Lab 8

Parmesh Mathur **2018A7PS0133G**

1. Showing a round of DHCP protocol.

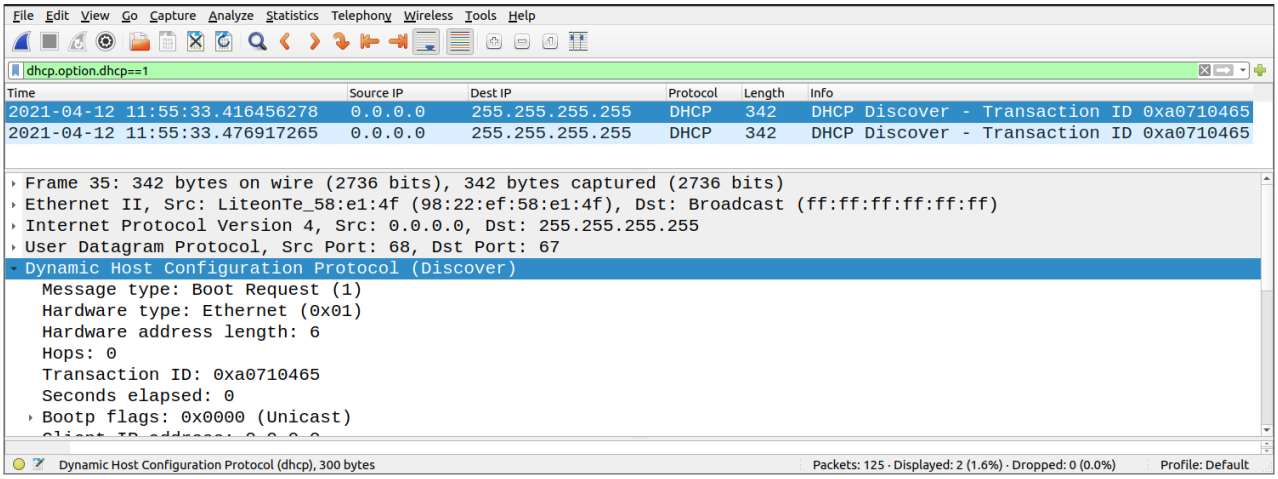
On Wireshark, the DHCP packets are filtered using the filter **`dhcp`**.

---

a. DHCP request, DHCP Discover

There are many possible DHCP request type packest, like discover, release and request. Here we consider discover packets.

To filter out only discover packets, the filter used: **`dhcp.option.dhcp == 1`**



The packet shows it is a DHCP Discover packet in the info column and in the packet information panel.

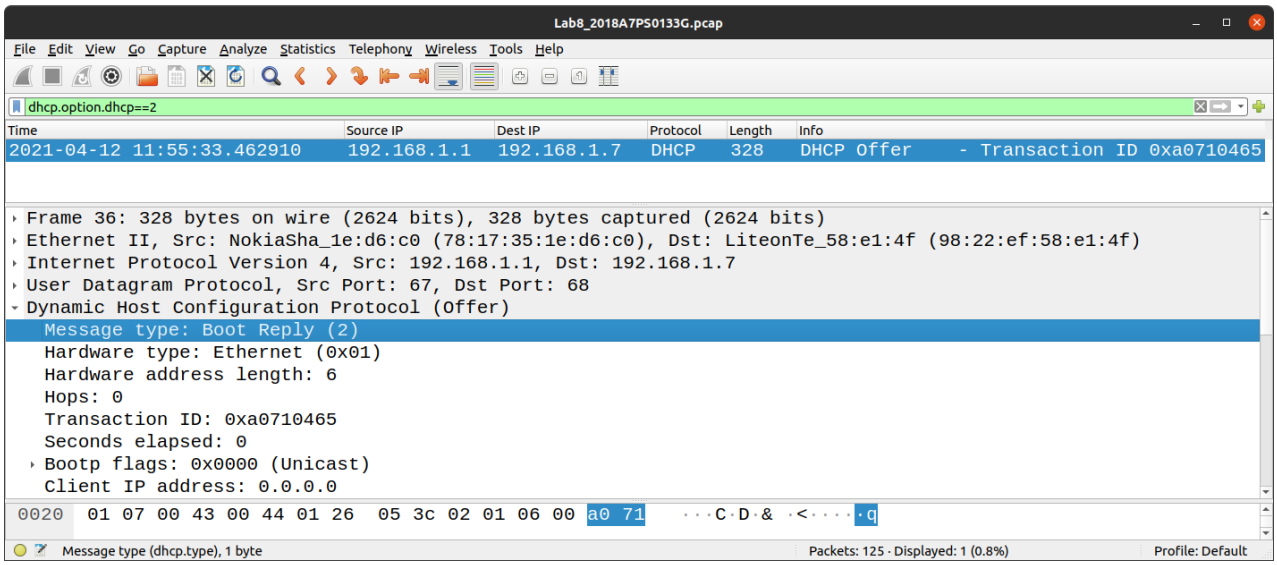
---

b. Reply to DHCP Discover, DHCP Offer

The DHCP Offer packet is the reply to our particular DHCP request, which is a DHCP discover packet. The other response (to a DHCP request packet) being the DHCP ACK packets.

To filter out only offer packets, the filter used: **`dhcp.option.dhcp == 2`**

P.T.O. for screenshot image



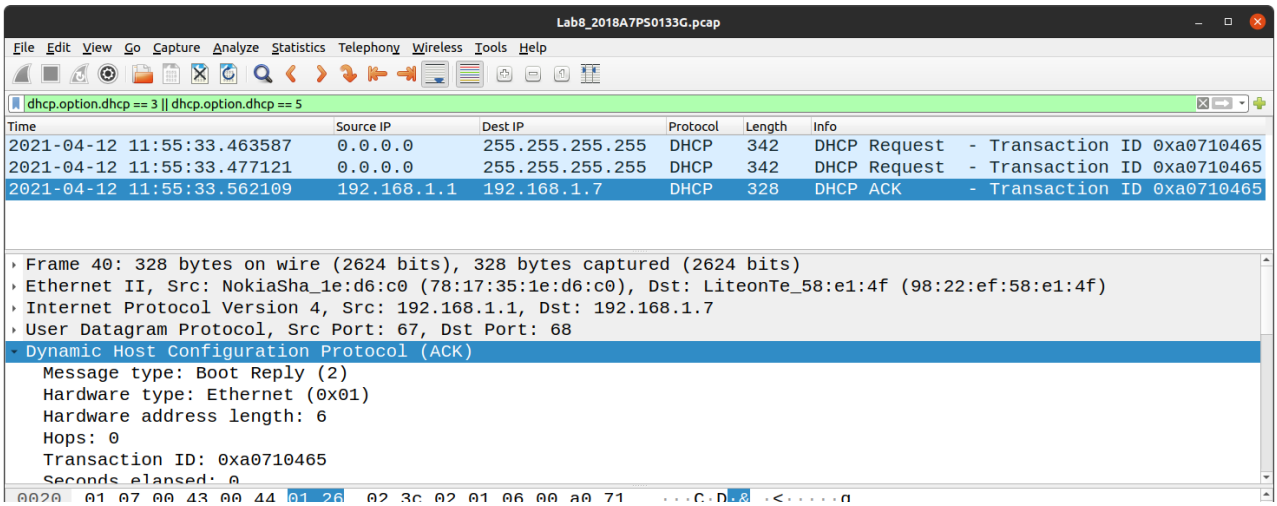
The packet shows it is a DHCP Offer packet in the info column and in the packet information panel (*highlighted in blue*).

---

c. DHCP ACK

The DHCP ACK packets are replies to the DHCP Request packets. To filter out only these two types of packets, the filter used:

```
dhcp.option.dhcp == 3 || dhcp.option.dhcp == 5
```

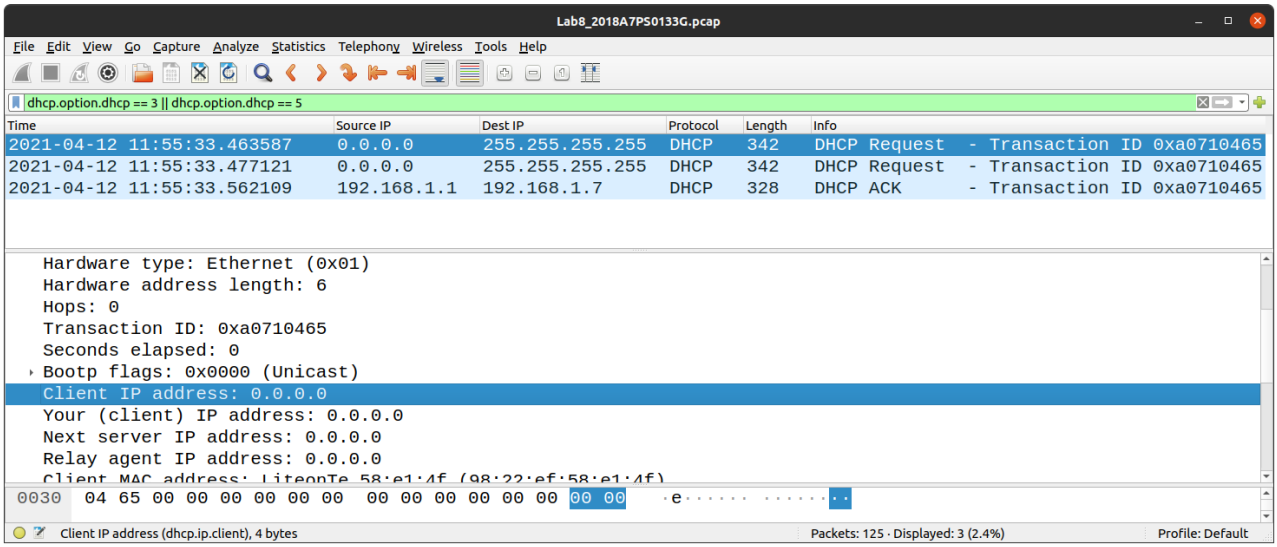


The packet information shows that the selected packet is a DHCP ACK packet (visible in the info cloumn as well as the packet information pane).

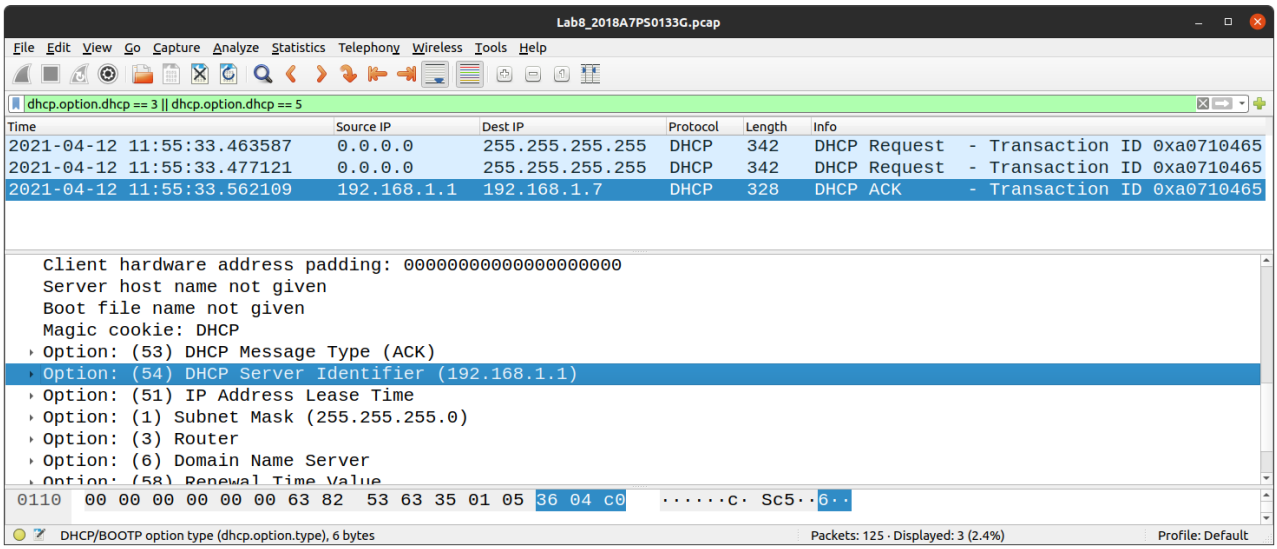
We conclude that the packets are from one ‘round’ of communication as they have the **same transaction ID (`0xa0710465`).**

d. DHCP server and client addresses

The DHCP cleint address is **`0.0.0.0`** (*highlighted in blue in the packet information pane* in the image below).



The DHCP server address is **`192.168.1.1`** (*highlighted in blue in the packet information pane* in the image below).



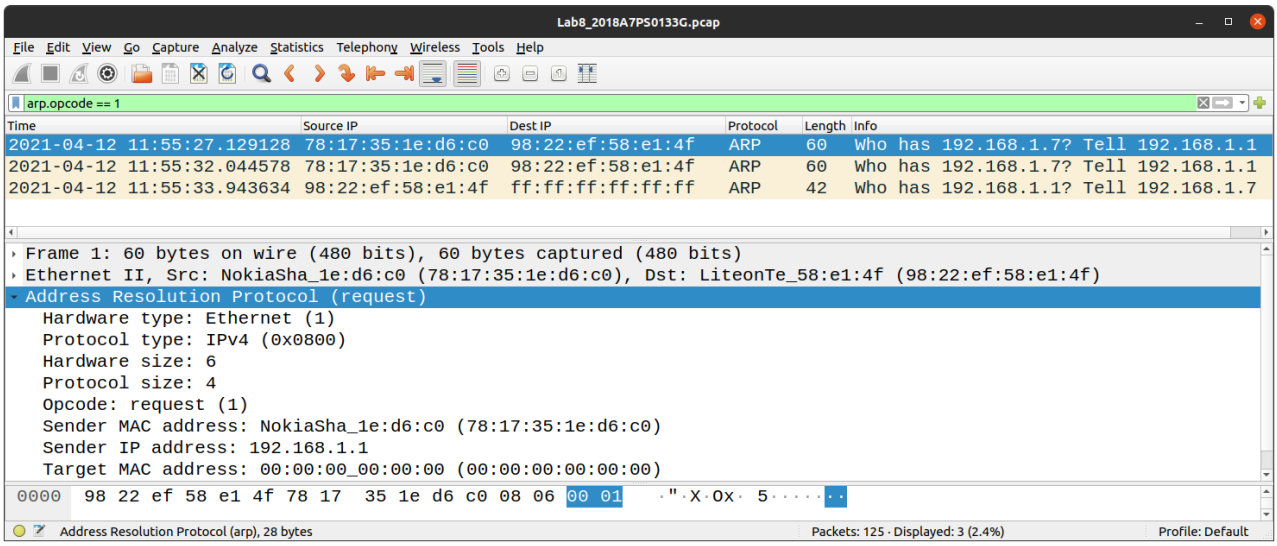
2. Showing a round of ARP protocol.

On Wireshark, the ARP packets are filtered using the filter **`arp.`**

---

a) ARP request

To filter out only requests, the filter used: **`arp.opcode == 1`**



We can see that the selected packet is an ARP request from both, the structure of the message ('`Who has <addr>`...') shown in the info column, or in the packet information pane, which explicitly mentions that the packet is a request packet (*highlighted in blue*).

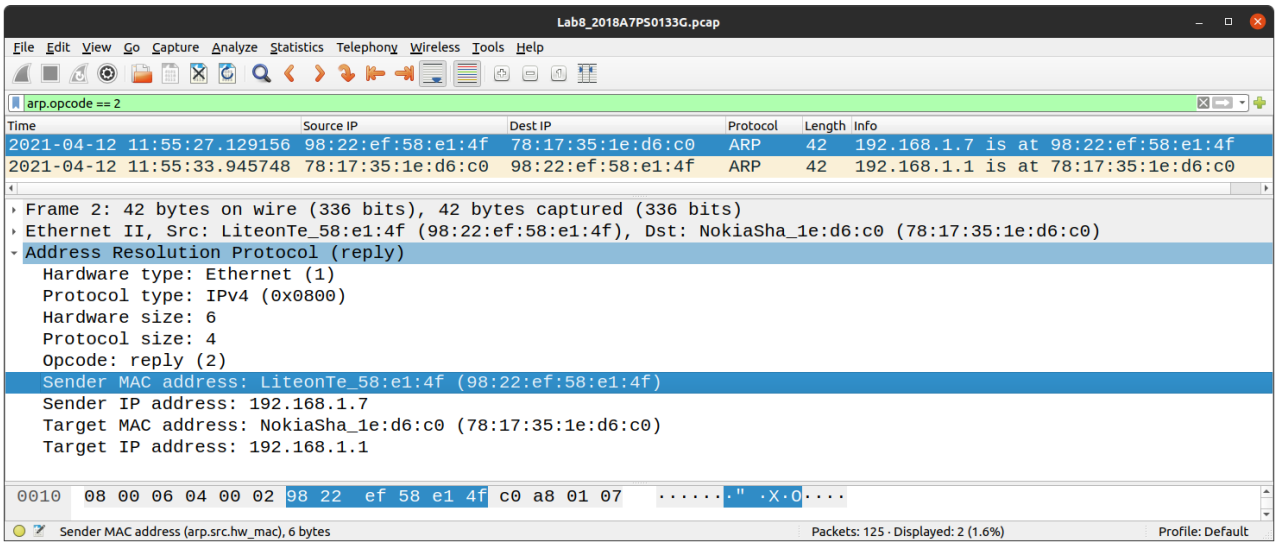
---

b) ARP reply

To filter out only replies, the filter used: **`arp.opcode == 2`**

In the below Image, the selcted packet is an ARP reply, which is evident by both, the message ('`<addr> is at`...') in the info column and in the packet information pane, which explicitly mentions that the packet is a reply packet (*highlighted in light blue in the second panel*).

P.T.O. for screenshot image



---

c) MAC address of replier

The MAC address of the replier is shown in the above image (*highlighted in blue*). It is **`98:22:ef:58:e1:4f`**.

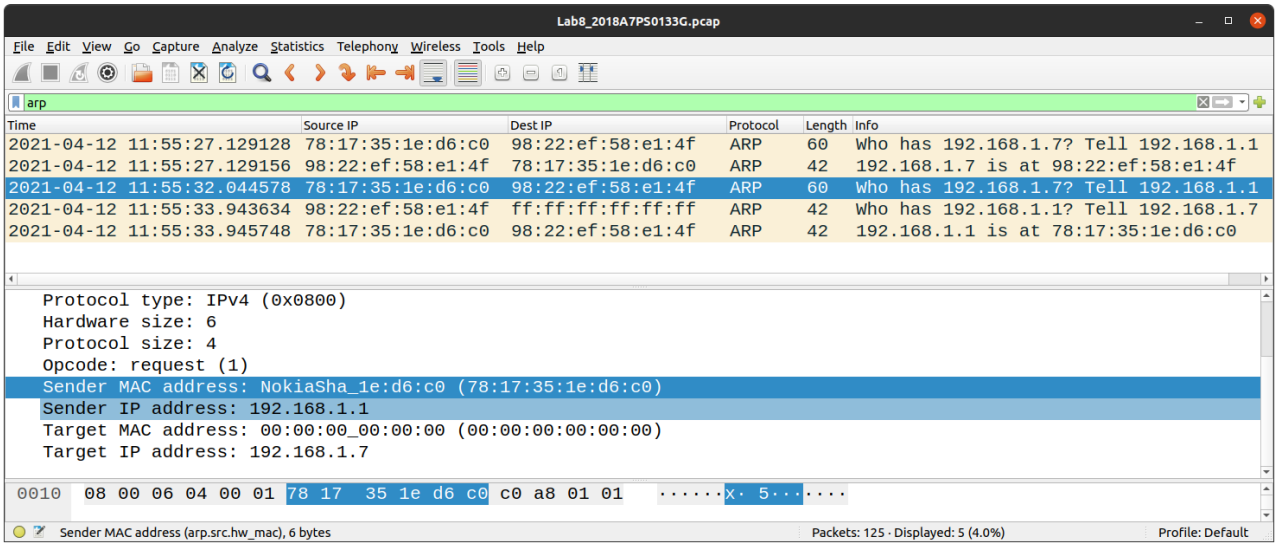
We can confirm this is the replier as it is the source of the reply message.

3. Finding the IP and MAC addresses of the Gateway router.

For a network with a DHCP server, the DHCP is always also the Gateway router. And we know *from part d) of question 1*, that the IP address of the DHCP router is **`192.168.1.1`**. Hence, the IP address of the Gateway router is also **`192.168.1.1`**.

Now, if we look into the packet information of any ARP packet that is a request from the gateway router (message ending with ...`Tell 192.168.1.1`), the sender address will be that of the Gateway router.

The filter used to discplay ARP packets is: **`arp`**



From the image, we match the IP address (already known) to the correspoonding MAC address (highlightd in darker blue in the packet information panel). Hence the MAC address of the Gateway router is known to be: **`78:17:35:1e:d6:c0`**.

`IP address: 192.168.1.1`
`MAC address: 78:17:35:1e:d6:c0`