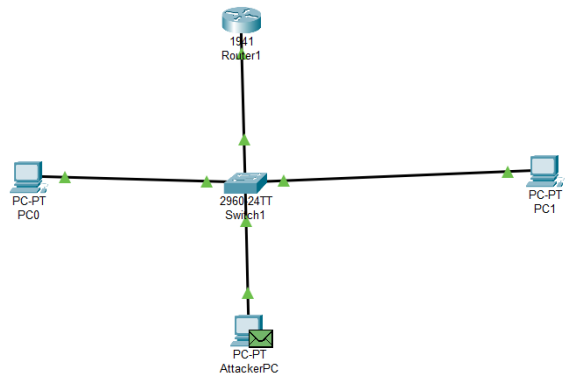
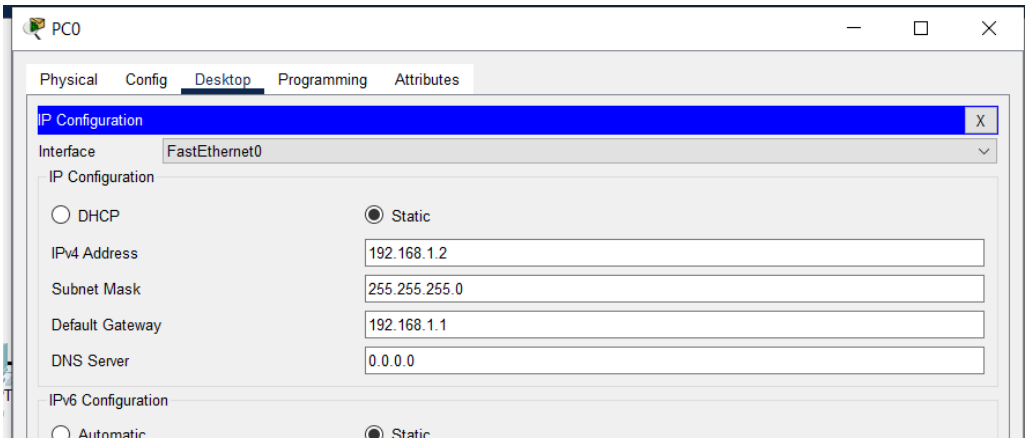
Q2)Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.

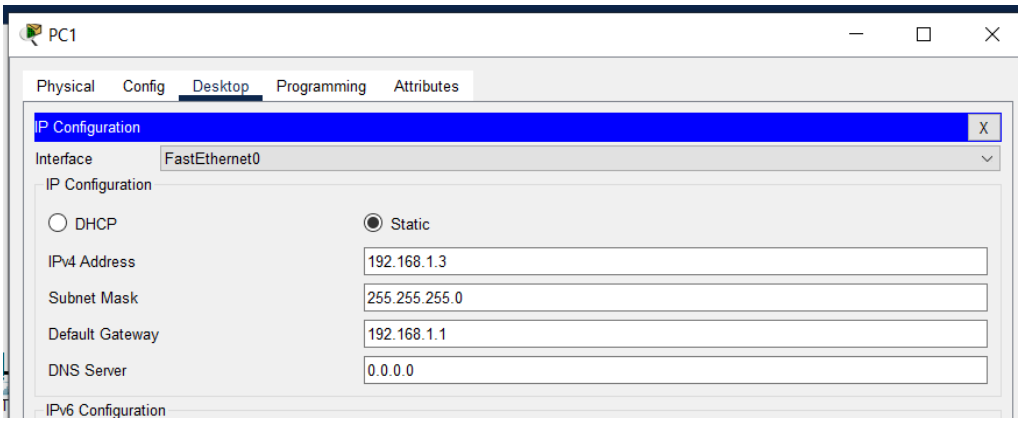


\

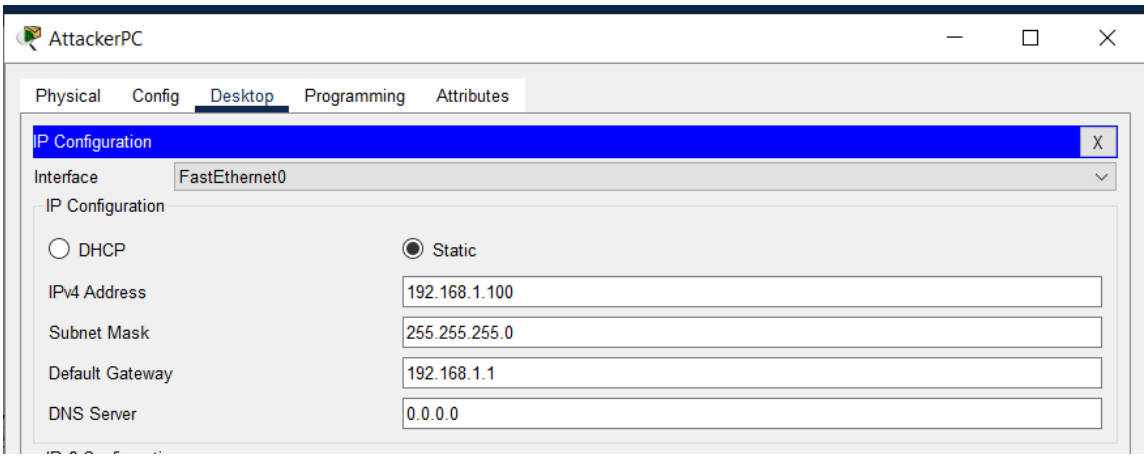
PC0 Configuration



PC1 Configuration



PC2 Configuration



Configuring Router

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, ch

Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

What is ARP Spoofing?

ARP (Address Resolution Protocol) spoofing is a type of cyber-attack where an attacker sends falsified ARP messages over a local network to associate their MAC address with the IP address of another device (typically a gateway or another host). This allows the attacker to intercept, modify, or even stop network traffic between legitimate devices.

How ARP Works Normally

ARP is used in IPv4 networks to map an **IP address** (logical) to a **MAC address** (physical). Here's how it works:

1. **Host A (192.168.1.2) wants to communicate with Host B (192.168.1.3).**
2. Host A checks its **ARP table** to see if it already knows Host B's MAC address.
3. If the MAC address is not known, Host A sends an **ARP request** as a broadcast

`"Who has 192.168.1.3? Tell 192.168.1.2."`

4. Host B (192.168.1.3) responds with an **ARP reply**, providing its MAC address.
5. Host A updates its ARP table with the correct MAC and starts communication.

How ARP Spoofing Works

An attacker can exploit ARP's lack of authentication by sending **fake ARP replies** to manipulate a victim's ARP table.

- The attacker (e.g., PC2) sends a **malicious ARP reply** to PC0, saying:

`"192.168.1.1 is at AA:AA:AA:AA:AA:AA" (attacker's MAC address)`

- PC0 believes this and updates its ARP table, thinking the attacker is the router.
- The attacker does the same with the router, sending:

`"192.168.1.2 is at AA:AA:AA:AA:AA:AA"`

- The router updates its ARP table, thinking PC2 (the attacker) is PC0.

Cisco Packet Tracer is a **network simulation tool**, not an actual emulator, meaning it simplifies many real-world network behaviors. While it accurately models networking concepts, **ARP spoofing is not fully supported** due to the following reasons:

1. Lack of ARP Poisoning Mechanism
2. No Packet Injection Support
3. Simplified Network Behavior
4. No Real Packet Capture and Forwarding