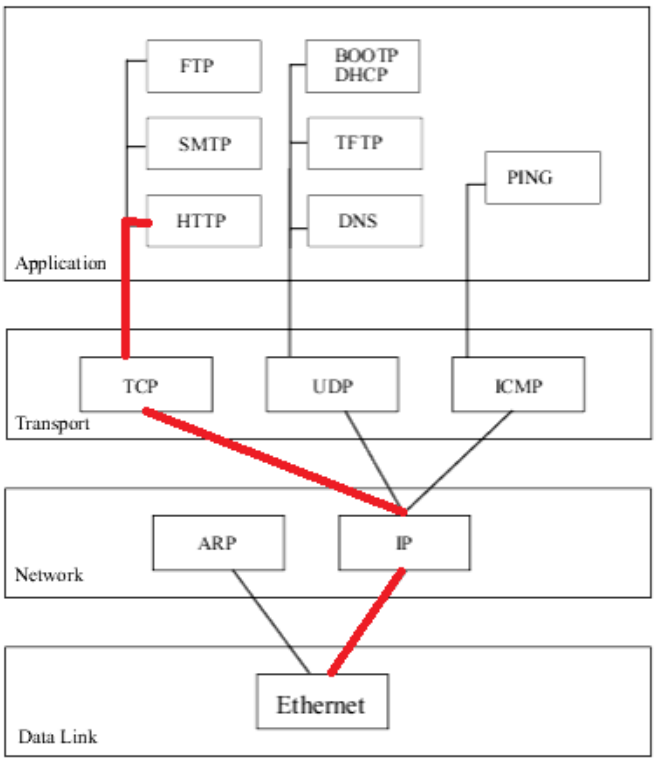
Lab Work No. 03
Ethernet and ARP Protocols Analysis Using Wireshark

1. Aim

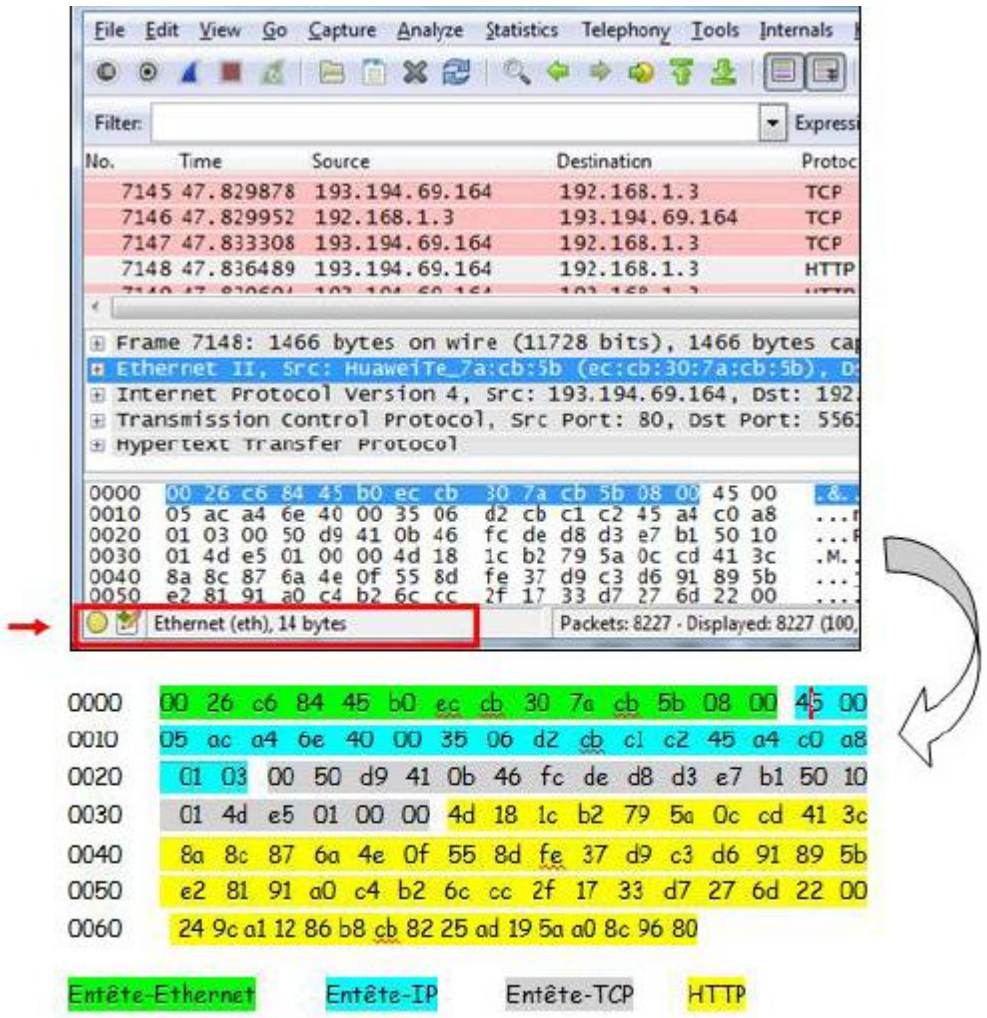
The aim of this lab is to study the functioning of the Ethernet and ARP protocols by analyzing network traffic using Wireshark.

2. Encapsulation in the TCP/IP Stack

For example, for an HTTP message, the encapsulation order is "HTTP-TCP-IP-Ethernet".
Note that in Wireshark, this order is displayed inversely as "Ethernet-IP-TCP-HTTP"



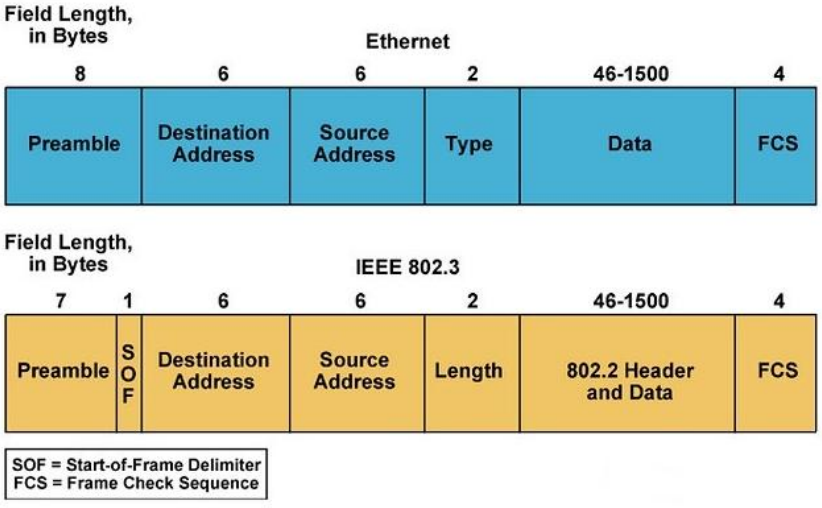
An Ethernet frame contains the "Ethernet Header" and the "Ethernet Data" field. The latter contains the IP packet, whose structure is not recognized by the Ethernet layer, so it is up to the upper layer to determine its header and data. Similarly, the IP Data field contains the TCP message, and so forth. The figure below illustrates the structure (as well as the succession of headers of different encapsulated protocols) for a captured HTTP message.



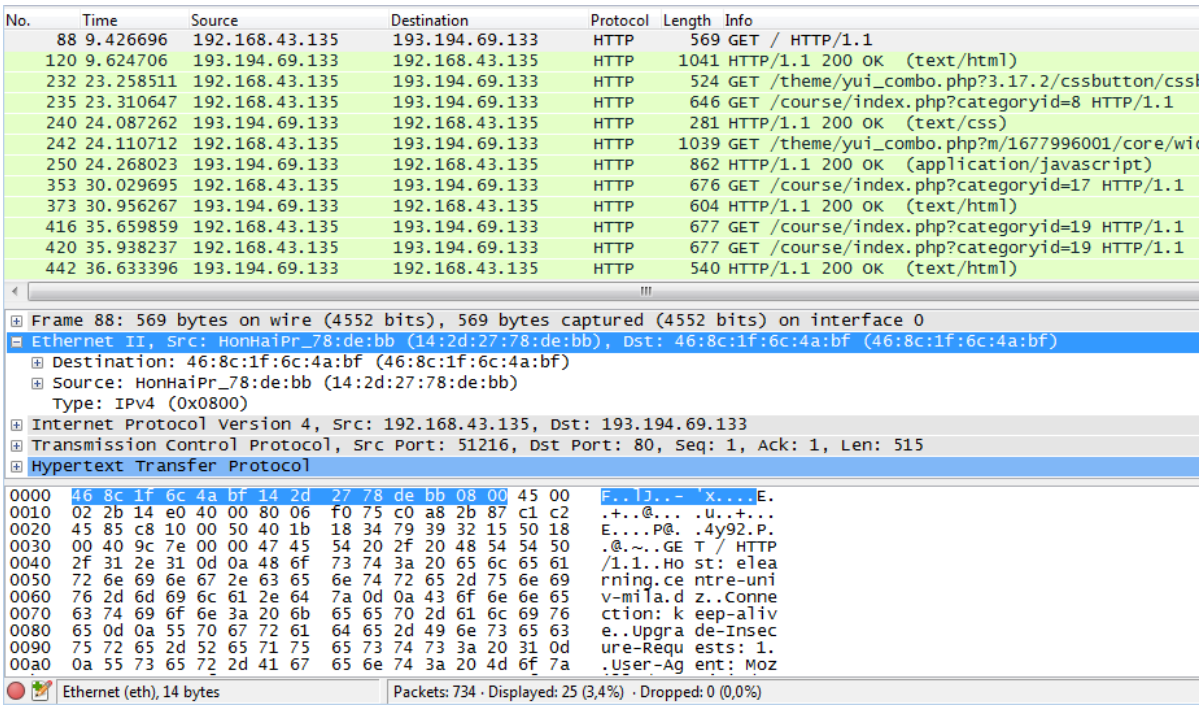
The header size of a packet can be calculated by knowing its structure (the different fields that compose it). For example, the Ethernet header is 14 bytes, while the IP and TCP headers are each 20 bytes. Note that the header size can be variable, as is the case for the HTTP header.
Wireshark also displays, at the bottom of the status bar, the header size of the selected protocol in zone (2). In the previous figure, the status bar indicates that the Ethernet header size is 14 bytes.

3. Ethernet Protocol

Here is the structure of the Ethernet frame:



A network traffic capture is performed using Wireshark. Select a packet in zone (1), and in zone (2), press [+] at the Ethernet level to view the different Ethernet header fields.

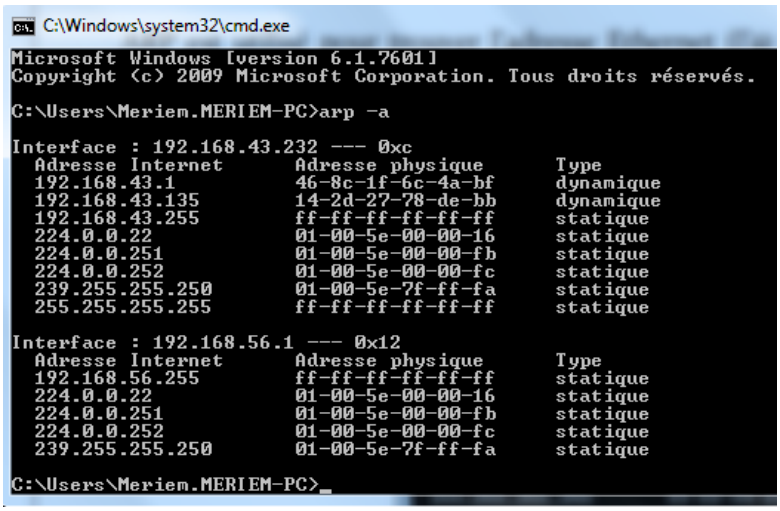


- **Observations:**
  - The "Preamble" field does not appear in the frame because it does not contain useful data; it only serves as a mechanism to help the network card identify the beginning of the frame.
  - There is a destination address and a source address fields. Wireshark deciphers the first three bytes of the address and indicates the manufacturer of the card, such as Huawei.
  - Ethernet frames are generally of type "Ethernet II," which is determined by the "Type" field. In the case of an Ethernet I (IEEE 802.3) frame, the "Length" field replaces the "Type" field, indicating the length of the Ethernet frame.
  - The "Type" field contains a hexadecimal value indicating the upper-layer protocol to which the frame belongs. For example, if its value is 0x0800, the frame is intended for the IP protocol, and the "Data" field of the Ethernet frame contains the IP packet.
  - The "Data" field begins with the Internet layer protocol header (in the figure, it is the IP packet header).
  - The "Data" field may contain padding data if the frame is smaller than 64 bytes.
  - There is no visible CRC field. It exists but is invisible to the system or Wireshark because it is directly processed by the Ethernet-level equipment that sends or receives frames, calculates the checksum, and verifies for errors.

4. ARP Protocol

ARP is used to find the corresponding Ethernet address (MAC address) for a local IP address. The [IP - MAC] combinations are stored in a cache memory, which can be manipulated using the following commands:

1. Check the ARP cache: Type the command **`arp -a`** in the command prompt.



2. Delete an entry from the ARP cache: Open the command prompt as an administrator and type the command: **`arp -d IP_ADDRESS`** (e.g., **`arp -d 192.168.1.1`** to remove the IP 192.168.1.1 from the ARP cache).

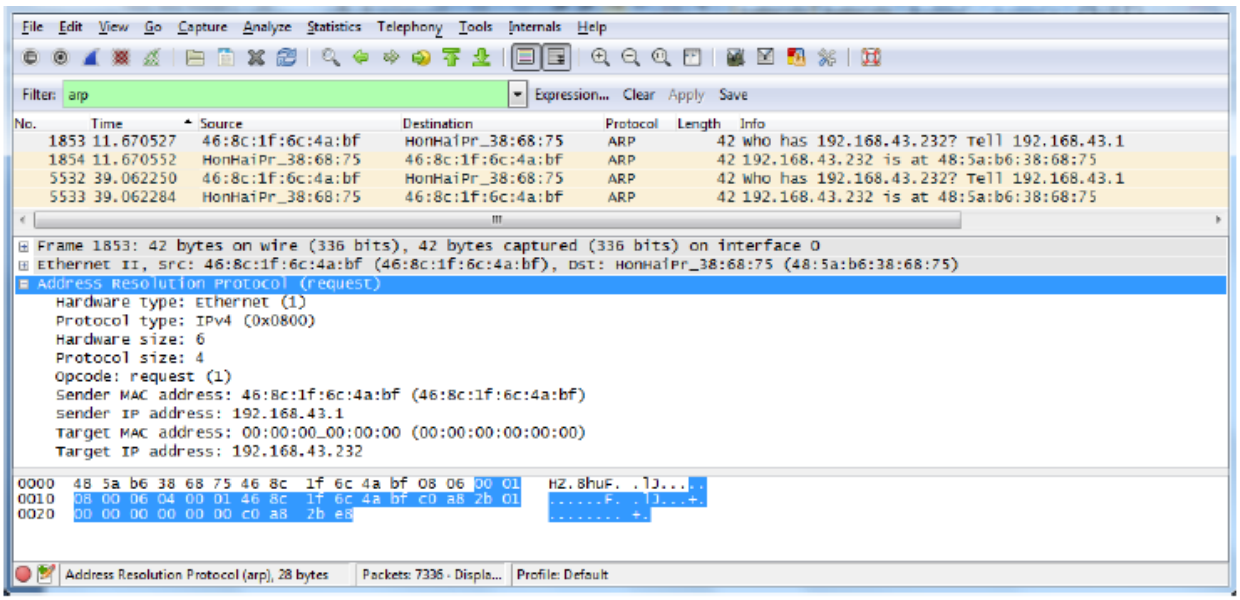
4.1. Capturing ARP Traffic

In the lab room, an internet-connected computer follows the following connection steps:

Any request sent by the computer goes through the gateway. This is also the typical setup for a home computer connected to the Internet via a modem, where the modem acts as the gateway.

- **Note:** To find out the IP address of the gateway, use the command **`netstat -r`**. The gateway address is the one corresponding to the **default destination 0.0.0.0**.

When using a web browser to load a webpage (e.g., the Google homepage), the computer must know the MAC address of the gateway. It uses the ARP protocol to find it. The ARP packet exchange captured by Wireshark resulted in the following:



Note that a filter is applied to display only ARP packets.
There are two types of ARP packets (distinguished by the Info column in zone 1):

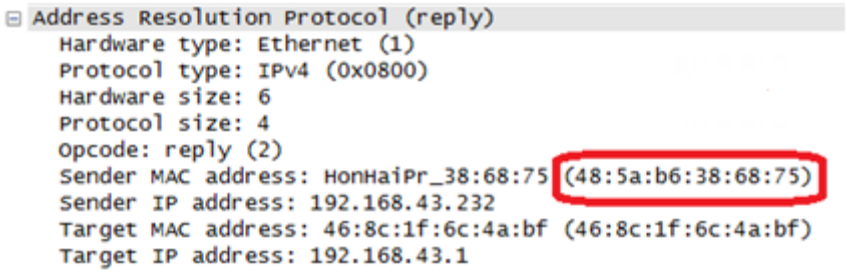
1. ARP Request Packet: The Info line contains "Who has 192.168.43.232? ..." (See frame no. 1853).
2. ARP Reply Packet: The Info line contains "IP_ADDRESS is at MAC_ADDRESS" (See frame no. 1854).

By selecting frame no. 1853 and clicking [+] on "Address Resolution Protocol" in zone (2), the following fields are displayed:

- "Hardware Type" and "Protocol Type": Indicate that the network card being queried is an Ethernet card, and its logical address is an IP address.
- "Hardware size" and "Protocol size": Define the sizes of the physical (MAC) and logical (IP) addresses as 6 bytes and 4 bytes, respectively.
- "Opcode": Contains the value request (1), indicating a request packet.
- "Sender MAC," "Sender IP," "Target MAC," and "Target IP": Define, respectively, the MAC and IP addresses of the sender and the MAC and IP addresses of the target.

For frame no. 1854, clicking [+] on "Address Resolution Protocol" reveals:

- The "Opcode" field contains the value reply (2), indicating a reply packet.
- The values of "Sender MAC," "Sender IP," "Target MAC," and "Target IP" are swapped, as the recipient becomes the sender.



In the request packet, the sender knows its own MAC and IP addresses, as well as the target IP address (the IP address for which the MAC address is being requested), so it fills them in. The target MAC address is unknown, so it is set to **00:00:00:00:00:00**. This address will be filled in by the sender once it receives the ARP reply.

5. Assigned Work

I. Capture network traffic as follows: Start a Wireshark capture, then load a webpage (e.g., **`elearning.centre-univ-mila.dz`**) via your browser. Stop the capture after a moment.

1. Identify a packet containing an HTTP GET message.
2. What is the destination MAC address in this packet? Is it your computer's Ethernet address? Explain.
3. Identify a packet containing an HTTP OK message.
4. What is the source MAC address in this packet? Is it the Ethernet address of the web server hosting the requested page? Explain.
5. What is the Ethernet broadcast address? Identify a broadcast Ethernet frame.
6. Which field in the Ethernet header determines the upper-layer protocol of the frame?
7. Provide an example (captured packet number) of an IP protocol-destined packet. What is the value of the previous field in this case?
8. For an HTTP packet, how many bytes does each header (Ethernet, IP, and TCP) occupy?

II. In this section, we attempt to make the machine use the ARP protocol to discover the MAC address of the local router (the gateway). Then, we analyze the captured traffic.

1. What is the gateway's IP address?
2. Is the gateway's IP address present in the ARP cache?
3. Delete the gateway's IP address from the ARP cache.
4. Capture network traffic using Wireshark while loading a webpage.
5. Filter captured packets to display only ARP packets.
6. Identify an ARP request packet.
7. Identify its corresponding ARP reply packet.
8. What is the "Opcode" value for both packets?
9. What is the ARP header size for a request? What about a reply?
10. What is the target MAC address in the ARP request packet?
11. Complete the following schema with the information from both ARP packets.