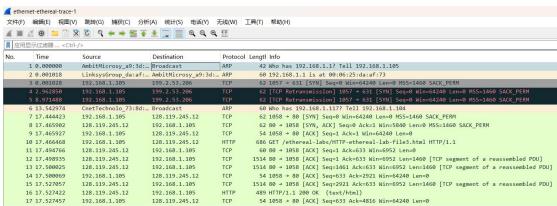
Experiment 4 - Usage of Wireshark

Directory

Part 1-Ethernet frame analyzing	2
1. Open file ethernetethereal-trace-1 in wireshark	
2. Analyze ARP frames	2
3. Question 10 of Wireshark Ethernet ARP v8.0.pdf	
4. Question 11 of Wireshark Ethernet ARP v8.0.pdf	4
5. Question 13 of Wireshark Ethernet ARP v8.0.pdf	
6. Question 14 of Wireshark Ethernet ARP v8.0.pdf	
Part 2-Address Resolution Protocol	

Part 1-Ethernet frame analyzing

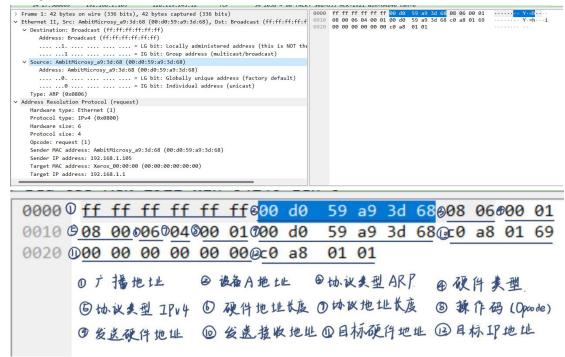
1. Open file ethernet--ethereal-trace-1 in wireshark



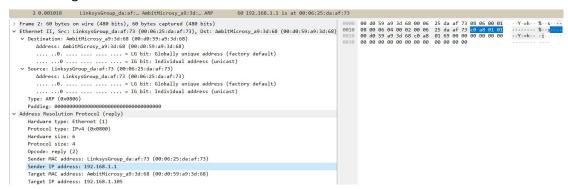
2. Analyze ARP frames

Establishing a TCP connection involves a three-way handshake, facilitated by ARP. As a result, there are three ARP data frames, which are detailed as follows.

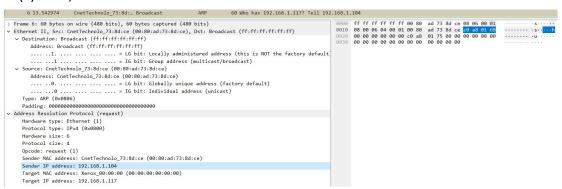
- (1) Device A needs to establish a connection with Device B.
- (2) Device A knows Device B's IP address but lacks its MAC address.
- (3) Device A broadcasts an ARP request into the network, where:
 - Sender Hardware Address is Device A's MAC address.
 - Sender Protocol Address is Device A's IP address.
 - Target Hardware Address is the broadcast address (typically represented by an all-ones MAC address, i.e., FF:FF:FF:FF:FF:FF).
 - Target Protocol Address is Device B's IP address.



- (4) All devices within the broadcast domain receive this ARP request.
- (5) Upon receiving the ARP request, Device B responds with an ARP reply, in which:
 - Source MAC Address is Device B's MAC address.
 - Source IP Address is Device B's IP address.
 - Target MAC Address is Device A's MAC address.
 - Target IP Address is Device A's IP address.



- (6) Upon receiving the ARP reply, Device A learns Device B's MAC address.
- (7) Now, Device A can use Device B's MAC address to establish a TCP connection.



Throughout this process, ARP's role is to resolve the mapping between the target device's IP address and MAC address, ensuring that before establishing a TCP connection, Device A is aware of Device B's MAC address for proper data transmission.

- 3. Question 10 of Wireshark_Ethernet ARP v8.0.pdf
- 10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

First handshake:

Source MAC Address: 00:d0:59:a9:3d:68

Source IP Address: c0 a8 01 69

Destination MAC Address: 00:00:00:00:00:00 (Unknown)

Destination IP Address: c0 a8 01 01

Second handshake:

Source MAC Address: 00:06:25:da:af:73

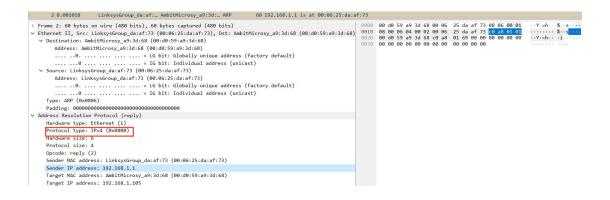
Source IP Address: c0 a8 01 01

Destination MAC Address: 00:d0:59:a9:3d:68

Destination IP Address: c0 a8 01 69

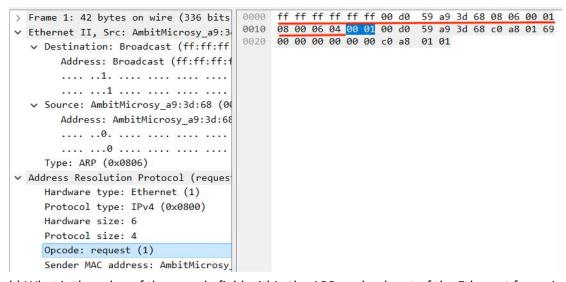
- 4. Question 11 of Wireshark_Ethernet_ARP_v8.0.pdf
- 11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

Hexadecimal value for the Ethernet Frame type field: 0x0800 Corresponding upper layer protocol: IPv4



- 5. Question 13 of Wireshark_Ethernet_ARP_v8.0.pdf
- 13. Now find the ARP reply that was sent in response to the ARP request.
- a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

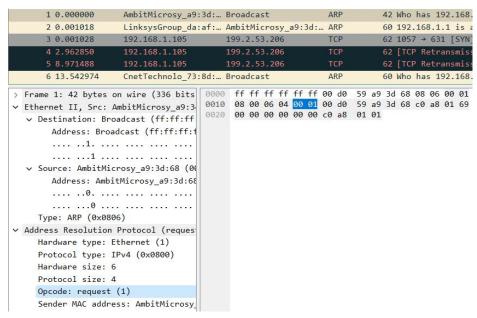
As indicated in the display, it begins 20 bytes from the very beginning of the Ethernet frame.



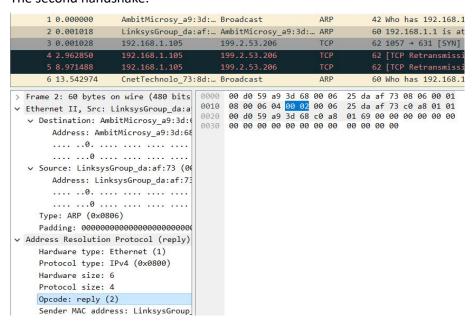
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

In the first handshake, the opcode field value is 1. In the second handshake, the opcode field value is 2.

The first handshake:



The second handshake:



c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

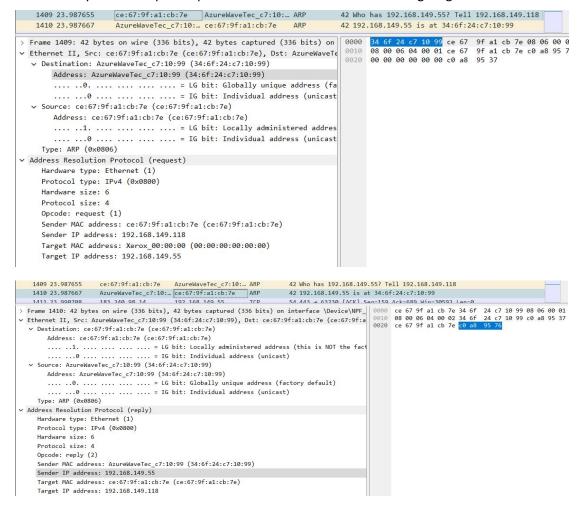
The "answer" to the earlier ARP request appears in the Sender IP address field of the ARP reply message, indicating the IP address of the machine querying the Ethernet address corresponding to its respective IP address.

```
Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
```

- 6. Question 14 of Wireshark_Ethernet_ARP_v8.0.pdf
- 14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Part 2-Address Resolution Protocol

Analyzing the TCP packets captured on my own. Here is an example of me accessing Baidu. The local client establishes a TCP connection with Baidu, involving a three-way handshake facilitated by ARP. The specific protocols are outlined in the following diagram.



First handshake:

Source MAC Address: ce:67:9f:a1:cb:7e

Source IP Address: c0 a8 95 76

Destination MAC Address: 00:00:00:00:00:00 (Unknown)

Destination IP Address: c0 a8 95 37

Second handshake:

Source MAC Address: 34:6f:24:c7:10:99

Source IP Address: c0 a8 95 37

Destination MAC Address: ce:67:9f:a1:cb:7e

Destination IP Address: c0 a8 95 76

Hexadecimal value for the Ethernet Frame type field: 0x0800 Corresponding upper layer protocol: IPv4

It begins 20 bytes from the very beginning of the Ethernet frame.

In the first handshake, the opcode field value is 1. In the second handshake, the opcode field value is 2.