**NAME**: S.PRIYADHARSHINI

**ROLL NO.:** CB.EN.P2CYS22010

**DATE:** 31.10.2022

# INTERNET PROTOCOL LAB – 5

## ANALYSING DHCP USING WIRESHARK

**AIM:**

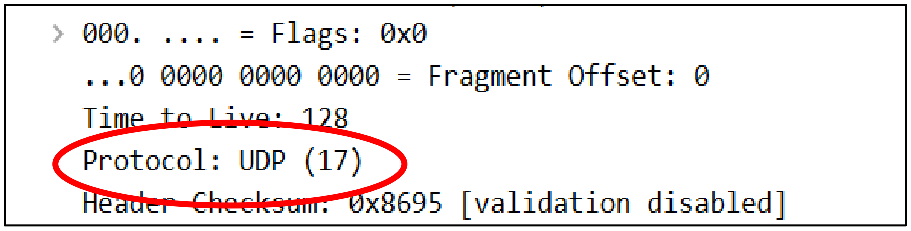
To analyze DHCP (Dynamic Host Configuration Protocol) using Wireshark.

**PROCEDURE:**

**1. Open the given pcap file "dhcp" in Wireshark to answer the following questions.**

**a) Are DHCP messages sent over UDP or TCP?**

DHCP messages are sent over UDP.



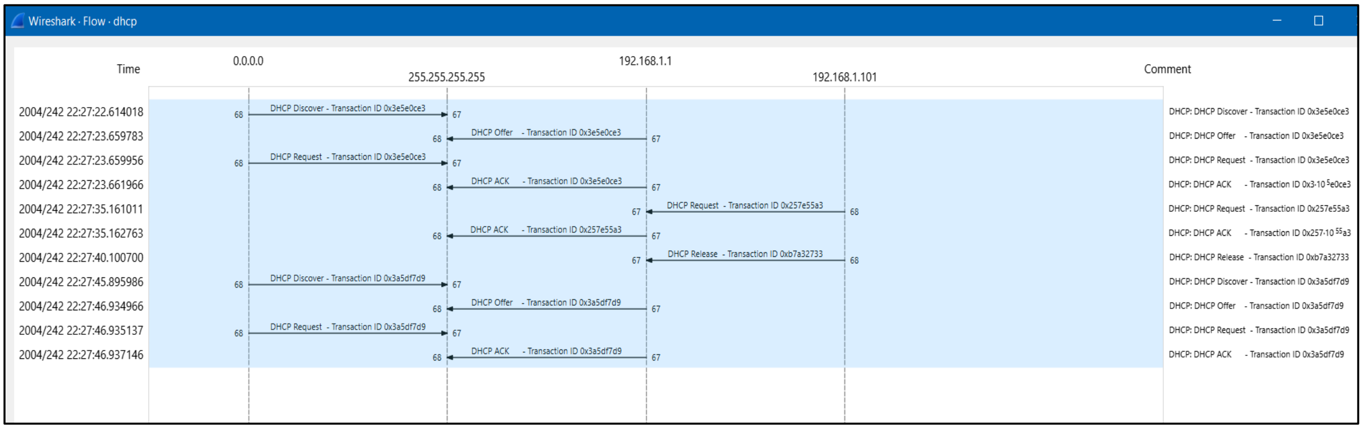
```
› 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: UDP (17)
  Header Checksum: 0x8695 [validation disabled]
```

**b) Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers.**

Statistics -> Flow graph  (choose limit to display filter to see dhcp only)

Discover, Request = source port – 68 , destination port – 67

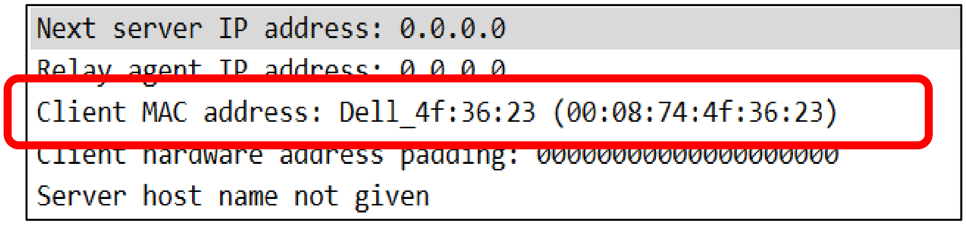
Offer, ACK = source port – 67 , destination port – 68



Wireshark · Flow · dhcp
0.0.0.0
255.255.255.255
192.168.1.1
192.168.1.101
68 DHCP Discover - Transaction ID 0x3e5e0ce3 67
68 DHCP Offer - Transaction ID 0x3e5e0ce3 67
68 DHCP Request - Transaction ID 0x3e5e0ce3 67
68 DHCP ACK - Transaction ID 0x3e5e0ce3 67
67 DHCP Request - Transaction ID 0x257e55a3 68
68 DHCP ACK - Transaction ID 0x257e55a3 67
67 DHCP Release - Transaction ID 0xb7a32733 68
68 DHCP Discover - Transaction ID 0x3a5df7d9 67
68 DHCP Offer - Transaction ID 0x3a5df7d9 67
68 DHCP Request - Transaction ID 0x3a5df7d9 67
68 DHCP ACK - Transaction ID 0x3a5df7d9 67

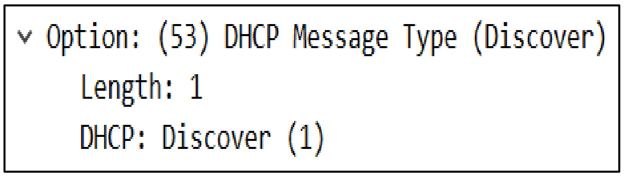
| Time | Comment |
|---|---|
| 2004/242 22:27:22.614018 | DHCP: DHCP Discover - Transaction ID 0x3e5e0ce3 |
| 2004/242 22:27:23.659783 | DHCP: DHCP Offer - Transaction ID 0x3e5e0ce3 |
| 2004/242 22:27:23.659956 | DHCP: DHCP Request - Transaction ID 0x3e5e0ce3 |
| 2004/242 22:27:23.661966 | DHCP: DHCP ACK - Transaction ID 0x3·10$^{5}$e0ce3 |
| 2004/242 22:27:35.161011 | DHCP: DHCP Request - Transaction ID 0x257e55a3 |
| 2004/242 22:27:35.162763 | DHCP: DHCP ACK - Transaction ID 0x257·10$^{55}$a3 |
| 2004/242 22:27:40.100700 | DHCP: DHCP Release - Transaction ID 0xb7a32733 |
| 2004/242 22:27:45.895986 | DHCP: DHCP Discover - Transaction ID 0x3a5df7d9 |
| 2004/242 22:27:46.934966 | DHCP: DHCP Offer - Transaction ID 0x3a5df7d9 |
| 2004/242 22:27:46.935137 | DHCP: DHCP Request - Transaction ID 0x3a5df7d9 |
| 2004/242 22:27:46.937146 | DHCP: DHCP ACK - Transaction ID 0x3a5df7d9 |

**c) What is the link-layer (e.g., Ethernet) address of your host?**

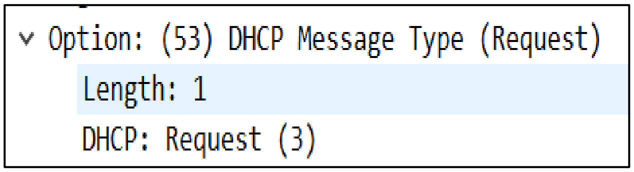


```
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)
Client hardware address padding: 00000000000000000000
Server host name not given
```

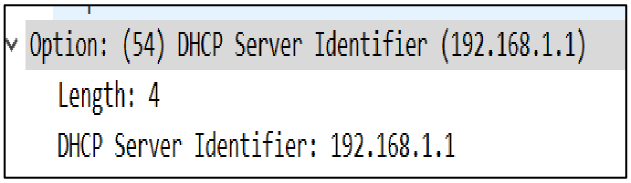
**d) What values in the DHCP discover message differentiate this message from the DHCP request message?**



```
v Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
```



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

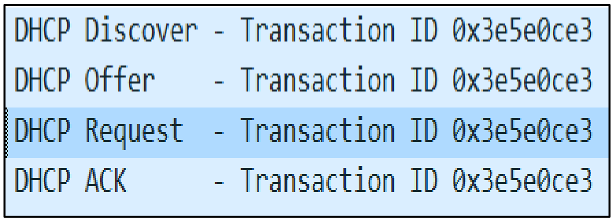


```
v Option: (54) DHCP Server Identifier (192.168.1.1)
    Length: 4
    DHCP Server Identifier: 192.168.1.1
```

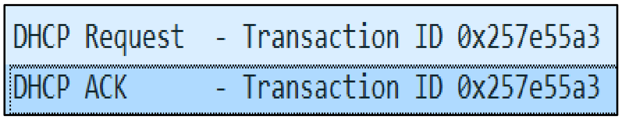
The difference is the DHCP Message Type and DHCP Server Identifier.

**e) What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?**

The transaction ID is different for a set of DHCP messages so that it will be easy to differentiate between different requests made by the user.

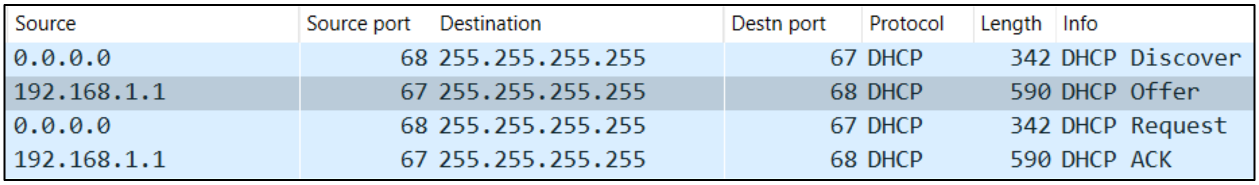


```
DHCP Discover - Transaction ID 0x3e5e0ce3
DHCP Offer    - Transaction ID 0x3e5e0ce3
DHCP Request  - Transaction ID 0x3e5e0ce3
DHCP ACK      - Transaction ID 0x3e5e0ce3
```



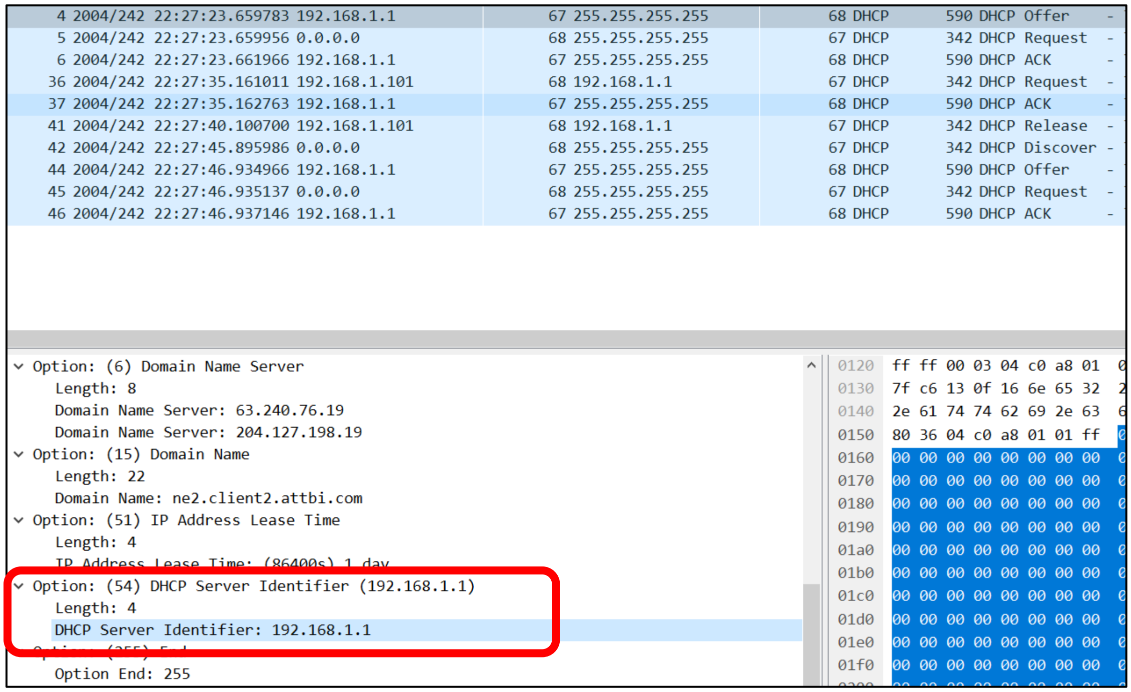
```
DHCP Request  - Transaction ID 0x257e55a3
DHCP ACK      - Transaction ID 0x257e55a3
```

**f) A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.**



| Source | Source port | Destination | Destn port | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 0.0.0.0 | 68 | 255.255.255.255 | 67 | DHCP | 342 | DHCP Discover |
| 192.168.1.1 | 67 | 255.255.255.255 | 68 | DHCP | 590 | DHCP Offer |
| 0.0.0.0 | 68 | 255.255.255.255 | 67 | DHCP | 342 | DHCP Request |
| 192.168.1.1 | 67 | 255.255.255.255 | 68 | DHCP | 590 | DHCP ACK |

## g) What is the IP address of your DHCP server?

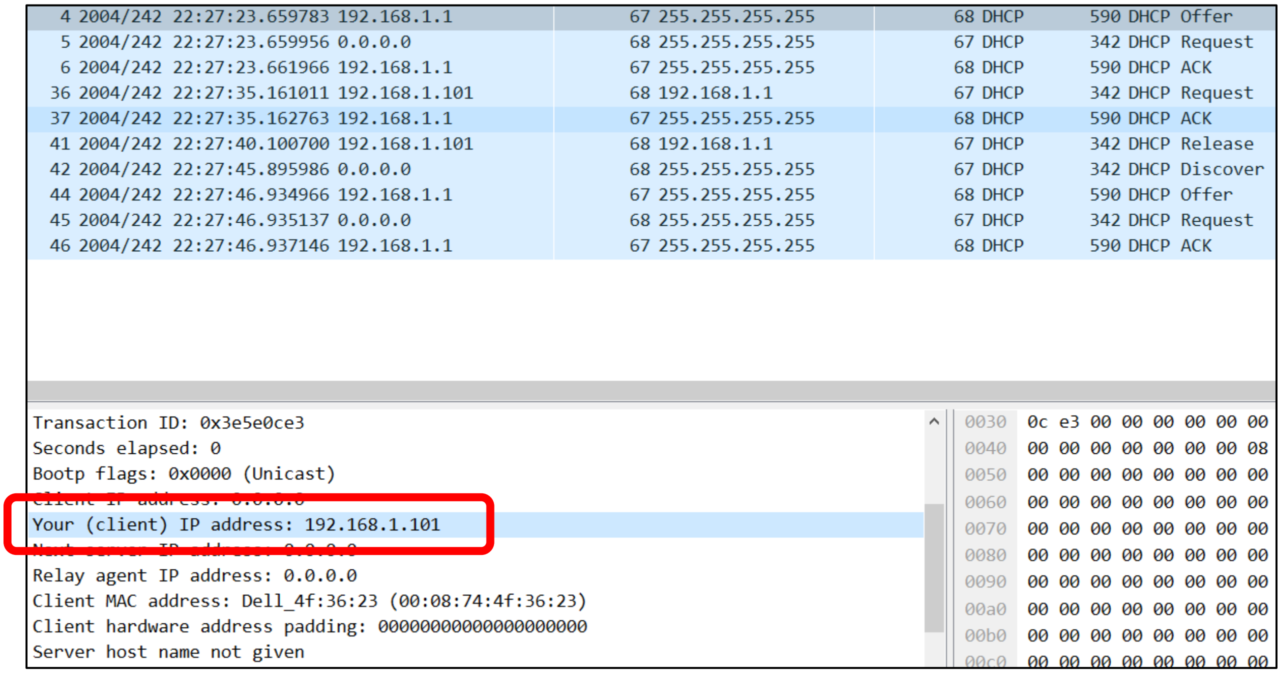


```
 4 2004/242 22:27:23.659783 192.168.1.1     67 255.255.255.255    68 DHCP    590 DHCP Offer    -
 5 2004/242 22:27:23.659956 0.0.0.0         68 255.255.255.255    67 DHCP    342 DHCP Request  -
 6 2004/242 22:27:23.661966 192.168.1.1     67 255.255.255.255    68 DHCP    590 DHCP ACK      -
36 2004/242 22:27:35.161011 192.168.1.101   68 192.168.1.1        67 DHCP    342 DHCP Request  -
37 2004/242 22:27:35.162763 192.168.1.1     67 255.255.255.255    68 DHCP    590 DHCP ACK      -
41 2004/242 22:27:40.100700 192.168.1.101   68 192.168.1.1        67 DHCP    342 DHCP Release  -
42 2004/242 22:27:45.895986 0.0.0.0         68 255.255.255.255    67 DHCP    342 DHCP Discover -
44 2004/242 22:27:46.934966 192.168.1.1     67 255.255.255.255    68 DHCP    590 DHCP Offer    -
45 2004/242 22:27:46.935137 0.0.0.0         68 255.255.255.255    67 DHCP    342 DHCP Request  -
46 2004/242 22:27:46.937146 192.168.1.1     67 255.255.255.255    68 DHCP    590 DHCP ACK      -
```

```
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
    Length: 4
    IP Address Lease Time: (86400s) 1 day
v Option: (54) DHCP Server Identifier (192.168.1.1)
    Length: 4
    DHCP Server Identifier: 192.168.1.1
  Option: (255) End
    Option End: 255
```

```
0120  ff ff 00 03 04 c0 a8 01  0
0130  7f c6 13 0f 16 6e 65 32  2
0140  2e 61 74 74 62 69 2e 63  6
0150  80 36 04 c0 a8 01 01 ff  0
0160  00 00 00 00 00 00 00 00  0
0170  00 00 00 00 00 00 00 00  0
0180  00 00 00 00 00 00 00 00  0
0190  00 00 00 00 00 00 00 00  0
01a0  00 00 00 00 00 00 00 00  0
01b0  00 00 00 00 00 00 00 00  0
01c0  00 00 00 00 00 00 00 00  0
01d0  00 00 00 00 00 00 00 00  0
01e0  00 00 00 00 00 00 00 00  0
01f0  00 00 00 00 00 00 00 00  0
```

**h) What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.**

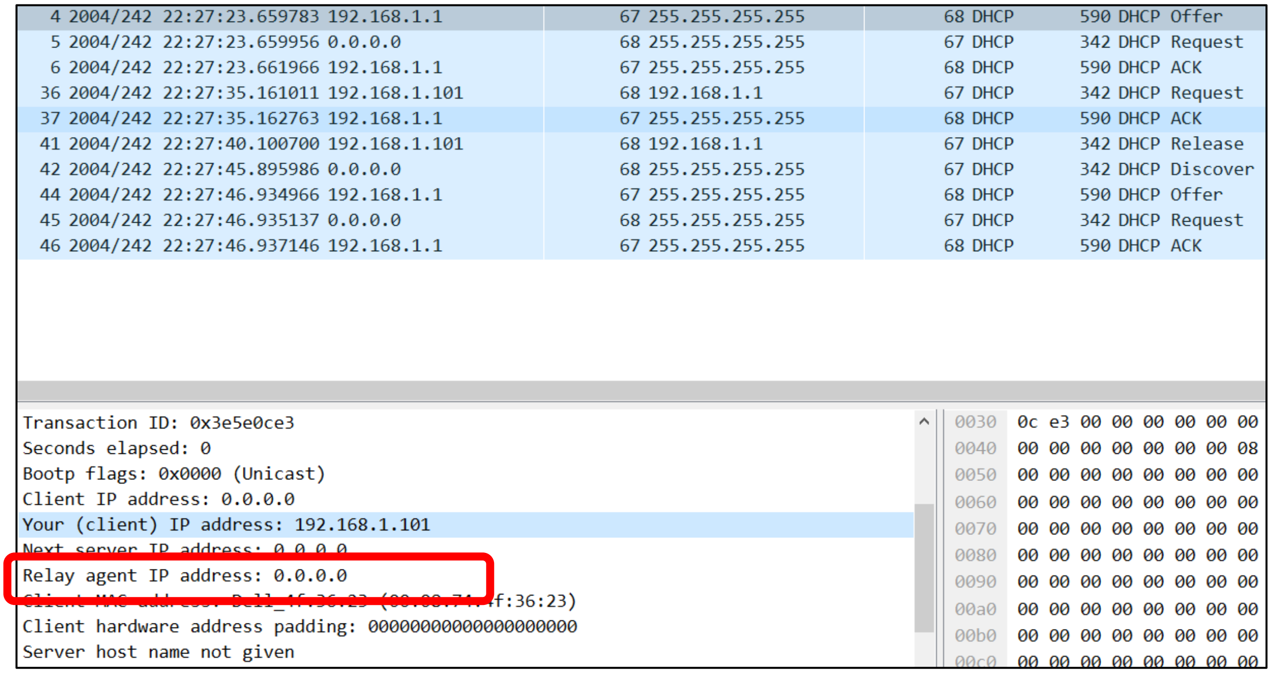


```
 4 2004/242 22:27:23.659783 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP Offer
 5 2004/242 22:27:23.659956 0.0.0.0          68 255.255.255.255    67 DHCP    342 DHCP Request
 6 2004/242 22:27:23.661966 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP ACK
36 2004/242 22:27:35.161011 192.168.1.101    68 192.168.1.1        67 DHCP    342 DHCP Request
37 2004/242 22:27:35.162763 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP ACK
41 2004/242 22:27:40.100700 192.168.1.101    68 192.168.1.1        67 DHCP    342 DHCP Release
42 2004/242 22:27:45.895986 0.0.0.0          68 255.255.255.255    67 DHCP    342 DHCP Discover
44 2004/242 22:27:46.934966 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP Offer
45 2004/242 22:27:46.935137 0.0.0.0          68 255.255.255.255    67 DHCP    342 DHCP Request
46 2004/242 22:27:46.937146 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP ACK
```

```
Transaction ID: 0x3e5e0ce3                              0030  0c e3 00 00 00 00 00 00
Seconds elapsed: 0                                      0040  00 00 00 00 00 00 00 08
Bootp flags: 0x0000 (Unicast)                           0050  00 00 00 00 00 00 00 00
Client IP address: 0.0.0.0                              0060  00 00 00 00 00 00 00 00
Your (client) IP address: 192.168.1.101                 0070  00 00 00 00 00 00 00 00
Next server IP address: 0.0.0.0                         0080  00 00 00 00 00 00 00 00
Relay agent IP address: 0.0.0.0                         0090  00 00 00 00 00 00 00 00
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)   00a0  00 00 00 00 00 00 00 00
Client hardware address padding: 00000000000000000000   00b0  00 00 00 00 00 00 00 00
Server host name not given                              00c0  00 00 00 00 00 00 00 00
```

**i)In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?**

In this experiment there is no relay agent (0.0.0.0).



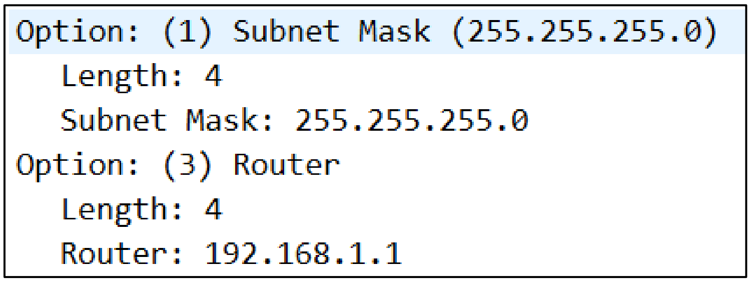
```
 4 2004/242 22:27:23.659783 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP Offer
 5 2004/242 22:27:23.659956 0.0.0.0          68 255.255.255.255    67 DHCP    342 DHCP Request
 6 2004/242 22:27:23.661966 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP ACK
36 2004/242 22:27:35.161011 192.168.1.101    68 192.168.1.1        67 DHCP    342 DHCP Request
37 2004/242 22:27:35.162763 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP ACK
41 2004/242 22:27:40.100700 192.168.1.101    68 192.168.1.1        67 DHCP    342 DHCP Release
42 2004/242 22:27:45.895986 0.0.0.0          68 255.255.255.255    67 DHCP    342 DHCP Discover
44 2004/242 22:27:46.934966 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP Offer
45 2004/242 22:27:46.935137 0.0.0.0          68 255.255.255.255    67 DHCP    342 DHCP Request
46 2004/242 22:27:46.937146 192.168.1.1      67 255.255.255.255    68 DHCP    590 DHCP ACK
```

```
Transaction ID: 0x3e5e0ce3                              0030  0c e3 00 00 00 00 00 00
Seconds elapsed: 0                                      0040  00 00 00 00 00 00 00 08
Bootp flags: 0x0000 (Unicast)                           0050  00 00 00 00 00 00 00 00
Client IP address: 0.0.0.0                              0060  00 00 00 00 00 00 00 00
Your (client) IP address: 192.168.1.101                 0070  00 00 00 00 00 00 00 00
Next server IP address: 0.0.0.0                         0080  00 00 00 00 00 00 00 00
Relay agent IP address: 0.0.0.0                         0090  00 00 00 00 00 00 00 00
Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)   00a0  00 00 00 00 00 00 00 00
Client hardware address padding: 00000000000000000000   00b0  00 00 00 00 00 00 00 00
Server host name not given                              00c0  00 00 00 00 00 00 00 00
```

**j) Explain the purpose of the router and subnet mask lines in the DHCP offer message.**

**Router:**

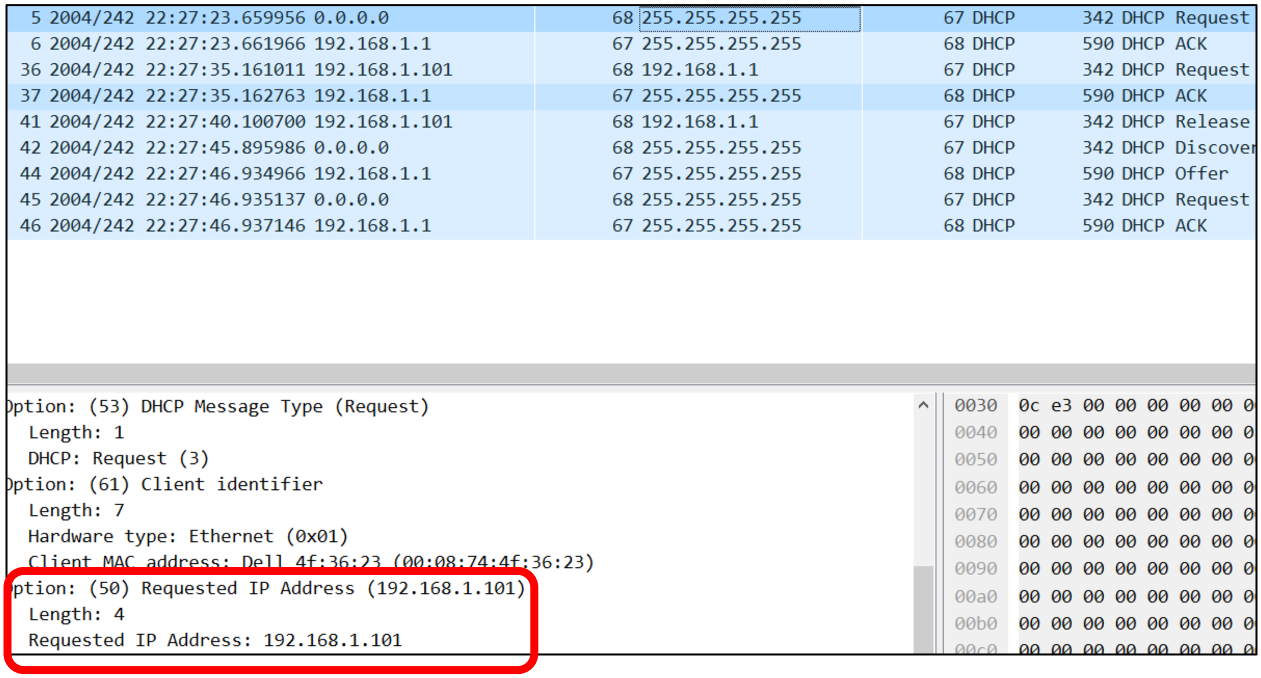
**Subnet mask:**



```
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
```

**k) In the DHCP trace file, the DHCP server offers a specific IP address to the client. In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?**

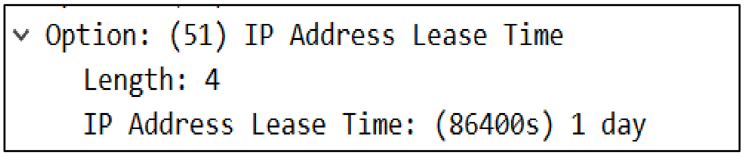
We can see that the client accepted the ip address (192.168.1.101) given from OFFER message. The client sent back REQUEST message with the same ip as the requested ip address (192.168.1.101).



```
 5 2004/242 22:27:23.659956 0.0.0.0         68 255.255.255.255   67 DHCP   342 DHCP Request
 6 2004/242 22:27:23.661966 192.168.1.1     67 255.255.255.255   68 DHCP   590 DHCP ACK
36 2004/242 22:27:35.161011 192.168.1.101   68 192.168.1.1       67 DHCP   342 DHCP Request
37 2004/242 22:27:35.162763 192.168.1.1     67 255.255.255.255   68 DHCP   590 DHCP ACK
41 2004/242 22:27:40.100700 192.168.1.101   68 192.168.1.1       67 DHCP   342 DHCP Release
42 2004/242 22:27:45.895986 0.0.0.0         68 255.255.255.255   67 DHCP   342 DHCP Discover
44 2004/242 22:27:46.934966 192.168.1.1     67 255.255.255.255   68 DHCP   590 DHCP Offer
45 2004/242 22:27:46.935137 0.0.0.0         68 255.255.255.255   67 DHCP   342 DHCP Request
46 2004/242 22:27:46.937146 192.168.1.1     67 255.255.255.255   68 DHCP   590 DHCP ACK
```

```
Option: (53) DHCP Message Type (Request)                  0030  0c e3 00 00 00 00 00 0
  Length: 1                                               0040  00 00 00 00 00 00 00 0
  DHCP: Request (3)                                       0050  00 00 00 00 00 00 00 0
Option: (61) Client identifier                            0060  00 00 00 00 00 00 00 0
  Length: 7                                               0070  00 00 00 00 00 00 00 0
  Hardware type: Ethernet (0x01)                          0080  00 00 00 00 00 00 00 0
  Client MAC address: Dell_4f:36:23 (00:08:74:4f:36:23)   0090  00 00 00 00 00 00 00 0
ption: (50) Requested IP Address (192.168.1.101)          00a0  00 00 00 00 00 00 00 0
  Length: 4                                               00b0  00 00 00 00 00 00 00 0
  Requested IP Address: 192.168.1.101                     00c0  00 00 00 00 00 00 00 0
```

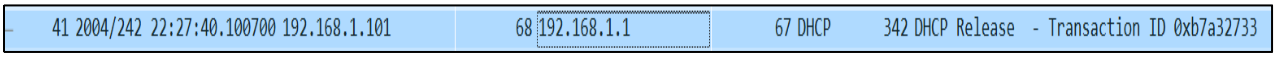
**l) Explain the purpose of the lease time. How long is the lease time in your experiment?**



```
v Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (86400s) 1 day
```

The lease time refers that the particular ip address is assigned to the particular client to only a specific period of time. Here it is 1 day.

**m) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?**

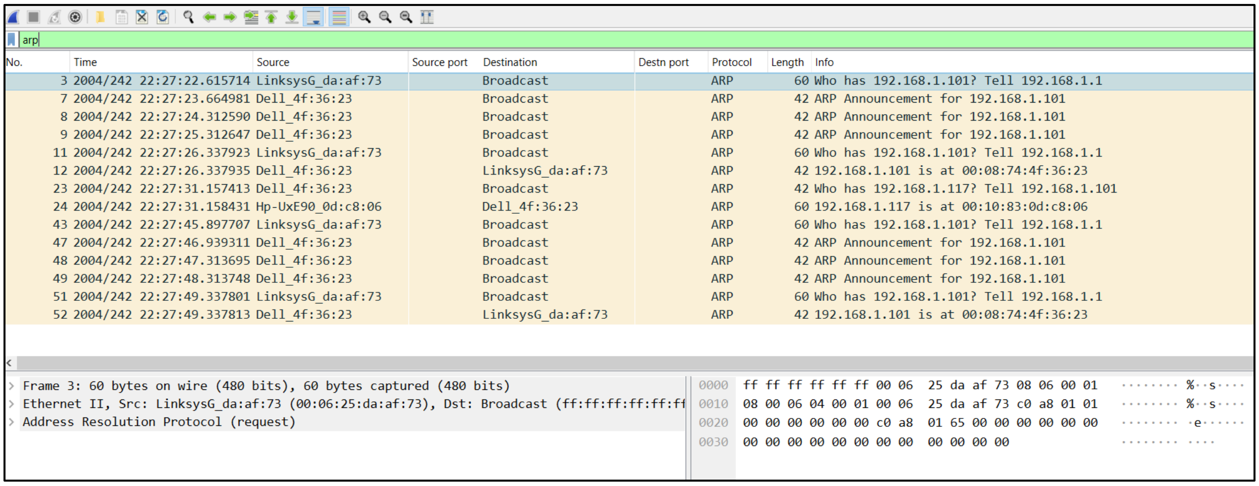


```
41 2004/242 22:27:40.100700 192.168.1.101    68 192.168.1.1    67 DHCP    342 DHCP Release  - Transaction ID 0xb7a32733
```

A DHCP Release message is sent by a DHCP client to release the IP address back to the server. If the client's DHCP release message is lost then the server will have to wait until the lease time is over in order to reassign that IP.

**n) Clear the DHCP filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.**

There were ARP packets sent and received during DHCP packet-exchange period. to check whether a particular IP address to be allocated to a system is assigned previously or not.



arp

| No. | Time | Source | Source port | Destination | Destn port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|
| 3 | 2004/242 22:27:22.615714 | LinksysG_da:af:73 | | Broadcast | | ARP | 60 | Who has 192.168.1.101? Tell 192.168.1.1 |
| 7 | 2004/242 22:27:23.664981 | Dell_4f:36:23 | | Broadcast | | ARP | 42 | ARP Announcement for 192.168.1.101 |
| 8 | 2004/242 22:27:24.312590 | Dell_4f:36:23 | | Broadcast | | ARP | 42 | ARP Announcement for 192.168.1.101 |
| 9 | 2004/242 22:27:25.312647 | Dell_4f:36:23 | | Broadcast | | ARP | 42 | ARP Announcement for 192.168.1.101 |
| 11 | 2004/242 22:27:26.337923 | LinksysG_da:af:73 | | Broadcast | | ARP | 60 | Who has 192.168.1.101? Tell 192.168.1.1 |
| 12 | 2004/242 22:27:26.337935 | Dell_4f:36:23 | | LinksysG_da:af:73 | | ARP | 42 | 192.168.1.101 is at 00:08:74:4f:36:23 |
| 23 | 2004/242 22:27:31.157413 | Dell_4f:36:23 | | Broadcast | | ARP | 42 | Who has 192.168.1.117? Tell 192.168.1.101 |
| 24 | 2004/242 22:27:31.158431 | Hp-UxE90_0d:c8:06 | | Dell_4f:36:23 | | ARP | 60 | 192.168.1.117 is at 00:10:83:0d:c8:06 |
| 43 | 2004/242 22:27:45.897707 | LinksysG_da:af:73 | | Broadcast | | ARP | 60 | Who has 192.168.1.101? Tell 192.168.1.1 |
| 47 | 2004/242 22:27:46.939311 | Dell_4f:36:23 | | Broadcast | | ARP | 42 | ARP Announcement for 192.168.1.101 |
| 48 | 2004/242 22:27:47.313695 | Dell_4f:36:23 | | Broadcast | | ARP | 42 | ARP Announcement for 192.168.1.101 |
| 49 | 2004/242 22:27:48.313748 | Dell_4f:36:23 | | Broadcast | | ARP | 42 | ARP Announcement for 192.168.1.101 |
| 51 | 2004/242 22:27:49.337801 | LinksysG_da:af:73 | | Broadcast | | ARP | 60 | Who has 192.168.1.101? Tell 192.168.1.1 |
| 52 | 2004/242 22:27:49.337813 | Dell_4f:36:23 | | LinksysG_da:af:73 | | ARP | 42 | 192.168.1.101 is at 00:08:74:4f:36:23 |

```
> Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 06  25 da af 73 08 06 00 01   ········ %··s····
0010  08 00 06 04 00 01 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 00 00 00 00 00 c0 a8  01 65 00 00 00 00 00 00   ········ ·e······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

**RESULT:**

Thus, DHCP protocols have been analyzed successfully using Wireshark.