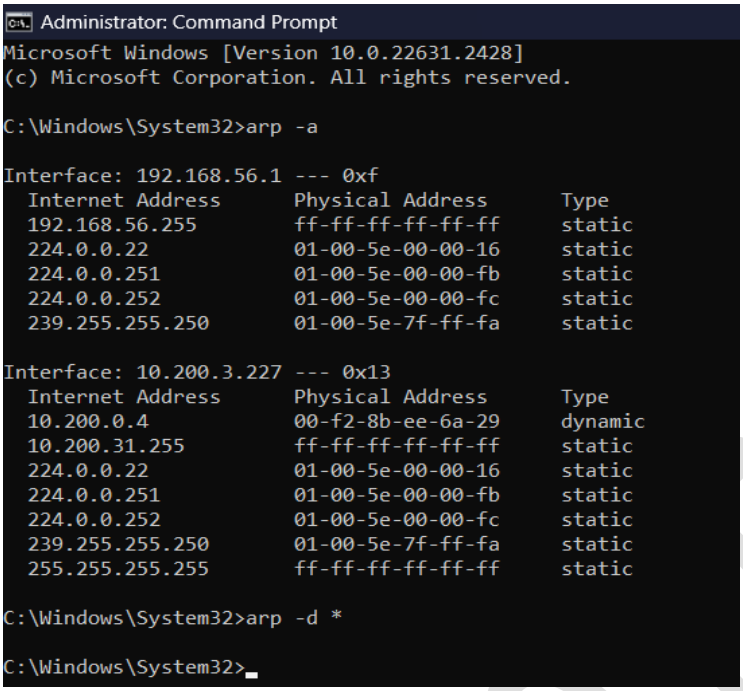

# LAB 9: Analysis of ARP packets through Wireshark and Introduction to static routing through packet tracer.

Akshar Panchani ID- 202101522

IT304 Computer Networks

11/22/23

## Exercise:




## 1.2:

1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

- Source address = 2c:3b:70:0e:62:6d

destination address = ff:ff:ff:ff:ff:ff.

2. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

- For ARP, the two-byte Ethernet Frame type field's hexadecimal value is 0x0806. In the destination address field, the LG bit is set to 1. It indicates that the address is local.

3. Download the ARP specification from ftp://ftp.rfc-editor.org/innotes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

-The ARP opcode field begins after 20 bytes of the 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 request is made?

- When an ARP request is made, the value of the opcode field in the ARP-payload portion of the Ethernet frame is 0x0001, indicating that it is a request..

(c) Does the ARP message contain the IP address of the sender?

- Yes, the ARP message contains the sender's IP address.

The sender's IP address is 10.200.3.227.

(d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

- The ‘target MAC address’ field is set to 00:00:00:00:00:00, which indicates that it is being queried.

4. 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?

-The ARP opcode begins after 20 bytes from the 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?

- The value of the opcode field within the ARP-payload part of the Ethernet Frame in which an ARP response is made is 0x0002 which indicates that it is a reply.

(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 response to the earlier ARP request appears in the ‘sender MAC address’ field and its value is 00:f2:8b:ee:6a:29. The sender IP address is set to 10.200.0.4.

5.What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

- The hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message are 00:f2:8b:ee:6a:29 and 2c:3b:70:0e:62:6d.

6.Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indiated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet trace?

The machine that issued the request is not ours, hence there is no reply in this trace. While the ARP reply is sent directly to the sender's Ethernet address, the ARP request is broadcast. This explains why the packet trace does not show the ARP reply.