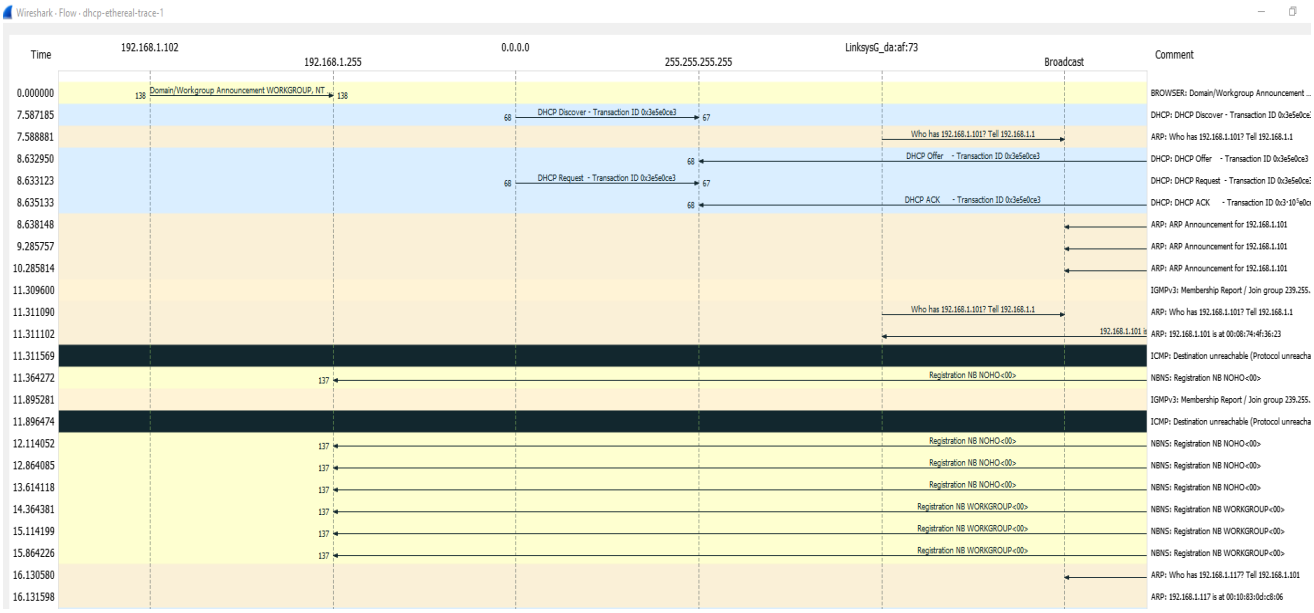
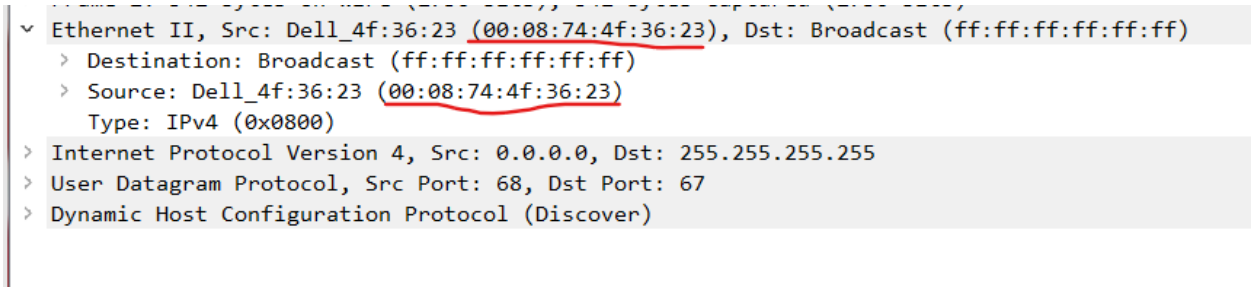
COMP 3203 Wireshark 7

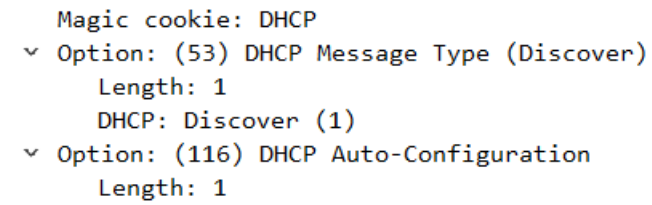
Name: Nirmith Victor D'Almeida
Number: 101160124

1. They are sent over UDP
2. 

Yes they are the same port number

3. 

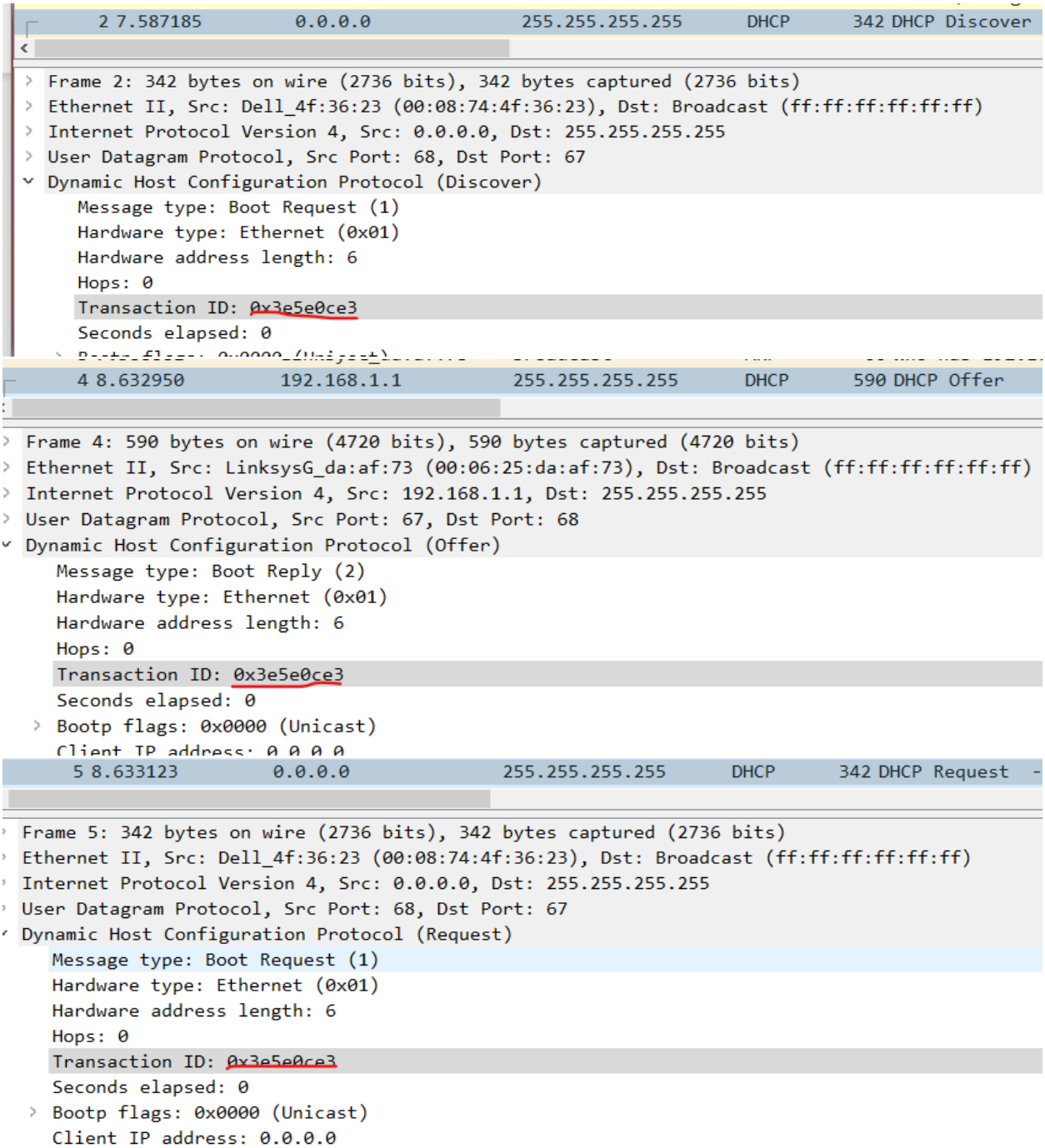
The link-layer address is 00:08:74:4f:36:23

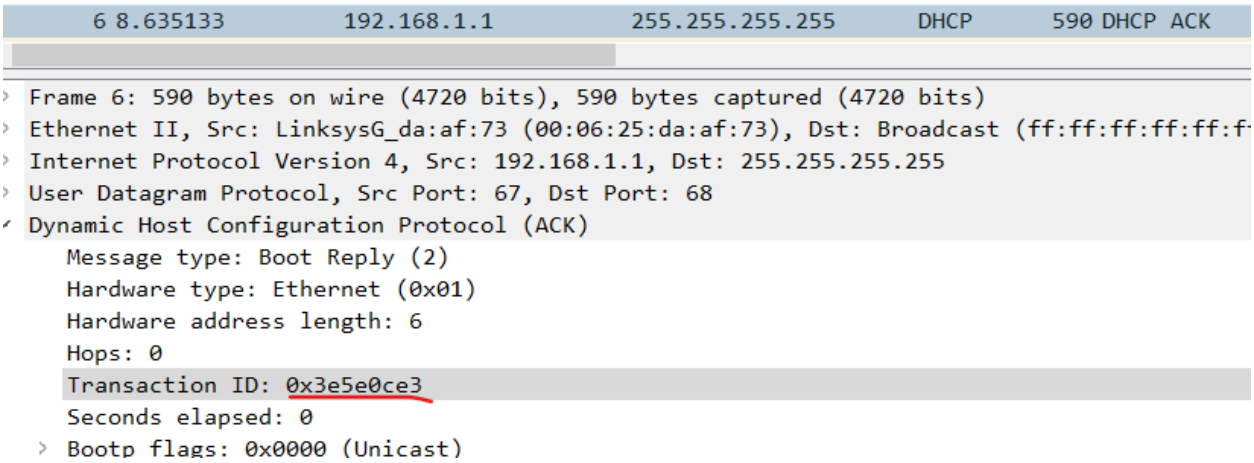
4. 

```
Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
```

From the above two images we can see the difference in the DHCP Message Type.

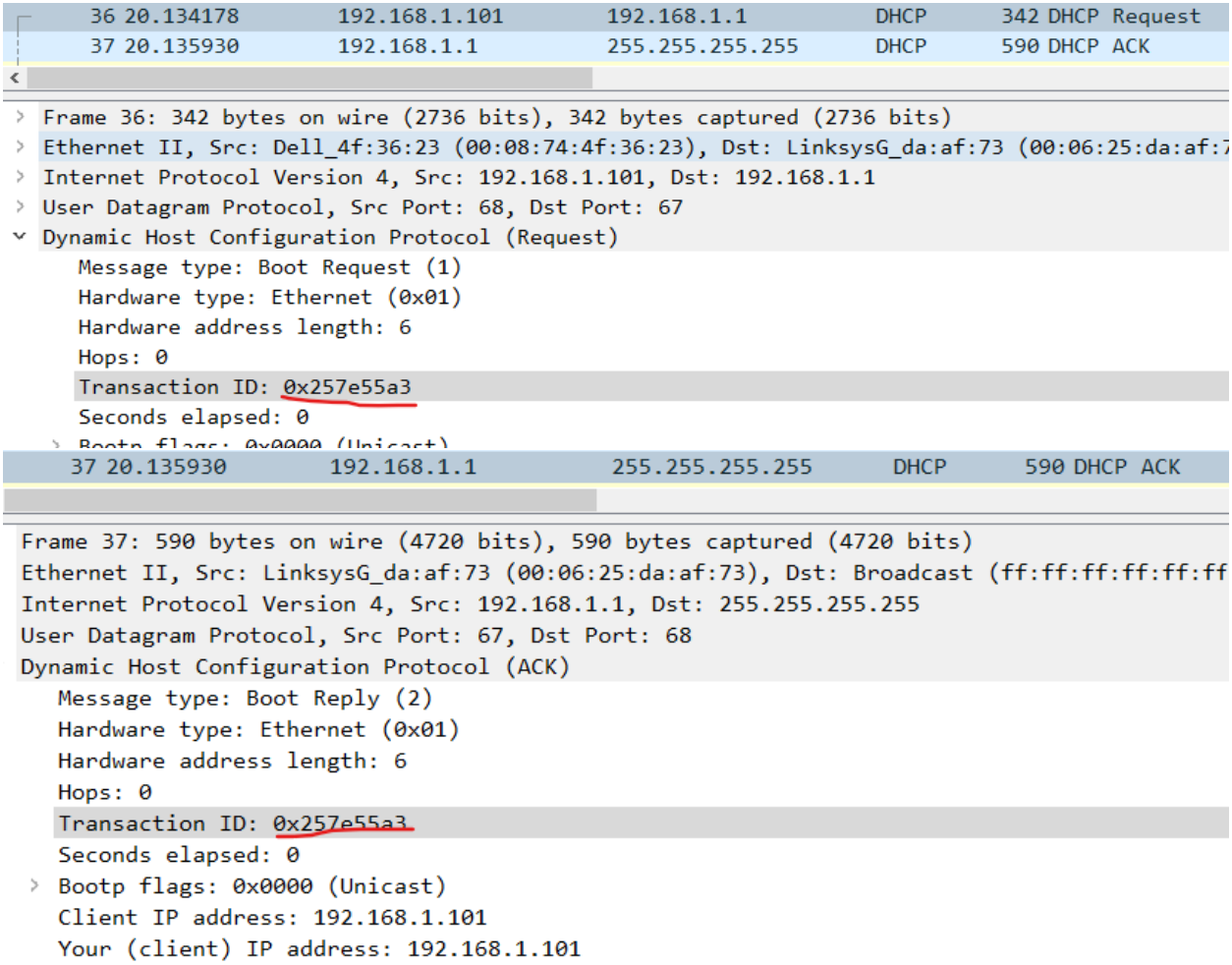
5. First Set





The value is 0x3e5e0ce3

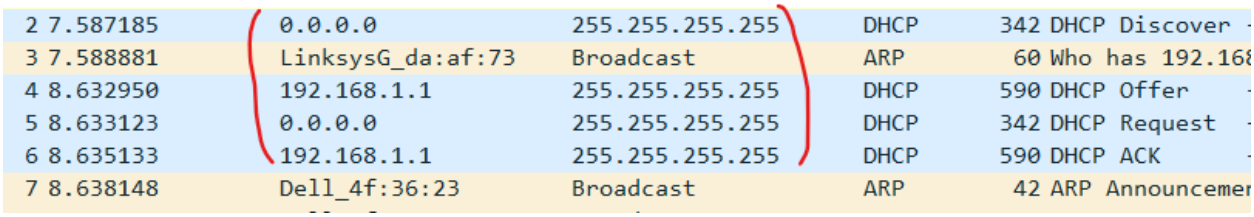
SECOND SET



The transcation ID of second set is 0x257e55a3

The purpose of the transaction ID is to identify if a message is part of a set of messages related to one transaction.

6.



2	7.587185	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover
3	7.588881	LinksysG_da:af:73	Broadcast	ARP	60 Who has 192.168
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK
7	8.638148	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcemer

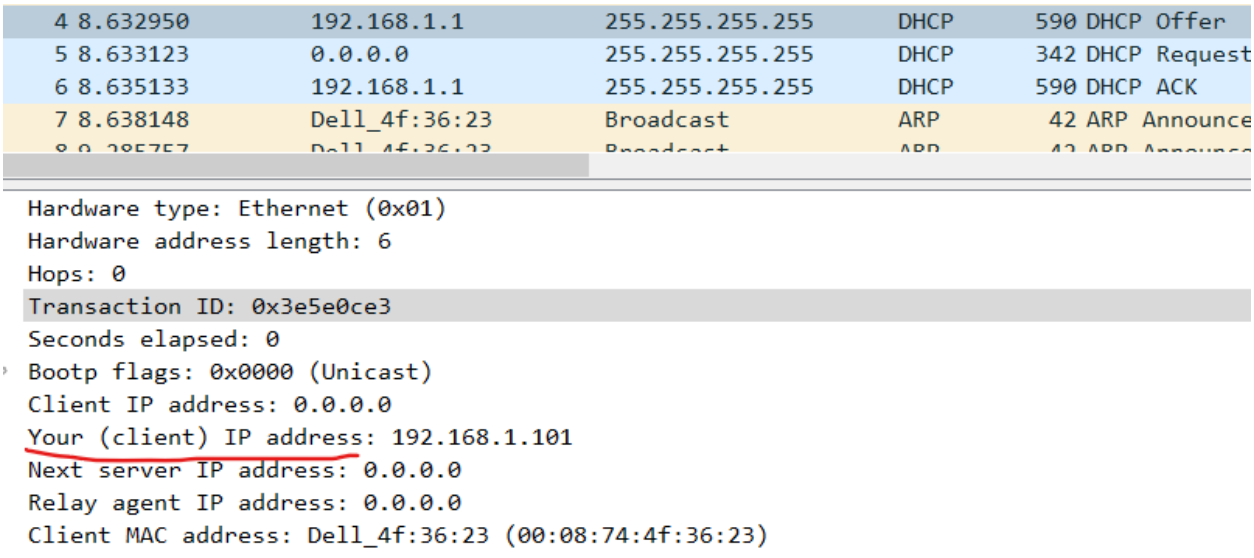
Discover -> Source 0.0.0.0 -> Destination 255.255.255.255

Offer -> Source 192.168.1.1 -> Destination 255.255.255.255

Request -> Source 0.0.0.0 -> Destination 255.255.255.255

ACK -> Source 192.168.1.1 -> Destination 255.255.255.255

7.



4	8.632950	192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK
7	8.638148	Dell_4f:36:23	Broadcast	ARP	42 ARP Announce

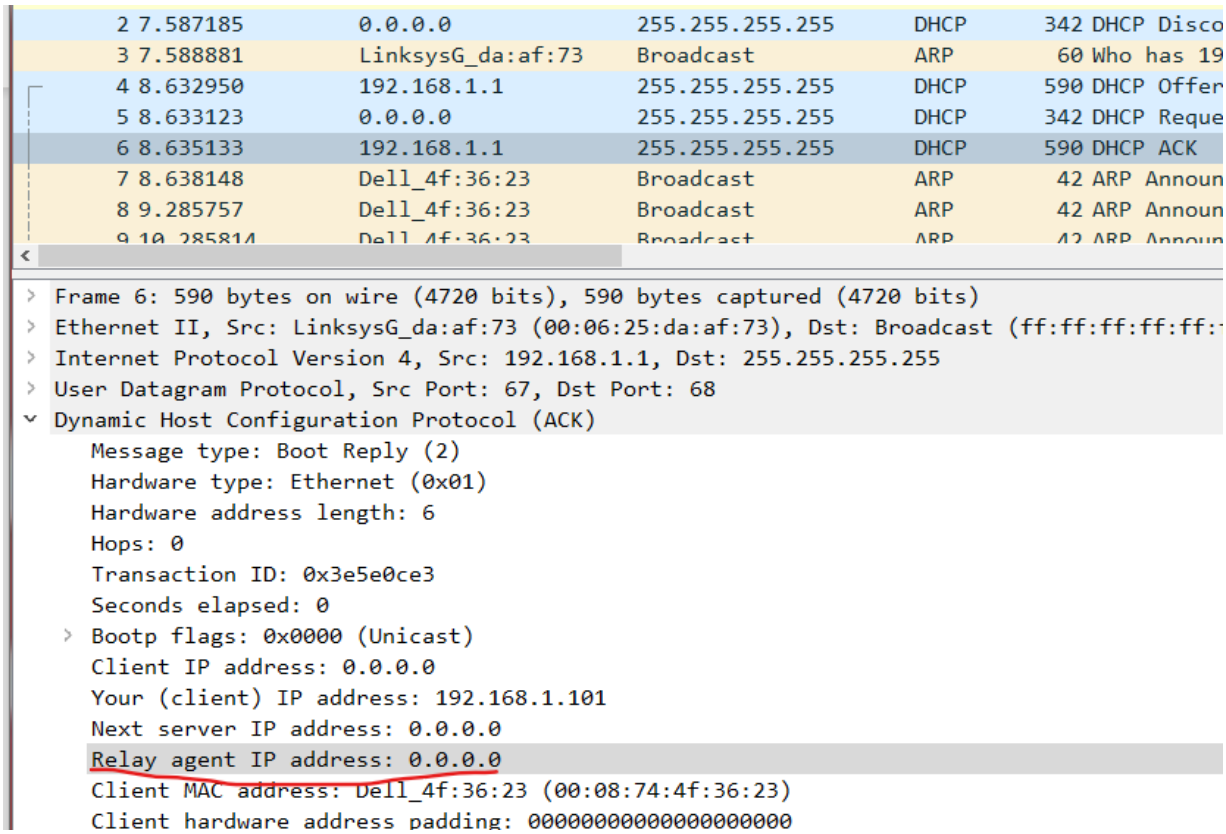
```
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x3e5e0ce3
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.101
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
```

The IP address is 192.168.1.1

8.

```
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x3e5e0ce3
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.101
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
v Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
v Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
v Option: (3) Router
    Length: 4
    Router: 192.168.1.1
v Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 63.240.76.19
    Domain Name Server: 204.127.198.19
v Option: (15) Domain Name
    Length: 22
    Domain Name: ne2.client2.attbi.com
v Option: (51) IP Address Lease Time
```

9.



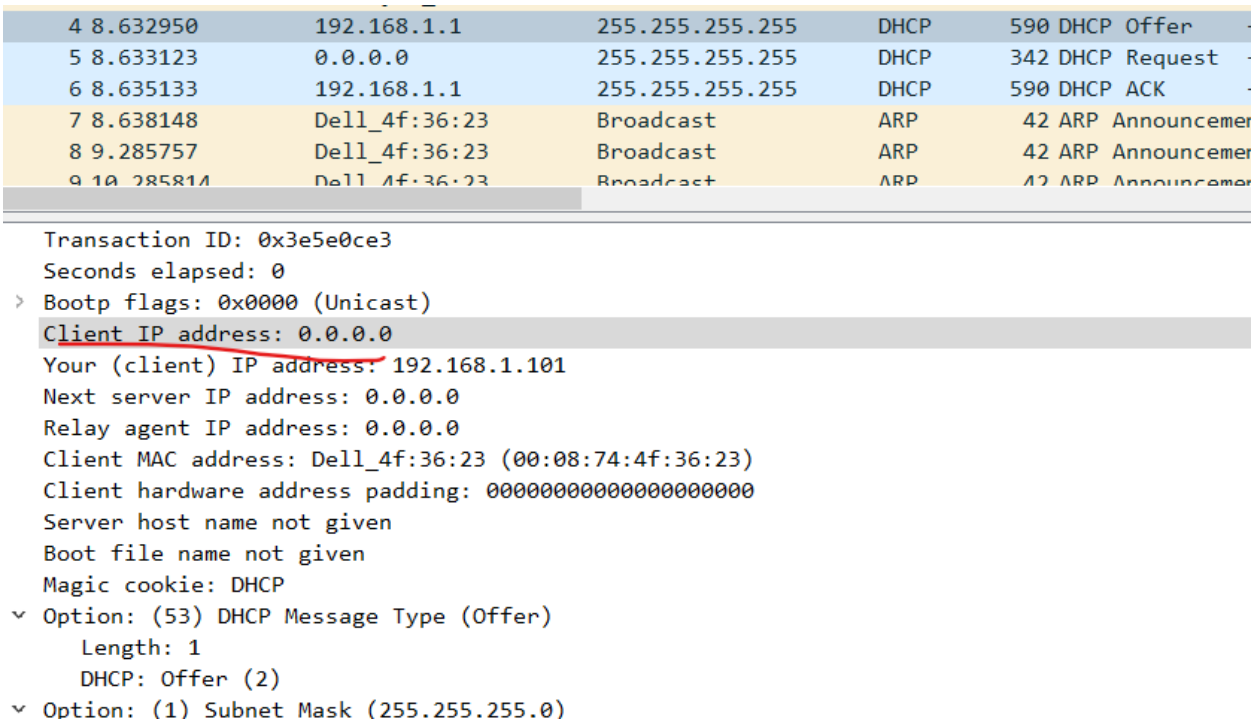
```
     2 7.587185    0.0.0.0           255.255.255.255   DHCP    342 DHCP Disco
     3 7.588881    LinksysG_da:af:73 Broadcast         ARP      60 Who has 19
     4 8.632950    192.168.1.1       255.255.255.255   DHCP    590 DHCP Offer
     5 8.633123    0.0.0.0           255.255.255.255   DHCP    342 DHCP Reque
     6 8.635133    192.168.1.1       255.255.255.255   DHCP    590 DHCP ACK
     7 8.638148    Dell_4f:36:23     Broadcast         ARP      42 ARP Announ
     8 9.285757    Dell_4f:36:23     Broadcast         ARP      42 ARP Announ
     9 10.285814   Dell_4f:36:23     Broadcast         ARP      42 ARP Announ

> Frame 6: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.101
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
    Client hardware address padding: 00000000000000000000
```

The IP address is 0.0.0.0

10. IP address for router help identify default internet gateway where as subnet mask line define the subnet that is available

```
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.101
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  v Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
  v Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
  v Option: (3) Router
      Length: 4
      Router: 192.168.1.1
  v Option: (6) Domain Name Server
      Length: 8
```

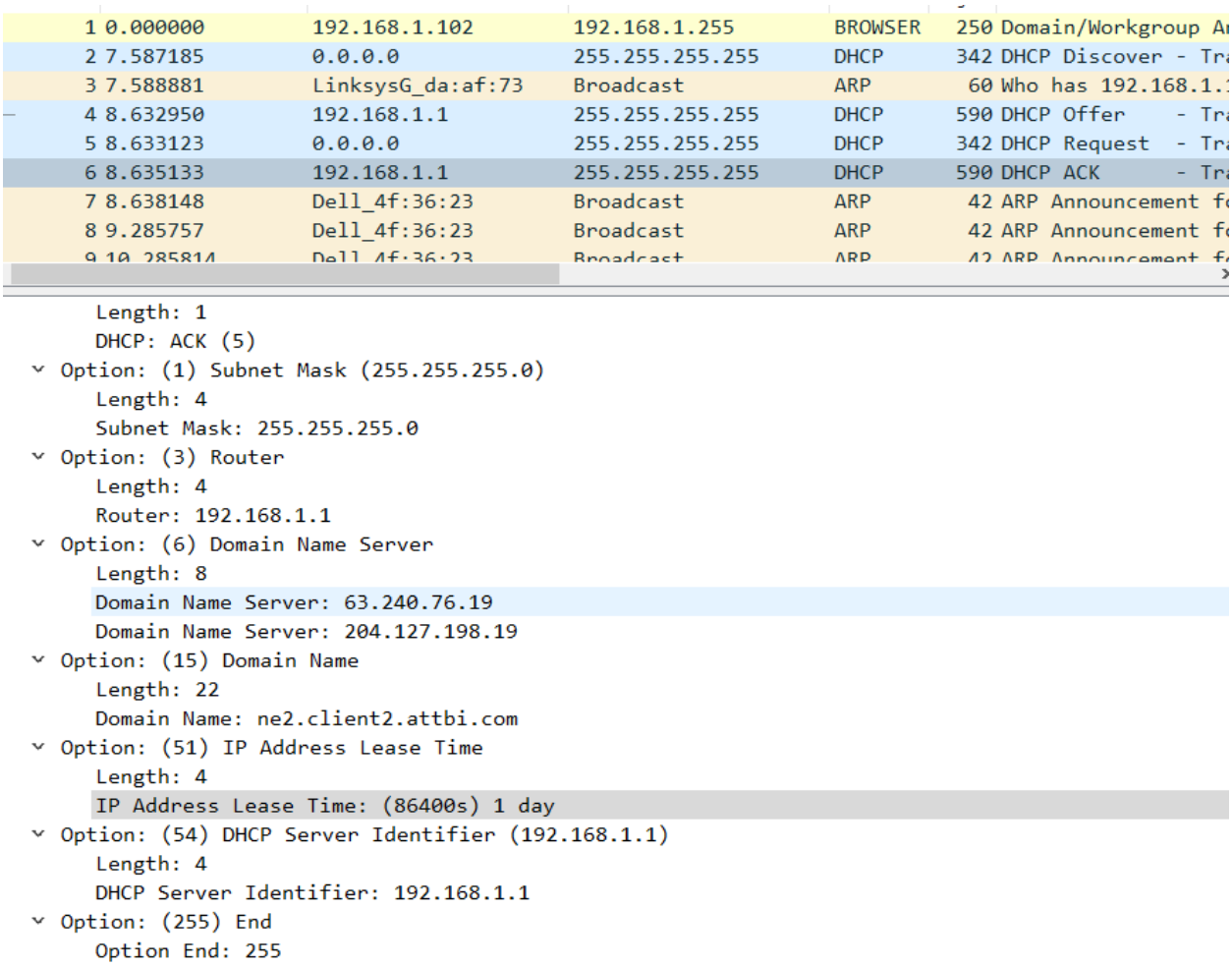
11.



4	8.632950	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK
7	8.638148	Dell_4f:36:23	Broadcast	ARP	42	ARP Announcemer
8	9.285757	Dell_4f:36:23	Broadcast	ARP	42	ARP Announcemer
9	10.285814	Dell_4f:36:23	Broadcast	ARP	42	ARP Announcemer

```
Transaction ID: 0x3e5e0ce3
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.101
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
v Option: (53) DHCP Message Type (Offer)
    Length: 1
    DHCP: Offer (2)
v Option: (1) Subnet Mask (255.255.255.0)
```

12.



1	0.000000	192.168.1.102	192.168.1.255	BROWSER	250 Domain/Workgroup A
2	7.587185	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Tr
3	7.588881	LinksysG_da:af:73	Broadcast	ARP	60 Who has 192.168.1.
4	8.632950	192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer - Tr
5	8.633123	0.0.0.0	255.255.255.255	DHCP	342 DHCP Request - Tr
6	8.635133	192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK - Tr
7	8.638148	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcement f
8	9.285757	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcement f
9	10.285814	Dell_4f:36:23	Broadcast	ARP	42 ARP Announcement f

```
    Length: 1
    DHCP: ACK (5)
  ⌄ Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
  ⌄ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
  ⌄ Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 63.240.76.19
    Domain Name Server: 204.127.198.19
  ⌄ Option: (15) Domain Name
    Length: 22
    Domain Name: ne2.client2.attbi.com
  ⌄ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
  ⌄ Option: (54) DHCP Server Identifier (192.168.1.1)
    Length: 4
    DHCP Server Identifier: 192.168.1.1
  ⌄ Option: (255) End
    Option End: 255
```

The lease time is 1 Day.
Purpose is amount of time the DHCP server assign an IP address to a client.

13. The DHCP release message tells the DHCP server that it wants to cancel the ip address offered. The DHCP doesn't issue an acknowledgment of receipt of the client's DHCP request. If the message is lost it (ip address) will just be there till the lease time expires.

14. Yes the ARP messages where sent during the DHCP packet exchange period. It asks if any of the machines are using that particular IP address.