

Assignments with NetGUI-Kathará

Assignment 1: Ethernet, Hub, Switch

Computer Networks

GSyC

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

2025

To complete this assignment, it is important that you prepare a document in which you will answer the questions presented in this handout. This document, which we will refer to as the practice report, must be submitted along with the traffic capture files requested in some sections. Keep in mind that the practice reports will be the main study material for this course, after the theory slides. For this reason, it is important that the reports are very thorough and include all the necessary explanations so that you can easily review the assignment after completing it.

1. Traffic capture file analysis

Open the capture file `pcap1.pcap` with **Wireshark** and answer the following questions:

1. Select the first packet in the capture by clicking on the first line in Panel 1 (packet list). It will be highlighted in a different color:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	13.0.0.13	21.0.0.21	TCP	74	54689 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460
2	0.004014	21.0.0.21	13.0.0.13	TCP	74	http > 54689 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
3	0.004322	13.0.0.13	21.0.0.21	TCP	66	54689 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0
4	8.895756	13.0.0.13	21.0.0.21	HTTP	92	GET /index.html HTTP/1.1
5	8.896086	21.0.0.21	13.0.0.13	TCP	66	http > 54689 [ACK] Seq=1 Ack=27 Win=5792 Len=0
6	15.845293	13.0.0.13	21.0.0.21	HTTP	78	Continuation or non-HTTP traffic

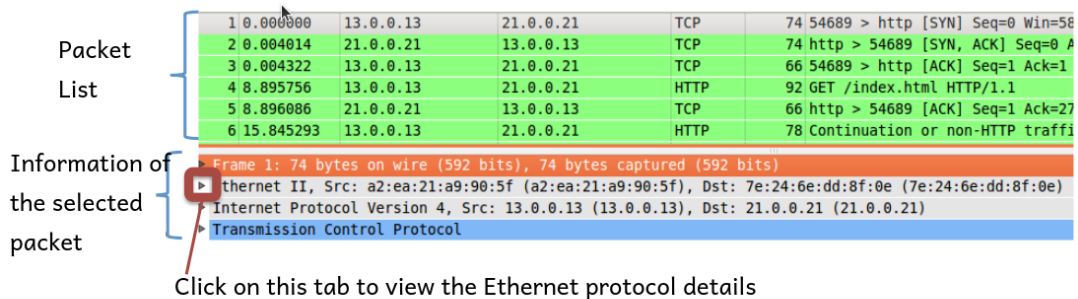
2. In Panel 1 (packet list), each packet displays:

- Its order number within the capture (column **No.**). Packet number 1 is the first one captured.
- Time in seconds since the first packet was captured (column **Time**). The first packet marks the time origin, so its time value is 0.000000 seconds. The second packet shows 0.004014 seconds, which means it was captured 0.004014 seconds after the first one. And so on.
- Source address of the packet (column **Source**). In this case, it shows the network layer source address (IP address).
- Destination address of the packet (column **Destination**). In this case, it shows the network layer destination address (IP address).
- The highest-level protocol recognized in the packet (column **Protocol**).
- Total length of the captured frame in bytes (column **Length**), excluding the CRC field (4 bytes).
- Summary of the most relevant information contained in the recognized protocols in the packet (column **Info**).

With the first packet selected, observe in Panel 2 of **Wireshark** the protocol details for that packet. Indicate which protocols are used in this first packet and to which layer of the TCP/IP architecture each of them corresponds.

3. With the first packet in the capture still selected, in the first tab (**Frame**) of Panel 2 you will find statistical information related to the capture of that packet. This is the only tab that does not contain information about any of the protocols in the packet, and in general, we will not need to consult it.

- The rest of the tabs in Panel 2 contain the headers of the protocols recognized in the packet, starting with **Ethernet** and continuing with higher-layer protocols.
- With the first packet in the capture selected, expand the tab corresponding to the Ethernet protocol. Indicate which fields you can see in the Ethernet header, and verify that the length of these fields matches what we have studied in the theory section. Write down the values of these fields. To do this, select the Ethernet tab in Wireshark and right-click to choose 'Copy all visible selected tree items' so that the Ethernet header fields are copied to the clipboard and you can paste them into your report document.



- Click on the **Type** field of the **Ethernet** header and observe how the corresponding value is highlighted in Panel 3, which displays the hexadecimal content of the packet. Notice that **Wireshark** interprets the **Type** value 0x0800 as the code associated with the IP protocol. What does this mean?
- Notice that the captures do not include the preamble or the start frame delimiter bytes. The Ethernet card hardware removes these fields, as they are not considered part of the actual Ethernet frame. Also observe that the CRC does not appear: the Ethernet card hardware checks its correctness and removes it from the frame. If the CRC were incorrect, the frame would be discarded and would not appear in the capture.
- Select the second packet and observe in Panel 2 of **Wireshark** the protocol details for that packet. Indicate which protocols are used in this second packet and to which layers of the TCP/IP architecture they correspond.
- With the second packet selected, expand the tab corresponding to the Ethernet protocol. Indicate which fields you observe in the Ethernet header. Based on the values of these fields, say whether you believe this second packet was sent by the same machine that sent the first packet.
- Look at the length of the first packet shown in the **Length** column in Panel 1. This length refers to the total length of the Ethernet frame excluding the CRC. To calculate the full length of the Ethernet frame, you need to add 4 bytes (CRC) to the value in the **Length** column. Do you think the first frame includes padding bits in Ethernet?
- If the **Length** column of the frame had a value of 60 bytes (meaning the total frame length would be 64 bytes: 60 plus 4 bytes for the CRC), could you tell whether that frame contains padding?
- Look at packet number 18. Indicate which protocols are used in that packet and to which layer of the TCP/IP architecture each one corresponds.
- Look at the frame length field of the Ethernet frame associated with packet number 18. If the machine sending that data had more data to send within frame 18, explain whether it could have included it in the data field of that frame.

Close the capture file **pcap1.pcap** and open the capture file **pcap2.pcap** with **Wireshark** and answer the following questions:

- With the first packet of the capture selected, expand the tab corresponding to the Ethernet protocol. Indicate which fields you observe in the Ethernet header. Write down the values of these fields.
- Look at the **Type** field. The value is different from the one you saw in the previous capture file. Which protocol does this value refer to?
- What does the value of the Ethernet destination address field in this first packet mean?

4. Look at the length field of the first frame. What is the total length of the frame including the CRC?
5. In this case, the packet is an ARP protocol message encapsulated within Ethernet. All ARP protocol messages have the same length: 28 bytes. The Ethernet header takes up 14 bytes and the CRC 4 bytes. Therefore, the total frame length would be 46 bytes, and padding is required to reach the minimum Ethernet frame length (64 bytes). The padding should be 18 bytes.
6. Observe the **Trailer** or padding field for this packet. What is its length? What do you think this field represents?

2. Ethernet Traffic Generation and Traffic Capture Analysis

Download all the network scenarios for this lab. One of these files will be used in this section. The remaining files will be used in later sections.

Uncompress the file `01-ethernet.tgz` using the right-click option (select “Extract to”).

From a terminal, run: `netgui-kathara.sh`

Load the scenario you just extracted: go to **File** → **Open** and navigate through the window to the folder where you placed the NeGUI scenario. Make sure the **Folder name** field shows the full path to that folder and ends with `01-ethernet`, which is the folder containing the scenario configuration. Once you click the **Open** button, you should see a diagram similar to the one shown in Figure 1:

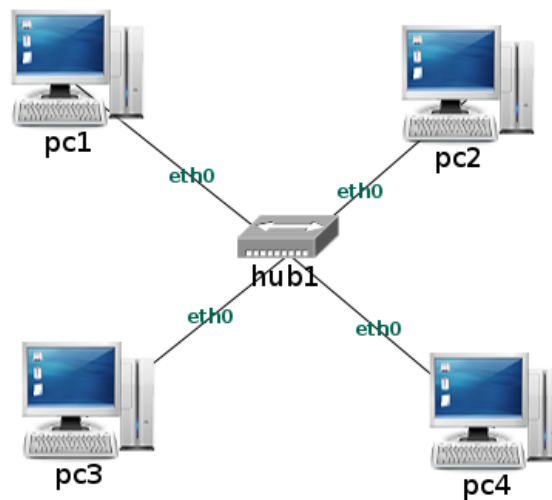


Figura 1: Scenario 01-ethernet.tgz

Start all PCs. You will notice that the machine icons now display green symbol, indicating that the machines are running. When the machines start up, they are automatically configured with a network-layer address, an IP address. The IP protocol will be studied in the next unit.

1. Check the Ethernet addresses configured on each of the interfaces of the machines. To do this, run the following command on `pc1`:

```
pc1:~# ip link show eth0
```

Write down the Ethernet addresses of each interface on all the PCs.

2. Start a traffic capture on `pc3`. To do this, run the following commands.

On `pc3`:

```
pc3:~# tcpdump -i eth0 -s 0 -w /shared/p1-ethernet.pcap
```

Now you will generate traffic as follows: **pc1** will send an Ethernet frame to **pc2**, and **pc2** will respond. To do this, execute the following command on **pc1**, replacing **<direcciónEthernetPc2>** with the Ethernet address of **pc2** (remove the **<** and **>** characters):

```
pc1:~# arping -c 1 <direcciónEthernetPc2>
```

Where:

- The Ethernet address we are using is the destination Ethernet address of the frames, in this case, that of **pc2**.
- The option **-c 1** makes **arping** send a single packet to **pc2** and have it respond.

For example, if the Ethernet address of **pc2** is 00:1a:1b:00:00:01, execute the following command on **pc1**:

```
arping -c 1 00:1a:1b:00:00:01
```

Interrupt the capture by pressing **Ctrl+C** in the **pc3** window.

Analyze the Ethernet frames that appear in the capture. For each packet, indicate:

- Source Ethernet address.
- Destination Ethernet address.
- What do you think would have been captured on the interfaces **pc1(eth0)**, **pc2(eth0)**, **pc4(eth0)** if we had also started **tcpdump** on those interfaces? Why?
- Indicate which machines receive the first captured frame and which machines process it and deliver it to the upper layer protocol.
- Indicate which machines receive the second captured frame and which machines process it and deliver it to the upper layer protocol.
- If the first frame had a destination address of **ff:ff:ff:ff:ff:ff**, indicate which machines would receive that frame and which machines would deliver it to the upper layer protocol.

2.1. Differences in the Behavior between a Hub and a Switch

Unzip the file **01-hub-switch1.tgz** and load the scenario in NetGUI, similar to the one shown in Figure 2. Start all network devices.

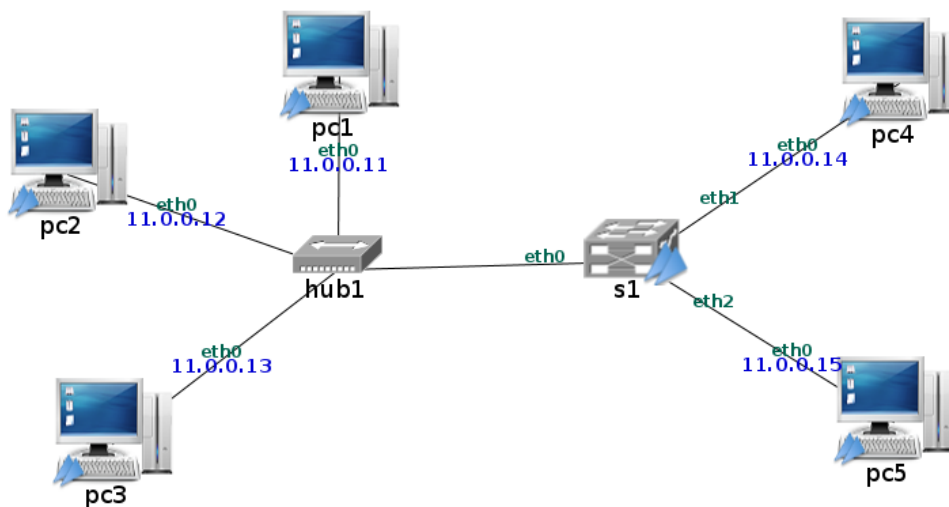


Figura 2: Scenario 01-hub-switch.tgz

1. Indicate the Ethernet address of **pc3**.
2. Verify that the table of learned Ethernet addresses in **s1** is empty (it only contains information about the switch's local interfaces).
3. What do you think will happen on **hub1** when the **arping** command is executed from **pc1** to **pc3**?
4. What do you think will happen on **s1** when the **arping** command is executed from **pc1** to **pc3**?
5. Start a traffic capture on **pc2** and another on **pc4**, saving the captured packets in two different files (**p1-switch1.pcap** and **p1-switch2.pcap** respectively). Run the **arping -c 3** command from **pc1** to **pc3** (the **-c 3** option sends 3 packets from **pc1** to **pc3** and receives a response for each send). Observe the table of learned Ethernet addresses on **s1** and explain its contents.
6. Interrupt the traffic captures and explain the messages captured on **pc2** and **pc4**. Relate the capture information to the contents of the learned address table on **s1**.
7. Clear the learned address table on **s1**. What do you think will happen on **s1** when the **arping** command is executed from **pc1** to **pc5**?
8. Verify your previous assumption by executing the **arping -c 3** command on **pc1** directed at **pc5** and performing traffic captures on **pc2** (in the file **p1-switch3.pcap**), **pc4** (in the file **p1-switch4.pcap**), and **pc5** (in the file **p1-switch5.pcap**) showing the exchanged traffic. Explain the contents of the learned address table, interrupt the captures, and explain the learned addresses in relation to the captured traffic.
9. To see how the learned address table changes in a switch, run the following command on **s1**:

```
watch -n 1 brctl showmacs s1
```

This **watch** command executes every second (**-n 1**) the command **brctl showmacs s1**. Run **arping -c 5** from **pc1** to **pc5**. Explain what you see in the learned address table. Indicate when the Ethernet addresses of **pc1** and **pc5** disappear. Once you finish this section, you can stop the **watch** command by pressing **Ctrl+c**.

10. Imagine that at some point, the learned address table of the switch looks like this (the switch's local addresses are not shown):

```
s1:~# brctl showmacs s1
port no mac addr          is local?    ageing timer
  1      <dir_Ethernet_pc2>    no           225.60
  3      <dir_Ethernet_pc5>    no           225.60
```

- a) Indicate which Ethernet frames **s1** would have forwarded to make this table possible.
 - b) What would happen if the switch received an Ethernet frame from **pc5** directed to **pc3**?
 - c) What would happen if the switch received an Ethernet frame from **pc4** directed to **pc5**?
 - d) How long would it take for the switch to remove the addresses of **pc2** and **pc5** from the learned address table?
11. Suppose **s1** receives the following Ethernet frame:

Ethernet Dest. Addr.	Ethernet Src. Addr.	Protocol	Content
ff:ff:ff:ff:ff:ff	<dir_Ethernet_pc1>	ARP	...

Indicate how the switch would behave in the following situations:

- a) The switch **s1** has an empty learned address table.
- b) The switch **s1** has the Ethernet address of **pc1** learned on port 1.

2.2. Influence of Physical Connection Changes on the Learned Address Table of a Switch

Uncompress the file **01-hub-switch2.tgz** and load the scenario in NetGUI, similar to the one shown in figure 3. Start all network devices.

- a) Run the **arping** command on **pc1** to send an Ethernet message from **pc1** to **pc4**.

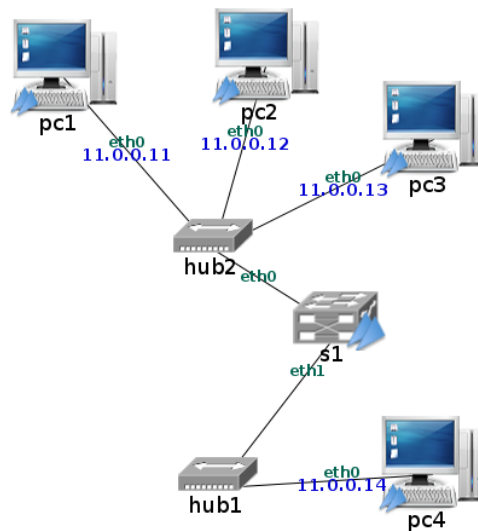


Figura 3: Scenario 01-hub-switch2.tgz

- b) Check the learned address table on **s1** and carefully observe the ports where **s1** has learned addresses.
- c) Run the command that shows the learned address table every second, to observe how its contents will change.
- d) Start a capture on **pc4** and save its content in the file **p1-switch6.pcap**.
- e) Before the entries in the learned address table on **s1** expire (they expire after 5 minutes), turn off **pc1** and remove the cable connecting it to **hub2**. Create a new cable connecting **pc1** to **hub1**. Go to the **01-hub-switch2** folder where you uncompressed the scenario and copy **lab2.conf** to **lab.conf**. Start **pc1**.
- f) Run **arping** on **pc3** to the Ethernet address of **pc1**.
- g) Interrupt the capture and observe how the learned address table on the switch changes. Explain what happened.

3. Assignment Submission

To submit the assignment, upload two files to the virtual classroom:

- The file with the practice report in pdf format: the answers to the questions in the practice.
- The captures **p1-ethernet.pcap** and from **p1-switch1.pcap** to **p1-switch6.pcap** inside a compressed file: **p1.zip**. To do this, first create a folder named **p1** and place all the capture files inside that folder. Then, right-click on the folder name and select 'Compress', name the archive '**p1**' and set the extension to '**.zip**'.