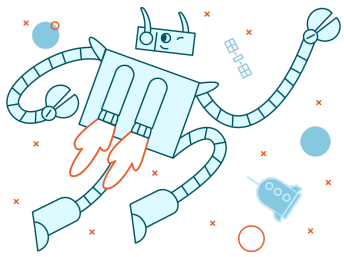
ARP Shark 🦈



Objective

In this exercise, you will use Wireshark to analyze a provided capture file containing ARP (Address Resolution Protocol) requests and responses. You will examine specific packets and answer questions about their contents and purpose.

Background

ARP is a protocol used to map IP addresses to MAC addresses within a local network segment. When a device wants to communicate with another device on the same network, it needs to know the MAC address of the destination device. ARP is used to broadcast a request to all devices on the network, asking for the MAC address associated with a specific IP address. The device with the requested IP address responds with its MAC address.

Prerequisites

- Wireshark installed on your computer
- The provided ARP capture file

Instructions

1. Open the provided ARP capture file in Wireshark.

2. For each packet, fill the following fields:
    - Ethernet layer:
        - Source MAC
        - Destination MAC
    - ARP layer:

        - Is it a request or reply?
        - Sender MAC
        - Sender IP
        - Target MAC
        - Target IP
    - Describe in your own words what you are seeing - what is the purpose of this packet? What's happening here?

3. Answer the following questions:
    - What is the purpose of an ARP request?
    - What is the purpose of an ARP reply?
    - What's the difference between the Destination MAC address in ARP replies and ARP requests? Why is that?
    - For the last packet - why do you think there is no ARP reply for this request? Try to give several possible reasons, based on what you see.

To submit

- Answers to the questions.