Configuration and Analysis of Address Resolution Protocol (ARP)

1. Aim

To construct a simple Local Area Network (LAN) using Cisco Packet Tracer to understand, observe, and verify the operational process of the Address Resolution Protocol (ARP).

---

2. Problem Statement

The task is to build a simulated network consisting of personal computers and a switch. This network will be used to generate traffic (using the ping command) that initiates the ARP process. The primary objective is to capture and analyze the ARP request and reply mechanism to understand how IP addresses are mapped to physical MAC addresses within a local network.

---

3. Scope of the Solution

This project is confined to a simulated environment using Cisco Packet Tracer. The scope includes:

- Creating a single, flat LAN topology (one broadcast domain).
- Statically assigning IPv4 addresses to end devices.
- Using Simulation Mode to observe the packet flow for ARP and ICMP protocols.
- Verifying the dynamic population of the ARP cache on a host machine.

The project does not cover routing, inter-VLAN communication, or ARP processes in more complex network architectures.

---

4. Required Components to Develop Solution

Software

- **Simulation Environment: Cisco Packet Tracer** (Version 8.2.1 or newer recommended)
- **Operating System:** Windows, macOS, or Linux

Hardware (Physical)

- A standard personal computer or laptop capable of running Cisco Packet Tracer.

Hardware (Simulated)

- **End Devices:** 2 x PCs
- **Network Device:** 1 x Cisco 2960 Switch
- **Cabling:** 2 x Copper Straight-Through Cables

---

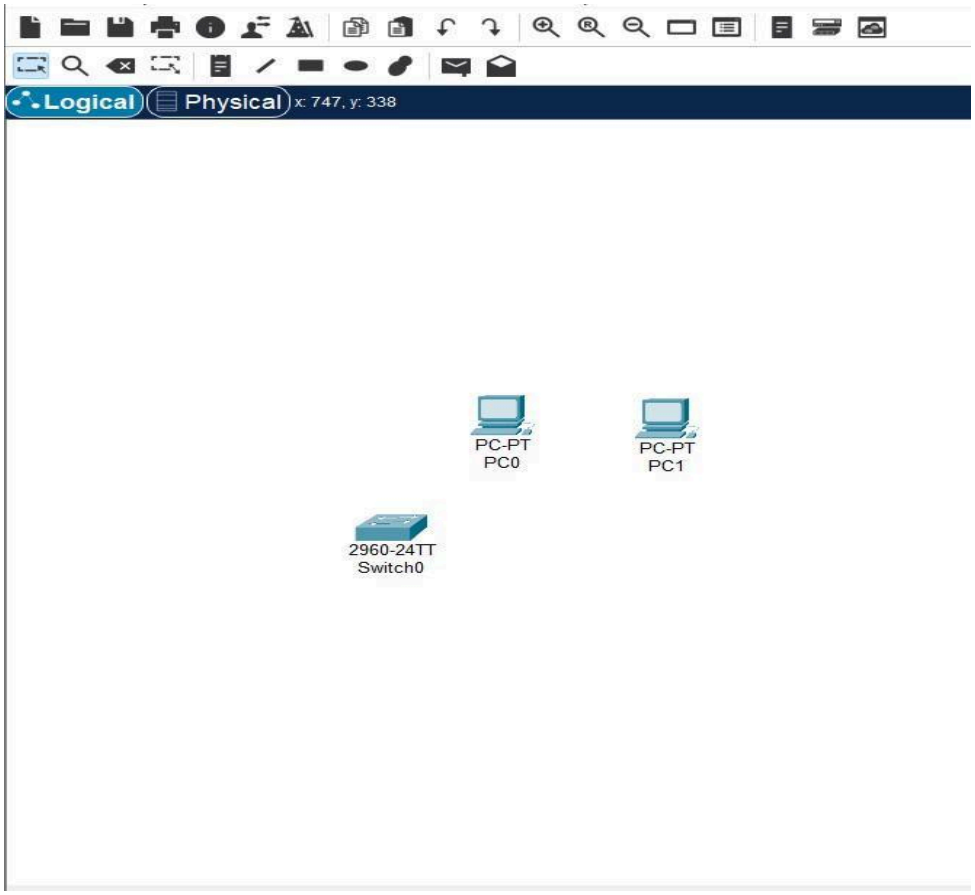
5. Simulated Circuit

The Cisco Packet Tracer simulation file containing the configured network topology is included in github repository.
https://github.com/edwinbenny809/ARP/blob/main/5BTRAM%20batch%202/Arp.pkt

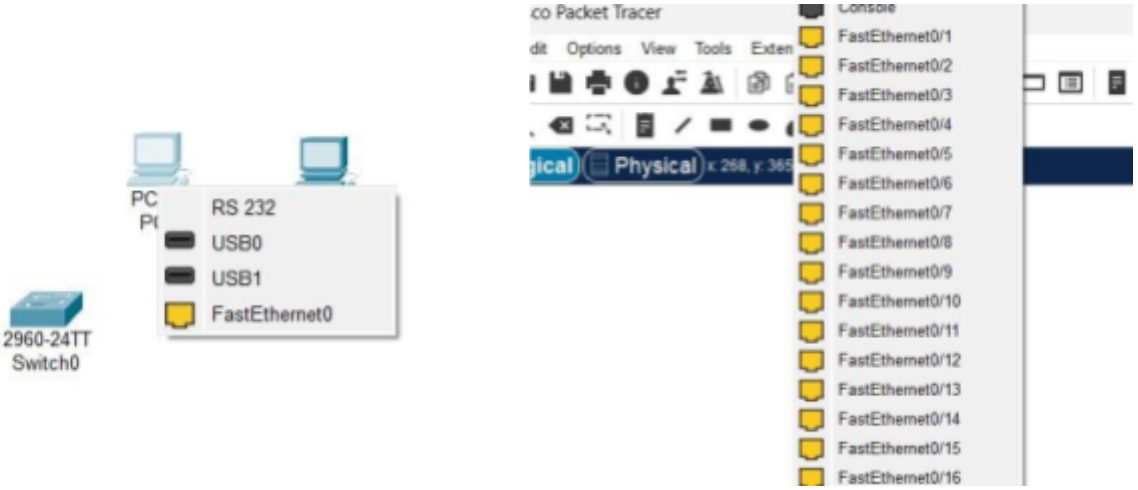
Step 1: Building the Network Topology

We begin by placing and connecting the necessary components in the Cisco Packet Tracer workspace.

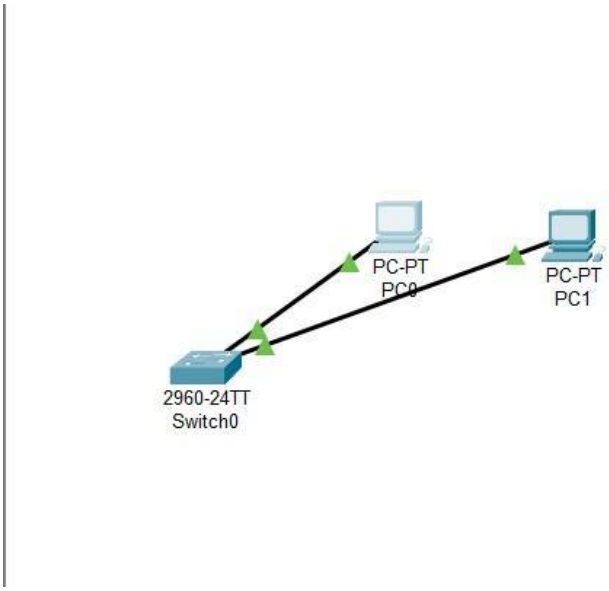
- **1a. Placing Devices:** Drag and drop one **2960 Switch** and two **PCs** from the device menus onto the workspace



- **1b. Connecting Devices:** Select the **Copper Straight-Through** cable from the "Connections" menu. Connect PC0's FastEthernet0 port to the switch's FastEthernet0/1 port. Repeat for PC1, connecting it to the switch's FastEthernet0/2 port.



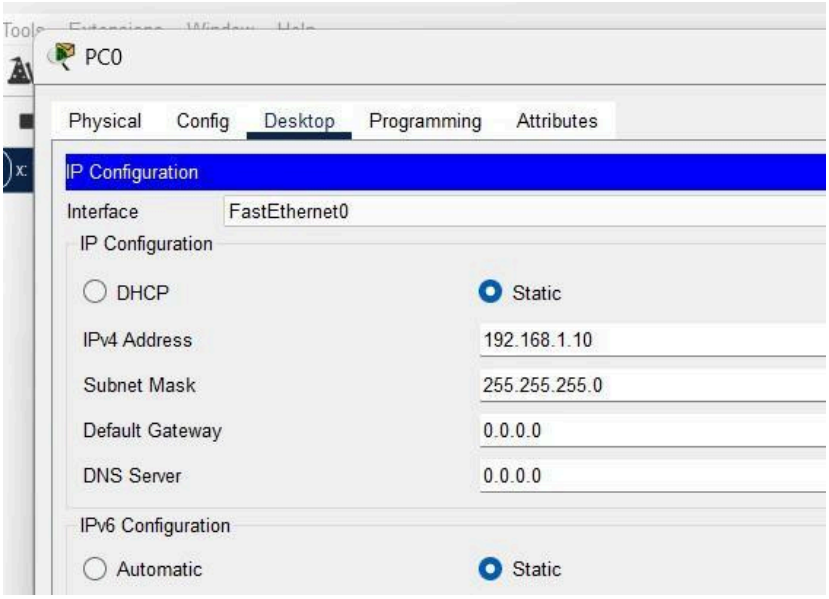
- **1c. Completed Topology:** After a few moments, the link lights on the connections will turn green, indicating a successful physical layer connection



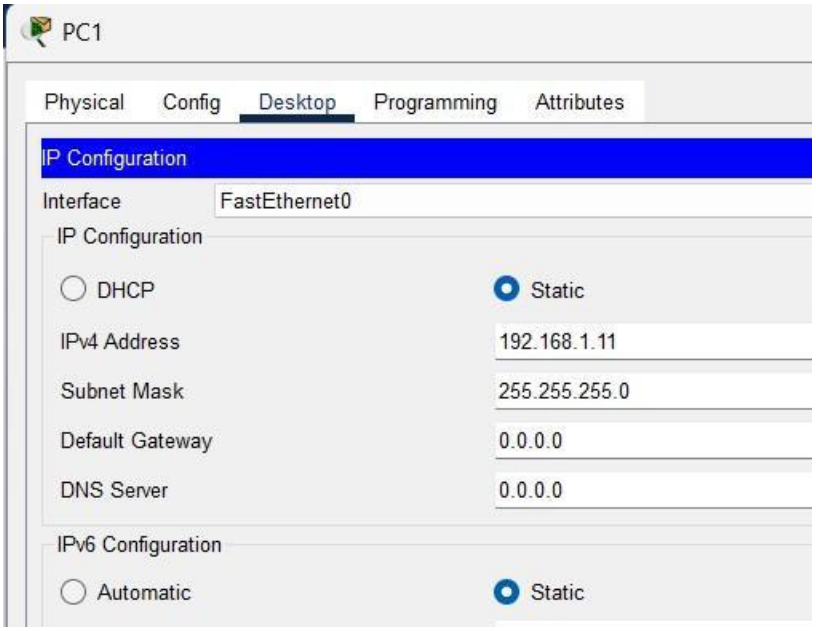
- **Step 2: Configuring IP Addresses**

Next, the PCs are configured with static IP addresses to ensure they are on the same network. ·

2a. PC0 Configuration (192.168.1.10)



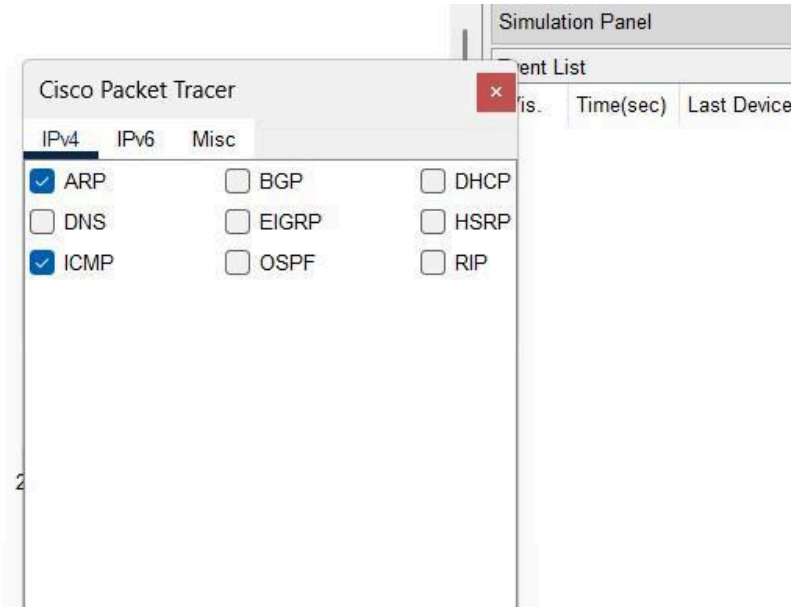
- **2b. PC1 Configuration (192.168.1.11)**



Step 3: Preparing the Simulation

We switch to **Simulation Mode** and filter the visible events to show only **ARP** and **ICMP** packets. This allows us to focus on the relevant traffic for this lab.

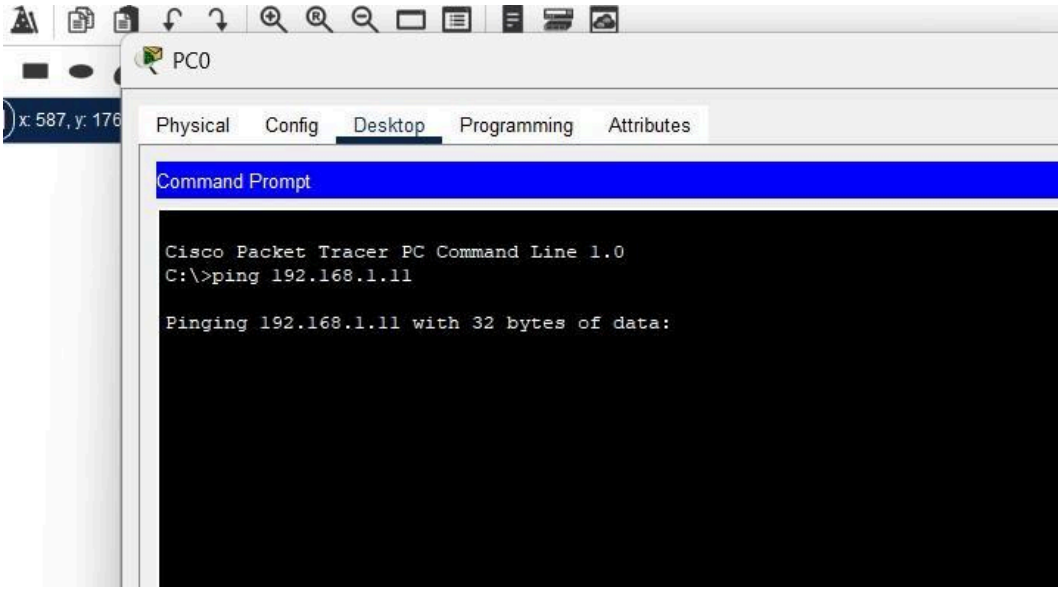
- **Simulation Panel with Filters**



- **Step 4: Initiating the ARP Process**

To trigger an ARP request, we attempt to ping PC1 from PC0. Since PC0 does not yet know PC1's MAC address, it must perform an ARP lookup first. An ARP packet is generated and the ICMP packet is queued.

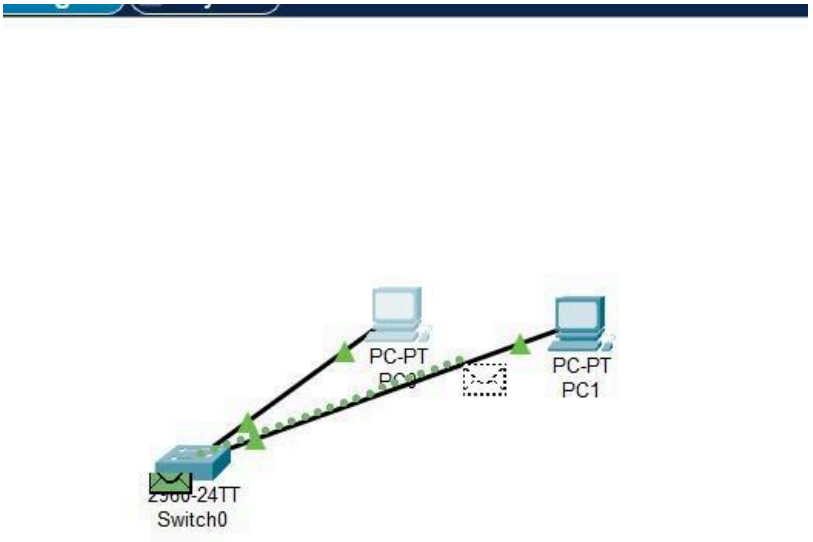
- **Ping Command in PC0's Command Prompt**



- **Step 5: The ARP Request (Broadcast)**

PC0 sends a broadcast ARP request to the switch. The switch, receiving a broadcast frame (destination MAC: FF:FF:FF:FF:FF:FF), forwards it out to all other ports.

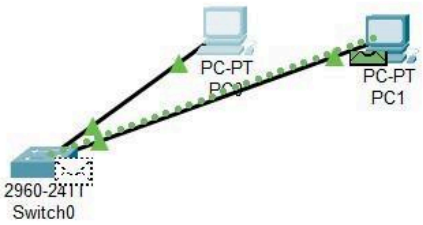
- **ARP Packet Broadcast from Switch**



- **Step 6: The ARP Reply (Unicast)**

PC1 recognizes its IP address in the ARP request and generates an ARP reply. This reply is a **unicast** frame, addressed directly to the MAC address of PC0, which PC1 learned from the initial request. ·

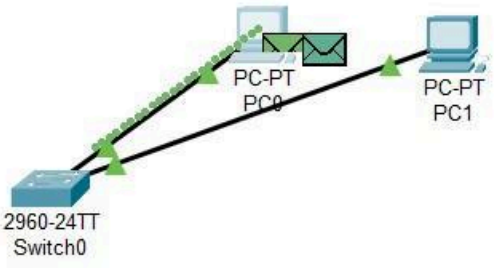
ARP Reply Sent from PC1



- **Step 7: Successful ICMP Communication**

Now that PC0 has received the ARP reply and knows PC1's MAC address, it can successfully send the queued ICMP (ping) packet. This packet is sent directly to PC1.

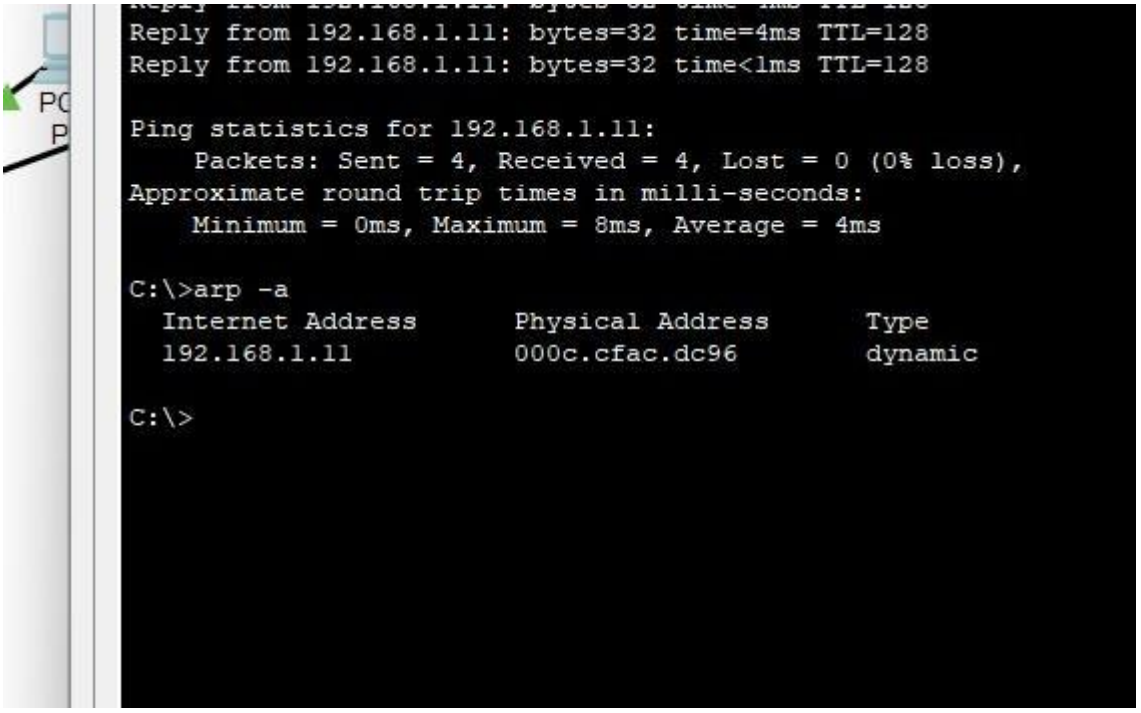
- **ICMP Packet Sent from PC0 to PC1**



- **Step 8: Verifying the ARP Table**

Finally, we can switch back to **Realtime Mode** and check the ARP table on PC0. The arp -a command shows that a dynamic entry has been created, mapping PC1's IP address to its physical MAC address, confirming the ARP process was successful.

- **Output of arp -a on PC0**


Reply from 192.168.1.11: bytes=32 time=4ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 8ms, Average = 4ms
C:\>arp -a
Internet Address Physical Address Type
192.168.1.11 000c.cfac.dc96 dynamic
C:\>