wPaul Williams Diaz
CIS 151 Prof. Brown

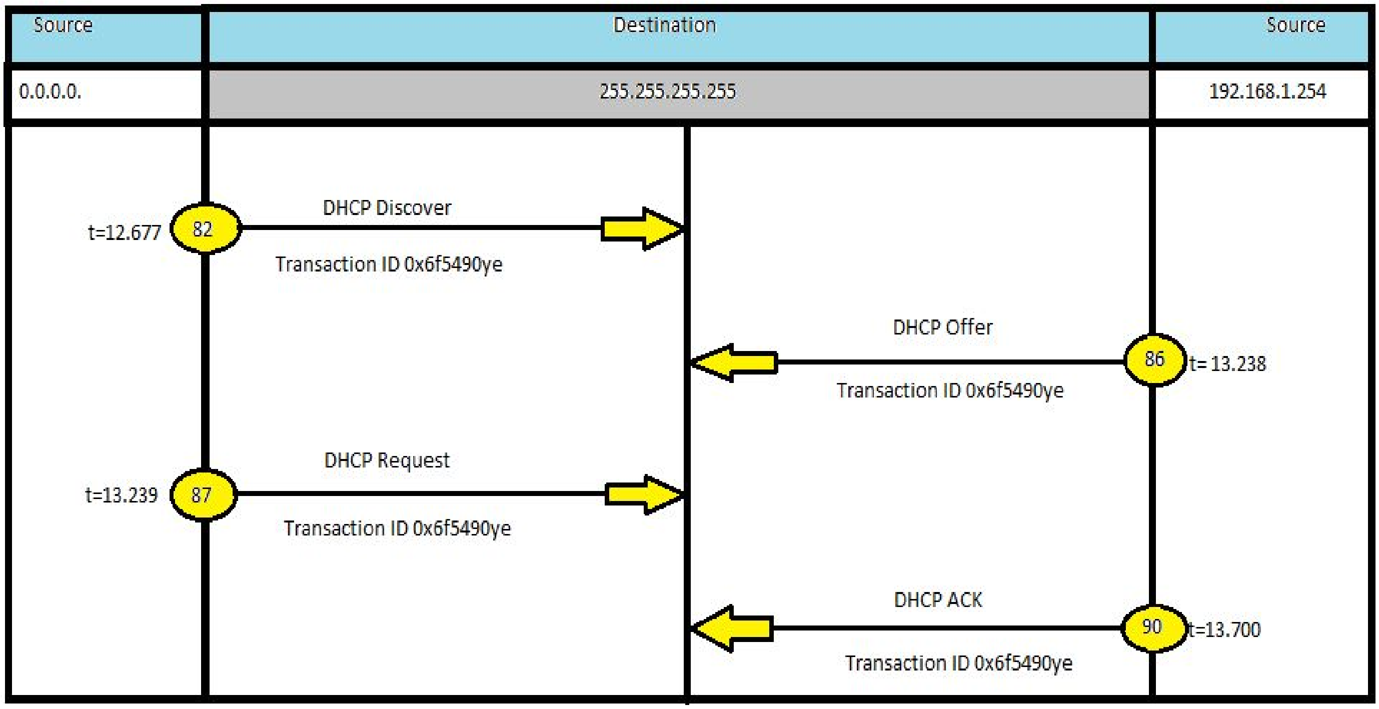
Wireshark LAB DHCP

1. Are DHCP messages sent over TCP or UDP?

Answer: DHCP messages were sent over UDP.

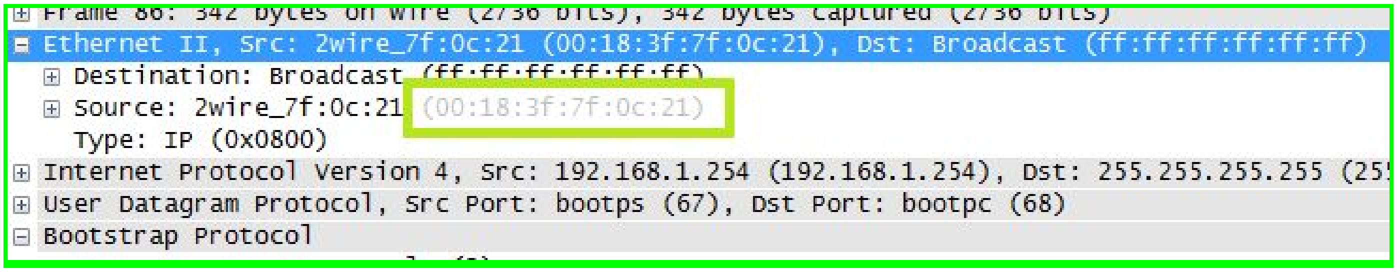
2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination ports numbers. Are the port numbers the same as in the example given in this lab assignment?

Answer: Yes, the port numbers are the same as in the example given to this lab assignment.



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

Answer: The link-layer of my host is 00:18:3f:7f:0c:21



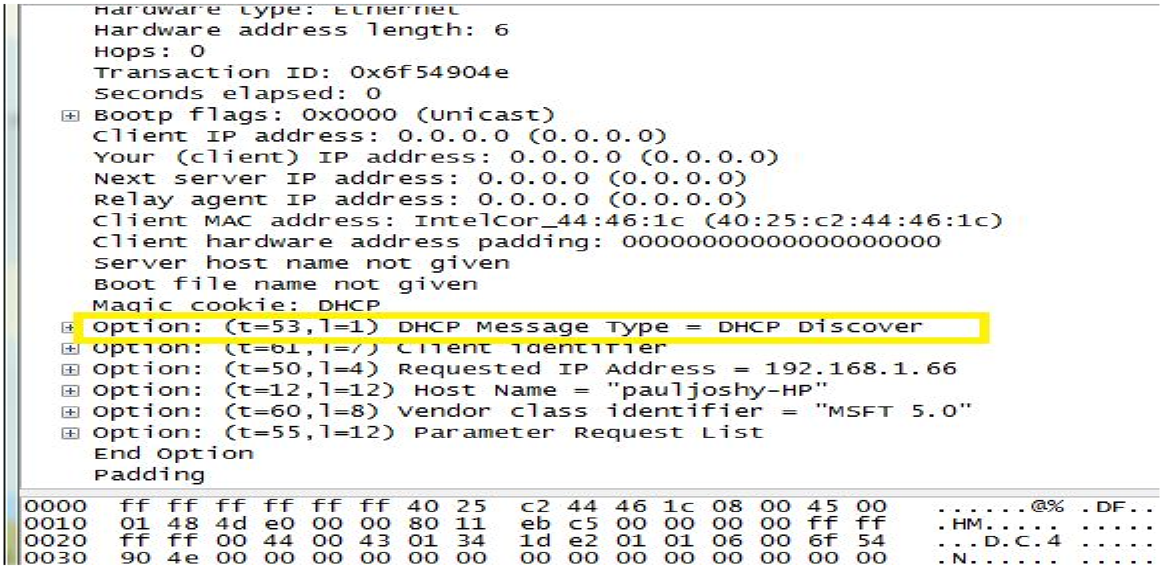
```
⊞ Frame 86: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊟ Ethernet II, Src: 2wire_7f:0c:21 (00:18:3f:7f:0c:21), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: 2wire_7f:0c:21 (00:18:3f:7f:0c:21)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.1.254 (192.168.1.254), Dst: 255.255.255.255 (25
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
```

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

Answer: The values that differentiate DHCP discover messages from request messages is the

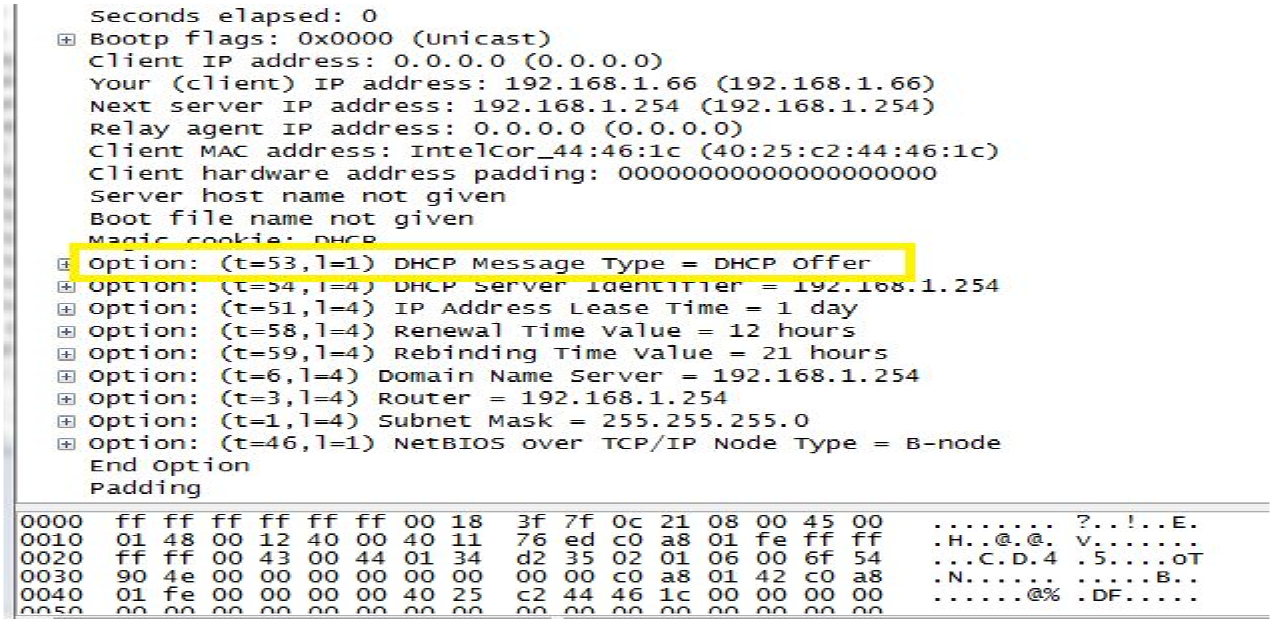
`option: (t=53, l=10 DHCP Message Type = DHCP Discover`

DHCP Discover Message



```
        Hardware type: Ethernet
        Hardware address length: 6
        Hops: 0
        Transaction ID: 0x6f54904e
        Seconds elapsed: 0
    ⊞ Bootp flags: 0x0000 (Unicast)
        Client IP address: 0.0.0.0 (0.0.0.0)
        Your (client) IP address: 0.0.0.0 (0.0.0.0)
        Next server IP address: 0.0.0.0 (0.0.0.0)
        Relay agent IP address: 0.0.0.0 (0.0.0.0)
        Client MAC address: IntelCor_44:46:1c (40:25:c2:44:46:1c)
        Client hardware address padding: 00000000000000000000
        Server host name not given
        Boot file name not given
        Magic cookie: DHCP
    ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
    ⊞ Option: (t=61,l=7) Client identifier
    ⊞ Option: (t=50,l=4) Requested IP Address = 192.168.1.66
    ⊞ Option: (t=12,l=12) Host Name = "pauljoshy-HP"
    ⊞ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
    ⊞ Option: (t=55,l=12) Parameter Request List
        End Option
        Padding

0000   ff ff ff ff ff ff 40 25  c2 44 46 1c 08 00 45 00   ......@% .DF..E.
0010   01 48 4d e0 00 00 80 11  eb c5 00 00 00 00 ff ff   .HM..... ........
0020   ff ff 00 44 00 43 01 34  1d e2 01 01 06 00 6f 54   ...D.C.4 ......oT
0030   90 4e 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .N...... ........
```

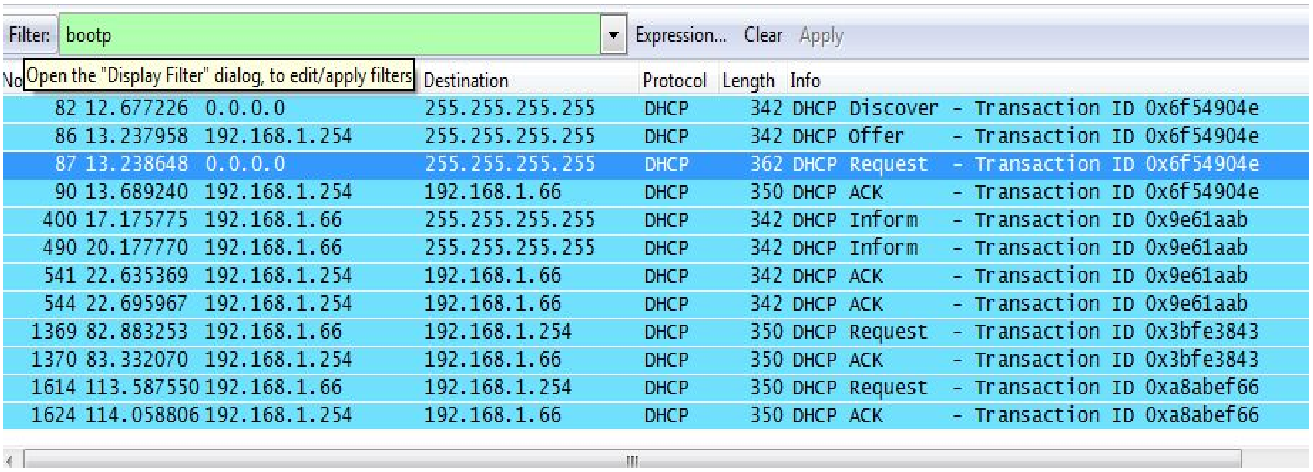
DHCP Offer Message



```
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.66 (192.168.1.66)
    Next server IP address: 192.168.1.254 (192.168.1.254)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: IntelCor_44:46:1c (40:25:c2:44:46:1c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.254
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.1.254
  ⊞ Option: (t=3,l=4) Router = 192.168.1.254
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=46,l=1) NetBIOS over TCP/IP Node Type = B-node
    End Option
    Padding

0000  ff ff ff ff ff ff 00 18  3f 7f 0c 21 08 00 45 00   ........ ?..!..E.
0010  01 48 00 12 40 00 40 11  76 ed c0 a8 01 fe ff ff   .H..@.@. v.......
0020  ff ff 00 43 00 44 01 34  d2 35 02 01 06 00 6f 54   ...C.D.4 .5....oT
0030  90 4e 00 00 00 00 00 00  00 00 c0 a8 01 42 c0 a8   .N...... .....B..
0040  01 fe 00 00 00 00 40 25  c2 44 46 1c 00 00 00 00   ......@% .DF.....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

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?

Answer: The first four DHCP messages (Discover/Offer/Request/ACK) `Transaction ID` is `0x6f54904e` The second set which (Request/ACK) DHCP message is `Transaction ID 0x3bfe3843.` During the request process, Transaction ID is used in order for the DHCP server can differentiate between request.

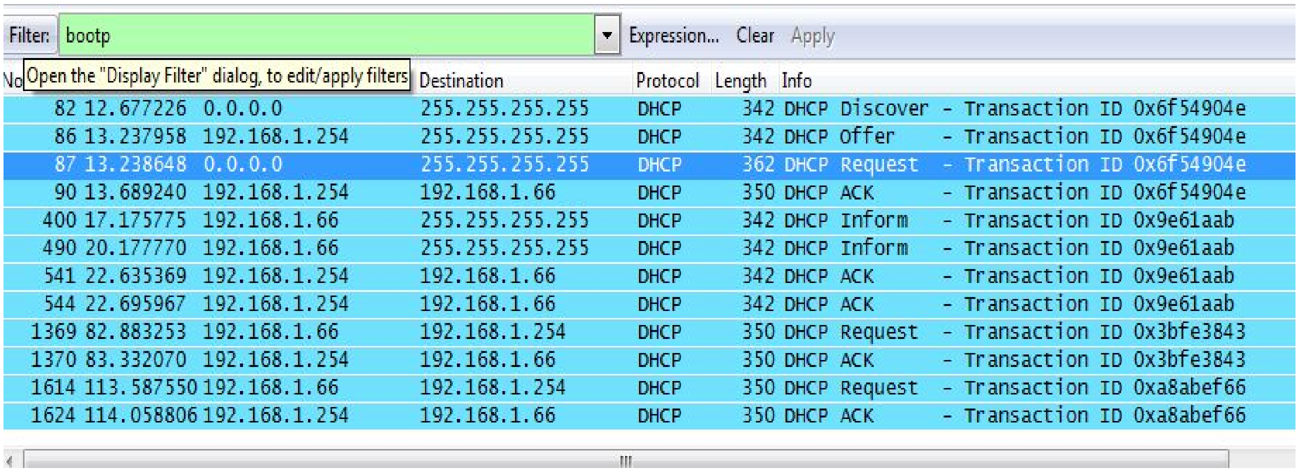


Filter: bootp
Expression... Clear Apply
Open the "Display Filter" dialog, to edit/apply filters

```
No                              Destination        Protocol Length Info
   82 12.677226  0.0.0.0        255.255.255.255    DHCP     342 DHCP Discover  - Transaction ID 0x6f54904e
   86 13.237958  192.168.1.254  255.255.255.255    DHCP     342 DHCP Offer     - Transaction ID 0x6f54904e
   87 13.238648  0.0.0.0        255.255.255.255    DHCP     362 DHCP Request   - Transaction ID 0x6f54904e
   90 13.689240  192.168.1.254  192.168.1.66       DHCP     350 DHCP ACK       - Transaction ID 0x6f54904e
  400 17.175775  192.168.1.66   255.255.255.255    DHCP     342 DHCP Inform    - Transaction ID 0x9e61aab
  490 20.177770  192.168.1.66   255.255.255.255    DHCP     342 DHCP Inform    - Transaction ID 0x9e61aab
  541 22.635369  192.168.1.254  192.168.1.66       DHCP     342 DHCP ACK       - Transaction ID 0x9e61aab
  544 22.695967  192.168.1.254  192.168.1.66       DHCP     342 DHCP ACK       - Transaction ID 0x9e61aab
 1369 82.883253  192.168.1.66   192.168.1.254      DHCP     350 DHCP Request   - Transaction ID 0x3bfe3843
 1370 83.332070  192.168.1.254  192.168.1.66       DHCP     350 DHCP ACK       - Transaction ID 0x3bfe3843
 1614 113.587550 192.168.1.66   192.168.1.254      DHCP     350 DHCP Request   - Transaction ID 0xa8abef66
 1624 114.058806 192.168.1.254  192.168.1.66       DHCP     350 DHCP ACK       - Transaction ID 0xa8abef66
```

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 message (Discover?Offer?Request?ACK DHCP), Indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

Answer: The valued used in IP datagrams in the four messages is 255.255.255.255 (destination address). Host’s IP address is 0.0.0.0. The server uses IP address of 192.168.1.66.



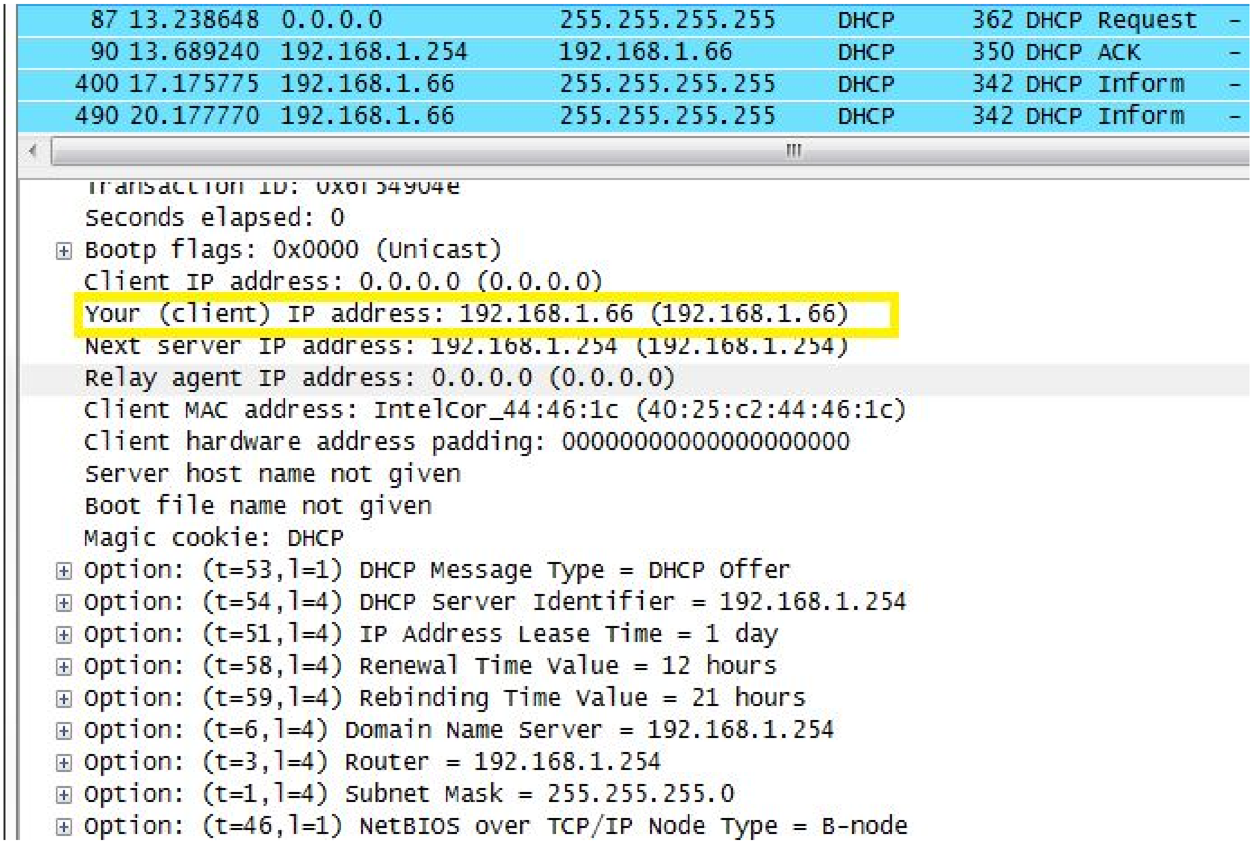
```
Filter: bootp

No Open the "Display Filter" dialog, to edit/apply filters Destination      Protocol Length Info
  82 12.677226  0.0.0.0        255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0x6f54904e
  86 13.237958  192.168.1.254  255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0x6f54904e
  87 13.238648  0.0.0.0        255.255.255.255  DHCP     362 DHCP Request  - Transaction ID 0x6f54904e
  90 13.689240  192.168.1.254  192.168.1.66     DHCP     350 DHCP ACK      - Transaction ID 0x6f54904e
 400 17.175775  192.168.1.66   255.255.255.255  DHCP     342 DHCP Inform   - Transaction ID 0x9e61aab
 490 20.177770  192.168.1.66   255.255.255.255  DHCP     342 DHCP Inform   - Transaction ID 0x9e61aab
 541 22.635369  192.168.1.254  192.168.1.66     DHCP     342 DHCP ACK      - Transaction ID 0x9e61aab
 544 22.695967  192.168.1.254  192.168.1.66     DHCP     342 DHCP ACK      - Transaction ID 0x9e61aab
1369 82.883253  192.168.1.66   192.168.1.254    DHCP     350 DHCP Request  - Transaction ID 0x3bfe3843
1370 83.332070  192.168.1.254  192.168.1.66     DHCP     350 DHCP ACK      - Transaction ID 0x3bfe3843
1614 113.587550 192.168.1.66   192.168.1.254    DHCP     350 DHCP Request  - Transaction ID 0xa8abef66
1624 114.058806 192.168.1.254  192.168.1.66     DHCP     350 DHCP ACK      - Transaction ID 0xa8abef66
```

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

Answer: The IP address of my DHCP server is 192.168.1.66.

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.

Answer: The IP address that DHCP server offering to my host 192.168.1.66.
The DHCP message that contains the offered IP address is
`DHCP Message Type = DHCP Offer.`

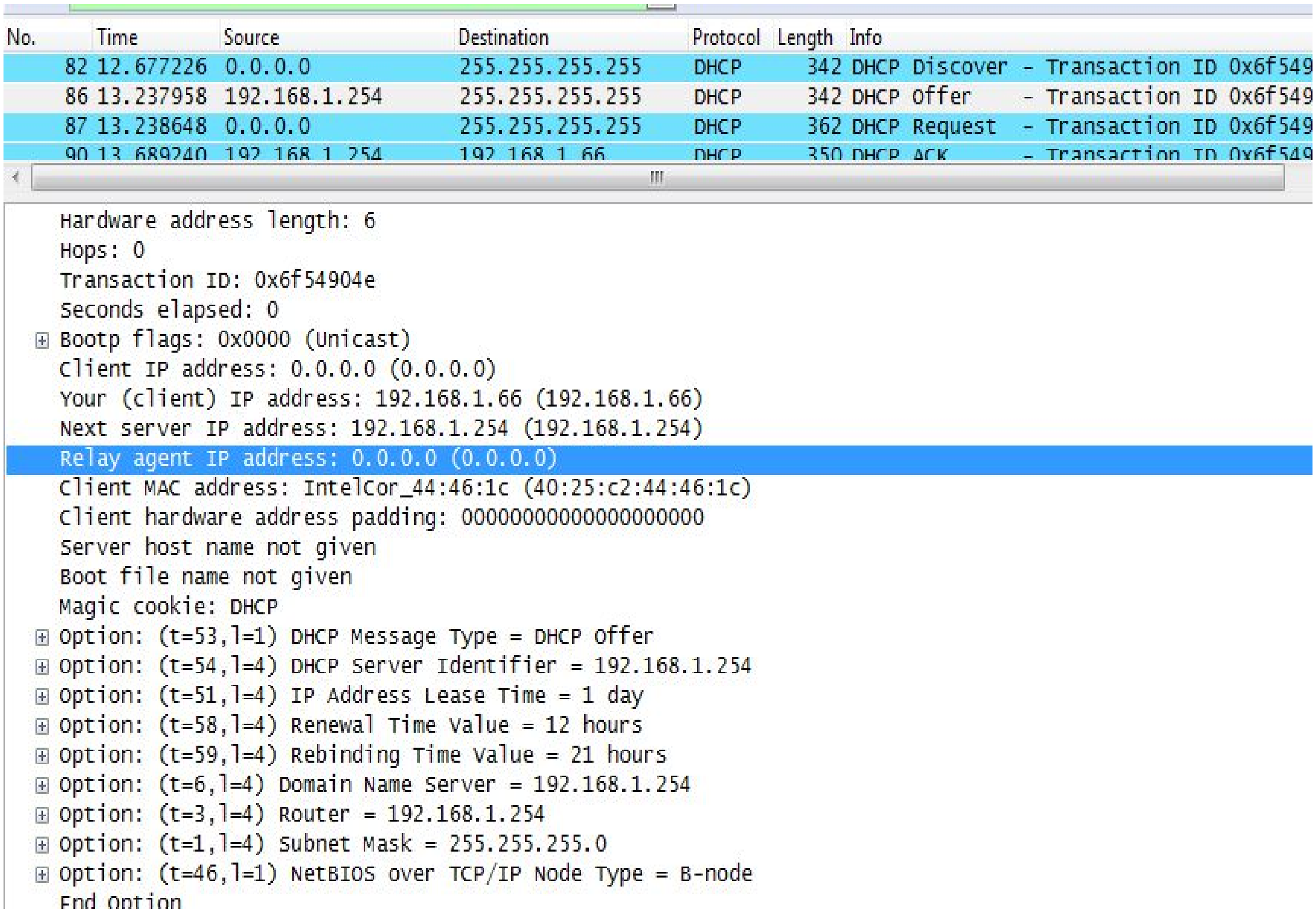


```
 87 13.238648  0.0.0.0        255.255.255.255  DHCP   362 DHCP Request  -
 90 13.689240  192.168.1.254  192.168.1.66     DHCP   350 DHCP ACK      -
400 17.175775  192.168.1.66   255.255.255.255  DHCP   342 DHCP Inform   -
490 20.177770  192.168.1.66   255.255.255.255  DHCP   342 DHCP Inform   -
```

```
    Transaction ID: 0x6f34904e
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.66 (192.168.1.66)
    Next server IP address: 192.168.1.254 (192.168.1.254)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: IntelCor_44:46:1c (40:25:c2:44:46:1c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.254
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.1.254
  ⊞ Option: (t=3,l=4) Router = 192.168.1.254
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=46,l=1) NetBIOS over TCP/IP Node Type = B-node
```

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 any relay agent in your experiment? If so, what is the IP address of the agent?

Answer: There is no relay agent because IP address is 0.0.0.0. It indicates that there is no DHCP relay used. In my experiment, there is no relay agent used.



```
No.     Time       Source          Destination      Protocol Length Info
     82 12.677226  0.0.0.0         255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0x6f549
     86 13.237958  192.168.1.254   255.255.255.255  DHCP      342 DHCP Offer    - Transaction ID 0x6f549
     87 13.238648  0.0.0.0         255.255.255.255  DHCP      362 DHCP Request  - Transaction ID 0x6f549
     90 13.689240  192.168.1.254   192.168.1.66     DHCP      350 DHCP ACK      - Transaction ID 0x6f549
```

```
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6f54904e
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.66 (192.168.1.66)
    Next server IP address: 192.168.1.254 (192.168.1.254)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: IntelCor_44:46:1c (40:25:c2:44:46:1c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.254
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
  ⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
  ⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
  ⊞ Option: (t=6,l=4) Domain Name Server = 192.168.1.254
  ⊞ Option: (t=3,l=4) Router = 192.168.1.254
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=46,l=1) NetBIOS over TCP/IP Node Type = B-node
    End Option
```

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

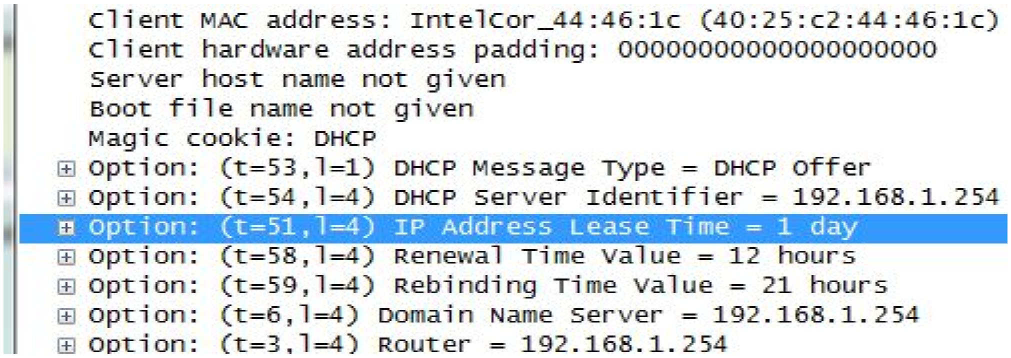
Answer: The router line tells the client what what its default must be and the subnet mask line tells the client which subnet mask it should use.

11. In the example in the screenshot in the assignment, the host requests the offered IP address in the DHCP request message. What happens in your own experiment?

Answer: In my experiment the host also requested the offered IP address in the DHCP request.

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

Answer: It will tell you the amount of time the IP address will be valid and in my experiment, there is only one day of IP address Lease Time.



```
  Client MAC address: IntelCor_44:46:1c (40:25:c2:44:46:1c)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
⊞ Option: (t=54,l=4) DHCP Server Identifier = 192.168.1.254
⊞ Option: (t=51,l=4) IP Address Lease Time = 1 day
⊞ Option: (t=58,l=4) Renewal Time Value = 12 hours
⊞ Option: (t=59,l=4) Rebinding Time Value = 21 hours
⊞ Option: (t=6,l=4) Domain Name Server = 192.168.1.254
⊞ Option: (t=3,l=4) Router = 192.168.1.254
```

13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgement of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

Answer: The purpose of DHCP Release is to cancel a DHCP lease on the IP address that a DHCP server has given. The DHCP server issue an acknowledgement of receipt of the client’s DHCP request, and if the DHCP release message is lost then it will be a problem to process DHCP release retransmission by a client. A client cannot get a DHCP release again until its timeout, that is when the lease period is over.

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.

Answer: Yes, there are ARP packets shown. DHCP server will broadcast an ARP request and find out if the IP address that will be offered is available or not, and if it is available, then it will be offered to a newly arriving client.