**Moulik Tammana**

**Q5. 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 analyse the source IP before and after NAT translation.**

**Steps to followed:**

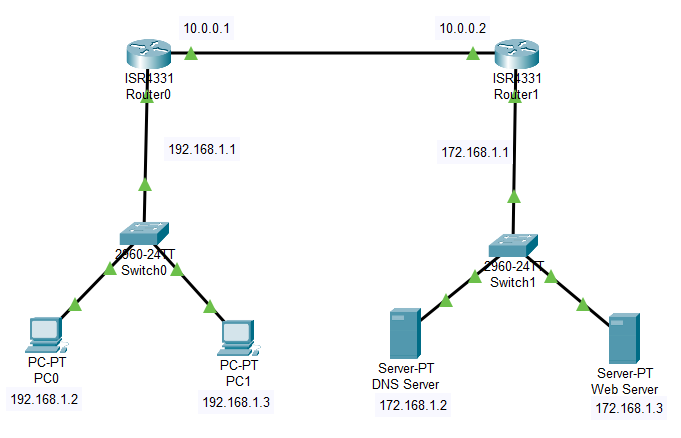
**Step 1: Create a network topology in Cisco Packet Tracer. Added 2 router, 2 servers, 2 switches, and 2 PC’s.**

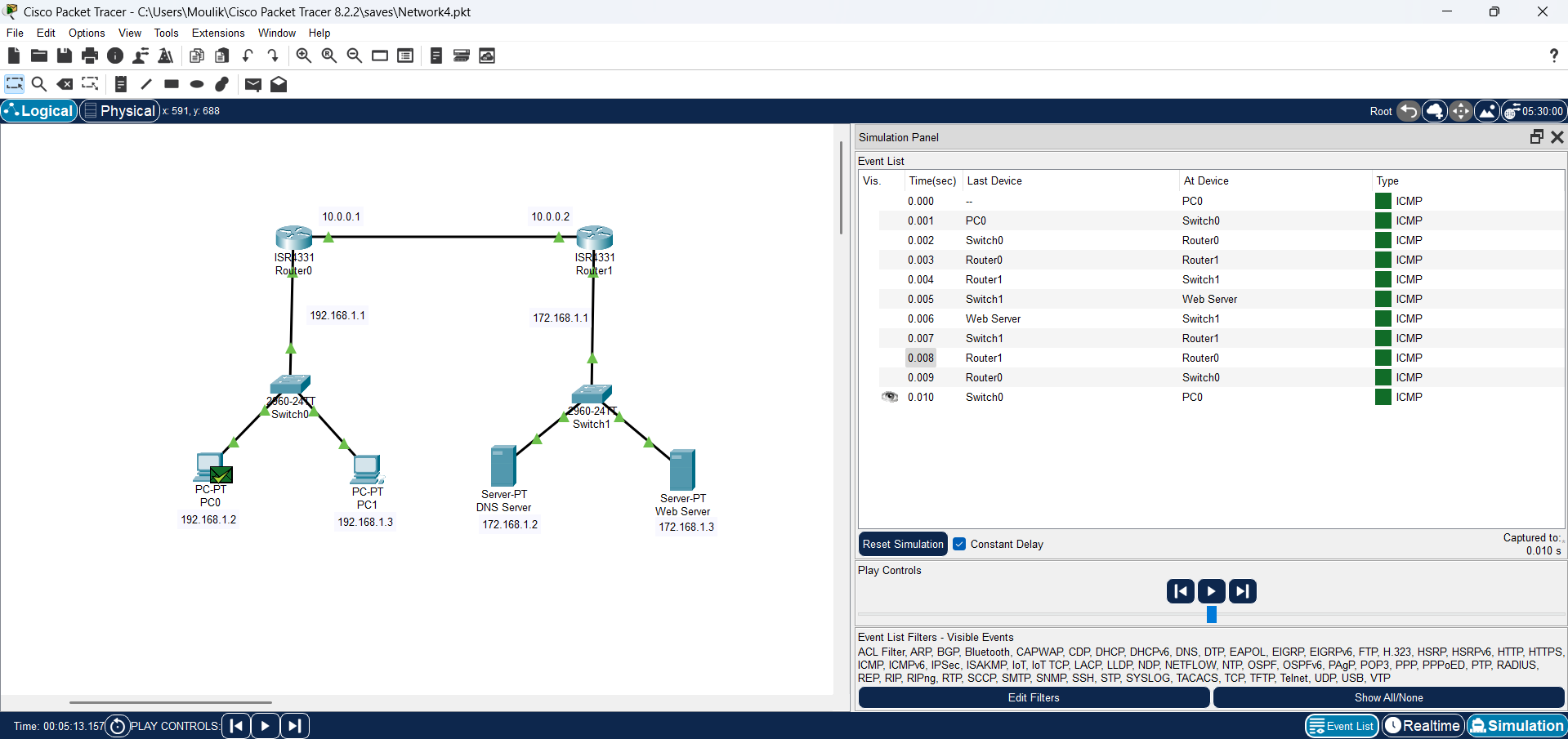
**Step 2: Assign IP addresses:**

* **Internal Network: 192.168.1.0/24 and assigned 192.168.1.2 and 192.168.1.3 to the two PC’s.**
* **Router Internal Interface (LAN): 10.0.0.1**
* **Router External Interface (WAN): 10.0.0.2**
* **Server IP addresses: Web server is 172.168.1.3 and DNS server is 172.168.1.2**

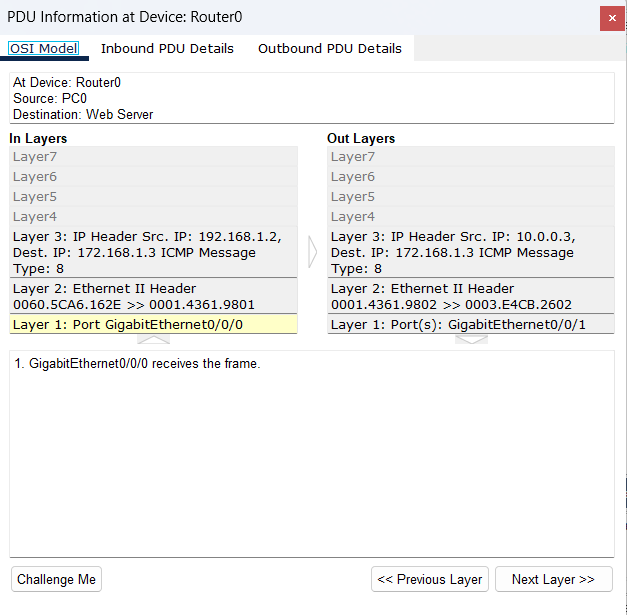
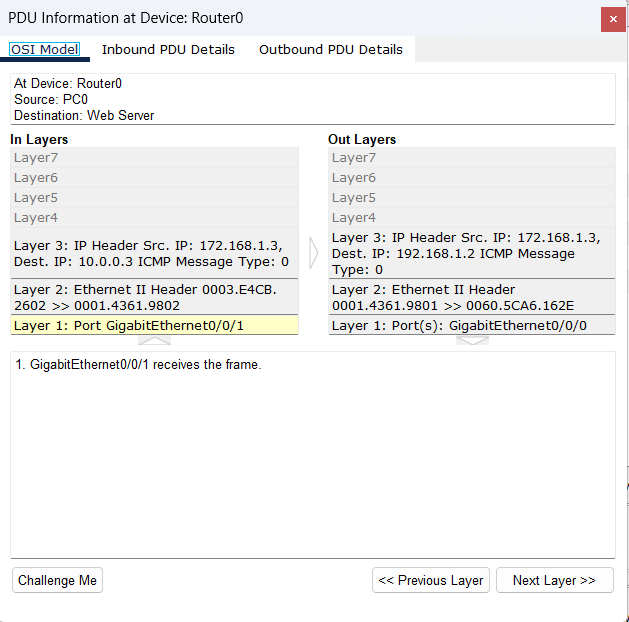
**Step 3: Configure static IP route in the routers**

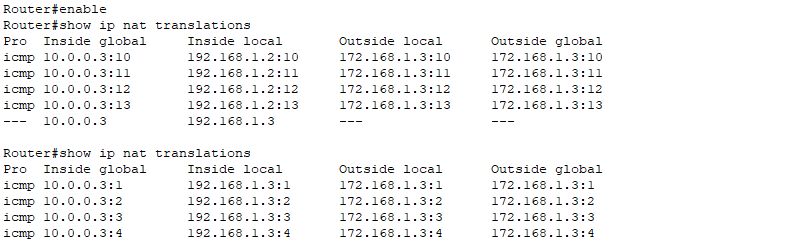
**Step 4: Enable NAT configuration to the LAN router by defining the inside and outside of the NAT interface.**

****



**The Below is the IP translation that is done in router0 due to NAT configuration, we can observe that the IP of the private network changes from 192.168.1.2/192.168.1.3 to 10.0.0.3 when packet is transmitted form the private to the public network. Similarly, when the packet is received at router0, the IP changes from 10.0.0.3 to 192.168.1.2/192.168.1.3.**

** **

****