# Computer Networks Lab 8 CS F303

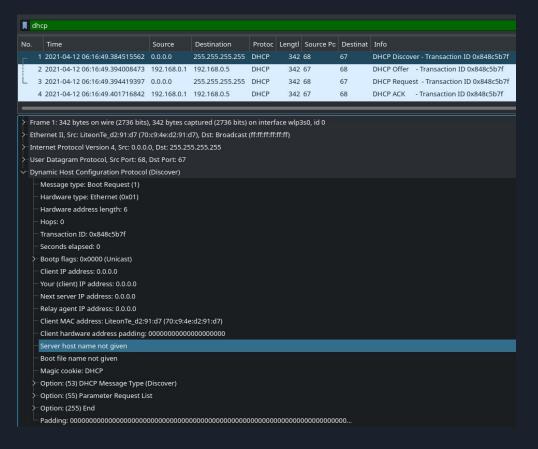
# Question 1

 Show a round of execution of the DHCP protocol. Show DHCP Request (2 marks), Reply (2 marks), and ACK messages (2 marks) in that round. Find out IP addresses of the DHCP server (2 marks) and client (2 marks). Write the filter and show the output in a screenshot.

#### Filter used in wireshark is dhcp

N d	<b>凤</b> dhcp									
No.	Time	Source	Destination	Protoc	Lengtl	Source Po	Destinat	Info		
-	1 2021-04-12 06:16:49.384515562	0.0.0.0	255.255.255.255	DHCP	342	68	67	DHCP Discover - Transaction ID 0x848c5b7f		
	2 2021-04-12 06:16:49.394008473	192.168.0.1	192.168.0.5	DHCP	342	67	68	DHCP Offer - Transaction ID 0x848c5b7f		
Ĺ	3 2021-04-12 06:16:49.394419397	0.0.0.0	255.255.255.255	DHCP	342	68	67	DHCP Request - Transaction ID 0x848c5b7f		
	4 2021-04-12 06:16:49.401716842	192.168.0.1	192.168.0.5	DHCP	342	67	68	DHCP ACK - Transaction ID 0x848c5b7f		

# 1.1 DHCP Request message

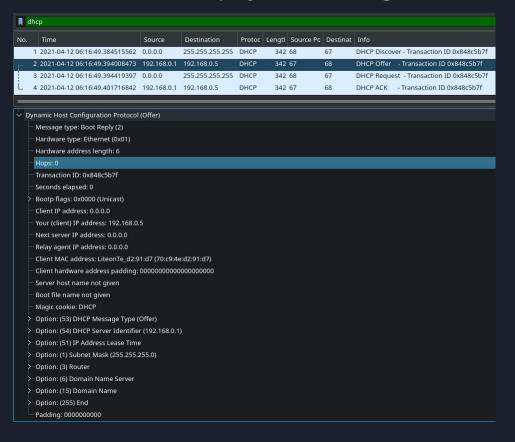


The request sent can be seen here.

As we can see it sends a request for various parameters.

All these packets are generated using the sudo dhcpcd -n command on arch linux

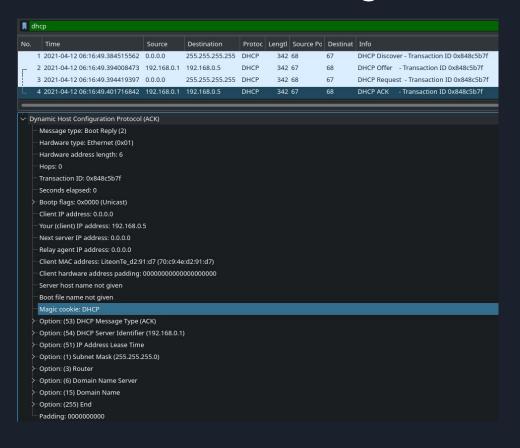
# 1.2 DHCP Reply message



This is the reply that the server sends to the client.

As we can see it contains the server ip, IP address lease time (2 hours in my case), the subnet mask, the DNS and other details.

# 1.3 DHCP ACK message



This is the ack message sent by server to client

The difference between the ack and the reply is the message type. Rest seems to be same.

# 1.4 IP addresses of the DHCP server and client

Server IP: 192.168.0.1

Client IP: 192.168.0.5

Both these values can be checked from the packets captured or from the DHCP message body Another way is using the filter:  $\underline{dhcp \&\& ip.dst==192.168.0.5}$ 

Here, ip.dst is local IP which we know. On arch, one can find IP using: <u>ss -au</u>

### Question 2

2. Show a round of execution of the ARP protocol. Show ARP Request (2 marks) and Reply (2 marks) messages in that round. Find the MAC address of the the replier (2 marks). Write the filter and show the output in a screenshot.

```
[susmit@ardra ~]$ sudo dhcpcd -k
sending signal ALRM to pid 75040
waiting for pid 75040 to exit
[susmit@ardra ~]$ sudo dhcpcd
dhcpcd-9.4.0 starting
dev: loaded udev
DUID 00:04:c1:f6:12:c3:0d:3a:11:e8:8a:95:8c:16:45:32:5b:bc
wlp2s0: connected to Access Point: Susmit
enp1s0: waiting for carrier
wlp2s0: IAID 4e:d2:91:d7
wlp2s0: soliciting an IPv6 router
wlp2s0: soliciting a DHCP lease
wlp2s0: offered 192.168.0.5 from 192.168.0.1
wlp2s0: probing address 192.168.0.5/24
wlp2s0: Router Advertisement from fe80::e66f:13ff:feb6:edd9
wlp2s0: no global addresses for default route
wlp2s0: requesting DHCPv6 information
wlp2s0: leased 192.168.0.5 for 7200 seconds
wlp2s0: adding route to 192.168.0.0/24
wlp2s0: adding default route via 192.168.0.1
forked to background, child pid 75713
[susmit@ardra ~]$
```

Commands run in the terminal to get arp packets

Filter used in wireshark is arp

# 2.1 ARP request message

<b>∏</b> ar	<b>■</b> arp								
No.	Time	Source	Destination	Protoc	Lengtl	Source Pc	Destinat	Info	
64	2021-04-12 12:09:36.860554656	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.5? (ARP Probe)	
7	2021-04-12 12:09:38.463269744	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.5? (ARP Probe)	
78	2021-04-12 12:09:39.573174803	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.5? (ARP Probe)	
86	2021-04-12 12:09:41.576413181	LiteonTe_d	Broadcast	ARP	42			ARP Announcement for 192.168.0.5	
88	2021-04-12 12:09:41.597055763	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.1? Tell 192.168.0.5	
90	2021-04-12 12:09:41.601442202	D-LinkIn_b	LiteonTe_d2:91:	ARP	42			192.168.0.1 is at e4:6f:13:b6:ed:d9	
4	2021-04-12 12:09:43.576468126	LiteonTe_d	Broadcast	ARP	42			ARP Announcement for 192.168.0.5	

As we can see, this message is a request message as stated in the opcode.

- > Frame 64: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp2s0, id 0
- > Ethernet II, Src: LiteonTe\_d2:91:d7 (70:c9:4e:d2:91:d7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (ARP Probe)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: request (1)
  - [Is probe: True]
  - Sender MAC address: LiteonTe\_d2:91:d7 (70:c9:4e:d2:91:d7)
  - Sender IP address: 0.0.0.0
  - Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00)
  - Target IP address: 192.168.0.5

# 2.2 ARP Reply message

<b>arp</b>	<b>■</b> arp								
No.	Time	Source	Destination	Protoc	Lengtl	Source Pc	Destinat	Info	
64	2021-04-12 12:09:36.860554656	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.5? (ARP Probe)	
71	2021-04-12 12:09:38.463269744	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.5? (ARP Probe)	
78	2021-04-12 12:09:39.573174803	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.5? (ARP Probe)	
86	2021-04-12 12:09:41.576413181	LiteonTe_d	Broadcast	ARP	42			ARP Announcement for 192.168.0.5	
88	2021-04-12 12:09:41.597055763	LiteonTe_d	Broadcast	ARP	42			Who has 192.168.0.1? Tell 192.168.0.5	
90	2021-04-12 12:09:41.601442202	D-LinkIn_b	LiteonTe_d2:91:	ARP	42			192.168.0.1 is at e4:6f:13:b6:ed:d9	
4	2021-04-12 12:09:43.576468126	LiteonTe_d	Broadcast	ARP	42			ARP Announcement for 192.168.0.5	
_				_	_				

As we can see, this message is a reply message as stated in the opcode.

- > Frame 90: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp2s0, id 0
- > Ethernet II, Src: D-LinkIn\_b6:ed:d9 (e4:6f:13:b6:ed:d9), Dst: LiteonTe\_d2:91:d7 (70:c9:4e:d2:91:d7)
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (2)
  - Sender MAC address: D-LinkIn\_b6:ed:d9 (e4:6f:13:b6:ed:d9)
  - Sender IP address: 192.168.0.1
  - Target MAC address: LiteonTe\_d2:91:d7 (70:c9:4e:d2:91:d7)
  - Target IP address: 192.168.0.5

# 2.3 MAC Address of replier

```
    Address Resolution Protocol (reply)

      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
     Hardware size: 6
     Protocol size: 4
     Opcode: reply (2)
     Sender MAC address: D-LinkIn_b6:ed:d9 (e4:6f:13:b6:ed:d9)
     Sender IP address: 192.168.0.1
      Target MAC address: LiteonTe_d2:91:d7 (70:c9:4e:d2:91:d7)
      Target IP address: 192.168.0.5
```

As we can see here, MAC address of sender of reply is: e4:6f:13:b6:ed:d9 (D-LinkIn b6:ed:d9)

## Question 3

Find the MAC address and the IP address of the Gateway router (2 marks). Write the filter and show the output in a screenshot.

No.	Time	Source	Destination	Protoc	Lengtl	Source Pc	Destinat	Info
75	2021-04-12 12:57:25.497541830	192.168.0.5	192.168.0.1	ICMP	98			Echo (ping) request id=0x000e, seq=1/256, ttl=64 (reply in 77)
77	7 2021-04-12 12:57:25.701494267	192.168.0.1	192.168.0.5	ICMP	98	2		Echo (ping) reply id=0x000e, seq=1/256, ttl=30 (request in 75)
78	3 2021-04-12 12:57:26.498651373	192.168.0.5	192.168.0.1	ICMP	98			Echo (ping) request id=0x000e, seq=2/512, ttl=64 (reply in 79)
L 79	9 2021-04-12 12:57:26.502726090	192.168.0.1	192.168.0.5	ICMP	98			Echo (ping) reply id=0x000e, seq=2/512, ttl=30 (request in 78)

> Frame 75: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0
> Ethernet II, Src: LiteonTe\_d2:91:d7 (70:c9:4e:d2:91:d7), Dst: D-LinkIn\_b6:ed:d9 (e4:6f:13:b6:ed:d9)

Destination: D-LinkIn\_b6:ed:d9 (e4:6f:13:b6:ed:d9)

- Address: D-LinkIn\_b6:ed:d9 (e4:6f:13:b6:ed:d9)

-.... ..0. .... .... - LG bit: Globally unique address (factory default)

--.... ...0 .... .... = IG bit: Individual address (unicast)

Source: LiteonTe\_d2:91:d7 (70:c9:4e:d2:91:d7)

- Address: LiteonTe\_d2:91:d7 (70:c9:4e:d2:91:d7)

--.... ..0. .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.1

> Internet Control Message Protocol

# 3.1 MAC and IP address of gateway router

MAC Address: e4:6f:13:b6:ed:d9 (D-LinkIn b6:ed:d9)

IP Address: <u>192.168.0.1</u>