
Before start the TP

Install VirtualBox and import the VM image given on Moodle

If you never used a linux terminal, you should read the following tutorial:

- <https://ubuntu.com/tutorials/command-line-for-beginners#1-overview>

You also find somme documentations about the tools use on the following links:

- <https://www.kathara.org/man-pages/kathara.1.html>
- https://access.redhat.com/sites/default/files/attachments/rh_ip_command_cheatsheet_1214_jcs_print.pdf
- <https://www.tcpdump.org/manpages/tcpdump.1.html>

TP1: Introduction to network tools and ARP

1. Open a terminal and clone the repository of the TP1

```
1 git clone https://forge.uclouvain.be/linfo2147/kathara-labs.git
```

after that you should have a folder named `kathara-labs` in your home directory. You can go to this folder by typing:

```
1 cd kathara-labs/tp1-intro
```

2. Start the Kathara environment

In the folder of the TP1, you will find the configuration file of the Kathara environment.

This environment emulates a network with this topology:

```
1  +-----+   +-----+   +-----+
2  |  PC2  | --- |  S1  | --- |  PC3  |
3  +-----+   +-----+   +-----+
4
5                |
6                |
7                +-----+
8                |  PC1  |
9                +-----+
```

You can start the environment by typing:

```
1 kathara lstart
```

After that, you should see multiple terminals opened. Each terminal represents a different device in the network.

Question 1: What is the MAC address of PC1?

3. Capture packets with tcpdump on S1

In the terminal of S1, type the following command:

```
1 tcpdump -w shared/s1.pcap
```

This command will capture all the packets that pass through the switch S1 and save them in the file `shared/s1.pcap`.

4. Show the ARP table of PC1 and PC2

In the terminal of PC1, type the following command:

```
1 ip neigh show
```

Question 2: What do you see in the ARP table of PC1?

5. Show the S1 Forwarding Table

In the terminal of S1, type the following command:

```
1 bridge fdb show
```

Question 3: What do you see in the forwarding table of S1?

5. Send a ping from PC1 to PC2

In the terminal of PC1, type the following command:

```
1 ping 10.0.0.11
```

Question 4: What do you see in the ARP table of PC1 after sending the ping?

Question 5: What do you see in the forwarding table of S1 ?

6. Stop the capture on S1

In the terminal of S1, type `Ctrl+C` to stop the capture.

7. Analyze the capture

Open the file `shared/s1.pcap` with Wireshark.

Question 6: What do you see in the capture ?

- What is the source MAC address of the ARP request ?
- What is the destination MAC address of the ARP request ?
- What is the source MAC address of the ARP reply ?
- Draw a timeline of the ARP request and reply

8. Add a IPv4 address to PC3

The PC3 has no IP address. Can you add an IP address to PC3 ?

Question 7: What is the command to add an IP address to PC3?

9. Test the connection between PC1 and PC3

Can you ping PC3 from PC1 ?

Question 8: What do you see in the ARP table of PC1 after sending the ping?

10. Add a static ARP entry on PC2 for PC3

You can add a static ARP entry on PC2 for PC3 by typing the following command:

```
1 ip neigh add <IP address of PC3> lladdr <MAC address of PC3> dev eth0
```

Question 9: What is the goal of adding a static ARP entry?

11. Test the connection between PC2 and PC3

Can you ping PC3 from PC2 ?

Question 10: This ping require the use of an ARP request ?

12. What is the IPv6 address of PC1 ?

Each device in the network has a link-local IPv6 address.

Question 11: What is PC1 global IPv6 address ?

Question 12: What is PC1 local IPv6 address and how is it constructed ?

13. Start the capture on S1

In the terminal of S1, type the following command:

```
1 tcpdump -w shared/s1.pcap
```

13. Add a IPv6 address to PC2

The PC2 has no global IPv6 address. Can you add an IPv6 address to PC2 ?

Question 13: What is the command to add an IPv6 address to PC2?

14. Test the connection between PC1 and PC2 in IPv6

Can you ping PC2 from PC1 in IPv6 ?

15. Stop the capture on S1 and analyze the capture

Open the file `shared/s1.pcap` with Wireshark.

Question 14: What do you see in the capture ?

- What is the type of the ICMPv6 packet ?
- What is the address of the source and destination of the ICMPv6 packet ?
- Draw a timeline of the ICMPv6 packet

16. Stop the Kathara environment

You can stop the Kathara environment by typing:

```
1 kathara lclean
```