Department of Electrical and Computer Engineering

ECE 363 Communications Networks
Lab 3

Name	Arfaz Hossain
Student no.	V00984826
Date	March 15, 2024
Lab Title	ARP, IP, and ICMP
Lab Section	B03

Introduction

In this laboratory session, our focus will be on exploring the Address Resolution Protocol (ARP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP). ARP plays a crucial role in associating known IP addresses with unknown MAC addresses. To delve into this concept, we will utilize Wireshark to dissect Ethernet frames specifically to scrutinize ARP messages. Furthermore, we will analyze the contents of IP frames and delve into the intricacies of ICMP messages.

Procedure

We explored ARP functions by analyzing the "ethernet-trace-1" trace, focusing on ARP request and reply messages. Then, we examined packets containing the HTTP GET message to understand IP header details. For Traceroute, we captured packets using Wireshark while executing the "traceroute www.engr.uvic.ca" command in the console. Analyzing the "tracert-trace-2" trace with an ICMP display filter, we answered questions based on the trace in Section 3.5.2.

Please Turn Over

Discussion

3.3.2 Answer the following questions based on the trace file ethernet-trace-1.

1. What are the hexadecimal values corresponding to the source and destination addresses in the Ethernet frame containing the ARP request message? *The hex value for the source address is 00:d0:59:a9:3d:68. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.*

2. Find the hexadecimal value corresponding to the two-byte Ethernet Frame type field. *The hex value for the two-byte Ethernet frame is ARP (0x0806), the corresponding upper layer protocol is ARP.*

3. Where is the ARP opcode (operation code) field located, i.e., how many bytes are there between the first bit of the opcode and the first bit of the ARP message? *The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.*

4. What is the value of the opcode field within the ARP-payload part of the Ethernet frame, in which an ARP request is made? *The hex value for opcode field withing the ARP-payload of the request is 0x0001, for request.*

5. Does the ARP message contain the IP address of the sender? *Yes, the ARP message containing the IP address 192.168.1.105 for the sender.*

6. Where is the ARP opcode field located, i.e., how many bytes are there between the first bit of the opcode and the first bit of the ARP message? *The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.*

7. 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 hex value for opcode field withing the ARP-payload of the request is 0x0002, for reply.*

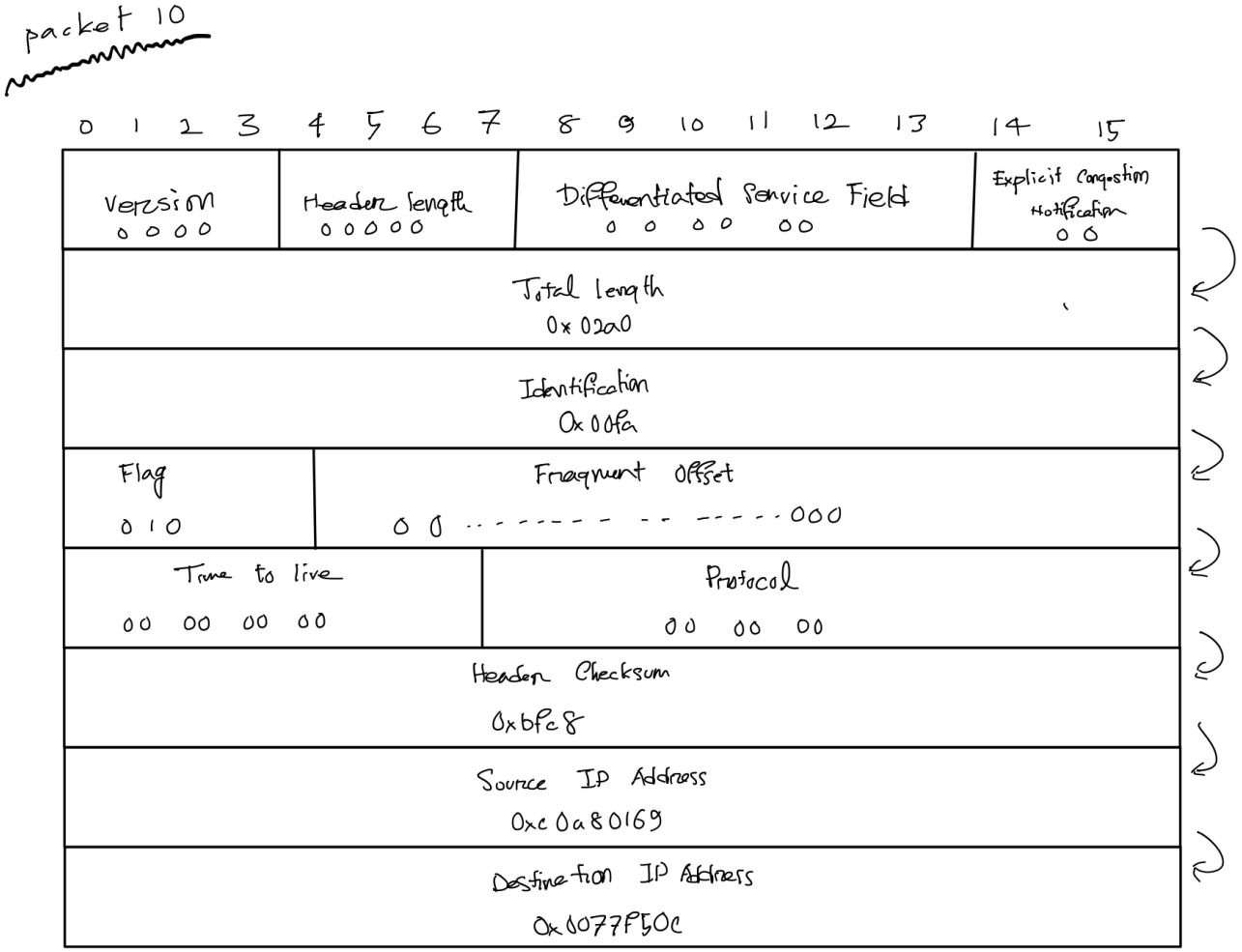
8. What is the MAC address answered to the earlier ARP query? *The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1.*

9. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message? *The hex value for the source address is 00:06:25:da:af:73 and for the destination is 00:d0:59:a9:3d:68 .*

10. Why are not there any ARP replies for the second ARP query (in packet No. 6)? *The absence of a response in this trace is due to our current location being different from the originating machine. While the ARP request is broadcasted, the ARP reply is directed specifically to the Ethernet address of the sender, hence it does not appear in this trace.*

3.4.2 Answer the following questions based on ethernet-trace-1.

1. **Sketch a figure of the packet you selected to show the location and size (in bytes) of the IP header fields, as well as their hexadecimal values.**



2. What are the IP and MAC addresses of the source and the destination, respectively? *The source: IP 192.168.1.105 and MAC 00:d0:59:a9:3d:68. The destination: IP 128.119.245.12 and MAC 00:06:25:da:af:73.*

3. How does the value of the Identification field change or stay the same for different packets? Is there any pattern if the value changes? *For that the ID field corresponds to a counter set by each host. And every time a host sends a message its counter is incremented by one. The two counters do not have the same value.*

4. How to judge whether a packet has been fragmented or not? *In this case, the flag of whether it is fragmented shows the value of 1, thus it is fragmented.*

3.5.2 Answer the following questions based on *ping-trace-1* and tracert-trace-2 respectively.

1. What is the IP address of the source host (client)? What is the IP address of the destination host (server)? *The IP address of the Source Host (Client) is 142.104.115.34, and the IP address of the Destination Host (Server) is 142.104.96.10.*

2. How long is the average Round-Trip Time (RTT)? *The average Round-Trip Time (RTT) is approximately 0.4672 ms.*

3. Examine one of the ping request packets. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are there in the checksum, sequence number, and identifier fields? *The ICMP type number is 8 and the code number is 0 for the ping request packet with number 634. The checksum field is 2 bytes, the sequence number field is 2 bytes, and the identifier fields is 2 bytes. The timestamp from ICMP data occupies 8 bytes.*

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are there in the checksum, sequence number, and identifier fields? *The ICMP packet type is Echo Reply (Type 0) and the code number is 0. Other fields in this ICMP packet include the checksum (2 bytes), sequence number (2 bytes), identifier fields (2 bytes), and timestamp from ICMP data (8 bytes).*

5. Examine the ICMP error packet, which could be found in the packets from tracert-trace-2. It has more fields than the ICMP echo packet. What are included in those fields? Find the TTL field and explain what it is. *(Packet 365) In the ICMP error packet, specifically, Type 11 indicates "TTL exceeded." This packet includes additional fields beyond the ICMP echo packet. One of these fields is the Time-To-Live (TTL) field. The TTL field signifies the number of hops a packet can traverse before it becomes invalid. With each hop, the TTL value decreases by one. When the TTL field reaches 1 and encounters a host other than the destination, an error reply is generated and sent back to the source.*

6. How many routers are there between the source and the destination (www.engr.uvic.ca) according to the trace file? Please draw a figure to show the sequences of these routers.

7. How long are the average RTTs between the source host and each router? (Recommend you to use a script language or other programming language to calculate it. *It is calculated by comparing the difference between the request and error response timestamps in Wireshark: 605 µs+318 µs+961 µs+843 µs+931 µs+1002 µs+743 µs=5.40300ms*

Conclusion

In this lab, students needed to show that ARP requests are broadcasted. ARP requests might not always get a response, especially if the destination IP isn't available. By looking at all the packets, it becomes clear that the identification fields act as unique counters for each host, increasing every time a message is sent. Ping measures network speed by calculating the time between sending a request and receiving a reply. Traceroute figures out network topology by sending out several requests with different time-to-live (TTL) values and uses the TTL Expired error messages to figure out distances.

Reference

1. ECE458. (2021). Ece458Lab. [Online]. Available: https://studentweb.uvic.ca/%7Ewenjunyang/ECE458/notes.html
2. A. Tanenbaum and D. Wetherall, Computer Networks, 5th ed. Prentice Hall, Oct. 2010.
3. J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 5th ed. Addison-Wesley Publishing Company, USA, 2009.