

LAB 2: IP Addresses and Host-to-Host Communication – part 1

Contents

Introduction to LAB 2	2
Exercise 1: Converting between the numeral systems	2
Task 1: Binary numbers to decimal	2
Task 2: Converting decimal numbers to binary	2
Task 3: Converting hexadecimal to binary numbers	3
Exercise 2: IP Addresses and Masks	3
Exercise 3: Explore the traffic flow and the message exchange between two directly connected hosts	4
Exercise 4: Explore the traffic flow and the message exchange between hosts connected with a Hub	16
Exercise 5: Explore the traffic flow and the message exchange between hosts connected with a Switch	19

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 the ARP table is 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 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

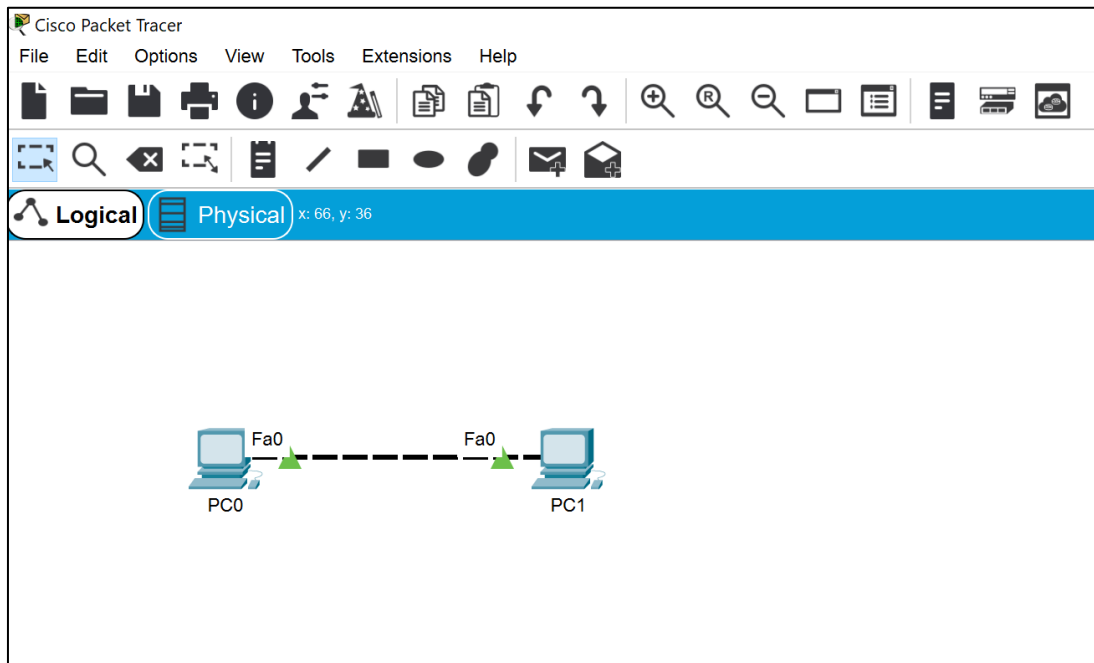
In this exercise, you are going to connect two PCs directly to each other with a cable (without using any networking device between them). You will setup IP addresses on their NICs (Network Interface Cards) from the **10.0.0.0/24** IP network in order to be able to ping between them. Note that all of the end devices (PCs or Laptops) in this Lab should have IP addresses from the same IP network/subnet (in this case it is 10.0.0.0/24). This is very important for this and for the next exercises from this lab as well, because if we have to connect devices from different networks/subnets, we will need a Layer 3 device (router or Layer 3 switch) to connect them. We are not discussing routing yet and we need to have all off the end devices belonging to the same network/subnet.

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.

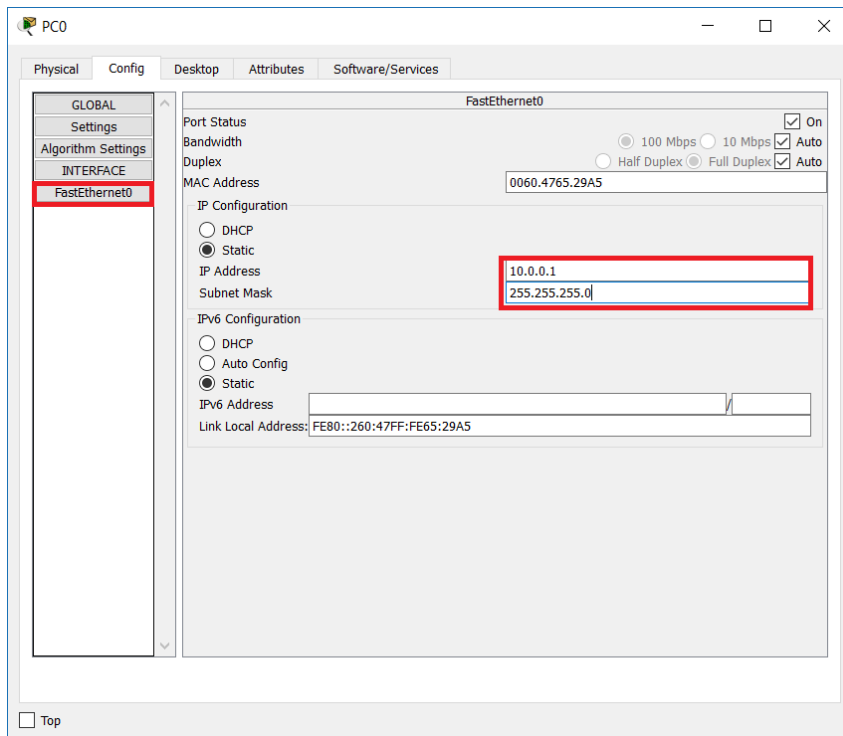
Note: In the following exercises, you will be asked to change the topology or part of it (for example change the Hub with a Switch). If this leads to unexpected behavior (like generating multiple ARP packets, or missing ARP), please create a

brand-new topology for each exercise (delete all the devices and add them again)
– this should be very fast process.

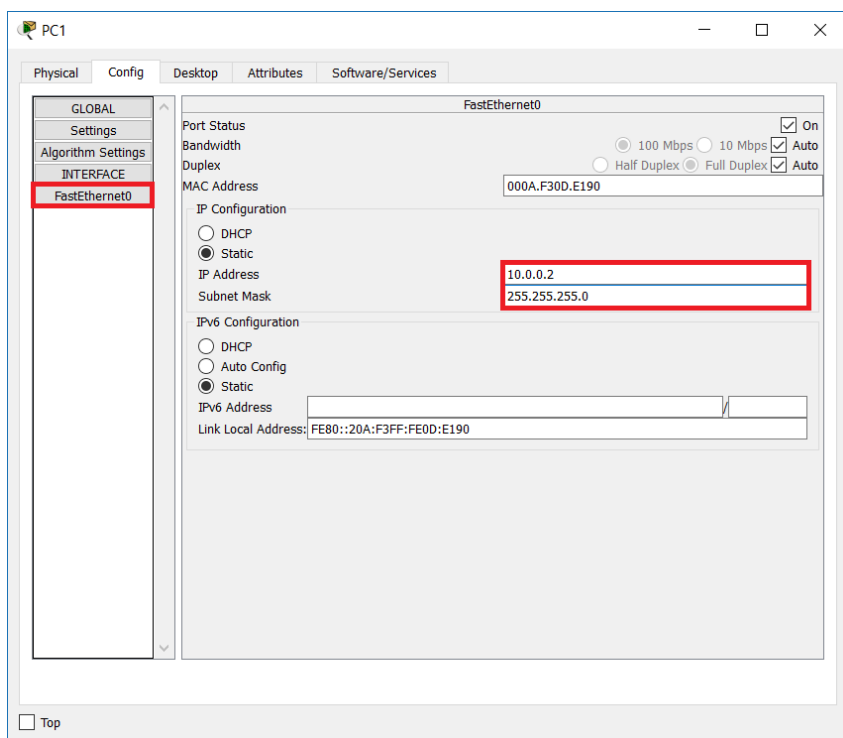
1. Open Cisco Packet Tracer. Move two end devices to the topology (select “PC” or “Laptop” type) and connect them directly. For the connection, you can use either the automatic connection or the crossover cable. Why crossover should be used? Because it connects devices from the same type (in this case, pc-to-pc)



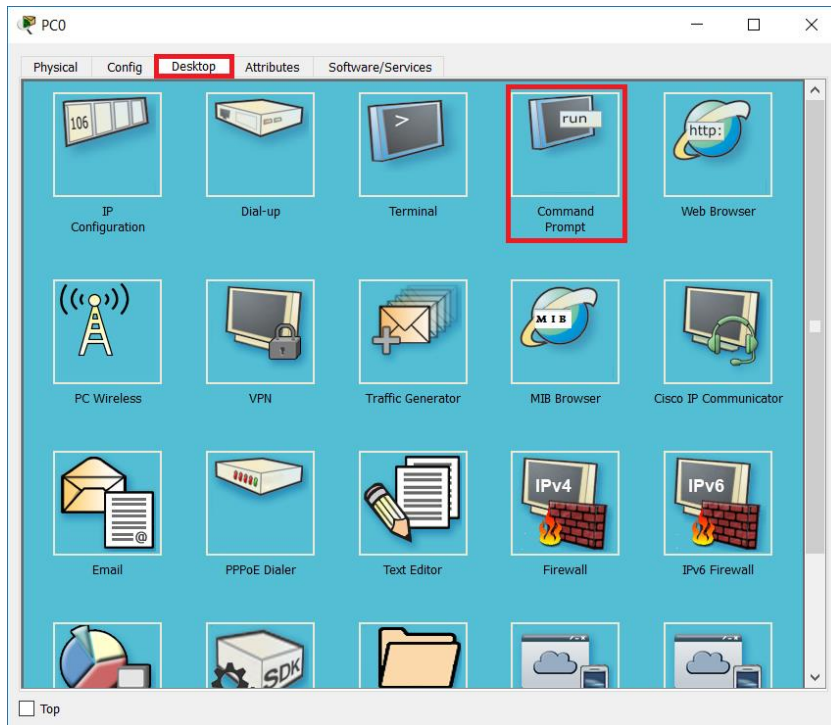
2. Click on the first pc (PC0), go to the config tab and select FastEthernet0 to setup an IP address. This will be the first address in the selected network: **10.0.0.1/24** (as you know, /24 is another representation of 255.255.255.0)



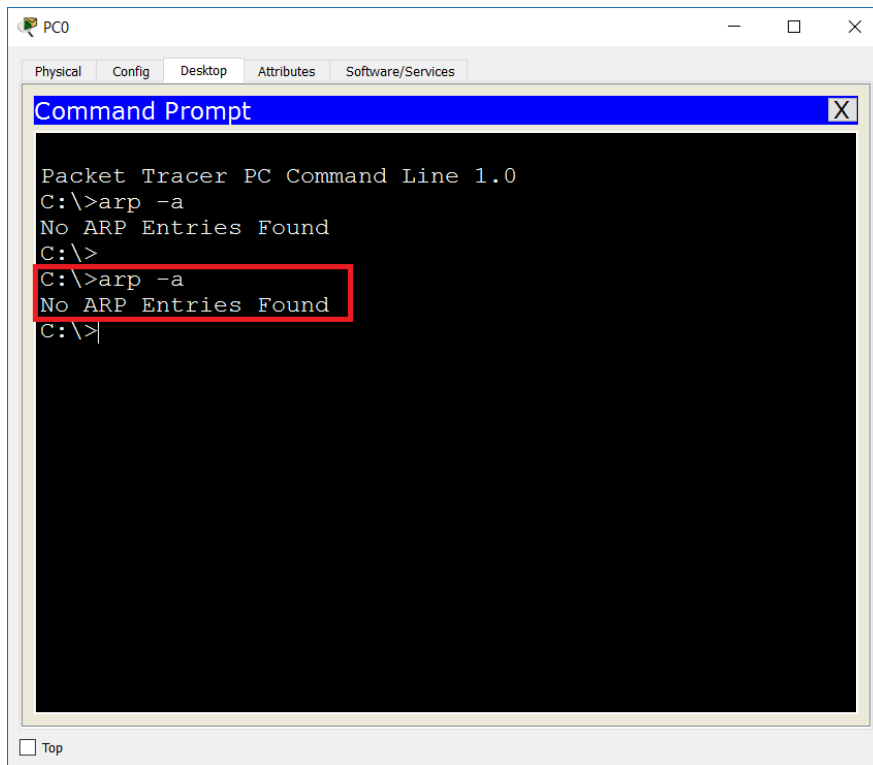
- Use the same steps to setup the second IP address, **10.0.0.2/24**, on the second pc (PC1)



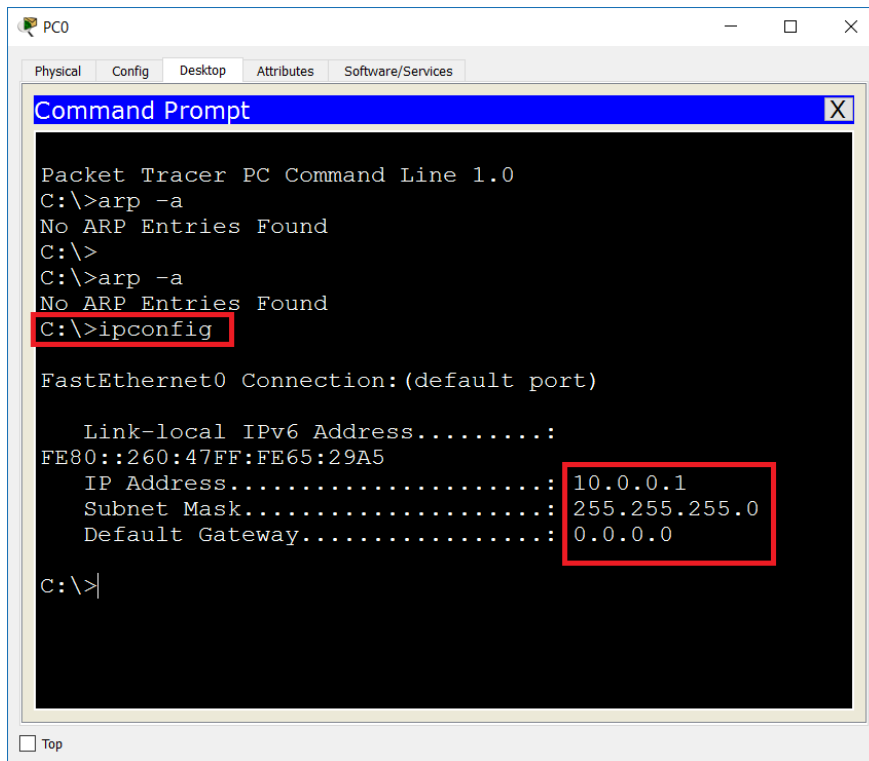
4. Back in PC0, go to the Desktop tab and the open a Command Prompt (We will sometimes refer to it as CLI – Command Line Interface)



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



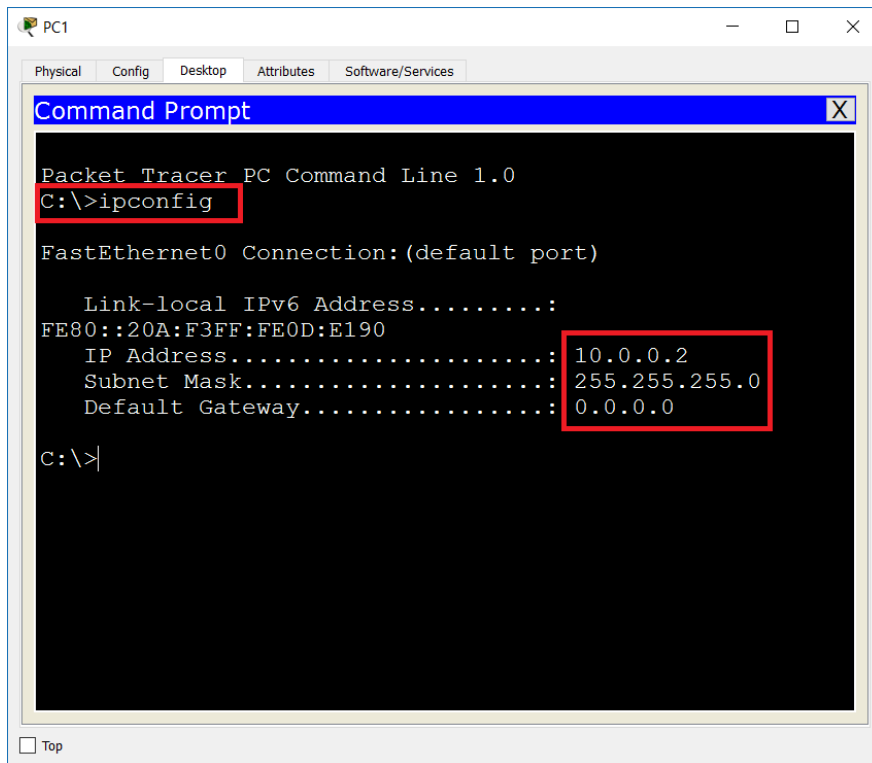
```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
C:\>arp -a
No ARP Entries Found
C:\>ipconfig

FastEthernet0 Connection:(default port)

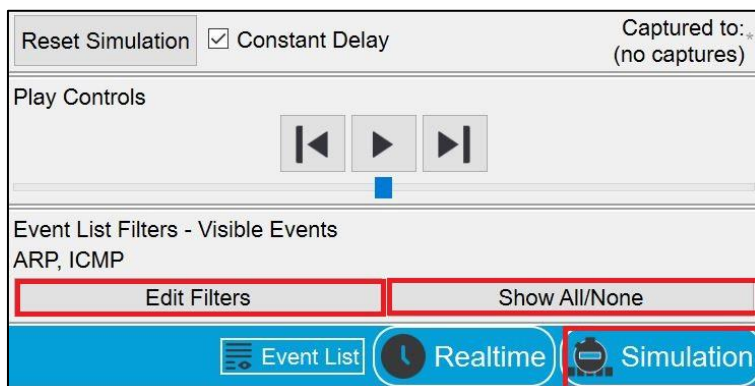
    Link-local IPv6 Address.....:
FE80::260:47FF:FE65:29A5
    IP Address.....: 10.0.0.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 0.0.0.0

C:\>
```

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



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 distracting. 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

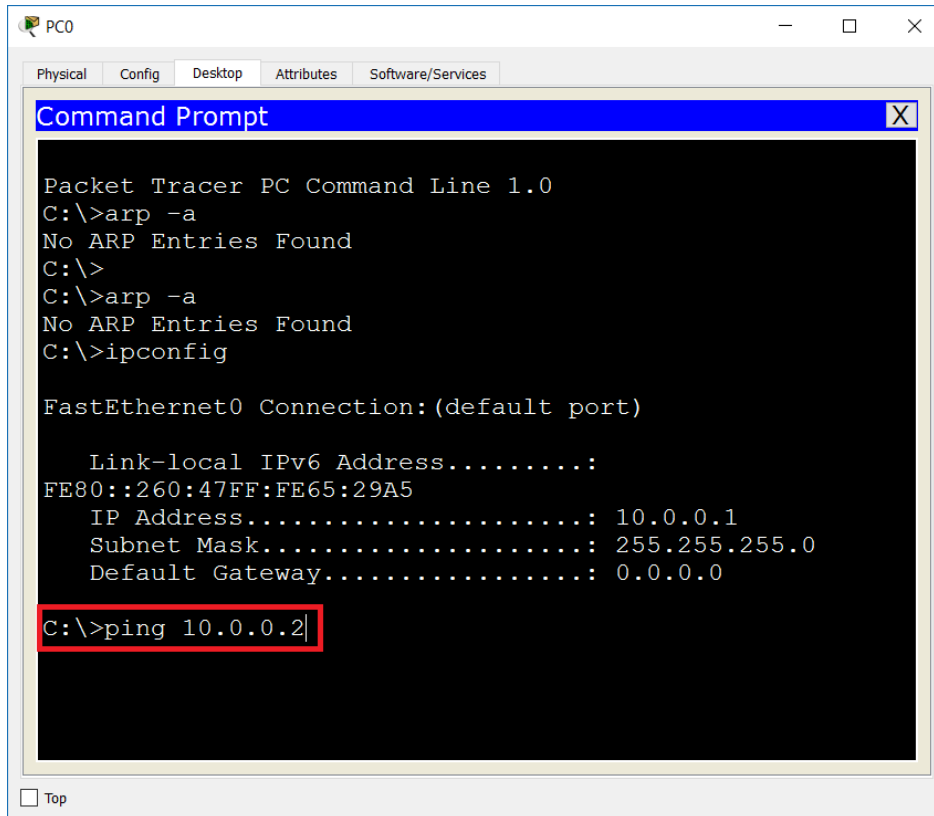


9. In the Edit Filters window, make sure to select only ARP and ICMP under the IPv4 section. All other protocols in this and the other sections (IPv6 and Misc) should be un-checked

IPv4	IPv6	Misc
<input checked="" type="checkbox"/> ARP	<input type="checkbox"/> BGP	<input type="checkbox"/> DHCP
<input type="checkbox"/> DNS	<input type="checkbox"/> EIGRP	<input type="checkbox"/> HSRP
<input checked="" type="checkbox"/> ICMP	<input type="checkbox"/> OSPF	<input type="checkbox"/> RIP

Edit ACL Filters

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**



The screenshot shows a Packet Tracer PC0 window with a Command Prompt open. The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
C:\>arp -a
No ARP Entries Found
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address.....:
FE80::260:47FF:FE65:29A5
    IP Address.....: 10.0.0.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 0.0.0.0

C:\>ping 10.0.0.2|
```

The command prompt window has a blue title bar with the text "Command Prompt" and a close button. The background is black with white text. The command "C:\>ping 10.0.0.2|" is highlighted with a red rectangular box.

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

Simulation Panel				
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.000	--	PC0	ARP
	0.001	PC0	PC1	ARP
	0.002	PC1	PC0	ARP
	0.002	--	PC0	ICMP
	0.003	PC0	PC1	ICMP
	0.004	PC1	PC0	ICMP
	1.006	--	PC0	ICMP
	1.007	PC0	PC1	ICMP
	1.008	PC1	PC0	ICMP
	2.010	--	PC0	ICMP
	2.011	PC0	PC1	ICMP
	2.012	PC1	PC0	ICMP
Visible	3.013	--	PC0	ICMP

Reset Simulation ☒ Constant Delay Captured to: 3.013 s

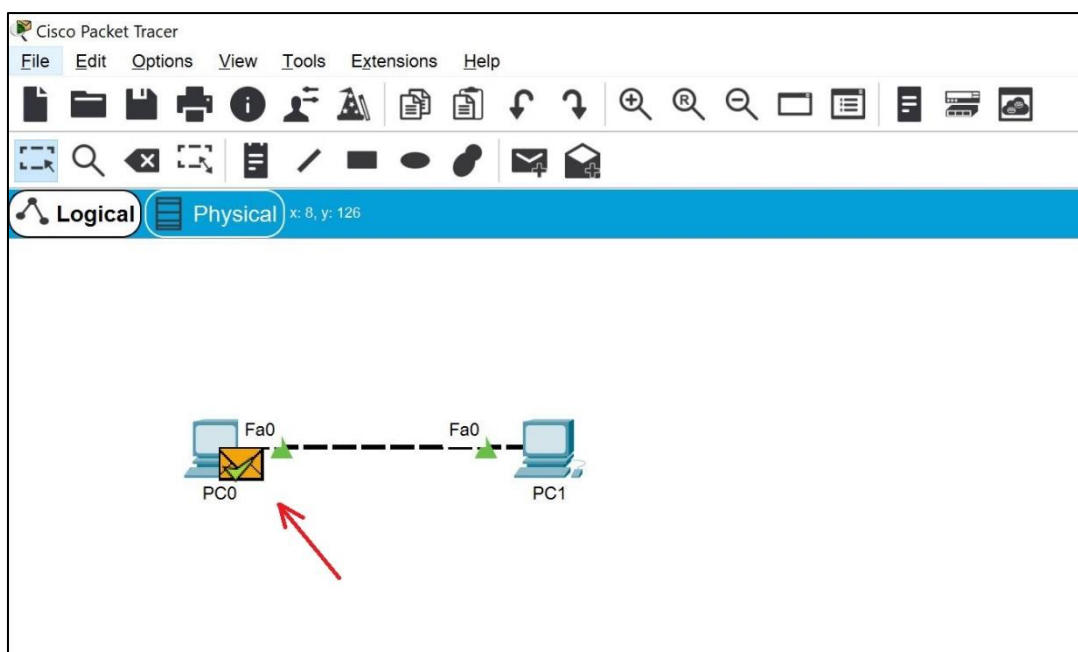
Play Controls

Event List Filters - Visible Events
ARP, ICMP

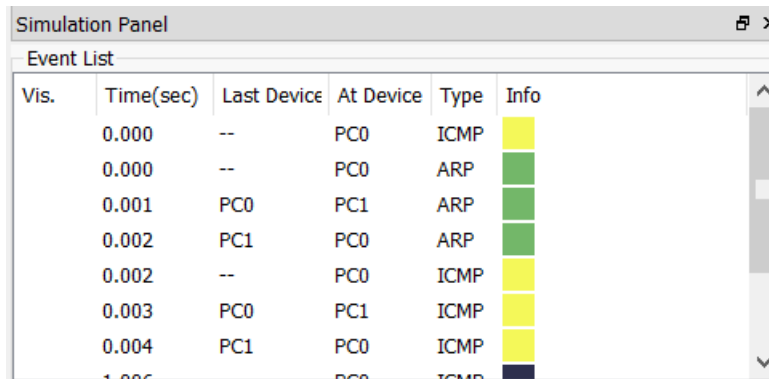
Edit Filters Show All/None

Event List Realtime Simulation

12. You can click on a packet to open more details about it, read additional information or take a quick test in the Challenge me section

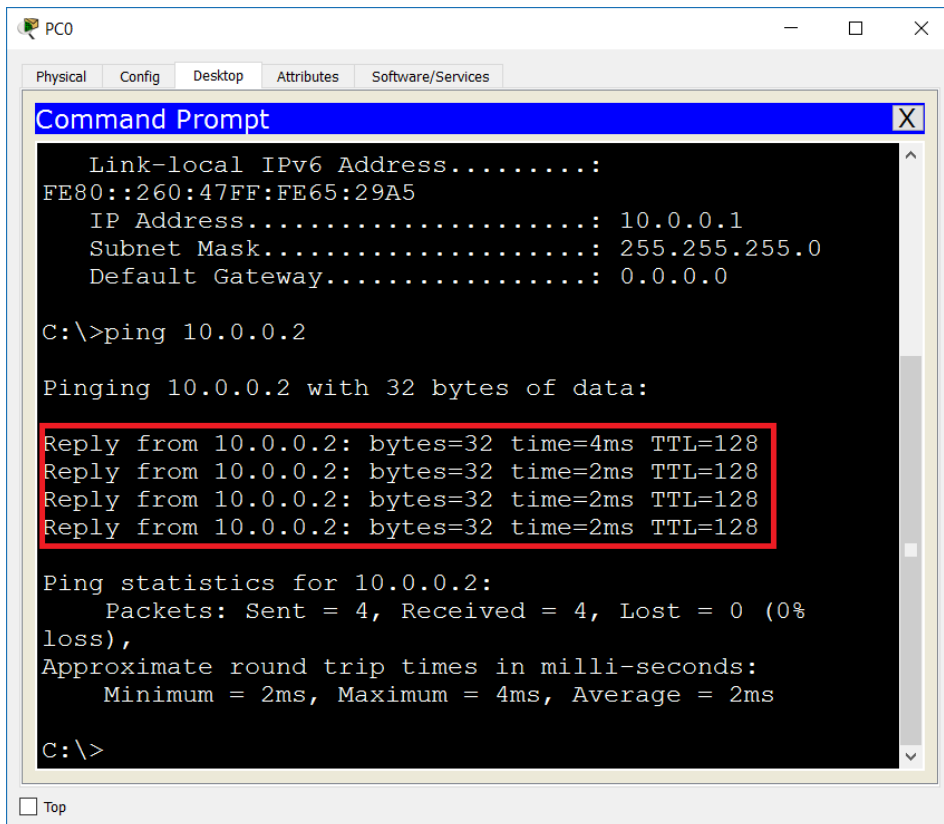


13. Check your Event List – you should have an ARP packet exchange at the beginning and then, when PC0 knows the MAC address of PC1, all the other packets are ICMP



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	
	0.000	--	PC0	ARP	
	0.001	PC0	PC1	ARP	
	0.002	PC1	PC0	ARP	
	0.002	--	PC0	ICMP	
	0.003	PC0	PC1	ICMP	
	0.004	PC1	PC0	ICMP	
	1.000	PC0	PC0	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



```
Link-local IPv6 Address.....: FE80::260:47FF:FE65:29A5
IP Address.....: 10.0.0.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 0.0.0.0

C:\>ping 10.0.0.2

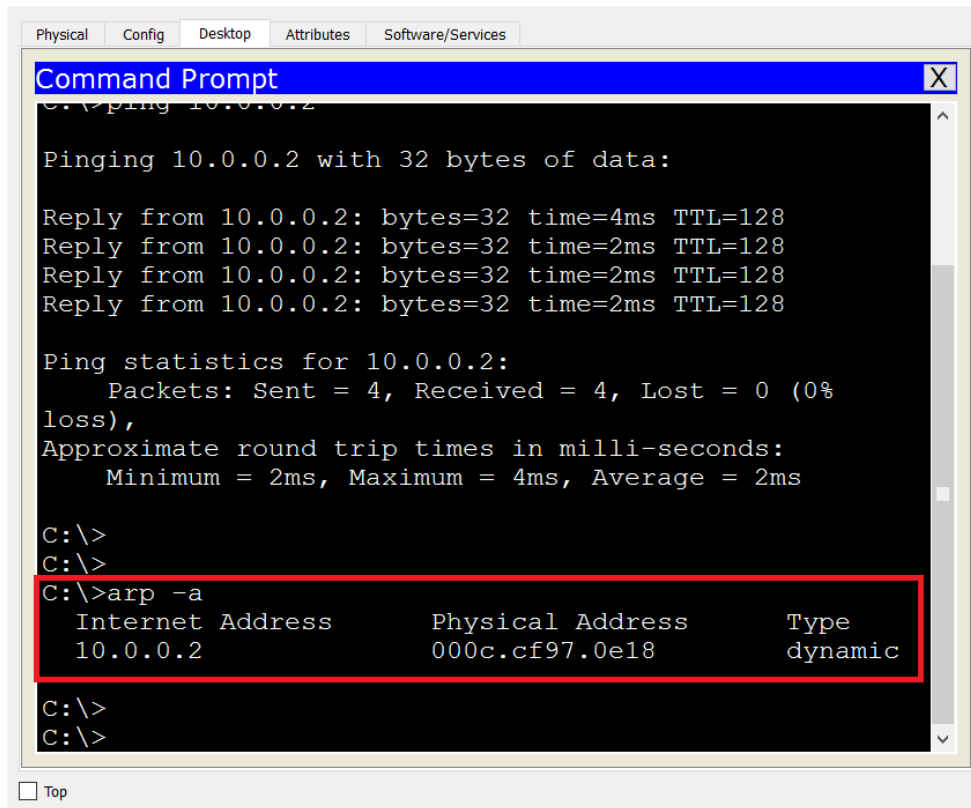
Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=4ms TTL=128
Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time=2ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>
```

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)



```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

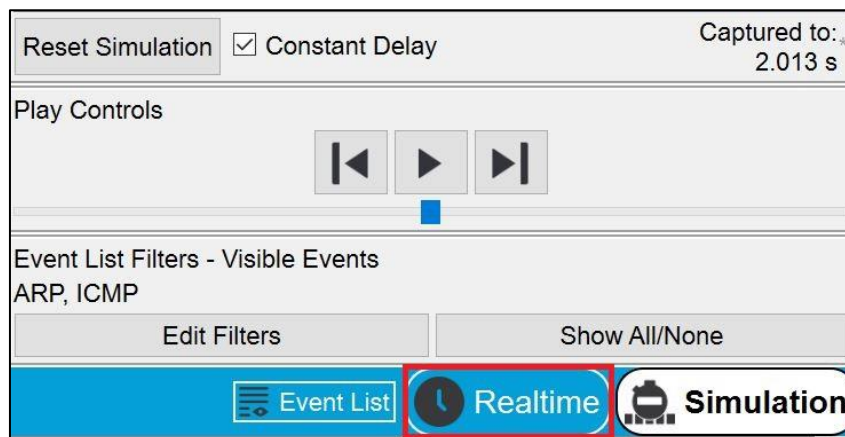
Reply from 10.0.0.2: bytes=32 time=4ms TTL=128
Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time=2ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\>
C:\>
C:\>arp -a
    Internet Address      Physical Address      Type
    10.0.0.2              000c.cf97.0e18       dynamic

C:\>
C:\>
```

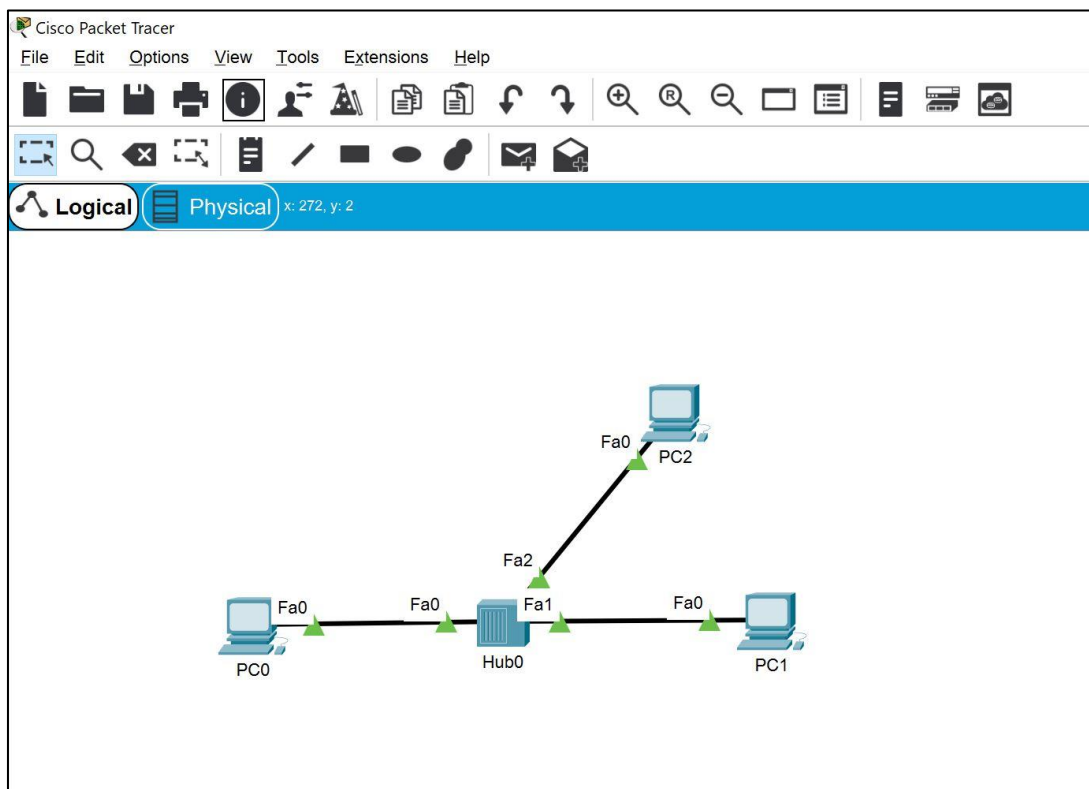
16. Click on Realtime to reset the clear the simulation mode (you will go back to in in the next exercises)



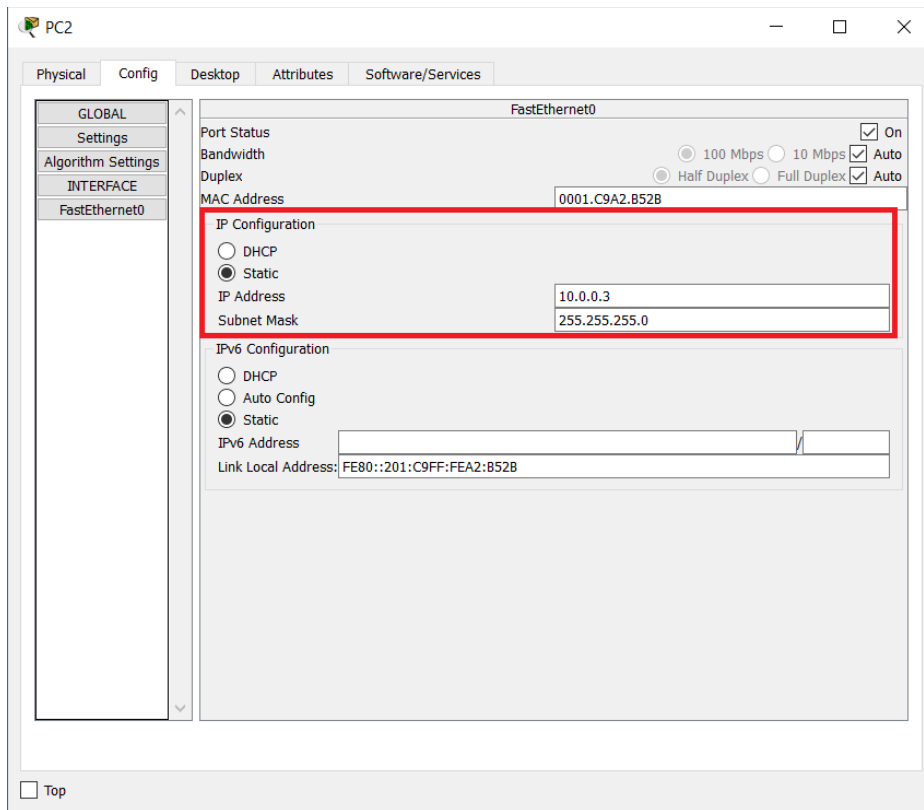
Exercise 4: Explore the traffic flow and the message exchange between hosts connected with a Hub

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.

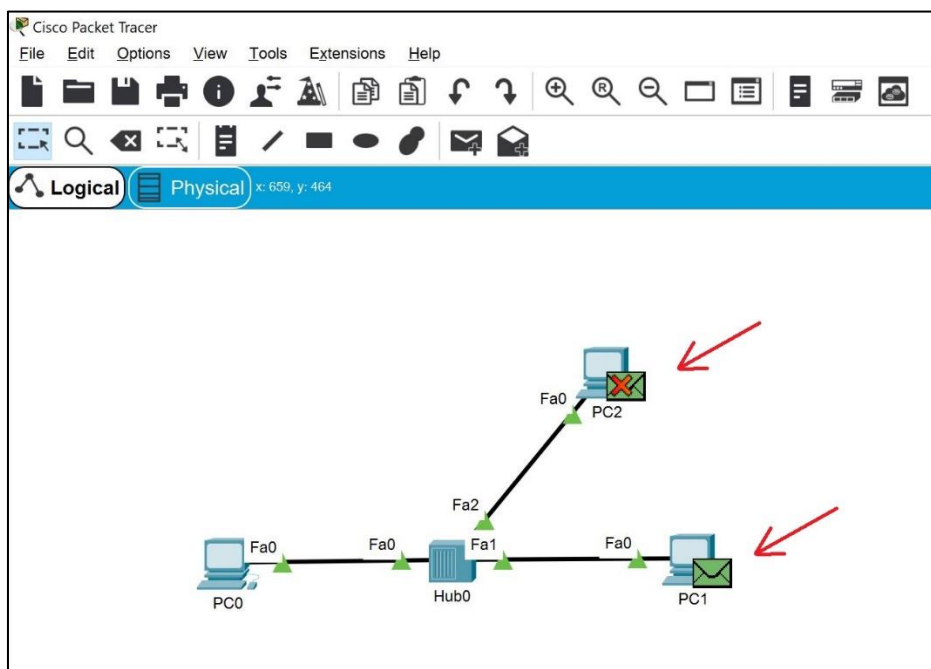
1. Delete the connection between the end devices, drag a Hub (Use PT-Hub, the first one) in the topology, drag one more generic end device (PC2) and connect them as shown in the screenshot (again, as noted before, you can start a new topology from zero – sometimes it can eliminate errors)



2. Open the configuration of PC2 and setup static IP address in the same IP network – 10.0.0.3/24



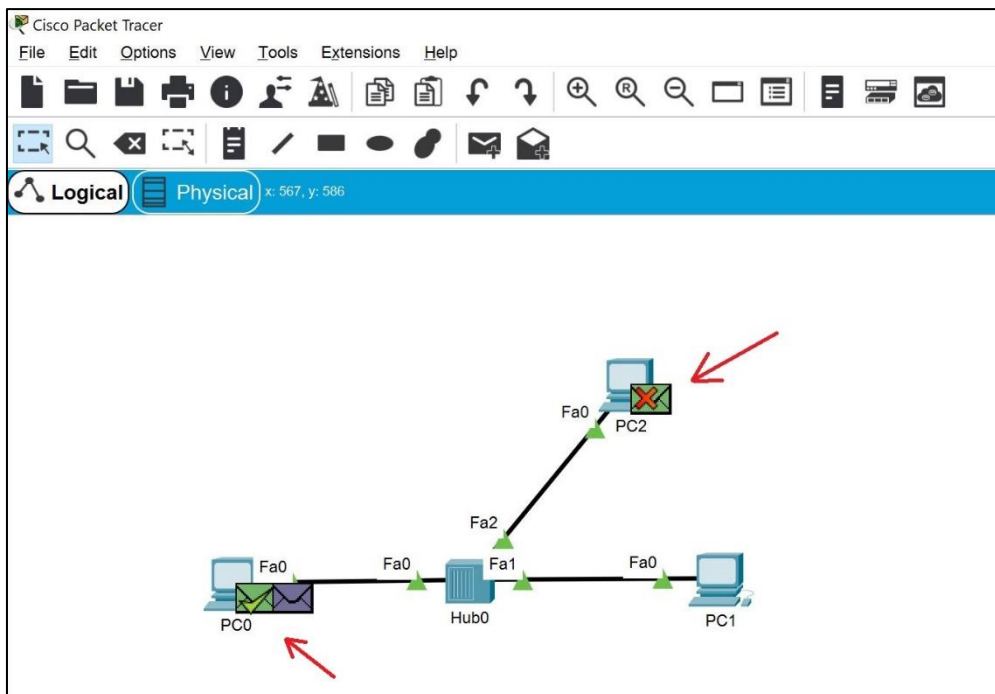
- Initiate ping to 10.0.0.2 (PC1) from the command line of PC0 and while clicking the Capture / Forward button, observe the packet exchange between the two hosts



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.

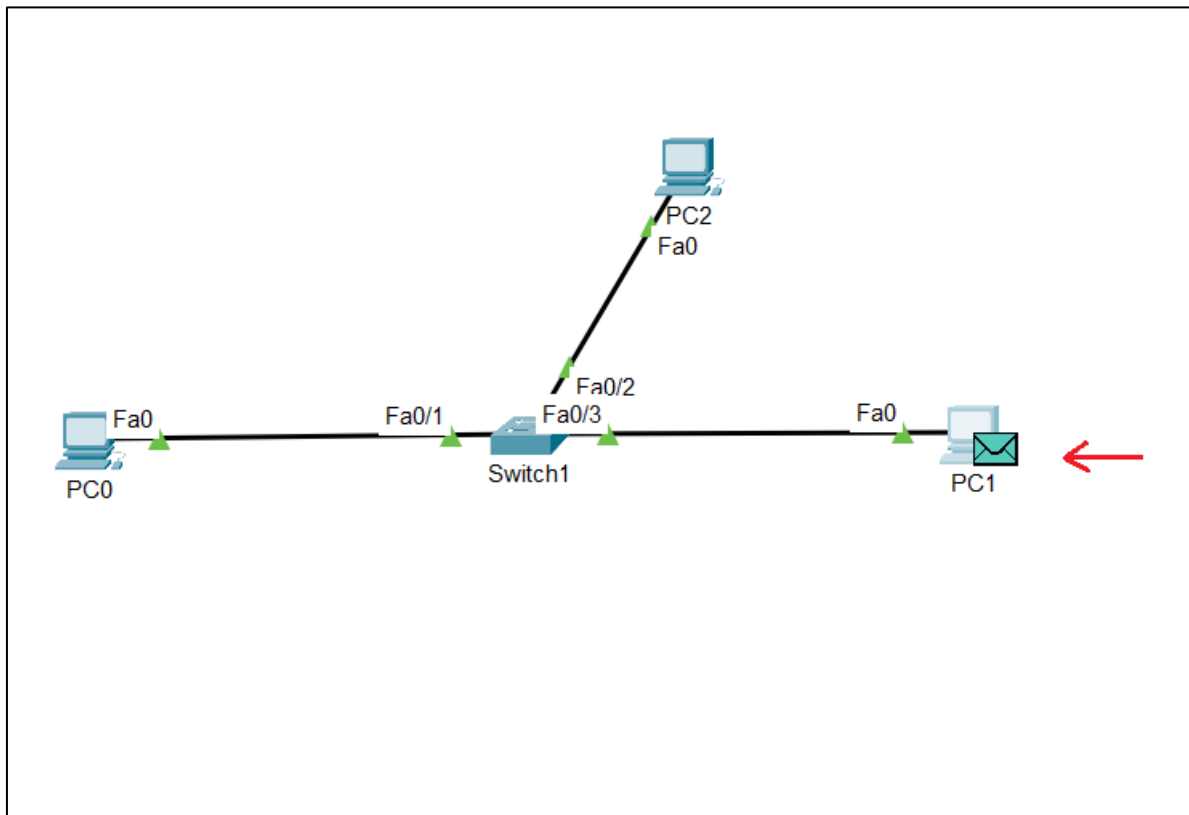
4. For example, have a look at the ICMP echo reply packet (this is the ping response) from PC1 – it goes to both PC0 and PC2

Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	
	0.001	PC0	Hub0	ICMP	
	0.002	Hub0	PC2	ICMP	
	0.002	Hub0	PC1	ICMP	

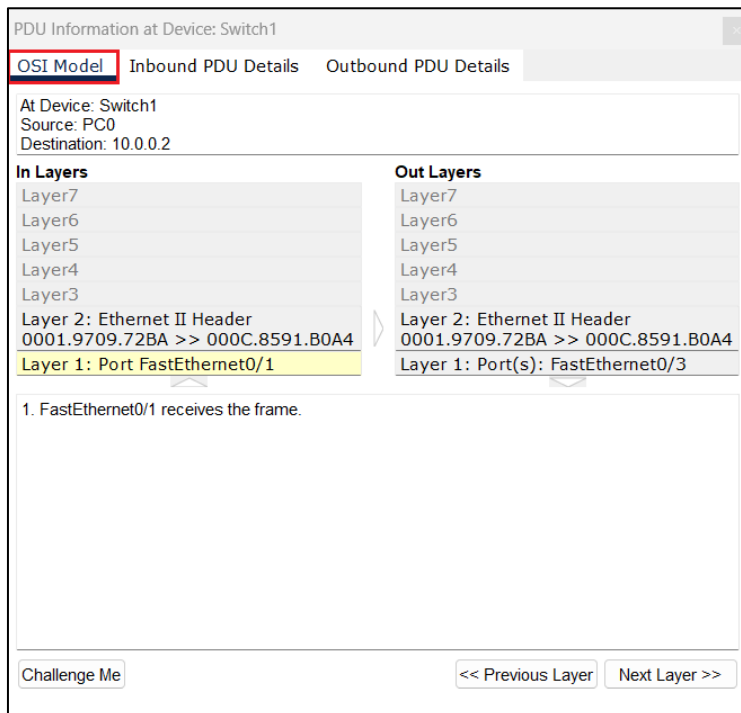


Exercise 5: Explore the traffic flow and the message exchange between hosts connected with a Switch

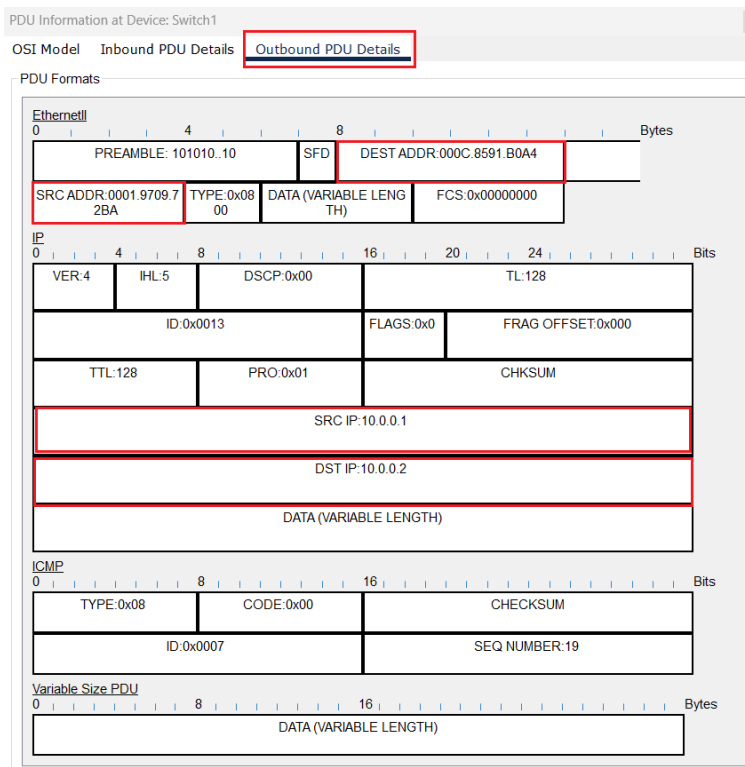
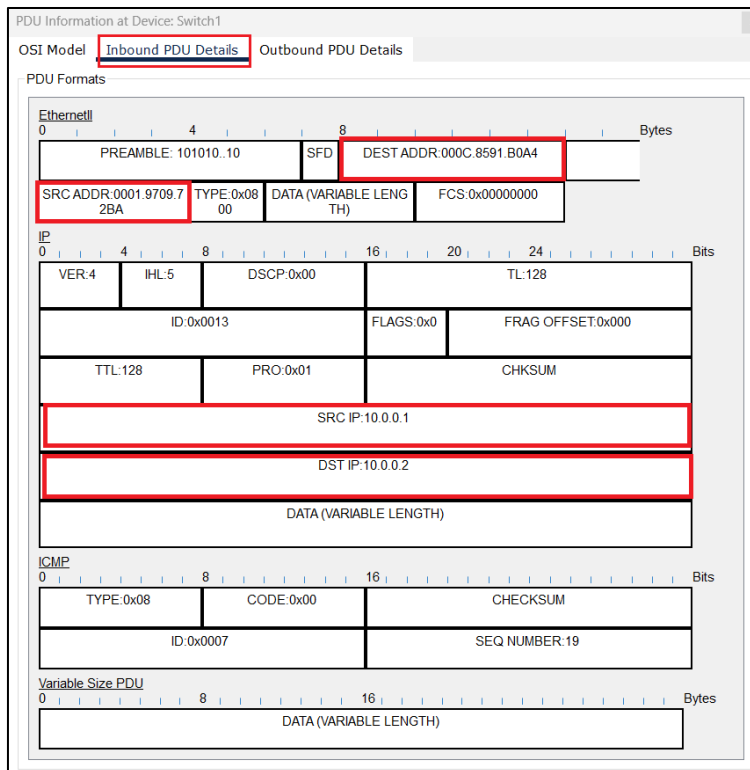
1. Change the topology by deleting the Hub and Inserting a Switch on the same place. Reconnect the three end devices again, so all of them connect directly to the switch (you can use 2960 as a Switch model). Once again, as noted before, you can start a new topology from zero – sometimes it can eliminate errors.
2. Repeat the procedure from Exercise 4 and you will notice that the hosts communicate similarly as if they had a Hub between them. But if you turn on the simulation mode again, you will notice one difference – (after one initial packet exchange) the switch will forward the packet with source PC0 and destination PC1 only to PC1 and will not bother PC2. This is because the switch builds a MAC address table (this will be discussed in more details in the next lecture and lab)



3. Still in simulation mode, click on the packet going to PC1. You can click on it at the moment when it exits PC0, when it is at the Switch, or when it is at PC1. When you click on the packet, a window showing the PDU will open and you will see three tabs – “OSI Model”, “Inbound PDU Details” and “Outbound PDU Details” (you may not see all three tabs, depending on at which point you click on the packet)



(Click “Next layer” here several times and read what is happening at each step)



Try to stop and open the packet at the different places on its way (from PC0 to PC1) and pay attention at the source and destination MAC and source

and destination IP addresses – they are always the same, unchanged. In our example, the source MAC and IP belong to PC0 and the destination MAC and IP belong to PC1 (can you confirm it?).

When the packet reaches PC1 and returns back (this is the ICMP echo reply), the source and destination MAC and IP addresses switch each-other (source becomes destination and destination becomes source), but you can monitor the same – source and destination MAC and IP are always the same during the entire packet journey on the way back – at PC1 (you have to look at “Outbound PDU details”), at the switch, and when reaching PC0 (look at “Inbound PDU details”).

You have completed LAB 2.