Middle East Technical University

Department of Computer Engineering

CENG 435

Data Communications and Networking

Fall 2022–2023

THE - 4

Due date: 2023-01-05

1 Introduction

You will analyze ICMP (Internet Control Message Protocol) messages at the Network Layer and the Link Layer for this assignment. Complete the assignment on a Linux machine, listening on your main internet interface (wireless or Ethernet). You can cite external sources (textbook, RFCs etc.).

2 ICMP Packet Analysis

2.1 Capture the Network Traffic

1. Start your Wireshark capture on the interface you use to connect to the Internet. Keep your browser, music client, chat client etc. open for this assignment.

2. Grab a terminal and run the `ping` binary with the given arguments:

   ```
   ping -c 10 1.1.1.1
   ```

   (You should not see a 100% packet loss at this step to continue with the assignment)

3. After the `ping` command is finished, you can stop the capture and save the capture as `<name_surname>.pcap`

4. Make sure that you see 10 `ICMP` requests and 10 `ICMP` responses in your capture

5. Take two screenshots that show the "Internet Control Message Protocol" details:

   - Wireshark "Packet Details" (by double-clicking on the packet) window that shows an `ICMP` request
   - Packet details window of an `ICMP` response

6. Run the following command on a terminal to get your routing table information;

```
ip route
```

7. Include the screenshots of the `ICMP` request, response and the routing table in your report

3 Questions

1. What are the IP addresses of the source host and the destination host of the request and the reply packets?
2. Check the packet information of the request and the reply packets. Is there a port number information in those packets? Why/why not?
3. Regarding the "type" and "code" fields in the request and the reply packets:
   (a) What is the purpose of the "type" field?
   (b) What is the purpose of the "code" field?
   (c) Explain the values in the "type" and "code" fields.
4. By looking at the `ICMP` request packet information, find how many bytes are transferred in total. Then, explain where these bytes are used in or what information they carry.
5. Considering your answer to the first question and the routing table you got; explain which single rule you should remove so that the outgoing packets will be dropped, and your machine cannot send any ping requests?
6. Focus on the Layer 2 on your Wireshark window for the following questions:
   (a) What is the 48-bit Ethernet address of your computer?
   (b) What is the 48-bit destination address in the Ethernet frame? Which machine does this Ethernet address belong to?
   (c) Quickly go over every packet you sniffed during the capture and pay attention to the `Type` field in Layer 2, how many values did you encounter? List and explain them.

4 Submission

This is an individual assignment. Upload your report `<name_surname>.pdf` and your `<name_surname>.pcap` file to our ODTUClass page.

5 Other Specifications

- Feel free to ask questions through ODTUClass discussions. This includes any homework question you find ambiguous. Ask for clarification rather than going with your assumption.
- See the course syllabus for the late submission policy.

- This is an individual assignment. Using any piece of code, discussion, explanation etc. that is not your own is strictly forbidden and constitutes as cheating. This includes friends, previous homework, or the Internet. The violators will be punished according to the department regulations.

5.1 Grading

- Please ensure that the screenshots you include in your report are legible.
- Answers without explanations or screenshots to support them (e.g. answering just "6" to a "How many…" question) will get no grade.