LAB 2: IP Addresses and Host-to-Host Communication

Contents

Introduction to LAB 2

In Lecture 2, you have learned about the different numeral systems, the subnet masks and their usage. You also learned what are the ARP and MAC address tables and how the computers and the networking devices use them. In this lab, you will make some conversions between the numeral systems and will determine some valid IP addresses and ranges based on network masks. Then, using Cisco Packet Tracer, you will monitor Host-to-Host communication at Layer 2 in different scenarios.

Exercise 1: Converting between the numeral systems

Task 1: Binary numbers to decimal

Convert the following binary numbers to decimal and write down the results in the table

Binary	Decimal
00001111	
11110000	
11111111	
10101010	
11111110	

Task 2: Converting decimal numbers to binary

Now, let us do the opposite - convert the decimal numbers in binary and fill in the table the results

Decimal	Binary
192	
168	
5	
240	
256	

Task 3: Converting hexadecimal to binary numbers

Why do we need the hexadecimal numbering system? Well, one reason is that the MAC addresses are represented in this format. In this task, you are asked to convert some MAC addresses into binary numbers. Please fill in the table respectively.

Hexadecimal (MAC Address)	Binary
10-1F-74-E2-2D-12	
B0-05-94-F4-A8-0D	
70-18-8B-C6-86-DC	
00-1F-3B-99-34-7D	
E8-11-32-4E-07-DB	

Who is the vendor of the network adapter that has the first in the table MAC address (10-1F-74-E2-2D-12)? How do you know it?

Exercise 2: IP Addresses and Masks

Given some IP networks and subnet masks, determine:

- The network address
- The broadcast address
- The first usable host address
- The last usable host address

| IP Network and Mask	Network Address	Broadcast Address	First host Address	Last Host Address
192.168.1.0/24				
192.168.0.0/24				
10.0.0.0/23				
15.137.14.128/25				
213.0.0.0/8				

Exercise 3: Explore the traffic flow and the message exchange between two directly connected hosts

In this exercise, you are going to connect two PCs directly to each other with a cable (without using any networking device between them). You will setup IP addresses on their NICs (Network Interface Cards) from the **10.0.0.0/24** IP network in order to be able to ping between them. As you already know, **ping** is Layer 3 protocol, which uses ICMP echo requests, and ICMP echo replies to check the IP connectivity between two hosts. You will closely monitor the network packet flow between the devices.

Note: In the following exercises, you will be asked to change the topology or part of it (for example change the Hub with a Switch). If this leads to unexpected behavior (like generating multiple ARP packets, or missing ARP), please create a brand-new topology for each exercise (delete all the devices and add them again) – this should be very fast process.

1. Open Cisco Packet Tracer. Move two end devices to the topology (select "PC" type) and connect them directly. For the connection, you can use either the automatic connection or the crossover cable.

Why crossover should be used? Because it connects devices from the same type (in this case, pc-to-pc)
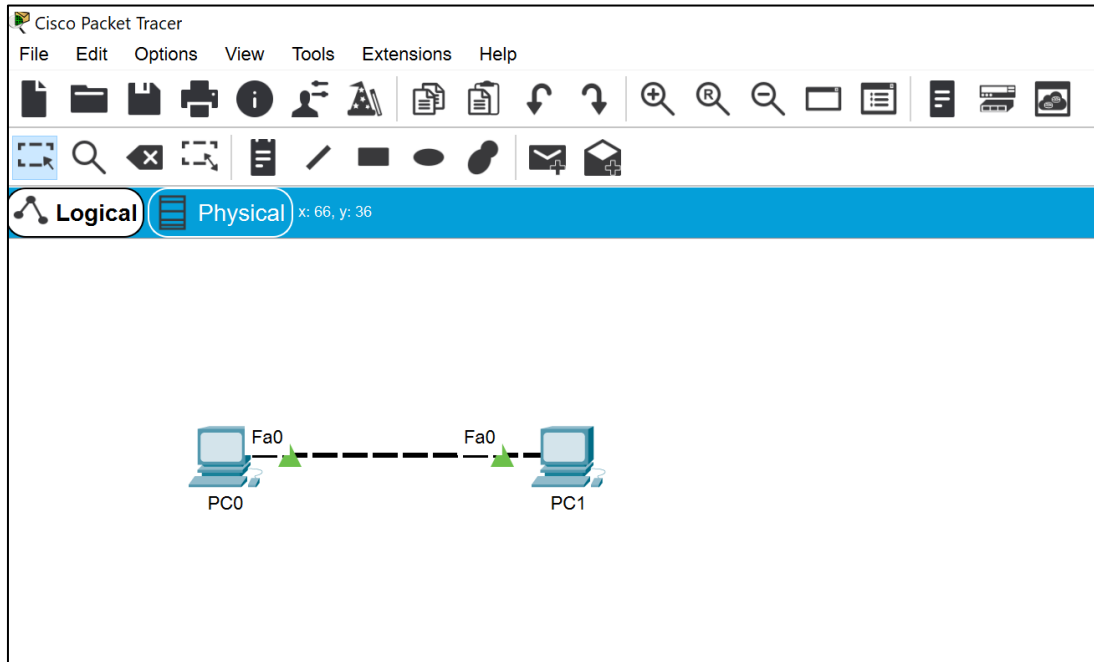

2. Click on the first pc (PC0), go to the config tab and select <u>FastEthernet0</u> to setup an IP address. This will be the first address in the selected network: **10.0.0.1/24** (as you know, /24 is another representation of 255.255.255.0)
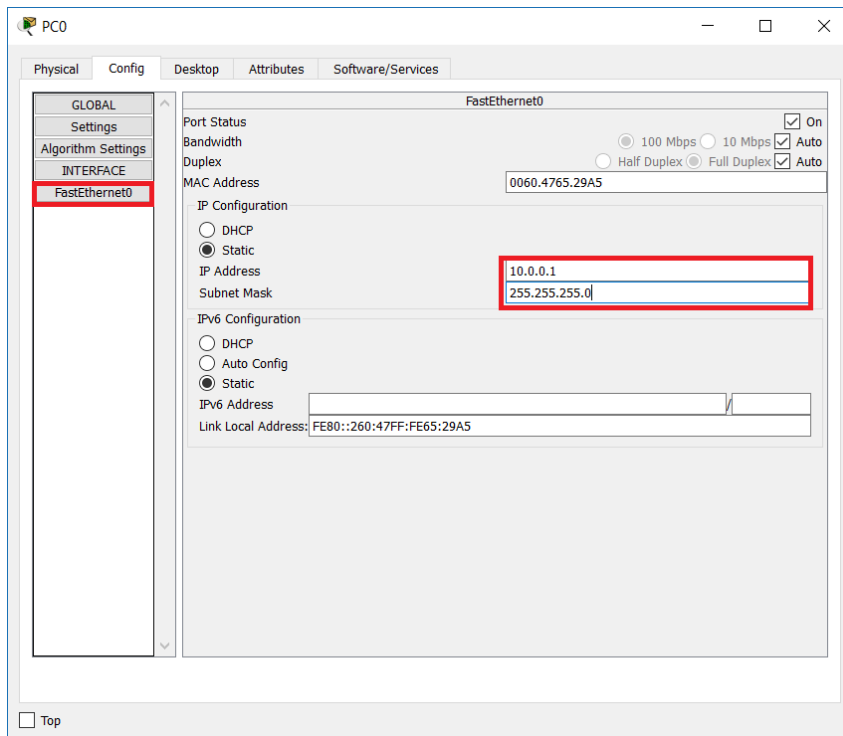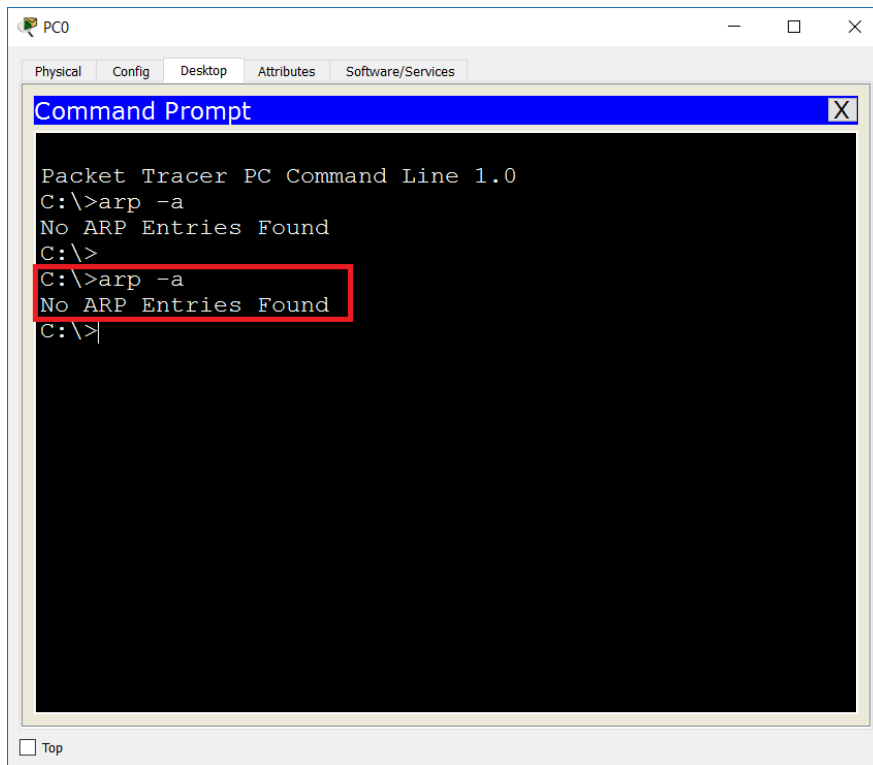
3. Use the same steps to setup the second IP address, **10.0.0.2/24**, on the second pc (PC1)
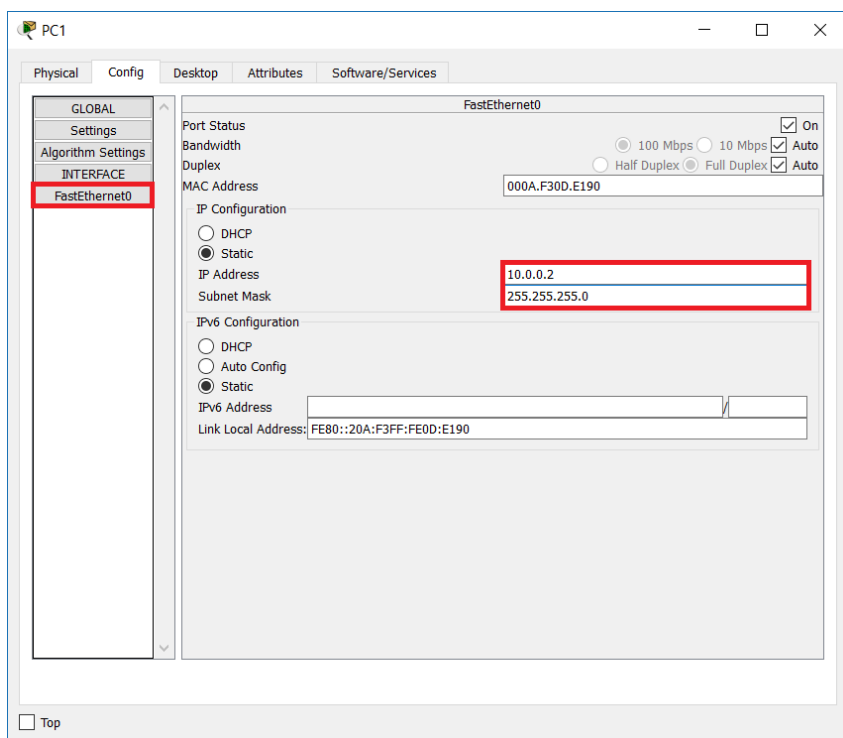
4. Back in PC0, go to the <u>Desktop</u> tab and the open a <u>Command Prompt</u> (We will sometimes refer to it as CLI – Command Line Interface)
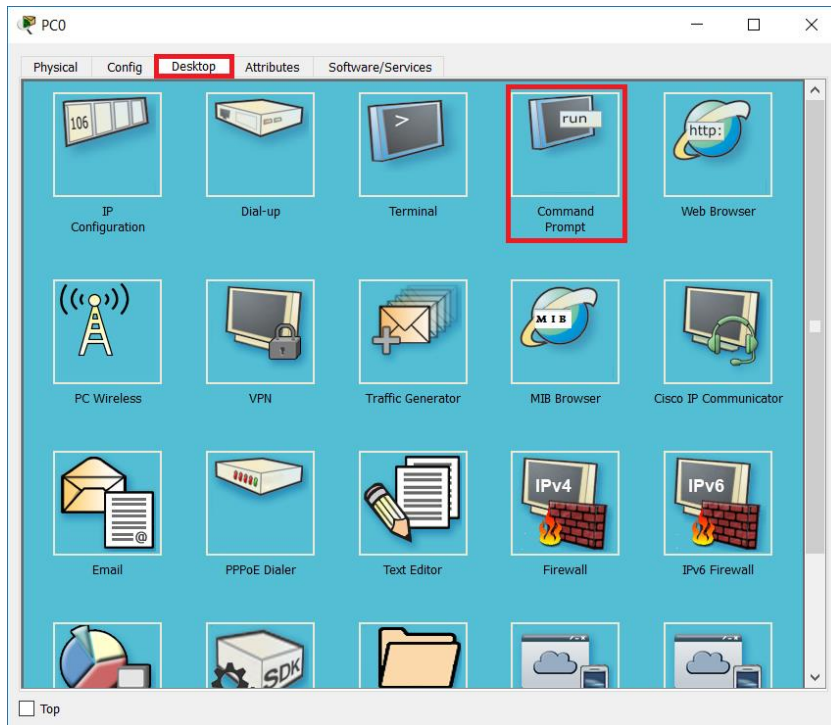
5. Since this is the beginning of our tests, PC0 should have empty ARP table. Make sure this is true by typing **arp -a** in the CLI

6. Check that you have the correct IP address and subnet mask on PC0 (10.0.0.1, 255.255.255.0) with the **ipconfig** command. Make sure that you do not have a default gateway in the configuration.
   Why a default gateway is not needed? In this exercise (and all other exercises below in Lab 2), you have connections that do not require routing. Instead, you connect devices, which belong to the same IP subnet – that is why there is no need for default gateway in these scenarios
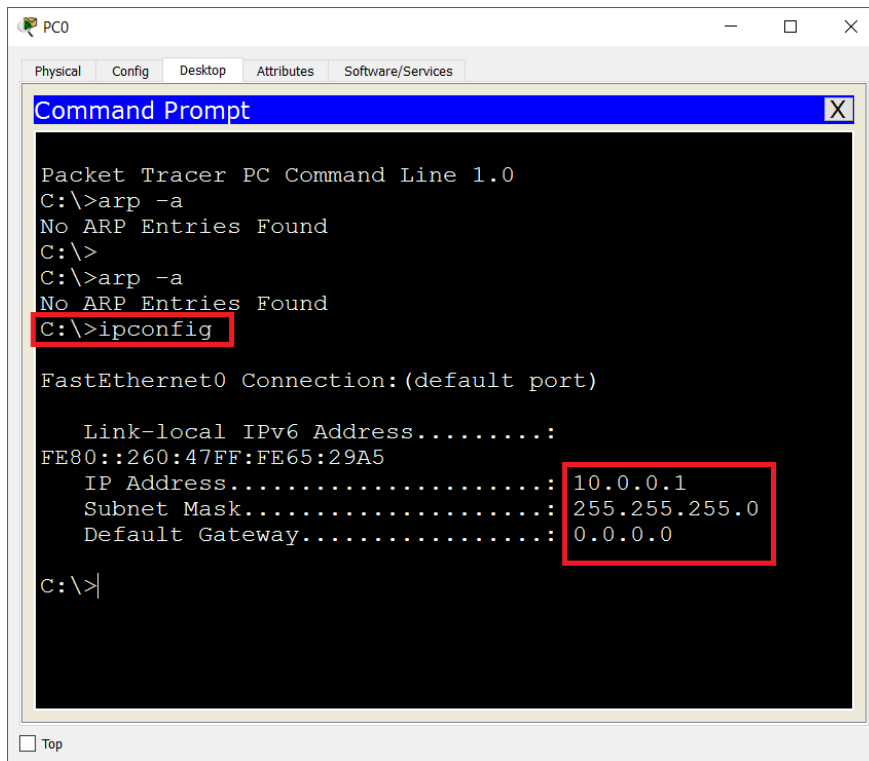
7. Open the second pc (PC1), go to the Desktop tab -> Command Prompt and check that you have the correct IP address and subnet mask (10.0.0.2, 255.255.255.0) with the **ipconfig** command

Follow us:
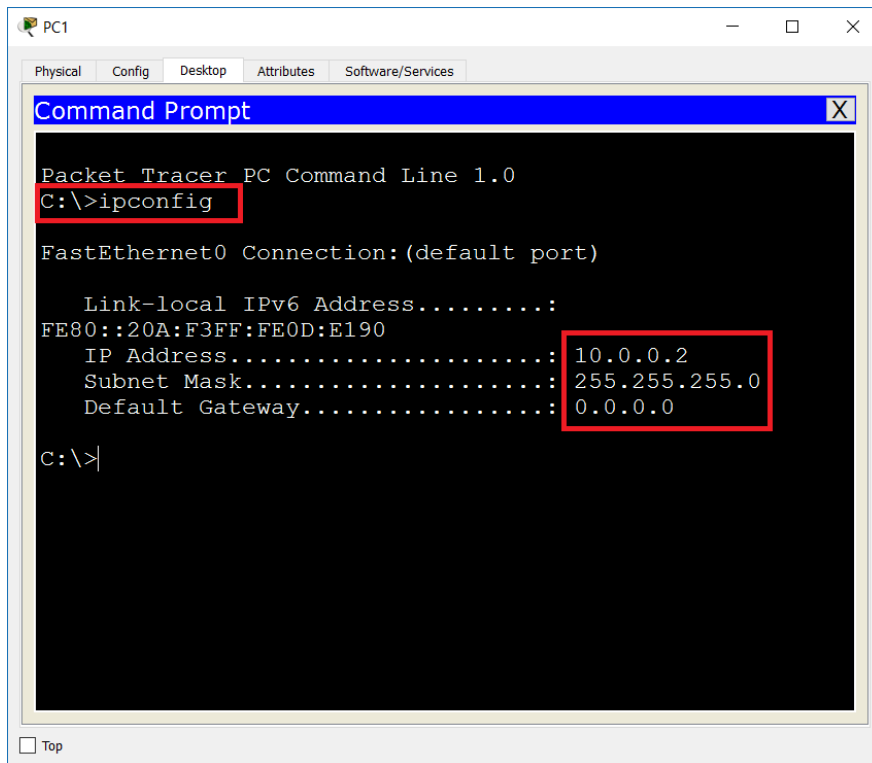
8. In the lower-right corner of Packet Tracer, click the icon to change to Simulation Mode (or press Shift + S). Now you can monitor each step in the communication and the packet exchange process. Before this, make sure that you do not monitor all the events since this can be distractive. For the purposes of this Lab, you will monitor ICMP (ping) and ARP packets. Click on Show All/None to deselect all the events and then click Edit Filters

Follow us:
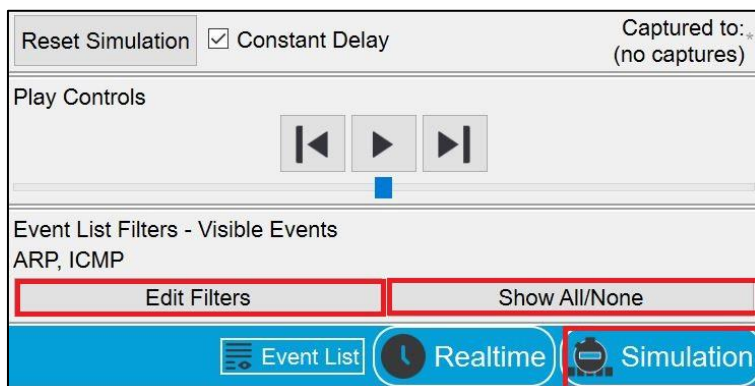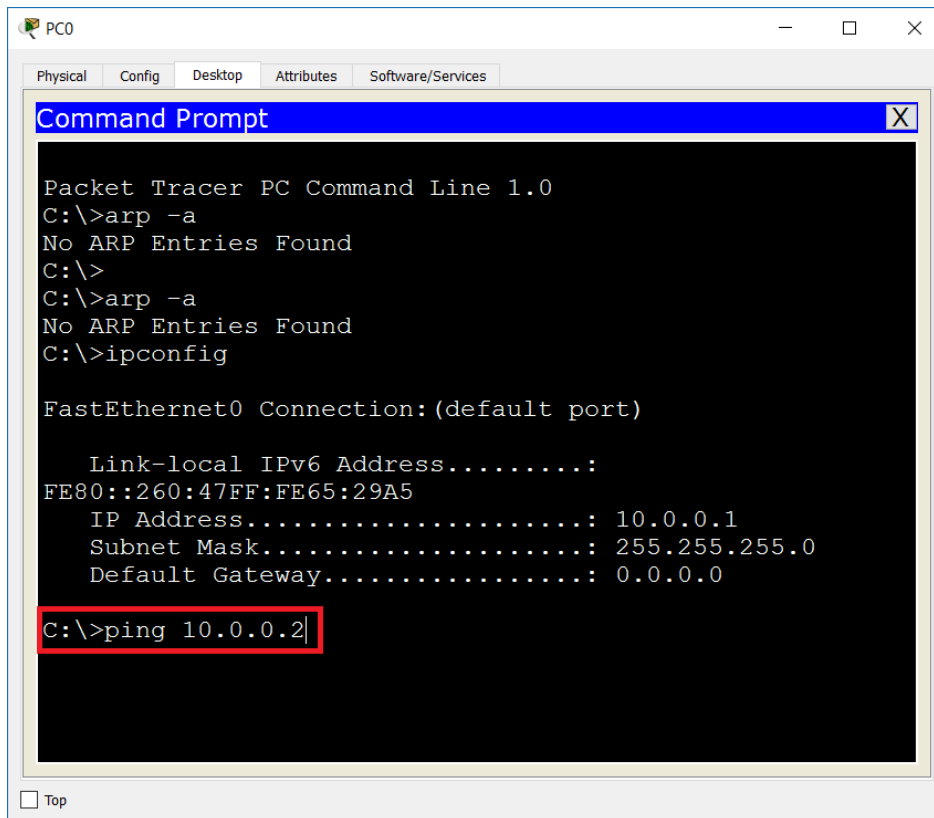
9. In the Edit Filters window, make sure to select only ARP and ICMP under the IPv4 section. All other protocols in this and the other sections (IPv6 and Misc) should be un-checked

10. Open again the command prompt of PC0 and start ping to 10.0.0.2 (PC1). Note that since you are in Simulation Mode, you will not see any results from this command at the moment. Just type **ping 10.0.0.2** and hit **Enter**

11. To start the packet exchange process, click on Capture / Forward button in the Simulation Panel. Note the two packets that PC0 is generating – ARP request and ICMP echo request. Continue to click on the Capture / Forward button to see each step of the packets
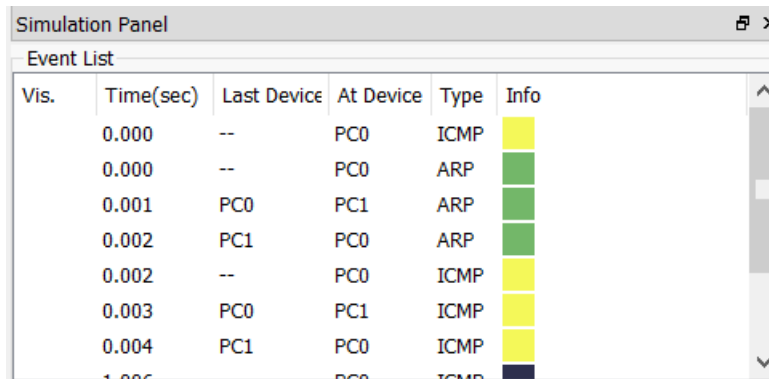
12. You can click on a packet to open more details about it, read additional information or take a quick test in the <u>Challenge me</u> section
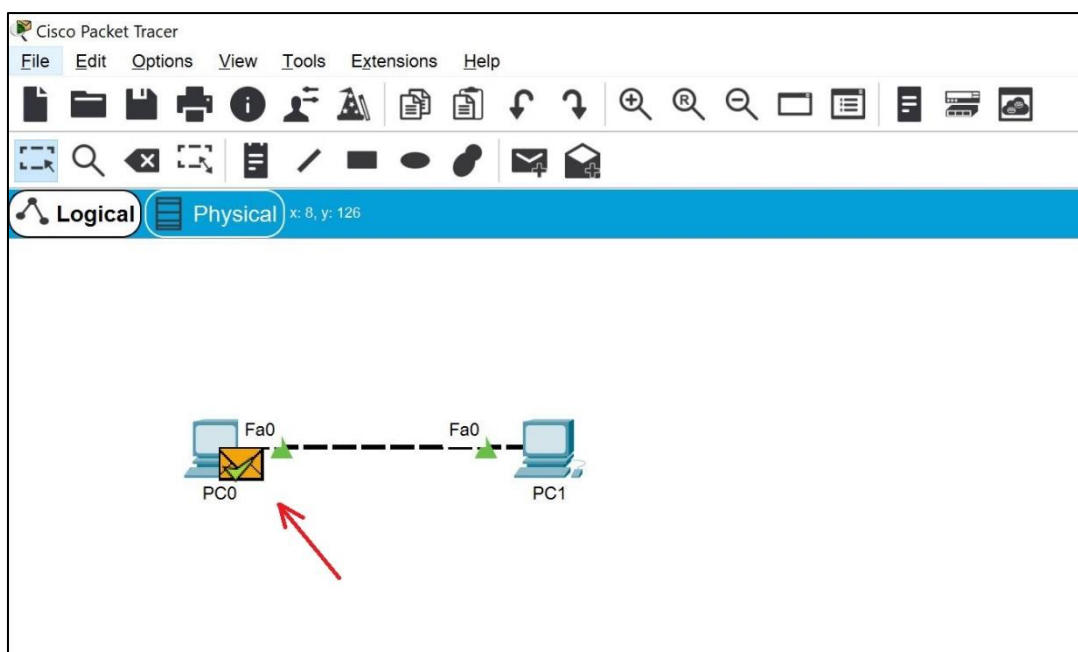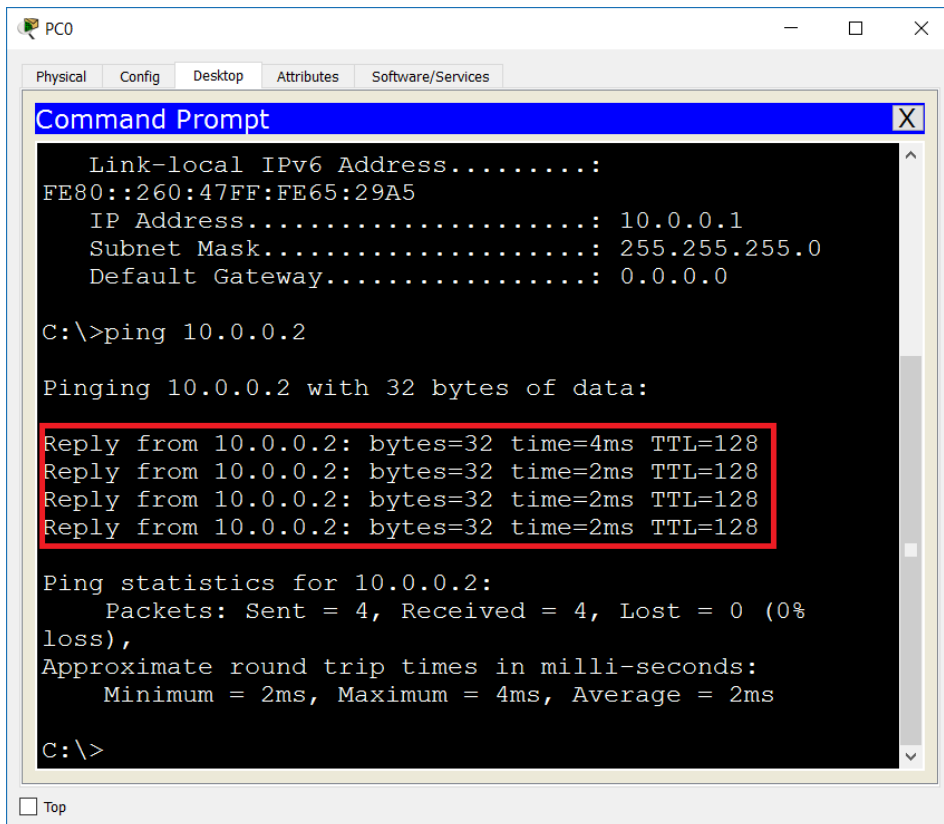
13. Check your <u>Event List</u> – you should have an ARP packet exchange at the beginning and then, when PC0 knows the MAC address of PC1, all the other packets are ICMP

14. Go back to the command prompt of PC0 and check that ping succeeded - all the four ICMP packets should have been sent and received successfully
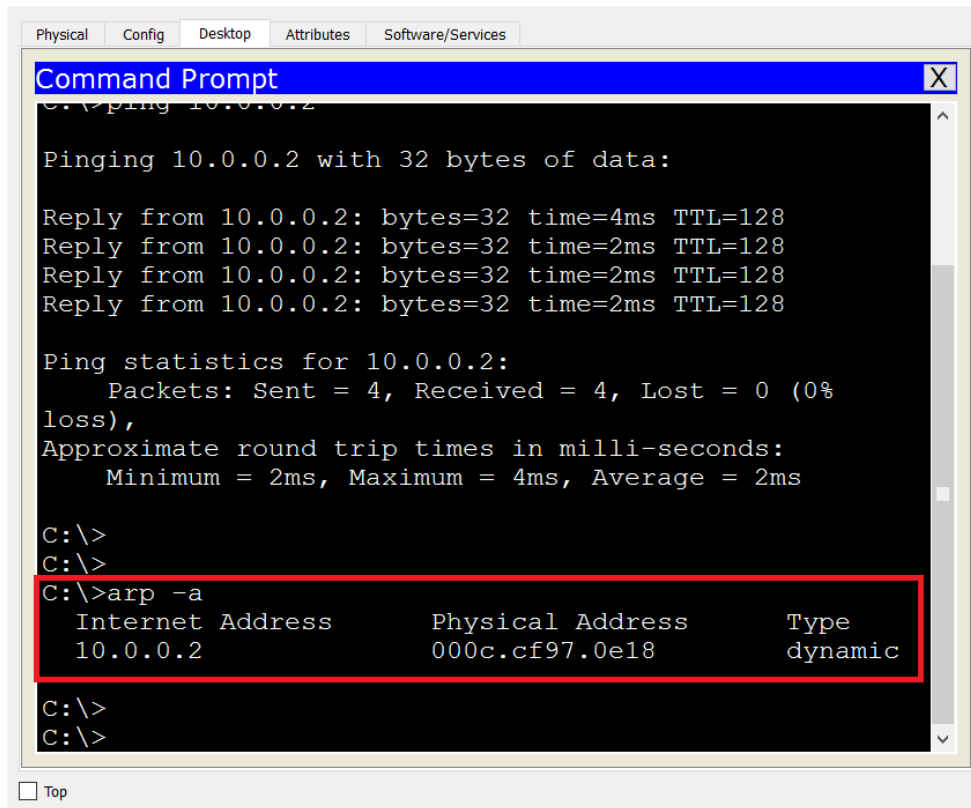
15. Check the ARP table of PC0 by typing **arp -a**. Now you can see an entry which shows the MAC address of PC1 (remember that before the ping, this table was empty)


16. Click on <u>Realtime</u> to reset the clear the simulation mode (you will go back to in in the next exercises)
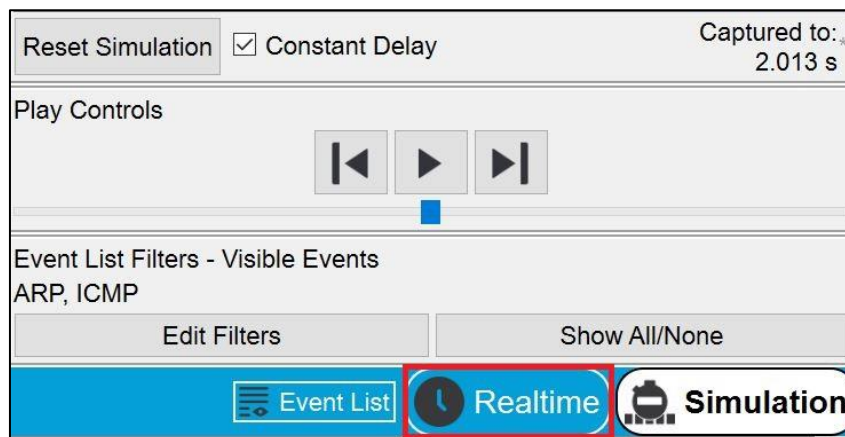
Exercise 4: Explore the traffic flow and the message exchange between hosts connected with a Hub

In this exercise, you will use network Hub to establish connection between the networking devices. You will observe the Hub behavior by monitoring the ICMP packet exchange. A Hub is a Layer 1 device, which simply retransmits each received packet to all other ports.

1. Delete the connection between the end devices, drag a Hub (Use PT-Hub, the first one) in the topology, drag one more generic end device (PC2) and connect them as shown in the screenshot (again, as noted before, you can start a new topology from zero – sometimes it can eliminate errors)
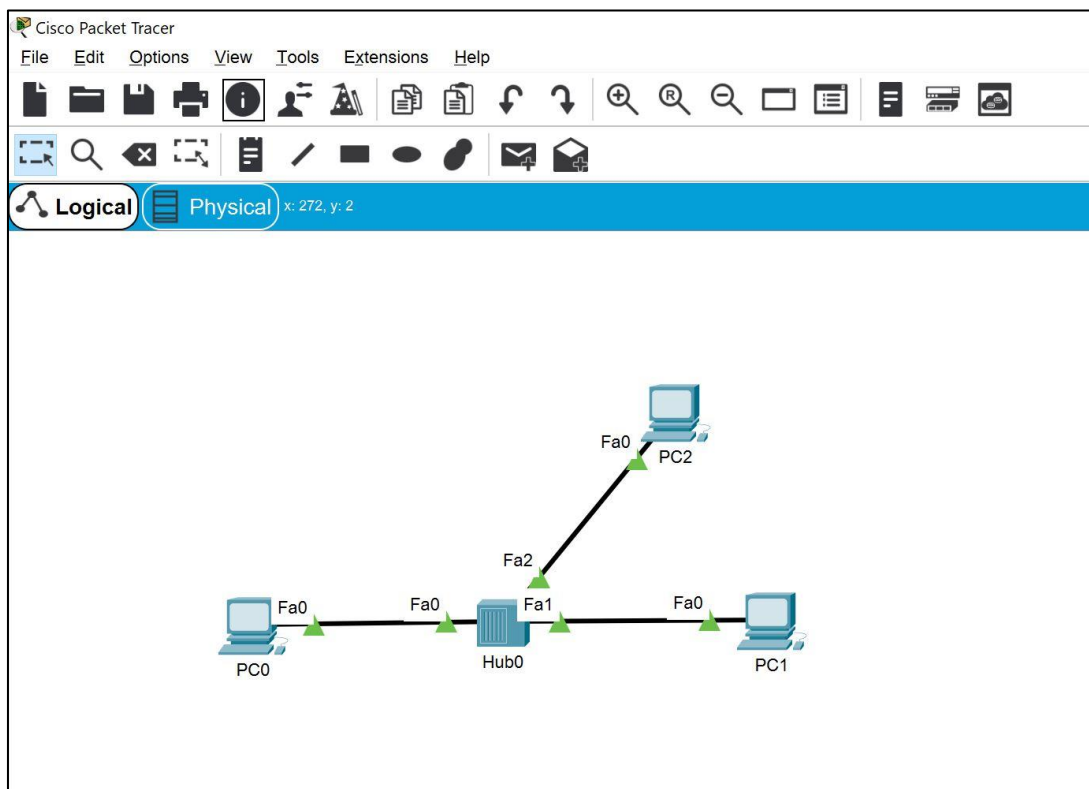
2. Open the configuration of PC2 and setup static IP address in the same IP network – 10.0.0.3/24
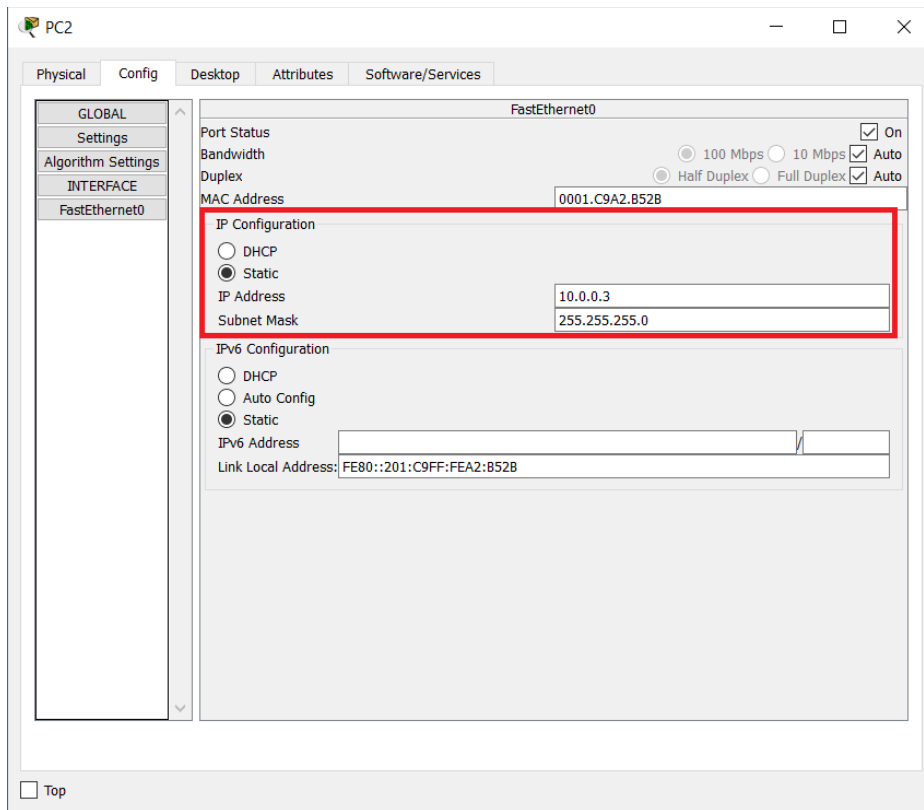
3. Initiate ping to 10.0.0.2 (PC1) from the command line of PC0 and while clicking the Capture / Forward button, observe the packet exchange between the two hosts
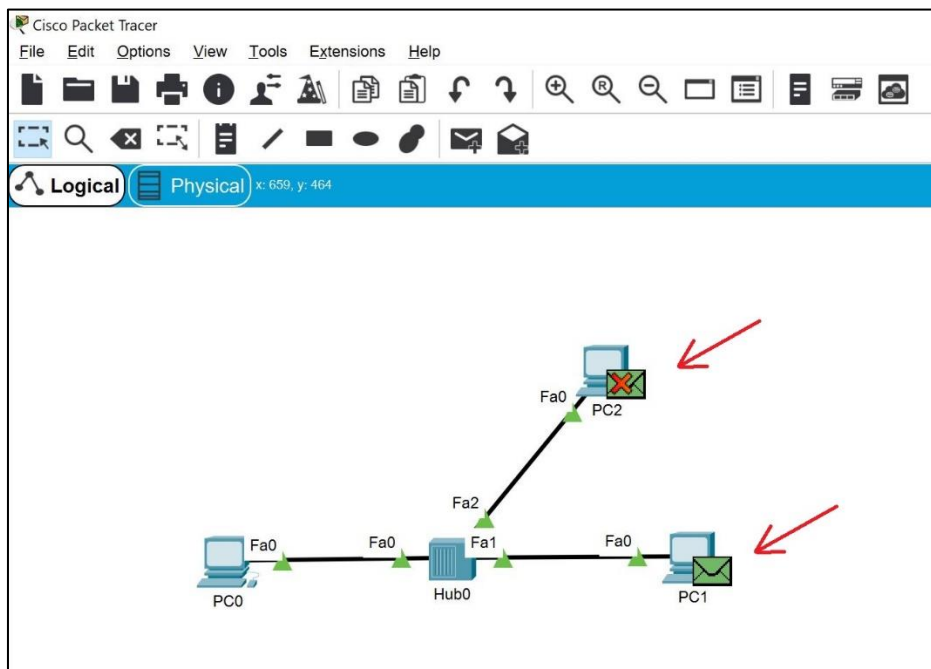
Note: PC0 now has the MAC address of the destination, PC1, in its ARP table. You can (optionally) clear the ARP table of PC0 by typing **arp -d** in the command line if you want to see the ARP message exchange again. In either case, the Hub will broadcast each message (either ARP or ICMP) to all ports except the port on which the packet is received.

4. For example, have a look at the ICMP echo reply packet (this is the ping response) from PC1 – it goes to both PC0 and PC2
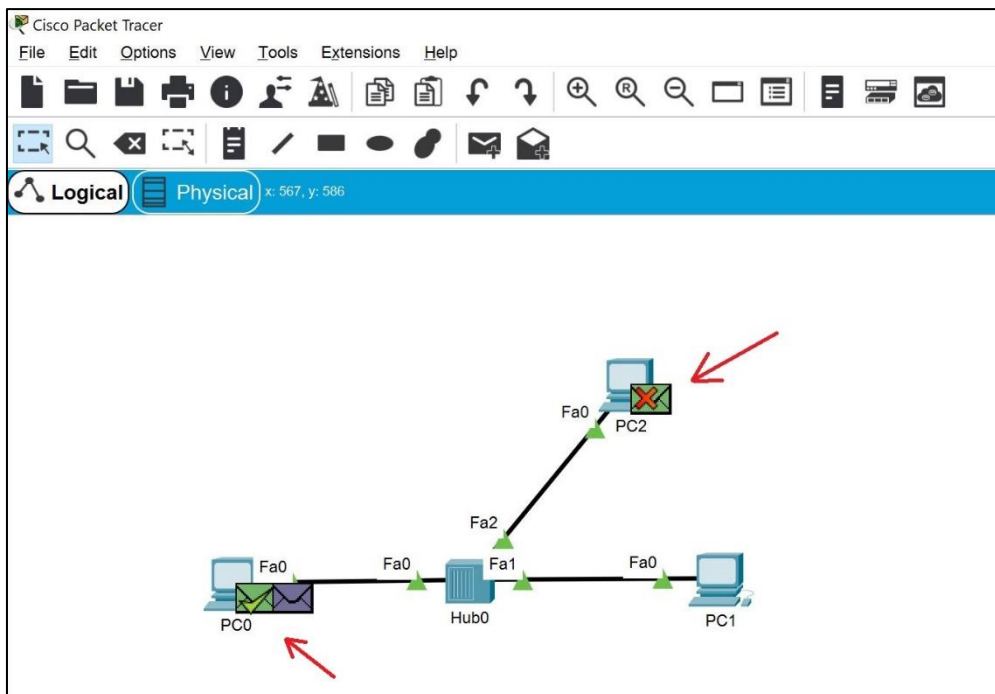

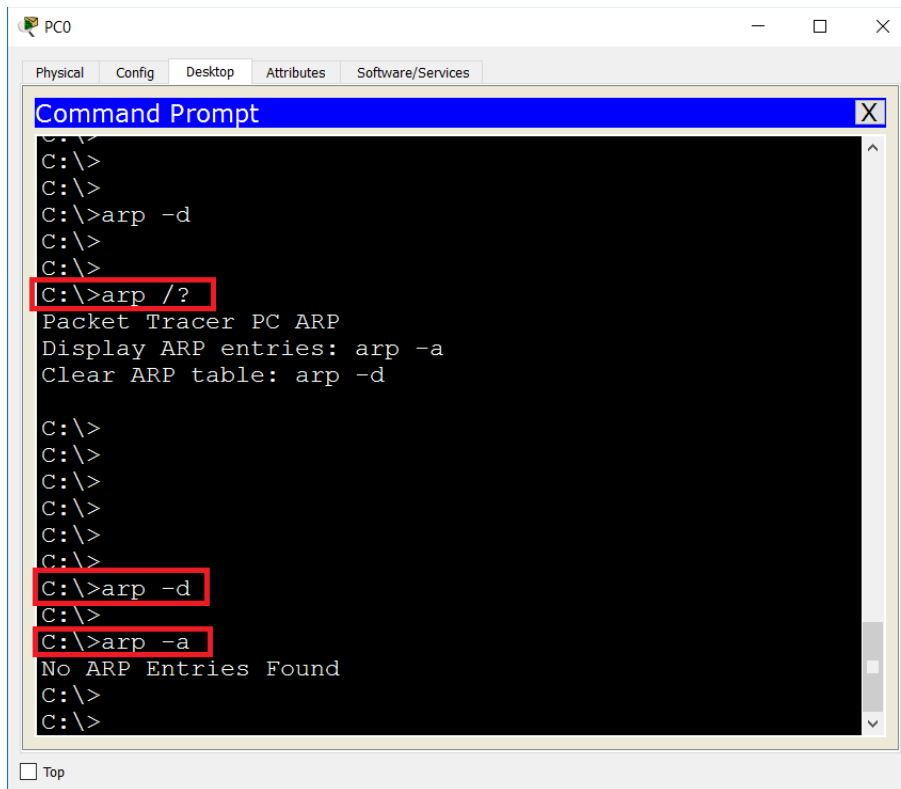5. Reset the simulation to prepare for the next exercise

Exercise 5: Explore the traffic flow and the message exchange between hosts connected with a Switch

In this exercise, you will observe the ICMP and ARP message exchange when we have our hosts connected with a Switch. As you know, a Switch is a Layer 2 device, which is more intelligent than a Hub. One reason is that it has a MAC address table. This table keeps records about the switch ports and the connected to them MAC addresses. This way, the forwarding decisions are more efficient and secure (instead of sending the packet out of each single port like the Hubs do). Again, you will use the 10.0.0.0/24 IP network with three end devices belonging to it (we still do not have routing here).

1. Delete the Hub and move a Switch to the topology (use 2960 as a Switch model). Connect the end devices to it as per the picture below
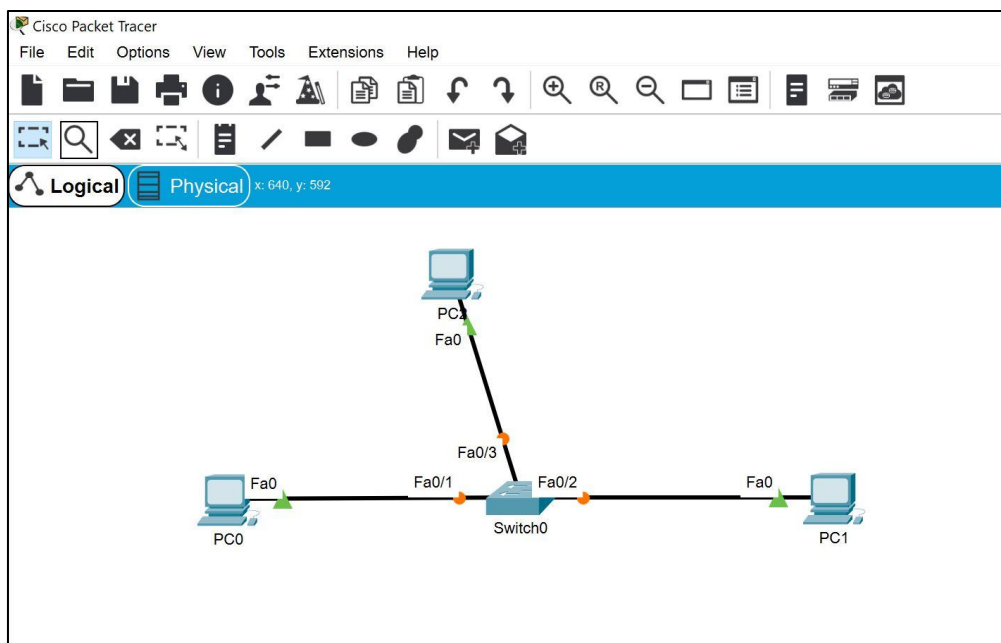
2. Consult the help about the Windows ARP command by typing **arp /?** and clear the ARP table of PC0 by typing **arp -d**. Then, check that it is deleted, and no entries exist by typing **arp -a**

3. Login to the CLI of your Switch and type **show mac address-table** to see that no entries exist before a communication is initiated. Sometimes, it may happen that you see entries in the MAC address table and this can happen because some of the hosts initiate [hidden] messages in the background and because of this the switch learns the connected MAC addresses. If this is the case, you can clear the table with the **clear mac address-table** command (from the privileged access mode)

Follow us:
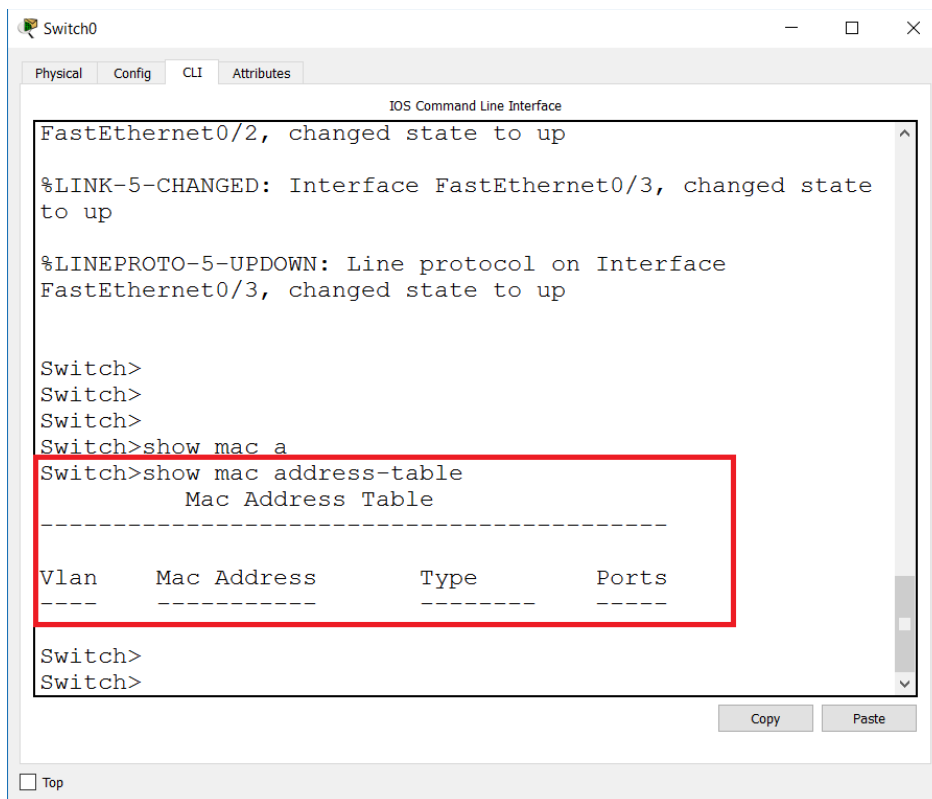
4. Initiate **ping 10.0.0.2** (this is PC1) from PC0. By clicking the Capture / Forward button, monitor the packet exchange. Observe that the ARP request will reach ALL connected devices (PC1 and PC2) although the client computers are connected through a Switch. This is so because the ARP destination is a Layer 2 broadcast address and in this particular situation, the switch will act like a Hub. Observe that after the initial ARP message exchange, all other ICMP packets are unicast (because the source now knows the destination MAC address) and also the switch will forward each subsequent packet to a single port – the one which is connected to the corresponding MAC address. This is because the MAC address table is built dynamically
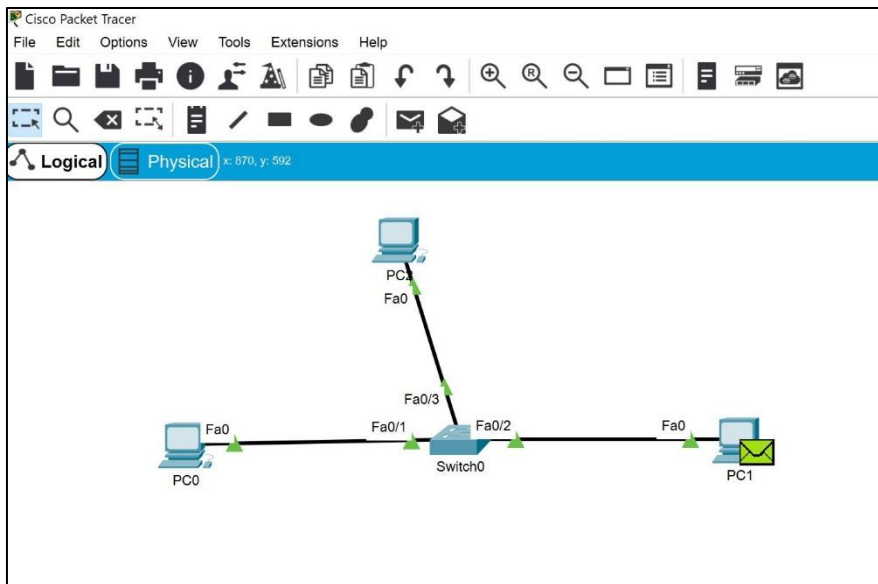
5. Connect to the switch and type again **show mac address-table**. Observe the new entries in the MAC address table

You have completed LAB 2.