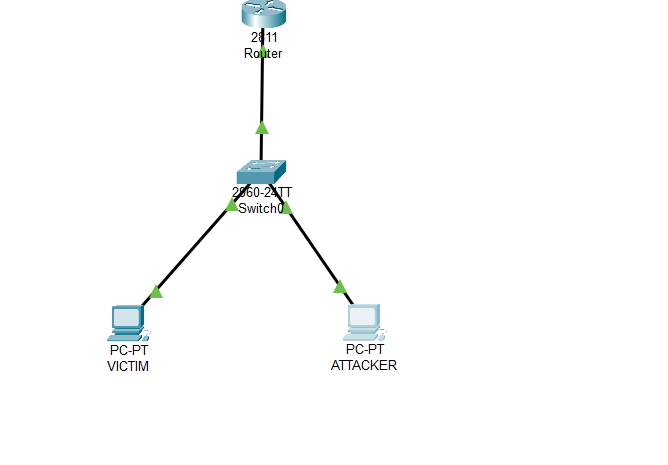
**Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.**

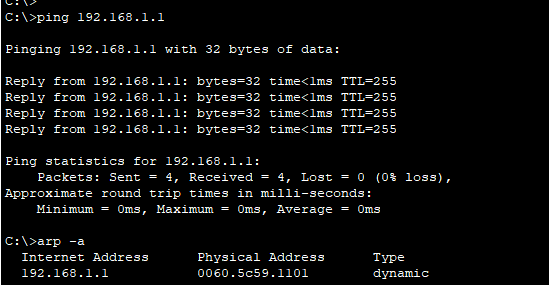
**STEPS FOLLWED:**

* Connected Victim PC, Router, and Attacker PC in a network and assigned IP addresses.
* Pinging the Router from the Victim PC to verify normal communication.
* Checked the ARP table on the Victim PC, which correctly mapped the Router's IP to its MAC address.
* Changed the MAC address of the Attacker PC to match the Router's MAC address.
* Cleared the ARP cache on the Victim PC to force an update.
* Pinging the Router again from the Victim PC after spoofing.
* The Victim PC updated its ARP table, now associating the Router's IP with the Attacker's MAC address.
* The packets meant for the Router started reaching the Attacker PC instead.

**Setting Up:**

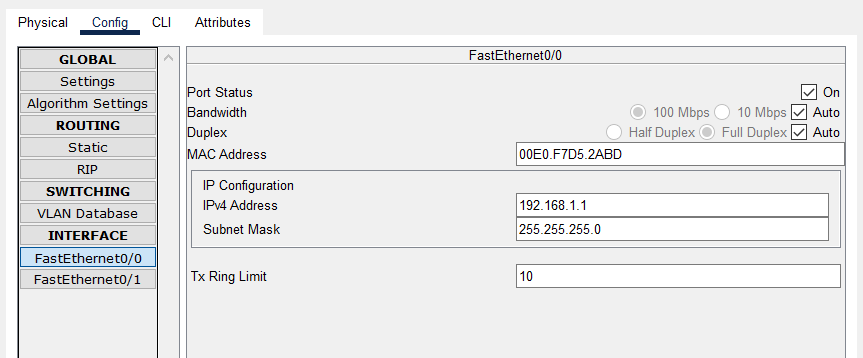
****

**Pinging the router from Victim PC before ARP Spoofing:**

****

**Manually simulating the ARP Spoofing attack:**

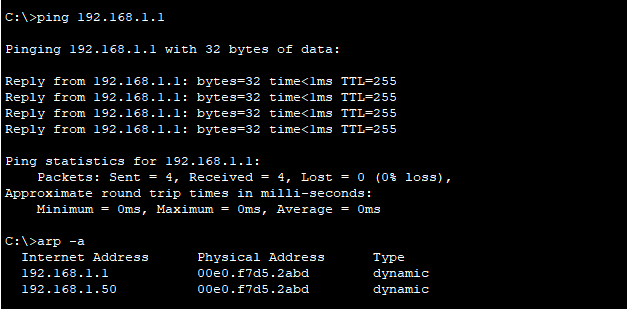
**Assigned the MAC address of the Attacker PC to the Router:**

****

**Pinging the Router from the Victim PC to Router after ARP Spoofing attack:**

**Now, the packets that are supposed to be transmitted to the router ad reaching the Attacker PC.**

**And, the ARP table got update**

****

**Behaviour of Devices When They Receive a Malicious ARP Response**

* The Victim PC mistakenly updates its ARP table, believing that the Attacker is the Router.
* The Victim sends all traffic meant for the Router to the Attacker instead.
* The Attacker can intercept, modify, or drop packets, leading to potential data theft or communication disruption.
* The Router may still receive some packets if ARP updates fluctuate, but the attack remains effective as long as the Victim keeps associating the Router’s IP with the Attacker’s MAC.