Lab 8 DHCP

Colin Monroe

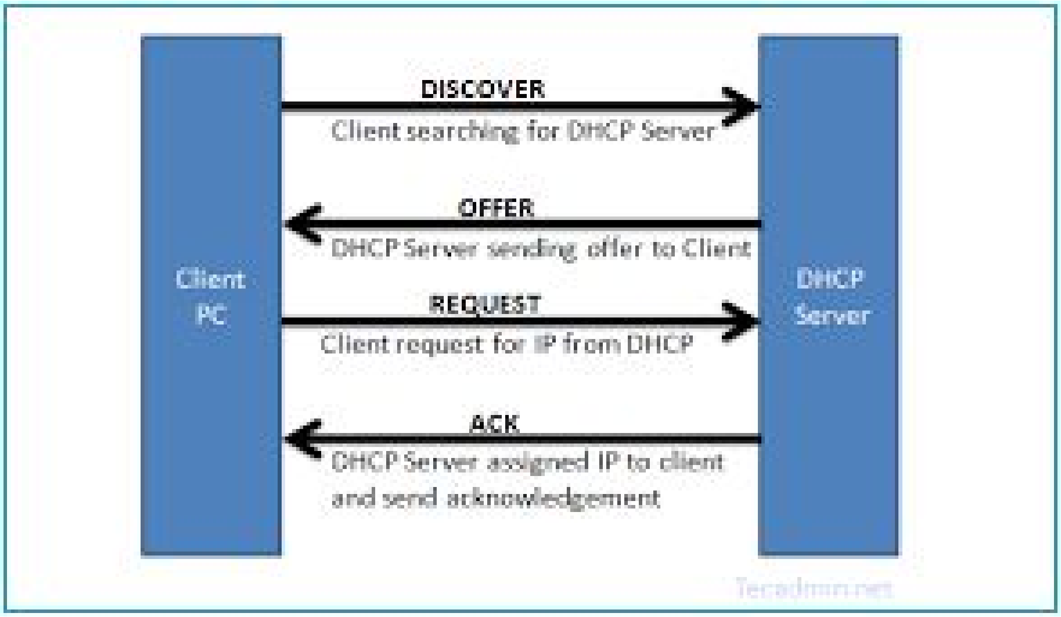
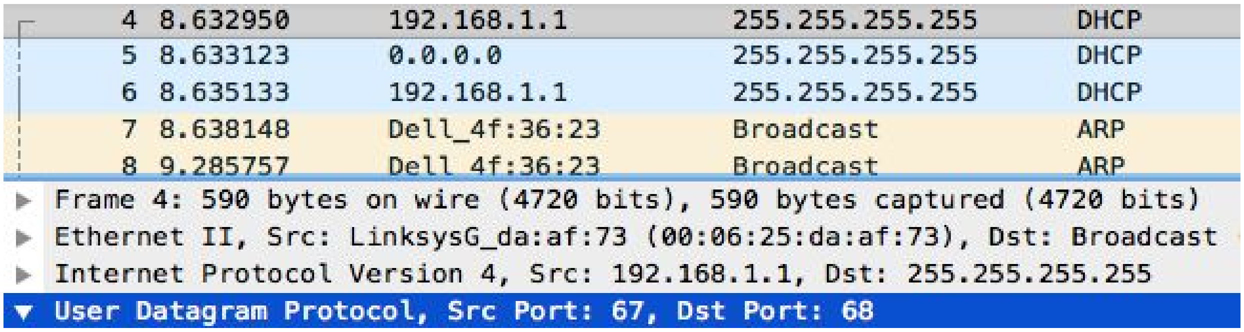

DISCOVER
Client searching for DHCP Server
OFFER
DHCP Server sending offer to Client
Client PC
DHCP Server
REQUEST
Client request for IP from DHCP
ACK
DHCP Server assigned IP to client and send acknowledgement
Tecadmin.net

Table of Contents:

I was unable to capture my own packets as I was doing it at school and the lab was not available. So I used the provided trace file to complete the assignment with the time I had available.

1. **Are DHCP messages sent over UDP or TCP?**



```
    4 8.632950      192.168.1.1        255.255.255.255     DHCP
    5 8.633123      0.0.0.0            255.255.255.255     DHCP
    6 8.635133      192.168.1.1        255.255.255.255     DHCP
    7 8.638148      Dell_4f:36:23      Broadcast           ARP
    8 9.285757      Dell_4f:36:23      Broadcast           ARP
▶ Frame 4: 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
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
▼ User Datagram Protocol, Src Port: 67, Dst Port: 68
```

Figure 1.

The Dynamic Host Protocol (DCHP) messages are sent over User Datagram Protocol (UDP) as shown in the above picture.

2. **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. Are the port numbers the same as in the example given in this lab assignment?**

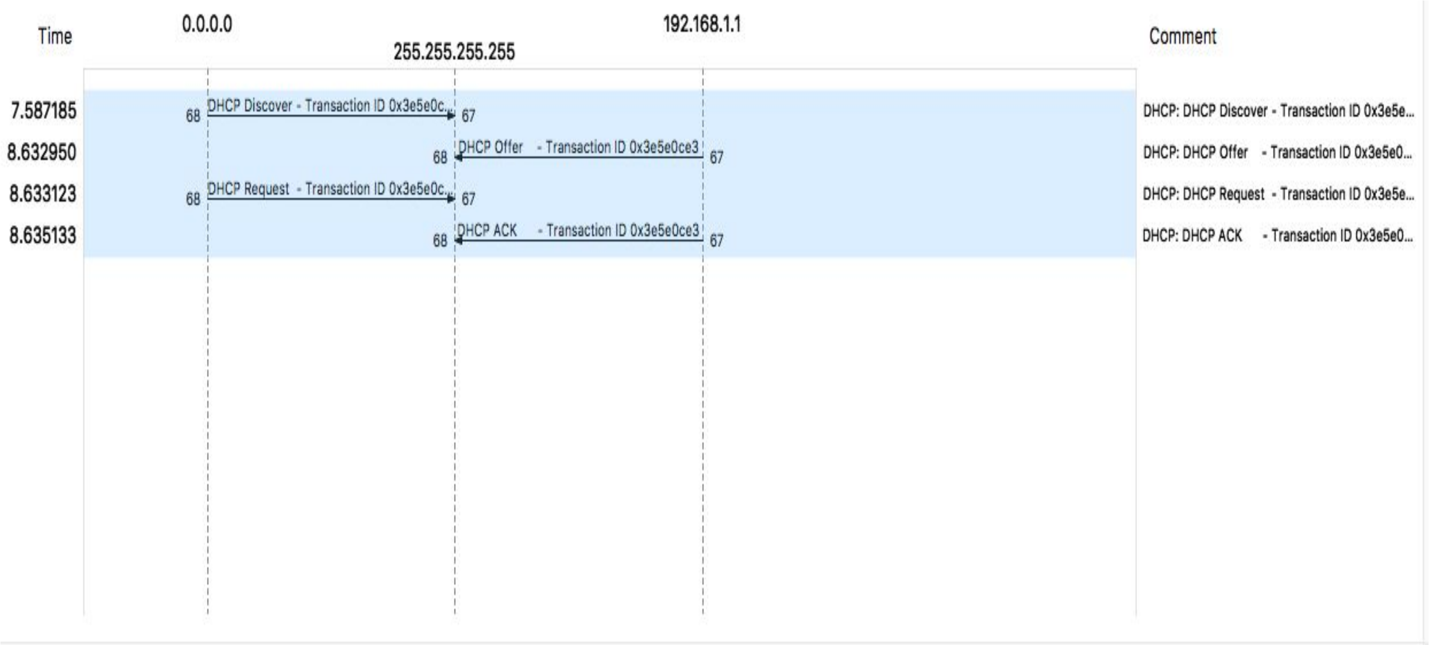
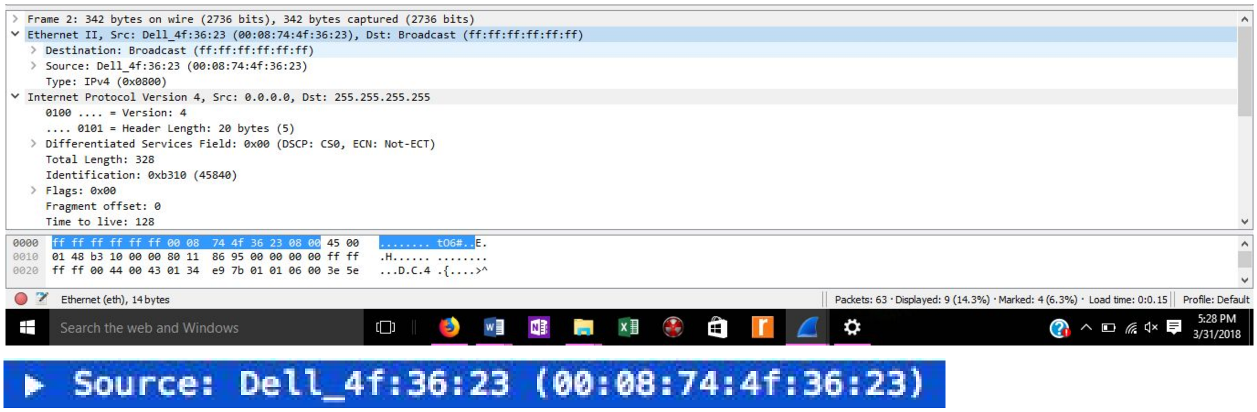

Time
0.0.0.0
255.255.255.255
192.168.1.1
Comment
7.587185
68
DHCP Discover - Transaction ID 0x3e5e0c...
67
DHCP: DHCP Discover - Transaction ID 0x3e5e...
8.632950
68
DHCP Offer - Transaction ID 0x3e5e0ce3
67
DHCP: DHCP Offer - Transaction ID 0x3e5e0...
8.633123
68
DHCP Request - Transaction ID 0x3e5e0c...
67
DHCP: DHCP Request - Transaction ID 0x3e5e...
8.635133
68
DHCP ACK - Transaction ID 0x3e5e0ce3
67
DHCP: DHCP ACK - Transaction ID 0x3e5e0...

Figure 2.

The port numbers are same as in the given example in this lab. This is due to the fact that they are both using the default UDP ports of 67 and 68 for DHCP.

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



```
> Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
v Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Dell_4f:36:23 (00:08:74:4f:36:23)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xb310 (45840)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128

0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 00 45 00   ........ tO6#..E.
0010  01 48 b3 10 00 00 80 11  86 95 00 00 00 00 ff ff   .H...... ........
0020  ff ff 00 44 00 43 01 34  e9 7b 01 01 06 00 3e 5e   ...D.C.4 .{....>^
```

Ethernet (eth), 14 bytes
Packets: 63 · Displayed: 9 (14.3%) · Marked: 4 (6.3%) · Load time: 0:0.15
Profile: Default
Search the web and Windows
5:28 PM
3/31/2018

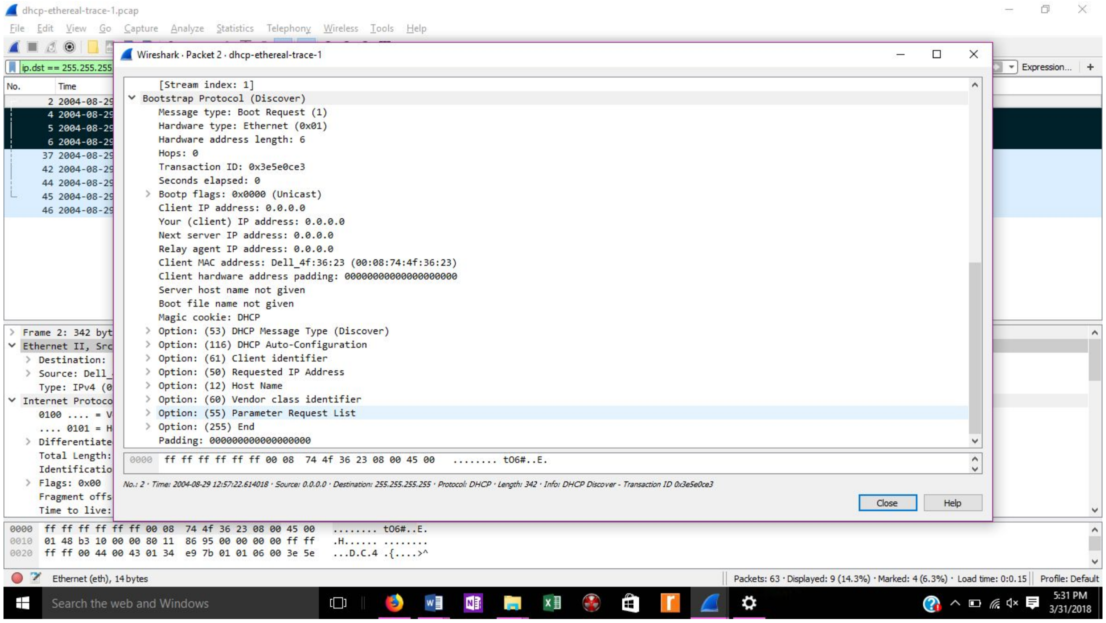
```
▶ Source: Dell_4f:36:23 (00:08:74:4f:36:23)
```

Figure 3.

The Link-layer, physical address(Media Access Control MAC), for my host was *00:08:74:4f:36:23*

4. What values in the DHCP discover message differentiate this message from the DHCP request message?

For the Discover DHCP packet:



Wireshark · Packet 2 · dhcp-ethereal-trace-1

```
    [Stream index: 1]
 ˅ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    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: 0.0.0.0
    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
  > Option: (53) DHCP Message Type (Discover)
  > Option: (116) DHCP Auto-Configuration
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 000000000000000000

0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 00 45 00   ........ tO6#..E.
```

No.: 2 · Time: 2004-08-29 12:57:22.614018 · Source: 0.0.0.0 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 342 · Info: DHCP Discover - Transaction ID 0x3e5e0ce3

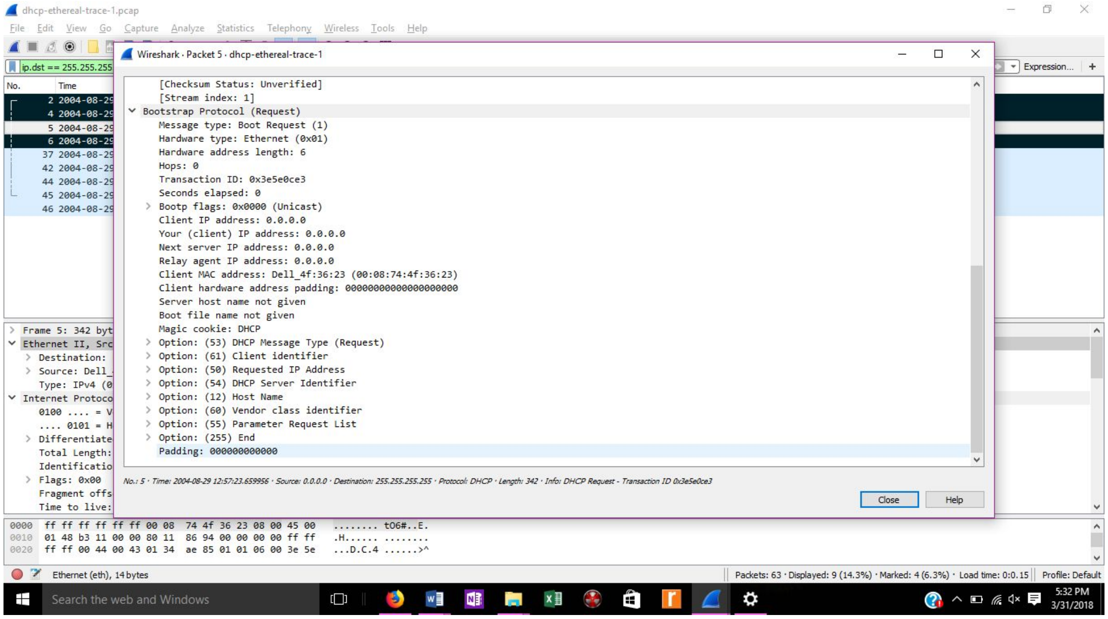
```
0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 00 45 00   ........ tO6#..E.
0010  01 48 b3 10 00 00 80 11  86 95 00 00 00 00 ff ff   .H...... ........
0020  ff ff 00 44 00 43 01 34  e9 7b 01 01 06 00 3e 5e   ...D.C.4 .{....>^
```

Ethernet (eth), 14 bytes | Packets: 63 · Displayed: 9 (14.3%) · Marked: 4 (6.3%) · Load time: 0:0.15 | Profile: Default

dhcp-ethereal-trace-1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 255.255.255
Expression...
No.
Time
Close
Help
Search the web and Windows
5:31 PM
3/31/2018

Figure 4.

For the Request DHCP packet:



Wireshark · Packet 5 · dhcp-ethereal-trace-1

```
    [Checksum Status: Unverified]
    [Stream index: 1]
 ˅ Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    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: 0.0.0.0
    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
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address
  > Option: (54) DHCP Server Identifier
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
    Padding: 000000000000
```

No.: 5 · Time: 2004-08-29 12:57:23.659956 · Source: 0.0.0.0 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 342 · Info: DHCP Request - Transaction ID 0x3e5e0ce3

```
0000  ff ff ff ff ff ff 00 08  74 4f 36 23 08 00 45 00   ........ tO6#..E.
0010  01 48 b3 11 00 00 80 11  86 94 00 00 00 00 ff ff   .H...... ........
0020  ff ff 00 44 00 43 01 34  ae 85 01 01 06 00 3e 5e   ...D.C.4 ......>^
```

Ethernet (eth), 14 bytes | Packets: 63 · Displayed: 9 (14.3%) · Marked: 4 (6.3%) · Load time: 0:0.15 | Profile: Default

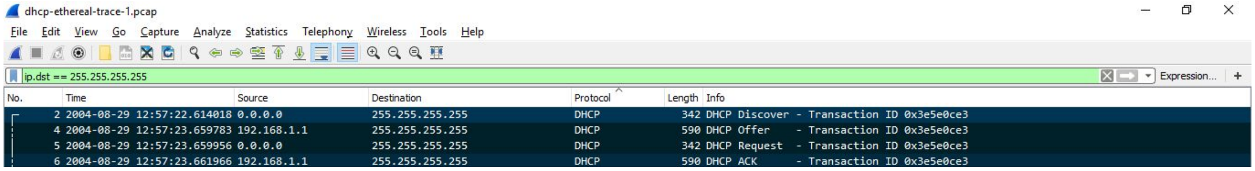
dhcp-ethereal-trace-1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 255.255.255
Expression...
No.
Time
Close
Help
Search the web and Windows
5:32 PM
3/31/2018

Figure 5.

The difference between these two DHCP packets is that Discover has a value of 1 and Request has a value of 3. These values can be seen in the bootp section. .

5. **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?**

First Set



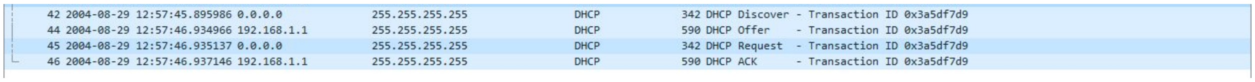
dhcp-ethereal-trace-1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
ip.dst == 255.255.255.255

No.   Time                        Source        Destination       Protocol  Length Info
    2 2004-08-29 12:57:22.614018 0.0.0.0       255.255.255.255   DHCP      342 DHCP Discover - Transaction ID 0x3e5e0ce3
    4 2004-08-29 12:57:23.659783 192.168.1.1   255.255.255.255   DHCP      590 DHCP Offer    - Transaction ID 0x3e5e0ce3
    5 2004-08-29 12:57:23.659956 0.0.0.0       255.255.255.255   DHCP      342 DHCP Request  - Transaction ID 0x3e5e0ce3
    6 2004-08-29 12:57:23.661966 192.168.1.1   255.255.255.255   DHCP      590 DHCP ACK      - Transaction ID 0x3e5e0ce3
```

The Transaction ID for the first four DHCP messages is *0x3e5e0ce3*.

Second Set



```
   42 2004-08-29 12:57:45.895986 0.0.0.0       255.255.255.255   DHCP      342 DHCP Discover - Transaction ID 0x3a5df7d9
   44 2004-08-29 12:57:46.934966 192.168.1.1   255.255.255.255   DHCP      590 DHCP Offer    - Transaction ID 0x3a5df7d9
   45 2004-08-29 12:57:46.935137 0.0.0.0       255.255.255.255   DHCP      342 DHCP Request  - Transaction ID 0x3a5df7d9
   46 2004-08-29 12:57:46.937146 192.168.1.1   255.255.255.255   DHCP      590 DHCP ACK      - Transaction ID 0x3a5df7d9
```

The Transaction ID for the second set of four DHCP messages is *0x3a5df7d9.*

The transaction ID field for DHCP packets is utilized for the client to keep track of what DHCP messages go together in a set.

6. **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.**

The 0.0.0.0 IP address is the IP datagram utilized until a new IP address can be agreed upon by client and server.

No.	Source IP	Destination IP
1-Discover	0.0.0.0	255.255.255.255
2-Offer	192.168.1.1	255.255.255.255
3-Request	0.0.0.0	255.255.255.255
4-ACK	192.168.1.1	255.255.255.255

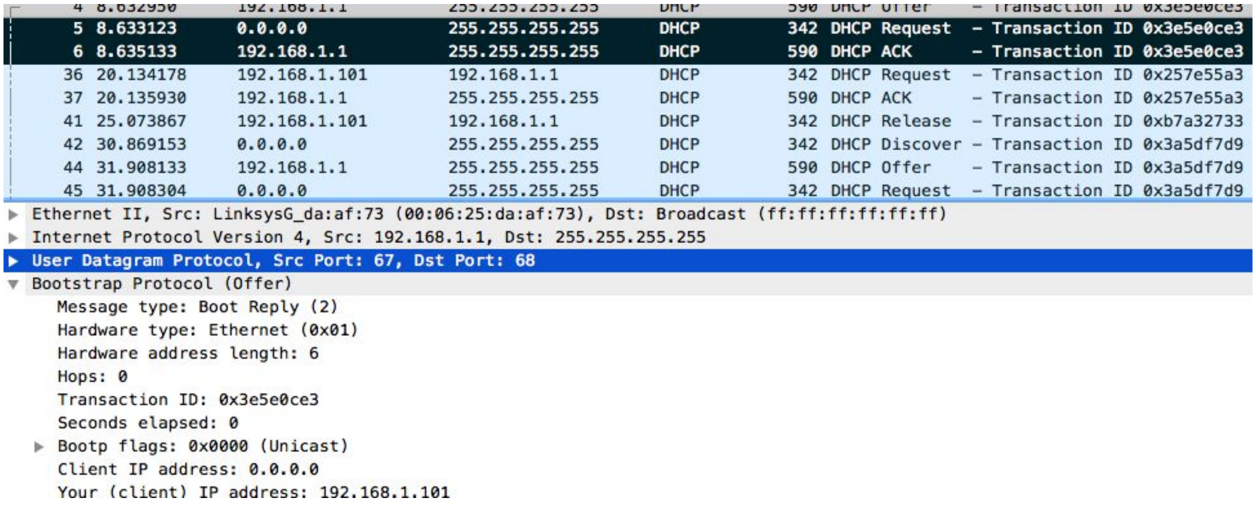
Figure 7.

7. **What is the IP address of your DHCP server?**

The IP address of the DHCP server is 192.168.1.1

8. **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.**

The DHCP offer message is the packet which contains the IP address 192.168.1.101 . This IP address is the one that is being offered by the server to the client.



```
   4 8.632950     192.168.1.1      255.255.255.255    DHCP      590 DHCP Offer    - Transaction ID 0x3e5e0ce3
   5 8.633123     0.0.0.0          255.255.255.255    DHCP      342 DHCP Request  - Transaction ID 0x3e5e0ce3
   6 8.635133     192.168.1.1      255.255.255.255    DHCP      590 DHCP ACK      - Transaction ID 0x3e5e0ce3
  36 20.134178    192.168.1.101    192.168.1.1        DHCP      342 DHCP Request  - Transaction ID 0x257e55a3
  37 20.135930    192.168.1.1      255.255.255.255    DHCP      590 DHCP ACK      - Transaction ID 0x257e55a3
  41 25.073867    192.168.1.101    192.168.1.1        DHCP      342 DHCP Release  - Transaction ID 0xb7a32733
  42 30.869153    0.0.0.0          255.255.255.255    DHCP      342 DHCP Discover - Transaction ID 0x3a5df7d9
  44 31.908133    192.168.1.1      255.255.255.255    DHCP      590 DHCP Offer    - Transaction ID 0x3a5df7d9
  45 31.908304    0.0.0.0          255.255.255.255    DHCP      342 DHCP Request  - Transaction ID 0x3a5df7d9
▶ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff: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
▼ Bootstrap Protocol (Offer)
    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
```

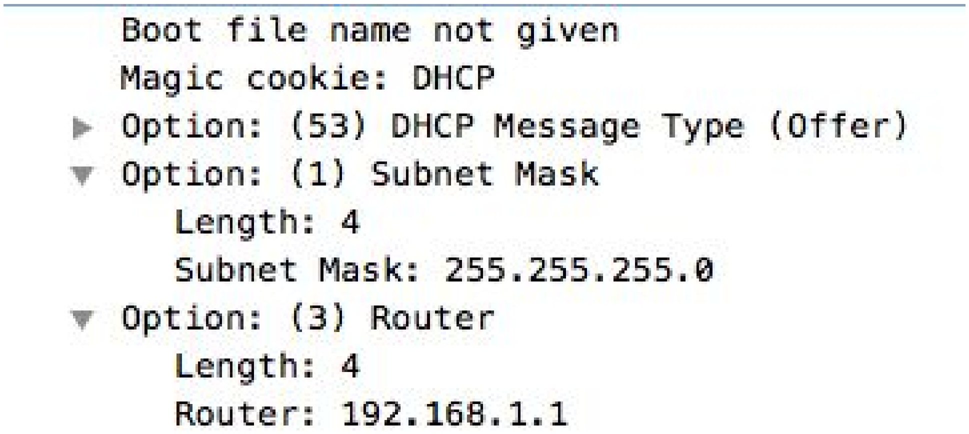
Figure 8.

9. **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?**

There does not seem to be any evidence that a relay agent was used in this trace file. A relay agent is typically used when the device and server are located in different subnets. Since the IP address is 0.0.0.0 this is a strong indication that a relay agents was not used as usually this would be the IP address of the relay agent instead.

In the experiment there is no evidence of a relay agent.

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



```
Boot file name not given
Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Offer)
▼ Option: (1) Subnet Mask
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
```

Figure 9.

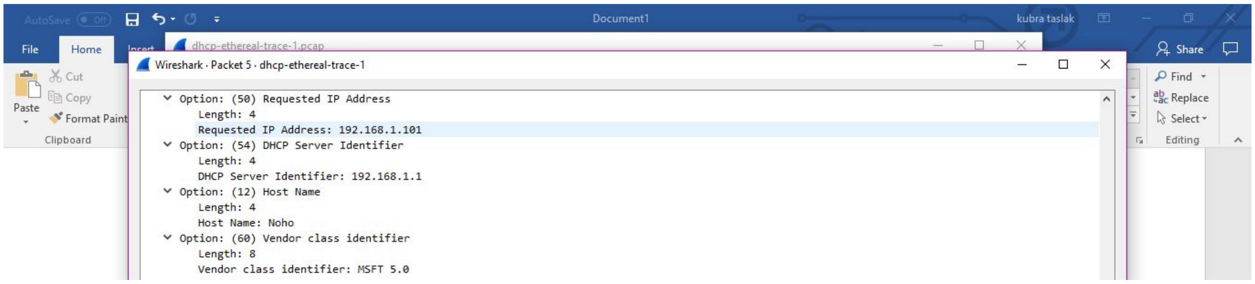
The purpose of the router line in the DHCP offer message is to inform the client where the default gateway is located. In this case the router is 192.168.1.1

The purpose of the subnet mask in the DHCP offer message is to inform the client which subnet mask should be used. In this case the subnet mask is 255.255.255.0

These attributes are important because along with the host IP and a DNS server it can allow the client to have connectivity to the internet.

11. **In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). 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 access?**

The client does accept the IP address as shown in Figure 10.The DHCP request packet from the client contains the IP address being requested under the field "requested IP address".



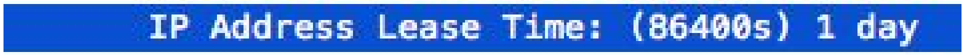
```
Option: (50) Requested IP Address
    Length: 4
    Requested IP Address: 192.168.1.101
Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.1.1
Option: (12) Host Name
    Length: 4
    Host Name: Noho
Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
```

Figure 10.

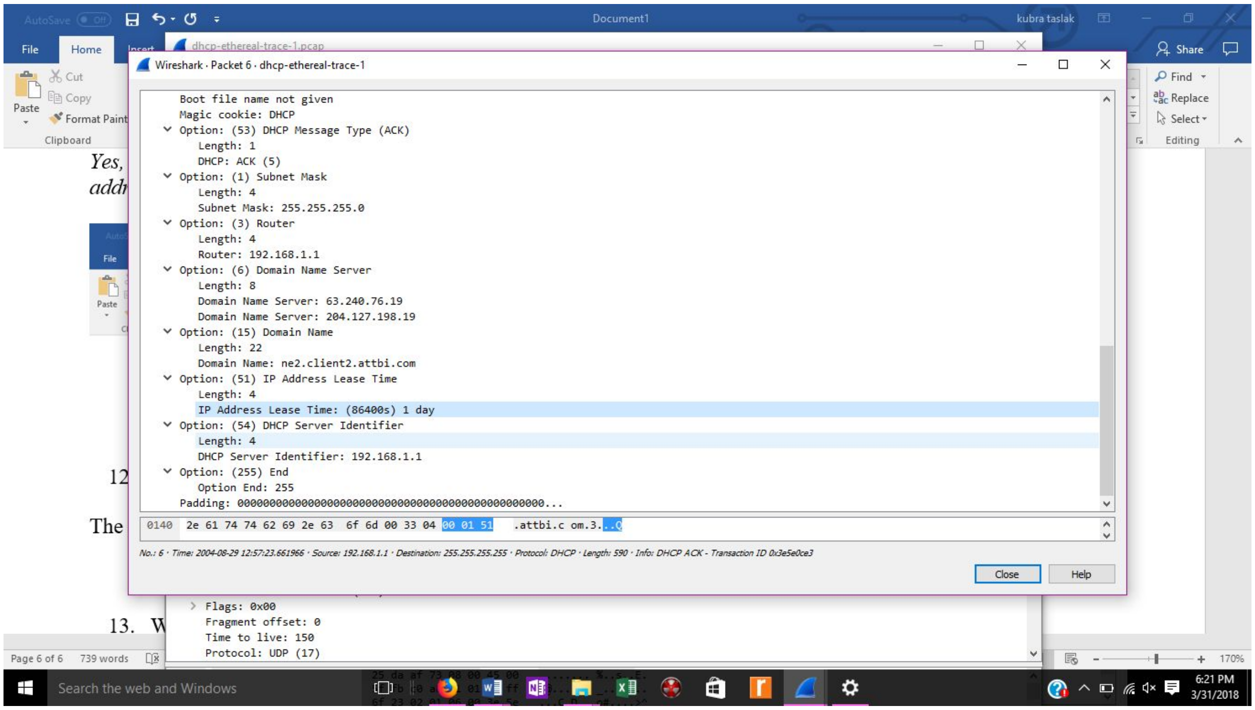
12. Explain the purpose of the lease time. How long is the lease time in your experiment?

The purpose of the lease time for DHCP is so that the client knows how long the agreed upon IP address is valid for. This is important as if IP addresses were permanently kept by inactive clients then there is the possibility of running out of IP addresses.

In this lab the IP lease time was 86400 second or 1 day.



```
IP Address Lease Time: (86400s) 1 day
```



Wireshark · Packet 6 · dhcp-ethereal-trace-1

```
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
    Length: 1
    DHCP: ACK (5)
Option: (1) Subnet Mask
    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
    Length: 4
    DHCP Server Identifier: 192.168.1.1
Option: (255) End
    Option End: 255
Padding: 000000000000000000000000000000000000000000000000...

0140  2e 61 74 74 62 69 2e 63  6f 6d 00 33 04 00 01 51   .attbi.c om.3...Q
```

No.: 6 · Time: 2004-08-29 12:57:23.661966 · Source: 192.168.1.1 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 590 · Info: DHCP ACK - Transaction ID 0x3e5e0ce3

```
> Flags: 0x00
  Fragment offset: 0
  Time to live: 150
  Protocol: UDP (17)
```

Figure 11.

13. 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?

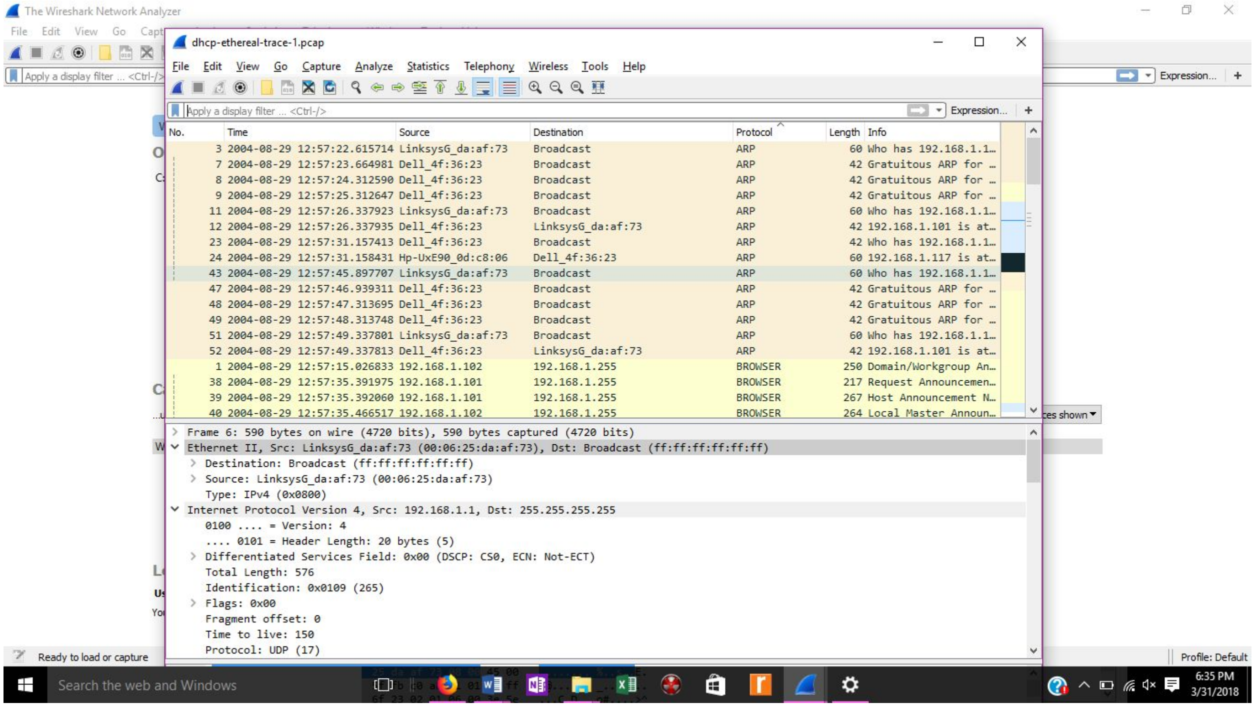
The purpose of the DHCP release message is when you need to get a new IP address so this allows you to shed your old one.

The DHCP server does not issue an acknowledgment of the client's DHCP request as it is a UDP packet.

If the client's DHCP release message is lost then the client will continue to release it and look for a new IP address. However, the server never receiving the message that the IP has been released will keep it reserved until there is a check on the lease time. After that the server will also discontinue the association of that IP address with that client.

14. **Clear the *bootp* 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.**

As seen in Figure 12. there is definitely ARP packets sent and received during the DHCP packet exchange period..This is due to the network updating the ARP tables so that the devices on the network now know which devices mac addresses are assigned to that IP address.


The Wireshark Network Analyzer
dhcp-ethereal-trace-1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Ready to load or capture
Profile: Default
Search the web and Windows
6:35 PM
3/31/2018

```
No.   Time                       Source              Destination        Protocol  Length Info
    3 2004-08-29 12:57:22.615714 LinksysG_da:af:73   Broadcast          ARP           60 Who has 192.168.1.1…
    7 2004-08-29 12:57:23.664981 Dell_4f:36:23       Broadcast          ARP           42 Gratuitous ARP for …
    8 2004-08-29 12:57:24.312590 Dell_4f:36:23       Broadcast          ARP           42 Gratuitous ARP for …
    9 2004-08-29 12:57:25.312647 Dell_4f:36:23       Broadcast          ARP           42 Gratuitous ARP for …
   11 2004-08-29 12:57:26.337923 LinksysG_da:af:73   Broadcast          ARP           60 Who has 192.168.1.1…
   12 2004-08-29 12:57:26.337935 Dell_4f:36:23       LinksysG_da:af:73  ARP           42 192.168.1.101 is at…
   23 2004-08-29 12:57:31.157413 Dell_4f:36:23       Broadcast          ARP           42 Who has 192.168.1.1…
   24 2004-08-29 12:57:31.158431 Hp-UxE90_0d:c8:06   Dell_4f:36:23      ARP           60 192.168.1.117 is at…
   43 2004-08-29 12:57:45.897707 LinksysG_da:af:73   Broadcast          ARP           60 Who has 192.168.1.1…
   47 2004-08-29 12:57:46.939311 Dell_4f:36:23       Broadcast          ARP           42 Gratuitous ARP for …
   48 2004-08-29 12:57:47.313695 Dell_4f:36:23       Broadcast          ARP           42 Gratuitous ARP for …
   49 2004-08-29 12:57:48.313748 Dell_4f:36:23       Broadcast          ARP           42 Gratuitous ARP for …
   51 2004-08-29 12:57:49.337801 LinksysG_da:af:73   Broadcast          ARP           60 Who has 192.168.1.1…
   52 2004-08-29 12:57:49.337813 Dell_4f:36:23       LinksysG_da:af:73  ARP           42 192.168.1.101 is at…
    1 2004-08-29 12:57:15.026833 192.168.1.102       192.168.1.255      BROWSER      250 Domain/Workgroup An…
   38 2004-08-29 12:57:35.391975 192.168.1.101       192.168.1.255      BROWSER      217 Request Announcemen…
   39 2004-08-29 12:57:35.392060 192.168.1.101       192.168.1.255      BROWSER      267 Host Announcement N…
   40 2004-08-29 12:57:35.466517 192.168.1.102       192.168.1.255      BROWSER      264 Local Master Announ…
```

```
> Frame 6: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 576
    Identification: 0x0109 (265)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 150
    Protocol: UDP (17)
```

Figure 12.