Assignment 2: network sniffing. Single student activity

In this assignment you have to monitor and investigate three (small) networks, within the Kathará framework. You have to download the lab package and run them, as described in the lab description. Here there are the assignment for each of the three labs:

Es1

In this lab you have to capture the DHCP exchange between the hosts of the network of the Exercise 1 of Assignment 1. The traffic has to be saved in a pcap file. The file has to contain only DHCP traffic. In the report you have to detail the capture command (program and filter used) to generate the pcap file.

The DHCP server is properly configured but is not executed at startup. You have to manually start it (when ready to capture) with the command

```
root@boundary:/# udhcpd
```

Es2

In this lab you have to perform a troubleshooting of the network configurations. Several host show an unexpected behaviour (like don't answer to ping of some hosts, but do answer to some others). You have to use wireshark/tcpdump to provide evidences about the bugs, namely packets that take anomalous paths (or do not have the right addresses). Moreover, you have to propose the required modifications in the configurations of the hosts you think are wrongly configured.

There are two subnets 192.168.10.16/28 and 192.168.20.32/29 and the boundary is the router between the two subnets.

Es3

The lab is similar to the network of Exercise 3 of Assignment 1, but now the routers use dynamic routing. You have to capture the RIP traffic exchanged in the network of the routers. The traffic has to be saved in a pcap file. The file has to contain only RIP traffic. In the report you have to detail the capture command (program and filter used) to generate the pcap file.

The RIP daemon is properly configured but is not executed at startup. You have to manually start it (when ready to capture) with the command executed on router1, router2 and border routers:

```
root@border:/# /etc/init.d/zebra start
```

Scheme of your hand-in

You have to prepare a document with the following structure:

Assignment 2: network sniffing.

Student name:
Student matricola:

1. Introduction
2. Es1: DHCP network
    1. Plan of the activities
    2. Implementation details
    3. Comments about the captured traffic
3. Es2: troubleshooting with wireshark
    1. Plan of the activities
    2. Implementation details
    3. Analysis of the bugs and proposed corrections
    4. Final remarks
4. Es3: two networks with dynamic routes
    1. Plan of the activities
    2. Implementation details

    3. Comments about the captured traffic
5. Final remarks