ECE 458

Communication Networks

Laboratory Experiment #3 Report

.

Introduction

In this lab we look at three protocols in such order:

1. Address Resolution Protocol (ARP)
2. Internet Protocol (IP)
3. Internet Control Message Protocol (ICMP)

ARP is the focus of the first half of this lab, here we look at how ARP functions by observing the header fields in Ethernet packets that carry the ARP message. The lab's second section focuses on studying IP frames by seeing and interpreting various fields in the IP header. The format and content of ICMP messages are the topic of the lab's final section [1].

Procedure

In the first part of the lab we learned about the functionality of Address Resolution Protocol (ARP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP).

During section 3.3 we observed the *“ethernet-trace-1”* trace file in order to explore ARP functions. We determined the hexadecimal values of the source and destination addresses in the Ethernet frame of the ARP request and of the two-byte Ethernet Frame field.

During section 3.4 we used *“ethernet-trace-1”* to investigate HTTP GET message structure and the bytes that make the packet. We sketched a figure of an HTTP GET message and determined its respective IP and MAC addresses for its source and destination. With the trace file we also observed any patterns of the identification field.

Section 3.5 required the use of Wireshark and the console to use a ping program to send a packet from the source host to the target IP address. Using a traceroute program the path that a packet takes from source to destination is determined. Using the *“ping-trace-1”* and *“tracert-trace-2”* we can determine the IP address of the client and server and packet average Round-Trip Time (RTT). Examining the ping request and reply packets we can determine the ICMP type and code numbers, and other information such as the bytes in the checksum, sequence number, and identifier fields.

The following tools were used to complete this lab:

- Wireshark with traces:
    - ethernet-trace-1
    - ping-trace-1
    - tracert-trace-2
- ECE 458 Lab Manual Chapter 3
- Console for use of commands *“ping www.engr.uvic.ca -c 10”* and *“traceroute www.engr.uvic.ca”*

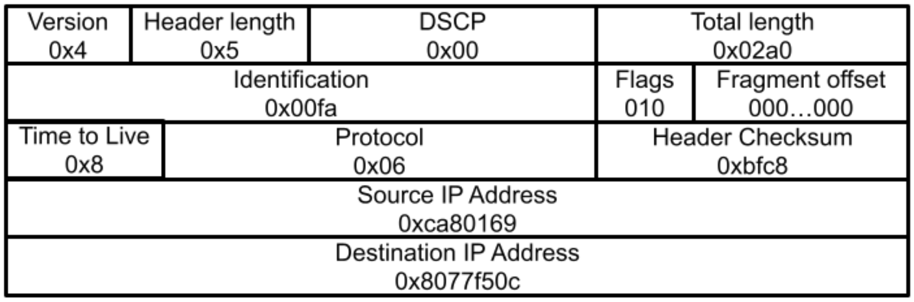
Discussion

3.3.2

1. In hexadecimal the destination address is **ff:ff:ff:ff:ff:ff** and the Source address is **00:d0:59:a9:3d:68** for the Ethernet frame containing the ARP request message.
2. The hexadecimal value corresponding to the two-byte Etherent frame type field is **0x0806**.
3. The ARP opcode (operation code) field is located 20 bytes from the start of the Ethernet frame. Between the first bit of the opcode and the first bit of the ARP message their contains the Hardware type (2 bytes), Protocol type (2 bytes), Hardware size (1 byte), Protocol size (1 byte), and Opcode (2 bytes).
4. The value of the opcode field within the ARP-payload part of the Ethernet frame is **0x0001**.
5. Yes, the ARP message contains the IP address of the sender. The IP address is **192.168.1.105**.
6. The ARP opcode field is located 6 bytes from the beginning of the ARP message.
7. The hex value of the opcode field within the ARP-payload part of the Ethernet frame in which the ARP response was made is **0x0002**.
8. The MAC address answered to the earlier ARP query is **00:06:25:da:af:73.**
9. The hexadecimal value for the Source address is **00:06:25:da:af:73**, and the Destination address is **00:d0:59:a9:3d:68**.
10. Because we are not at the computer that submitted the request, it is unreachable, or the IP is not assigned to any machine on the local network, there are no ARP replies for the second ARP query (in packet No. 6). We can see in the trace that the ARP request has a broadcast destination, and that the ARP reply is transmitted back to the sender's Ethernet address.

3.4.2

1. As recommended in 3.4.1 this sketch uses packet No.10 in the “ethernet-trace-1” [2].



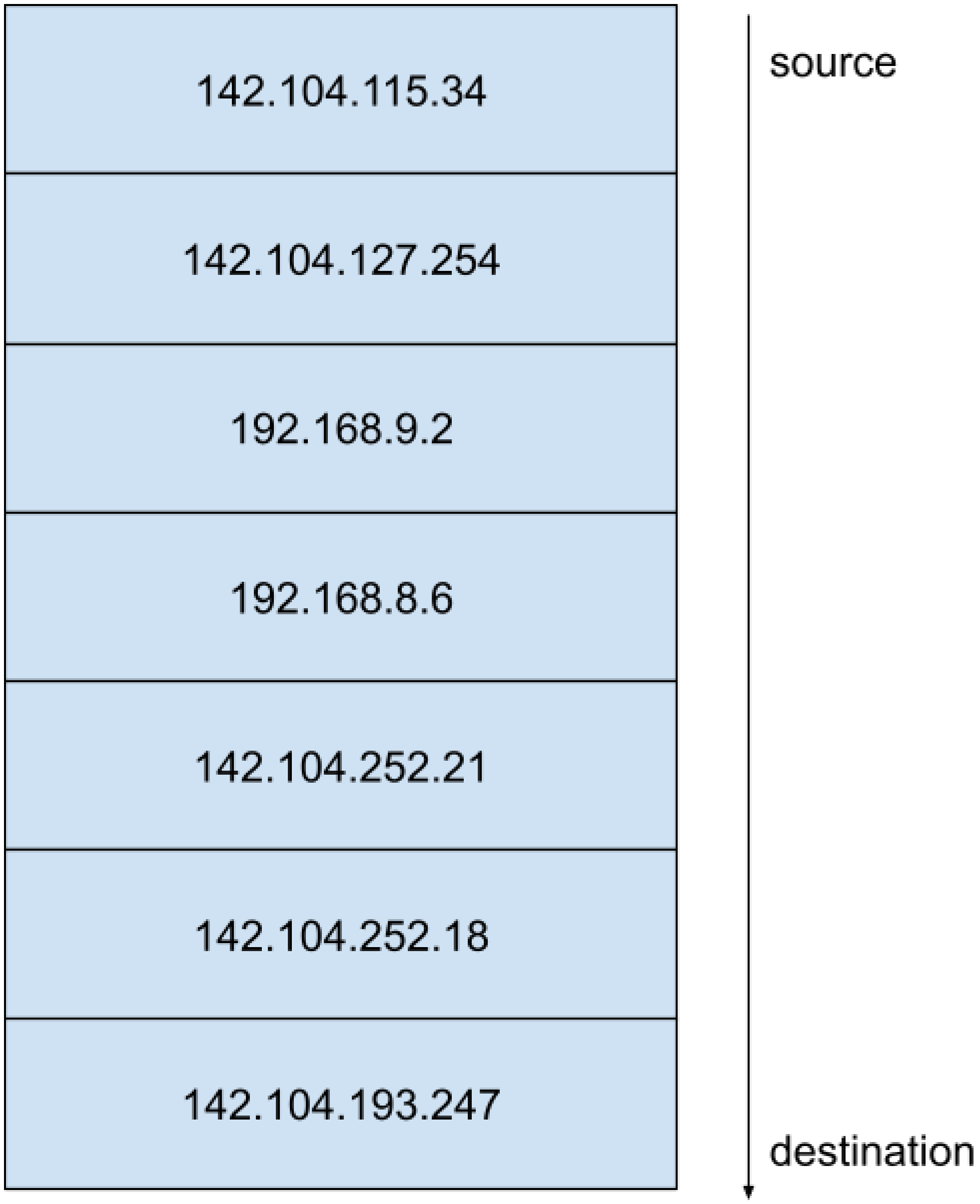
<table>
<tr><td>Version
0x4</td><td>Header length
0x5</td><td>DSCP
0x00</td><td colspan="2">Total length
0x02a0</td></tr>
<tr><td colspan="3">Identification
0x00fa</td><td>Flags
010</td><td>Fragment offset
000…000</td></tr>
<tr><td>Time to Live
0x8</td><td colspan="2">Protocol
0x06</td><td colspan="2">Header Checksum
0xbfc8</td></tr>
<tr><td colspan="5">Source IP Address
0xca80169</td></tr>
<tr><td colspan="5">Destination IP Address
0x8077f50c</td></tr>
</table>

2. The source IP address is **192.168.1.105** and the source MAC address is **00:d0:59:a9:3d:68**. The destination IP address is **1128.119.245.12** and the destination MAC address is **00:06:25:da:af:73**.
3. The identification field corresponds to a counter set by each host, everytime a host sends a message its counter increments by one. The two counters do not have the same value.
4. To determine whether a pocket has been fragmented or not we can observe the fragment offset; if the fragment offset is 0 then the packet has not been fragmented [3].

3.5.2

1. The source host IP address is **142.104.115.34** and the destination host IP address is **142.104.96.10**.
2. The average RTT is roughly $0.247 \times 2 = 0.494ms$
3. For packet number 634, the ICMP type is 8 and the code number is 0. The ICMP packet has a Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE) and Timestamp from icmp data field.. The Checksum field is 2 bytes, Sequence Number is 2 bytes, and the Identifiers are 2 bytes long.
4. For packet number 635, the ICMP type is 0 and the code number is 0. The ICMP packet has a Checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE) and Timestamp from icmp data field.. The Checksum field is 2 bytes, Sequence Number is 2 bytes, and the Identifiers are 2 bytes long.
5. Packet 365 is delivered in error. The packet is of Type 11, which corresponds to the time-to-live (TTL) being exceeded. The TTL field indicates the number of hops being done for a packet before it is invalidated. Each hop done decreases the TTL field by 1; when the TTL value reaches 1 at the destination host, an error reply is generated and returned to the source host [4].

6. There are 8 total routers, including the source.



source

142.104.115.34

142.104.127.254

192.168.9.2

192.168.8.6

142.104.252.21

142.104.252.18

142.104.193.247

destination

7. The average RTT value would be:
   $0.605ms + 0.318ms + 0.961ms + 0.843ms + 0.931ms + 1.002ms + 0.743ms = 5403ms$

Conclusion

In this lab we learned about the Address Resolution Protocol (ARP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP). We learned that ARP is a standard method used to find a host's hardware address if only the network layer address is known. The IP Protocol is a network layer communication protocol that performs two basic functionalities; routing and addressing with the IP address. Whereas, ICMP is used to send control messages to network devices and hosts, and is used in network troubleshooting and analyze applications like traceroute and ping.

The first section of the lab focused on exploring the ARP functions by observing the *"ethernet-trace-1"* file in Wireshark. Here we learned how to determine the hexadecimal value and source and destination addresses in the Ethernet frame. We were asked to demonstrate why ARP requests are not guaranteed a reply, and will not receive one if the destination IP is unavailable.

In Section 3.4 we selected a a packet and identified the various components of the IP header fields. It was found by analyzing the packets in the trace file, that the identification fields are unique counters, and for each host an incrementation is done each time a message is sent.

In the last part of the lab we calculated the Round-Trip Time and average Round-Trip time between source host (client) and destination host (server). We learned that ping is a troubleshooting tool used to test packet loss and network delay by finding the time between request and reply messages. Traceroute, on the other hand, was used to determine the path that a packet takes from the source to destination.

References

[1] *ECE458*. [Online]. Available: https://studentweb.uvic.ca/~wenjunyang/ECE458/notes.html.

[2] "TCP/IP Reference: Nmap network scanning," *TCP/IP Reference | Nmap Network Scanning*. [Online]. Available: https://nmap.org/book/tcpip-ref.html.

[3] Red, "IP fragmentation in Wireshark (1)," *trueneutral*, 20-Jan-2015. [Online]. Available: https://www.trueneutral.eu/2015/wireshark-frags-1.html.

[4] B. Ghosh, *Packet filter analysis for ICMP in Wireshark*, 01-Jan-1967. [Online]. Available: https://linuxhint.com/pack_filter_icmp_wireshark/. [Accessed: 13-Mar-2022].

Feedback

There are quite a lot of questions in this experiment that don't help with lecture material comprehension, i.e., finding source and destination addresses was time consuming and didn't help with my understanding.