LAB 3: IP Addresses and Host-to-Host Communication – part 2

Contents

[Introduction to the LAB 2](#_Toc134103140)

[Exercise 1: Explore and monitor the MAC address table of a switch 2](#_Toc134103141)

[Exercise 2: Explore the traffic flow and the message exchange between hosts connected with a Router 6](#_Toc134103142)

# Introduction to the LAB

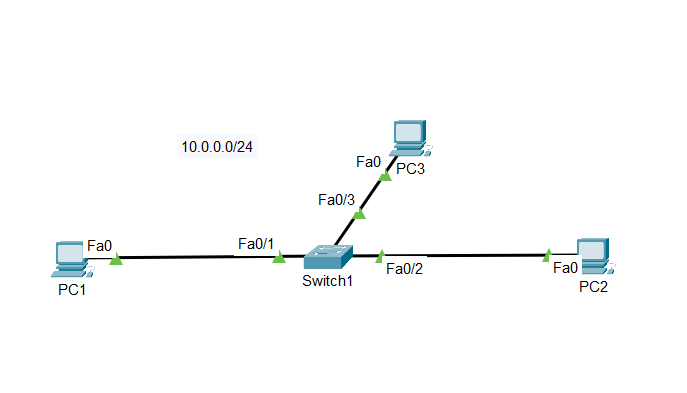
In Lecture 3, you have learned more about the host-to-host communication, the ARP and the MAC address tables. You have also learned that when communicating through a router (or a L3 switch), the source and destination MAC addresses of the frames change on each hop. In this lab, you will practice this knowledge by monitoring the building of the switch MAC address table as first. Then, you will observe the frame/packet behavior when it travels from one host to another and there is a Layer 3 device (router in this case) between them.

# Exercise 1: Explore and monitor the MAC address table of a switch

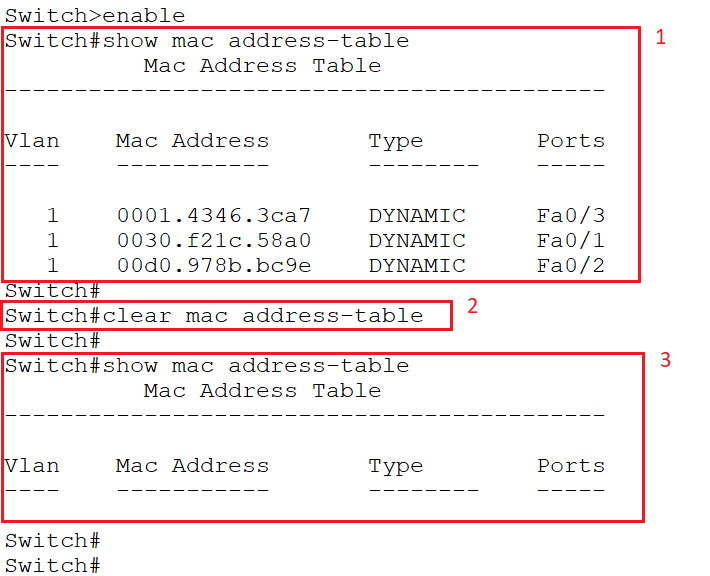
The topology in this exercise will be the same (or very similar to) as the one from the previous lab (Lab 2), exercise 5 – you will have several hosts connected with a switch.

As discussed in the previous lab, after one initial packet exchange, the switch will forward the packets between the source and the destination hosts directly, without bothering the other connected host. This is because of the MAC address table. As you know, a switch is a layer 2 device, which is more intelligent than a hub. One reason is exactly the 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).

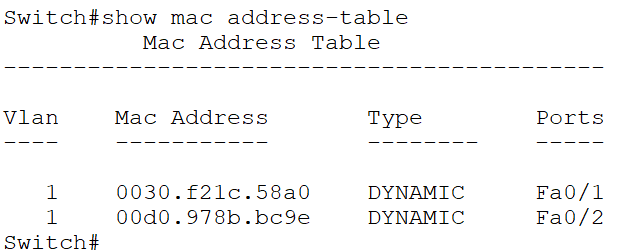
1. Create the topology (use 2960 as a Switch model). Connect the end devices to it as per the picture below:



1. Assign the IP addresses statically on the end devices as follows:
   1. **PC1**: 10.0.0.1/24
   2. **PC2**: 10.0.0.2/24
   3. **PC3**: 10.0.0.3/24
2. Login to the CLI of your switch and type **show mac address-table** (you can do it from the user exec or from the privileged exec mode) 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 (marked as “1” in the screenshot below). If this is the case, you can clear the table with the **clear mac address-table** command from the privileged exec mode (marked as “2” in the screenshot below). Then, repeat the **show mac address-table** command and you should see no entries (marked as “3” in the screenshot below)



1. Initiate **ping 10.0.0.2** (this is PC2) from PC1. Then, go to the switch CLI and type again **show mac address-table**. You should see two entries – one for **PC1** and the other for **PC2**.

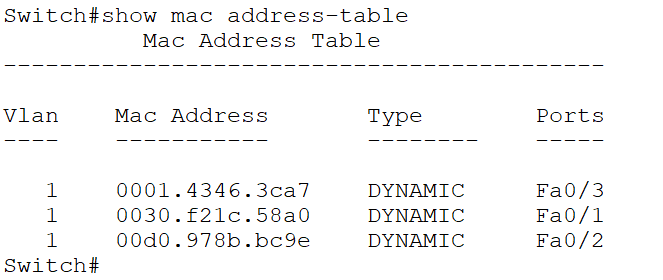


Note: The exact MAC addresses on your MAC address table will most likely be different from the screenshot above. Compare what you see in the MAC address table with the actual MAC addresses of your connected hosts.

Explanation: When the ping is initiated, the ICMP echo request packet will reach the switch. The switch will have a look at the destination MAC address and since the MAC table is empty, it will not know where (out of which port) to send it. That is why it will send it out of all ports/interfaces, except for the one it was received. So, it will act as a hub and will send it out of Fa0/2 and Fa0/3. But in the background, the switch will write the first entry into its MAC address table – the source MAC address is coming from Fa0/1. Then, when **PC2** replies with ICMP echo reply, the switch will look into the destination MAC address (this is the **PC1** MAC) and will see that it is associated with Fa0/1. But in the background, it will also write the second entry into the MAC address table – in this case the source MAC address (the **PC2**) is coming from Fa0/2. This is the reason why after you run the ping command (or any other IP communication), the switch will have two entries in its MAC address table.

1. In order to see the third entry in the MAC address table (the one for Fa0/3 and the MAC address of **PC3**), you have to somehow make **PC3** to send traffic to the switch. Note that this can be done in two ways:
   1. You can go on **PC3** and ping one of the others (**PC1** or **PC2**)
   2. From **PC1** or **PC2**, ping **PC3**. This way, when PC3 responds (with ICMP echo reply), the switch will notice the source (**PC3**) MAC address and will write it in the MAC address table

Choose one option from a. or b. and after this, type again **show mac address-table**. Observe the new entries in the MAC address table



Note: Since these entries are dynamic, they expire after a certain amount of time. This is called “aging” and by default is 300 seconds. This is not configurable (at least in the current version, 8.2.1) in Cisco Packet Tracer. After they expire, the switch will go through the same process of dynamically learning the MAC addresses of the connected devices.

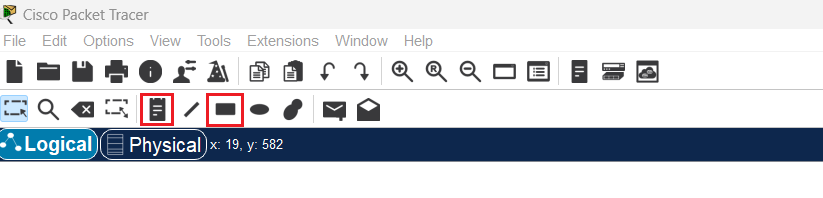
Note: You can also monitor this step by step by using the simulation mode. Do not forget the ARP protocol (explained and showed in the previous lecture and lab) and the fact that when you first initiate the ping command, the ARP request (which is broadcast) is the first thing that happen. Some entries in the switch MAC address table can be filled from the ARP messages, since they also carry the source MAC addresses.

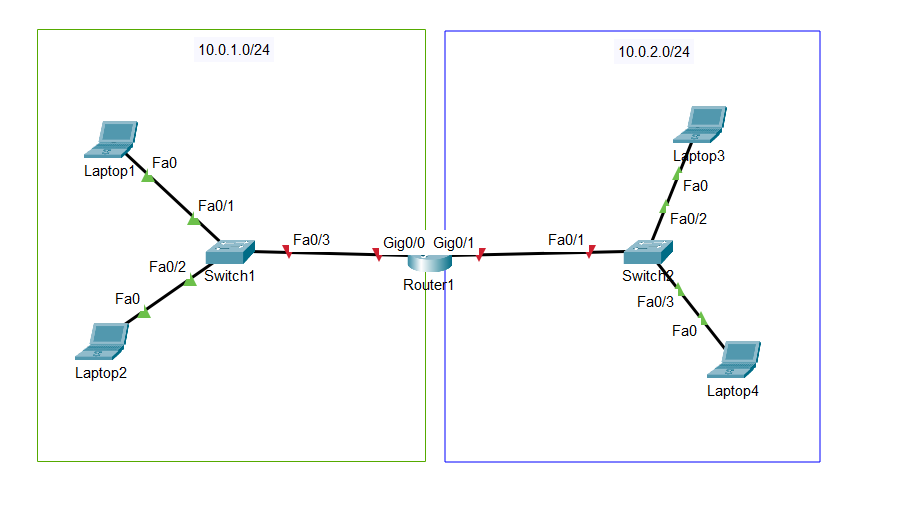
# Exercise 2: Explore the traffic flow and the message exchange between hosts connected with a Router

In this exercise, we will create a layer 3 network, meaning that we will use a router and two separate networks/subnets. The idea is to show the host-to-host communication when there is a router between the source and destination hosts.

1. Create the topology
   1. You will need the following devices (just move them to the topology area):
      * One router (use 2911)
      * Two switches (use 2960)
      * Four end devices (you can use either PC or Laptop)
   2. Rename the devices and connect them as per the picture below

Note: The green rectangle, the blue rectangle and the notes with the subnets are optional and just for illustration. You can create them by using the “Place note” and “Draw rectangle” functionality





* 1. Setup the IP addresses of the hosts
     + **Laptop1**: 10.0.1.1/24
     + **Laptop2**: 10.0.1.2/24
     + **Laptop3**: 10.0.2.1/24
     + **Laptop4**: 10.0.2.2/24

Note: This one is important! Notice that **Laptop1** and **Laptop2** belong to one network (which is 10.0.1.0/24) but **Laptop3** and **Laptop4** belong to another network (which 10.0.2.0/24). This means that **Laptop1** and **Laptop2** can communicate “directly”, without the need of a layer 3 device. The same is valid for **Laptop3** and **Laptop4**. But, if you need to connect **Laptop1** to **Laptop3** for example, you will need to configure layer 3 device between them (this is our **Router1** in this case) and a “default gateway” for the end devices.

* 1. Configure the router

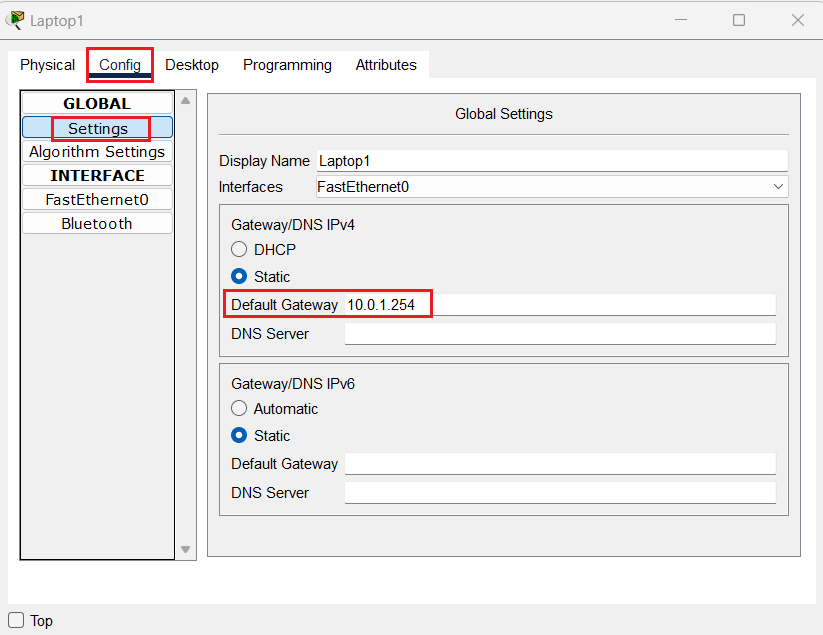
The router should be configured by enabling its interfaces (they are shut down by default) and configuring IP addresses on them. Note that the router is part of both networks (10.0.1.0/24 and 10.0.2.0/24)

* + - Click on the CLI, type “no” on the “Would you like to enter the initial configuration dialog? [yes/no]” and hit Enter
    - Type the following commands to configure the left (g0/0) interface:
* **enable** (goes into the privilege exec mode)
* **conf t** (goes into the global configuration mode)
* **int g0/0** (goes into the specific interface configuration mode)
* **no shut** (enables the interface)
* **ip address 10.0.1.254 255.255.255.0** (configures the IP address of the interface)
* **exit** (goes back to global configuration mode)
  + - Type the following commands to configure the right (g0/1) interface:
* **int g0/1** (goes into the specific interface configuration mode)
* **no shut** (enables the interface)
* **ip address 10.0.2.254 255.255.255.0** (configures the IP address of the interface)

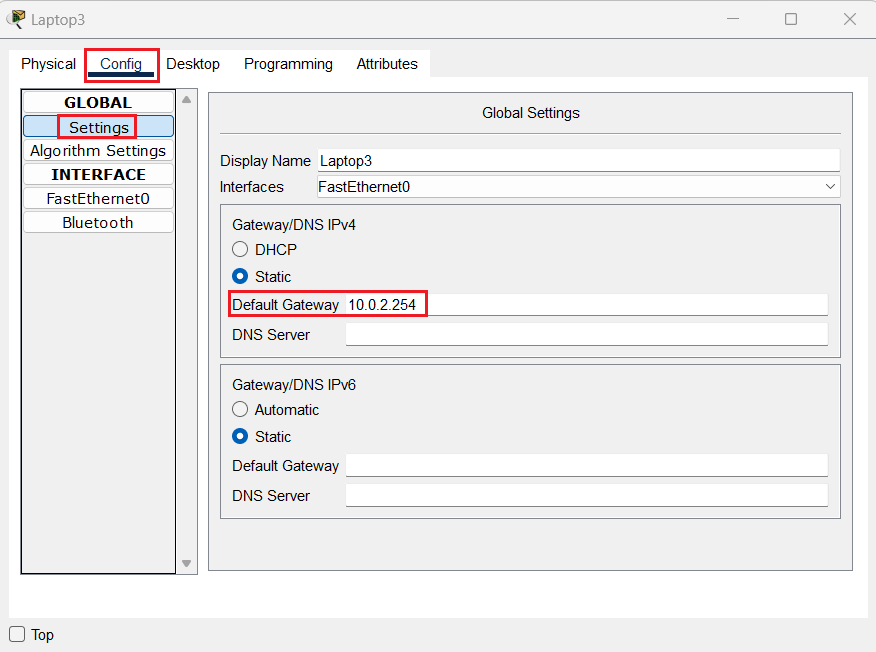
Note: When you enable the router interfaces (no shut), you will see that the link lights (if enabled from the preferences) will become green.

* + - Configure default gateway on the end devices

In order to be able to send traffic to a host from a different network/subnet, each host should have a default gateway configured (or a specific static route), pointing to the closest router/interface. On **Laptop1** and **Laptop2**, go to Config -> Settings and in the “Gateway/DNS IPv4” part make sure that “Static” is selected. Then, configure the default gateway to 10.0.1.254. This is the IP address of G0/0 interface of **Router1**.



Similarly, for **Laptop3** and **Laptop4**, configure a default gateway of 10.0.2.254. This is the IP address of the G0/1 interface of **Router1**.



1. Ping within and between the subnets
   1. Ping within the subnets

Try pinging **Laptop2** from **Laptop1** and **Laptop4** from **Laptop3**. This communication does not require a default gateway since it stays within a subnet. As you have done in the previous lab, you can monitor (in simulation mode) the packets and se that the source and destination MAC and IP addresses stay the same during the entire journey of the packet

* 1. Ping between the subnets

This and the next steps show the big difference in the host-to-host communication when we have a layer 3 device between the hosts.

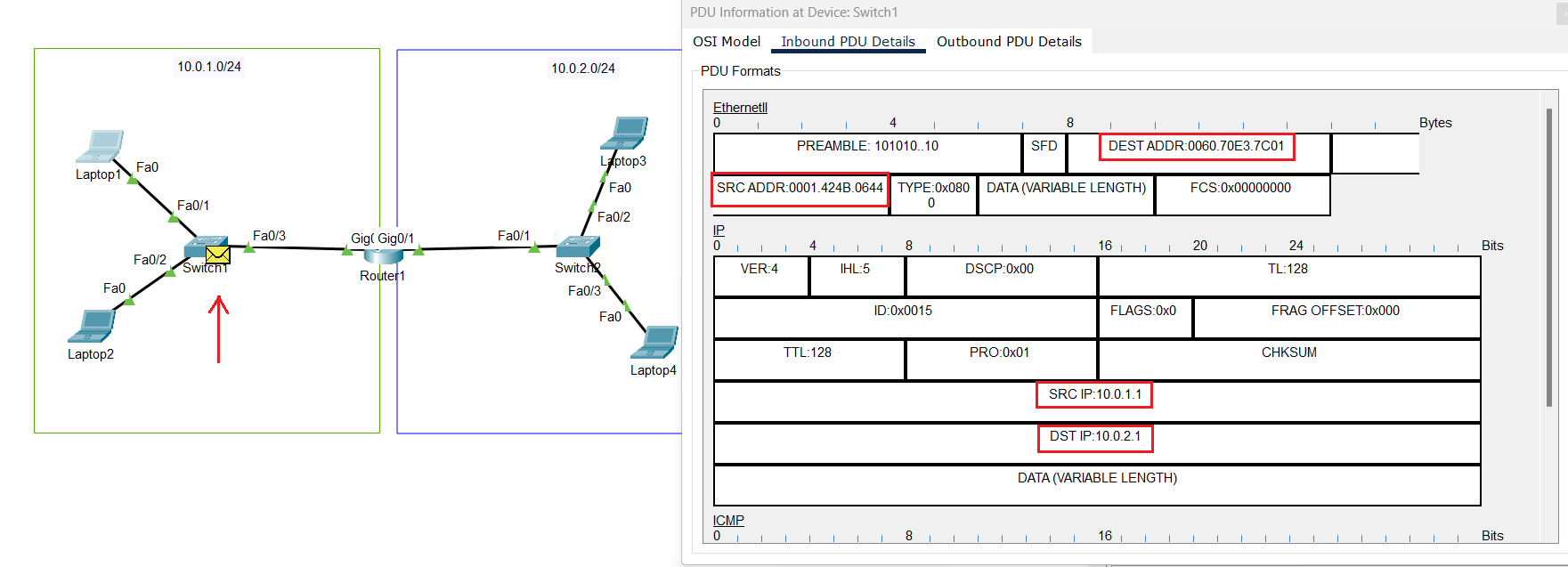
Ping the IP address of **Laptop3** (10.0.2.1) from **Laptop1**. Note that there can be a delay and you may loose one or two ICMP echo requests in the beginning. This is normal and the reason is ARP - **Laptop1** needs some time to find the MAC address of the destination.

But in fact, the MAC address of the destination is not the MAC address of **Laptop3**, it is the one of G0/0 port of **Router1**!

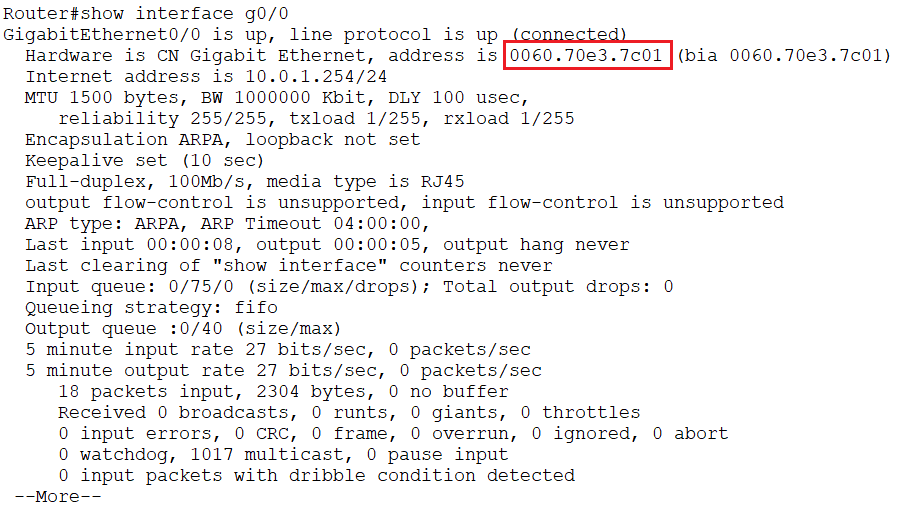
* 1. Monitor the addresses in simulation mode

When you verify that you can ping between the subnets, try another ping with simulation mode enabled and monitor the difference of the source and destination MAC addresses when the frame is on the left of **Router1** (in the green rectangle) and when it is on the right of **Router1** (in the blue rectangle):

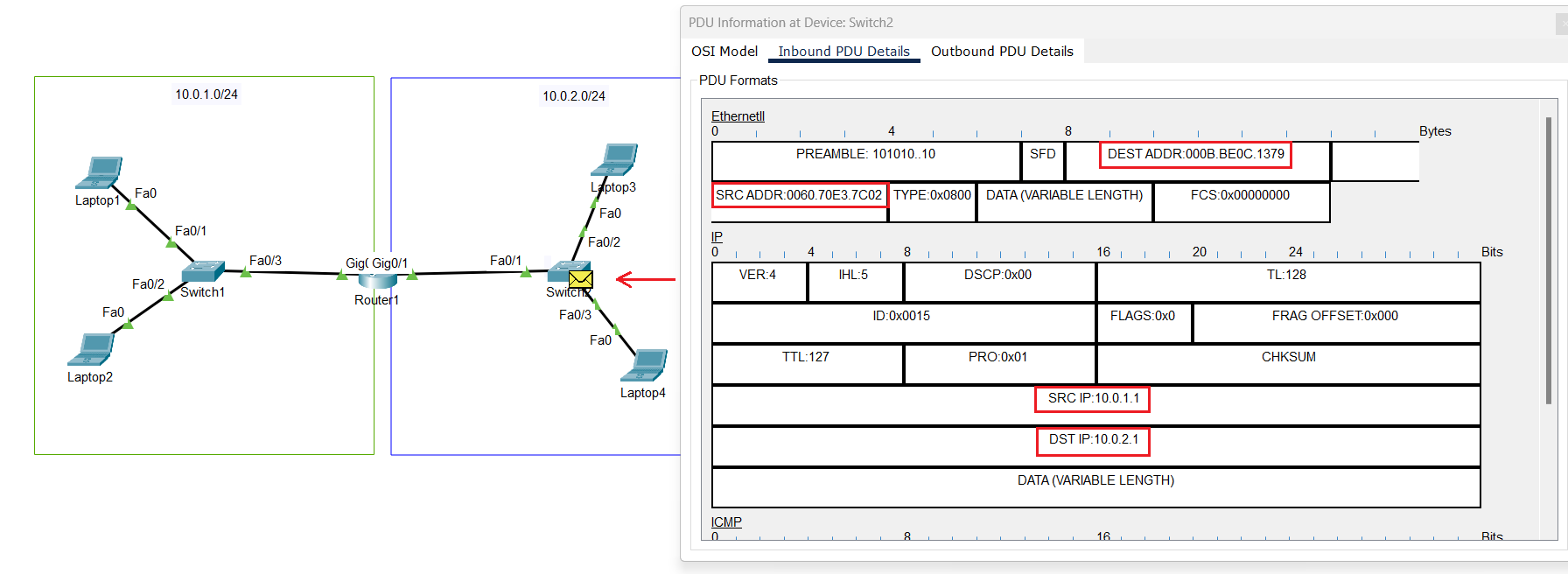
* During the first part, you can open the frame when it is reaching the first switch. Carefully compare the source and destination MAC addresses and you will find that the source MAC belongs to **Laptop1** and the destination MAC belongs to G0/0 of **Router1**.



Note: You can check the MAC address of the laptop with “ipconfig /all” and the MAC of G0/0 by typing “show interface g0/0” from privilege exec mode on **Router1**



* During the second part, you can open the frame when it is reaching the second switch. Again, carefully compare the source and destination MAC addresses and you will find that the source MAC belongs to G0/1 of **Router1** and the destination MAC belongs to the final destination, **Laptop3**



You have now proved that when the two communicating devices are divided with a router, the frame has different source and destination MAC addresses on the left side and on the right side of the router. That is why it is said that the source and destination MAC addresses are changed on every “hop” (meaning routing device). Also note that the source and destination IP addresses are unchanged on the left and on the right side. This is typically how the frame/packet travels during a “normal” routing. If we have NAT (Network Address Translation), the source/destination IP addresses can be changed as well. We will discuss NAT later in the module.

You have completed LAB 3.