University of Victoria

Department of Electrical and Computer and Engineering

ECE 458

Laboratory BO 1

Experiment #3
ARP, IP, and ICMP

Mar 24, 2021

Report submitted on Mar 24, 2021

Gucheng Wang
V00942654

Introduction:

In this lab, we will investigate Address Resolution Protocol (ARP), Internet Protocol (IP) and Internet Control Message Protocol (ICMP). ARP allows known IP addresses to be associated with unknown MAC addresses. We will use Wireshark to examine Ethernet frames for ARP messages. And the contents of IP frames and content of ICMP messages will be examined as well.

Procedure:

• Download and open the trace named “ethernet-trace-1”.
• This trace was captured when a host retrieved a long document.
• The ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs.
• Find the ARP request message and answer questions 1-5 in Section 3.3.2.
• Find the ARP reply that was sent in response to the ARP request and answer questions 6-10 in Section 3.3.2.

Discussion Questions:

3.3.2

1.
Source address: 00:d0:59:a9:3d:68
Destination address: ff:ff:ff:ff:ff:ff

2.
The value is 0x0806

3.
It contains: Hardware type (2 bytes); Protocol type (2 bytes); Hardware size (1 byte); Protocol size (1 byte), and; Opcode (2 bytes)..

4.
The value is 0x0001.

5.
Yes, the IP address is 192.168.1.105.

6.
6 bytes from the very beginning of the ARP message

7.
The value is 0x0002

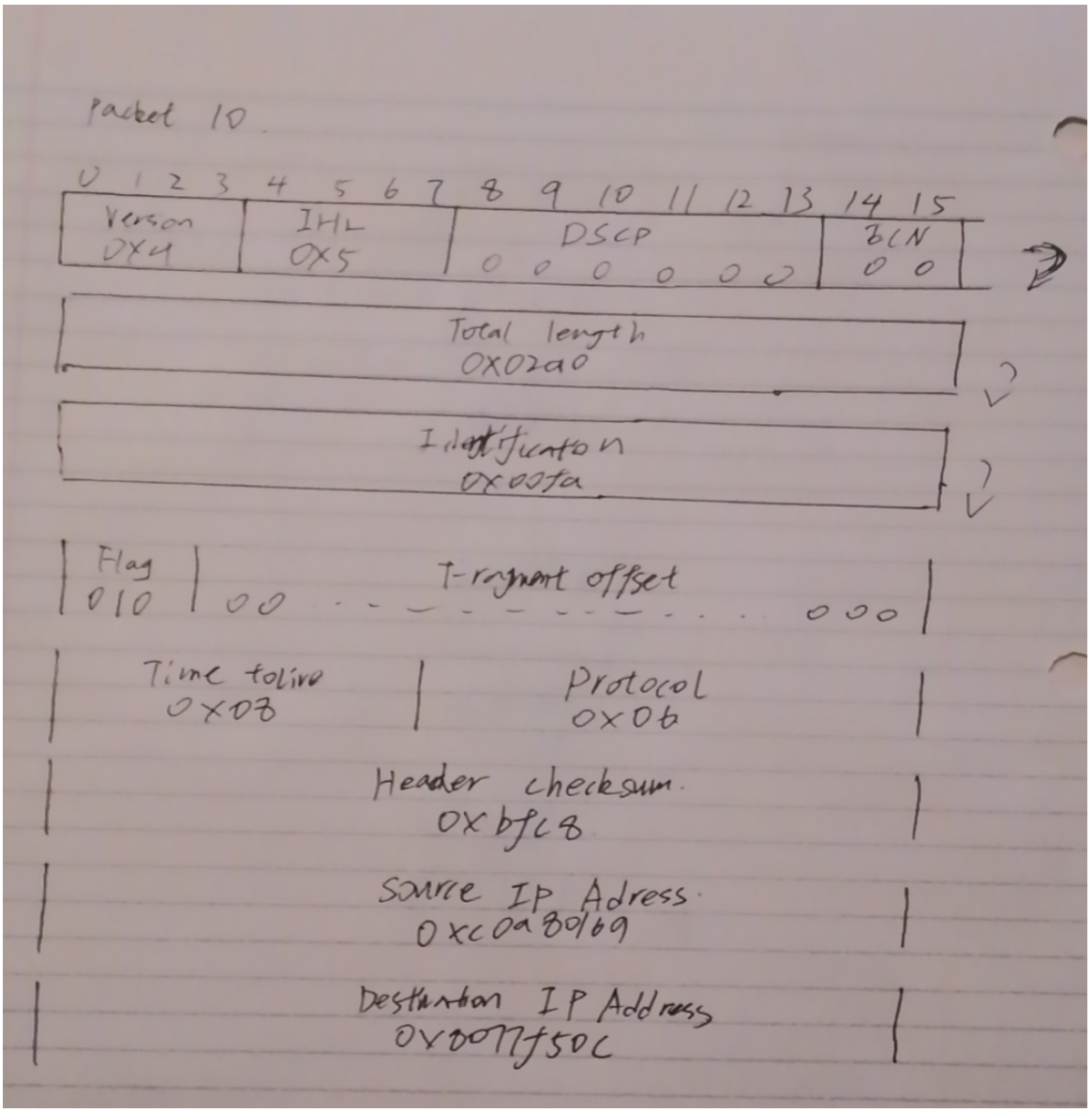
8.
MAC address: 00:06:25:da:af:73.

9.
Source address: 00:06:25:da:af:73
Destination address: 00:d0:59:a9:3d:68

10.
For that the owner is unreachable or the IP is not owned by anyone on the local network.

3.4.2

1.



2.
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.
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.
In this case, the flag of whether it is fragmented shows the value of 1, thus it is fragmented.

3.5.2

1.
Source IP: 142.104.115.34 Destination IP: 142.104.96.10

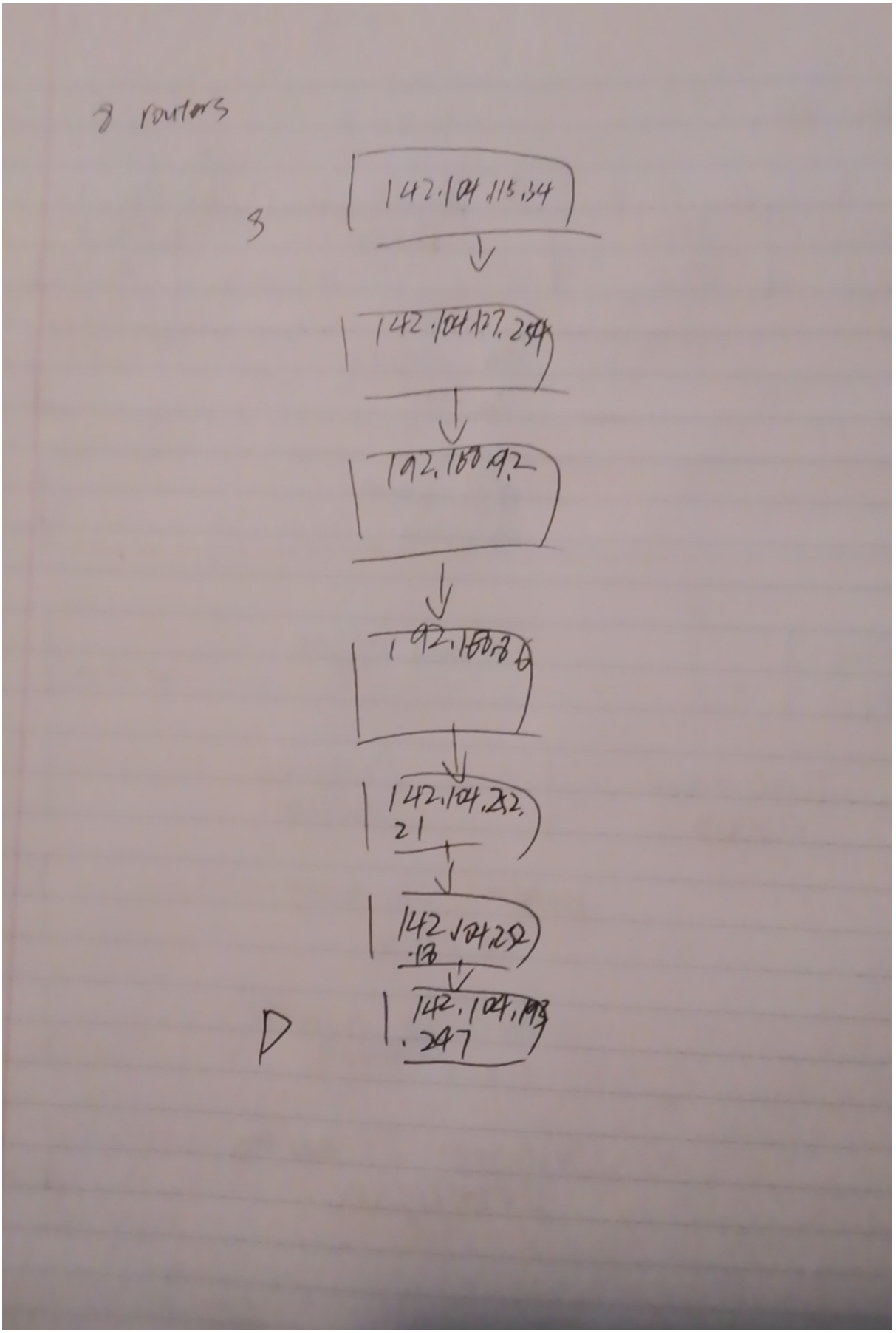
2.
It is about 0.4672 ms.

3.
For number 634, the ICMP type is 8 and the code number is 0. Checksum :2 bytes; Sequence number: 2 bytes; Identifier fields: 2 bytes; Timestamp from ICMP data: 8 bytes.

4.
For number 635, the ICMP type is 0 and the code number is 0. Checksum :2 bytes; Sequence number: 2 bytes; Identifier fields:2 bytes; Timestamp from ICMP data: 8 bytes.

5.
Packet 365: The error packet has Type 11, referring to “TTL exceeded”. The Time-ToLive field indicates the number of hops that a packet can make before it is invalidated. Each time a hope occurs the TTL value is decremented by one. When the TTL field is one and it reaches a host different from the destination, an error reply is generated and returned to the source.

6.



7.
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 are asked to demonstrate that ARP requests are broadcast. ARP requests are not guaranteed a reply, and will not receive one if the destination IP is unavailable. By analyzing all the packets, it shows that the identification fields are unique counters for each host that increments each time a message is sent. And Ping determines network speed by finding the time between request and reply message was sent. Traceroute determines network topology by sending out multiple requests with staggered TTLs and uses the TTL Expired error messages to determine distances.

Reference:

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

Feedback:

It is very necessary to let students have a chance to ask what they are confused about, for that it is remotely done in the lab, students find it very hard to ask questions.