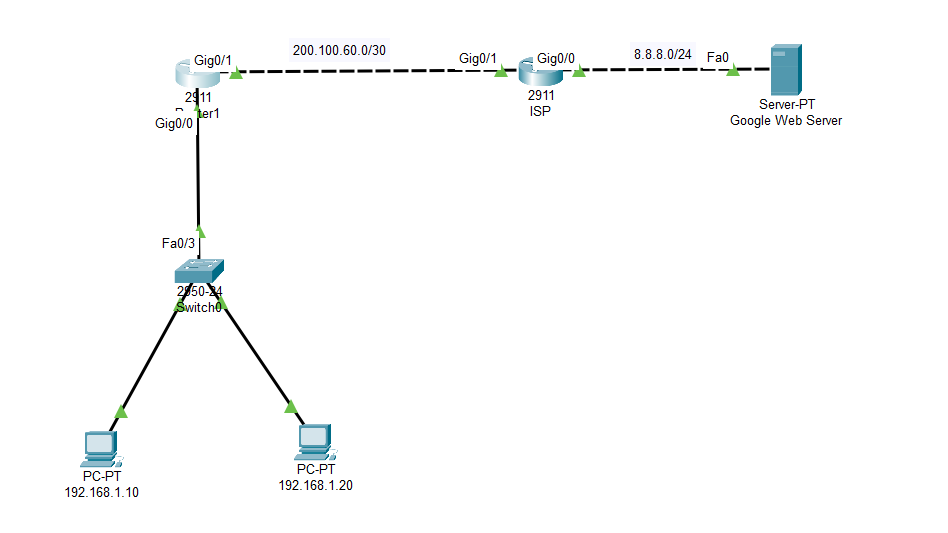
**Test connectivity by pinging an external public IP.**

**Capture the traffic in Wireshark and analyze the source IP before and after NAT translation.**

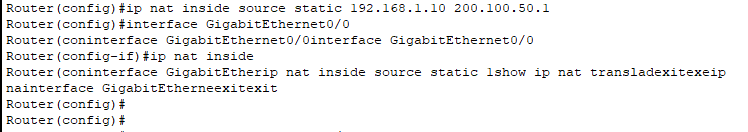
**Steps Followed:**

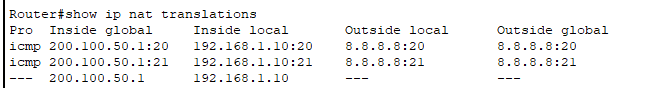
* Configured a router with NAT to enable internal devices (192.168.1.x) to access the internet.
* Assigned private IPs (192.168.1.x) to internal devices and connected them to the router.
* Configured the router’s inside and outside interfaces for NAT.
* Created a NAT to translate private IPs into a public IP (200.100.50.1).
* Verified NAT functionality by pinging 8.8.8.8 from the internal device (192.168.1.10).
* Observed the source IP before NAT as 192.168.1.10 (private IP).
* Observed the source IP after NAT as 200.100.50.1 (translated public IP).

**Setting Up:**

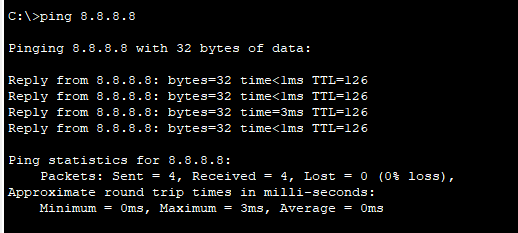
****

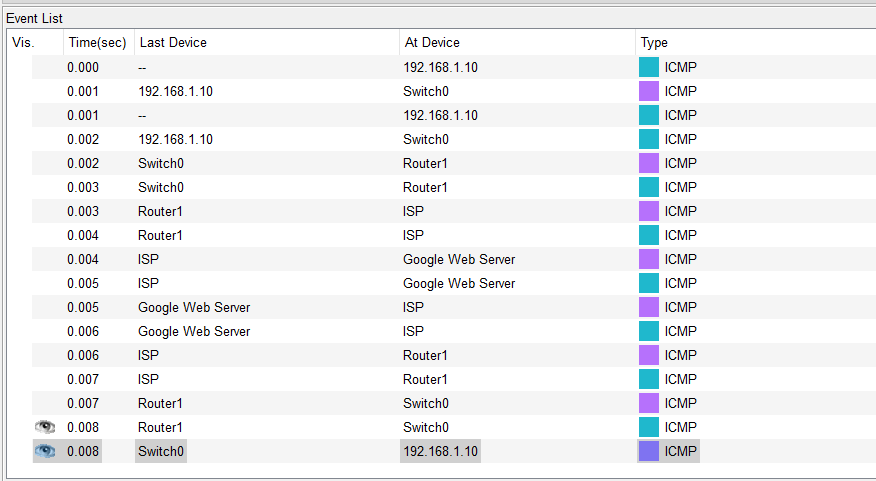
**NAT Configuration:**

****

****

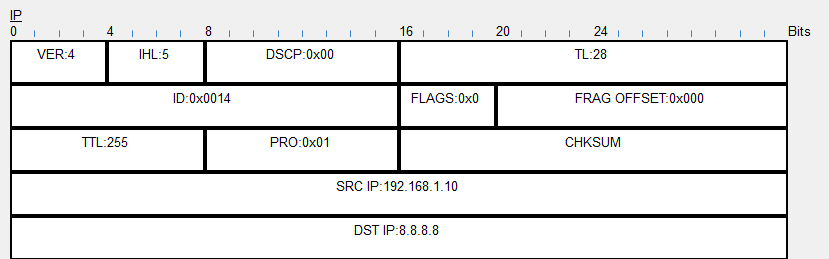
**Pinging 8.8.8.8 from 192.168.1.10:**

****

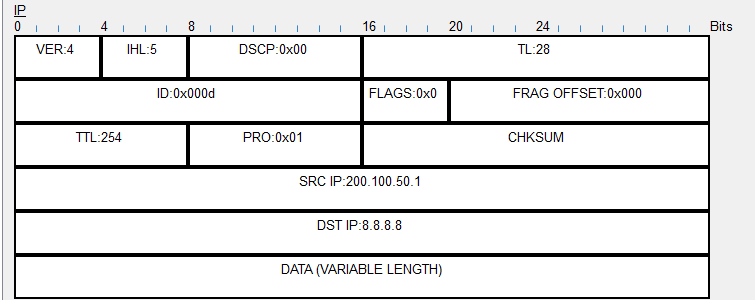
****

**Source IP before and after NAT translation:**

**Before the NAT translation, the Source IP is 192.168.1.10**

****

**After the NAT translation, the Source IP has become 200.100.50.1**

****

**Observation**

The router successfully translated the private IP (192.168.1.10) to a public IP (200.100.50.1), allowing internet access. This confirms that NAT is functioning correctly, ensuring internal devices can communicate externally while remaining hidden within the local network.