Ethernet Frame Capture and Analysis with Scapy

Objective:

To familiarize students with the practical aspects of packet capture and analysis using Scapy, while gaining a deeper understanding of Ethernet frames and IP headers.

Requirements:

Python environment with Scapy installed.
Network access for live packet capture.

Project Tasks:

1. Setup:

(1) Ensure Scapy is properly installed.

Windows:

- Option 1: Use Oracle virtual box with virtual machine (recommend)
- https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-on-a-virtual-machine-using-virtualbox#1-overview
-

- Option 2: Use Windows Subsystem for Linux (WSL)

https://ubuntu.com/tutorials/install-ubuntu-on-wsl2-on-windows-11-with-gui-support#1-overview

Mac OS:

- https://scapy.readthedocs.io/en/latest/installation.html
-

(2) Review basic Scapy functions related to packet capture.

https://www.geeksforgeeks.org/packet-sniffing-using-scapy/

2. Packet Capture:

- Write a Python script using Scapy to capture 15 Ethernet frames.

3. Frame Analysis:

- For each captured Ethernet frame:
    - Extract and print:
        - Source MAC address
        - Destination MAC address
    - Check if it contains an IP layer. If yes:
        - Extract and print:
            - IP version
            - Source IP address
            - Destination IP address

4. Data Extraction:

- From each captured Ethernet frame:
    - Extract and print the first 42 bytes in hex format.
    - Format the bytes for readability: print every 8 bytes on a new line, with a space between every 2 bytes.

5. Wireshark Capture same packets:

- Use Wireshark to capture same packets, show at least one packet first 42 bytes same as the one captured by your python program,

5. Documentation:

- Students should document your observations and highlite the indientical first 42 bytes in both wireshark and terminal output screen shots.

Deliverables:

Python Script: A well-commented script that performs the packet capture and analysis as described above.
Report: A 2-3 page report detailing:

- The student's approach to the problem.
- Key observations from the captured data.
- Any challenges faced and how they were overcome.

Evaluation Criteria:

Functionality: Does the script correctly capture and analyze the frames?

Code Quality: Is the code well-organized and commented?
Report: Clarity of explanations, depth of analysis, and presentation.

Hints for Project

In order to understand this Project, you need to have some knowledge on Ethernet frames. Ethernet frame formatting is shown in Figure 1. The preamble is omitted since it is used for synchronization.

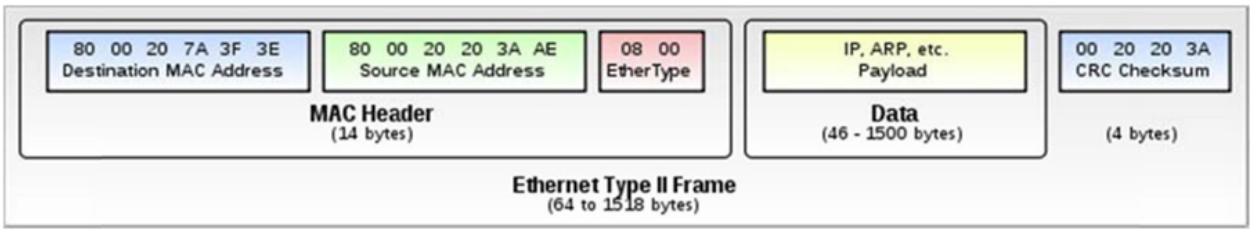

Figure 1

The MAC header contains three parts with a total length of 14 bytes: Destination MAC address, Source MAC address and frame type. Here, frame type (Ether Type) indicates the payload data type. Two common types are 0x0800 (IP) and 0x0806 (ARP).

You need to output the MAC header (14 bytes) and the first 28 bytes from the payload in Project 1.