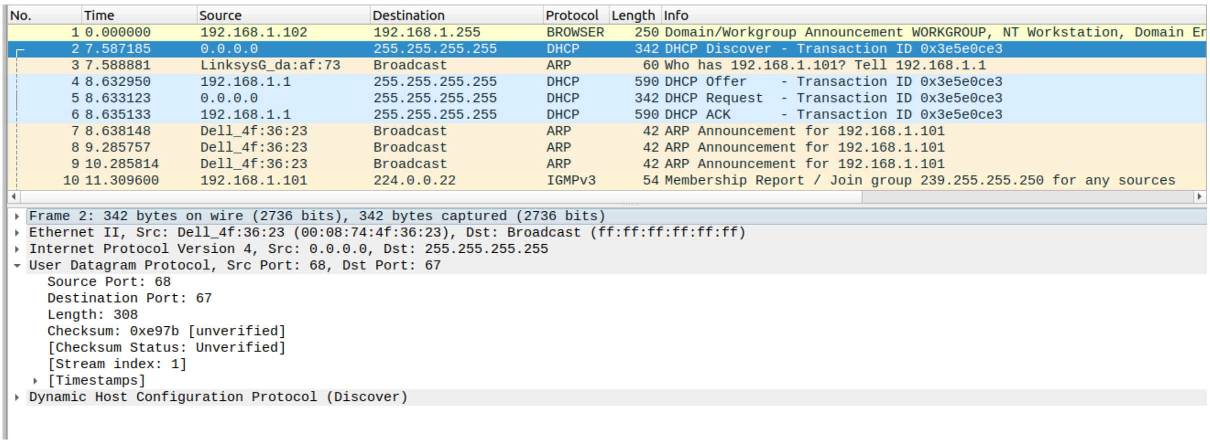
Lab_4b_Wireshark_DHCP_v8.0

1. Are DHCP messages sent over UDP or TCP?

Answer:



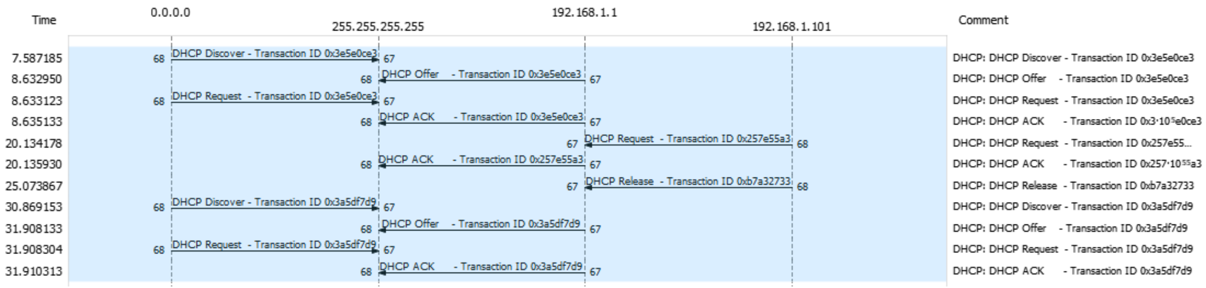
```
No.   Time        Source             Destination        Protocol  Length Info
    1 0.000000    192.168.1.102      192.168.1.255      BROWSER    250 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Er
    2 7.587185    0.0.0.0            255.255.255.255    DHCP       342 DHCP Discover - Transaction ID 0x3e5e0ce3
    3 7.588881    LinksysG_da:af:73  Broadcast          ARP         60 Who has 192.168.1.101? Tell 192.168.1.1
    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
    7 8.638148    Dell_4f:36:23      Broadcast          ARP         42 ARP Announcement for 192.168.1.101
    8 9.285757    Dell_4f:36:23      Broadcast          ARP         42 ARP Announcement for 192.168.1.101
    9 10.285814   Dell_4f:36:23      Broadcast          ARP         42 ARP Announcement for 192.168.1.101
   10 11.309600   192.168.1.101      224.0.0.22         IGMPv3      54 Membership Report / Join group 239.255.255.250 for any sources

› Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
› Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
⌄ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0xe97b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  › [Timestamps]
› Dynamic Host Configuration Protocol (Discover)
```

DHCP messages are 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 port numbers. Are the port numbers the same as in the example given in this lab assignment?

Answer:



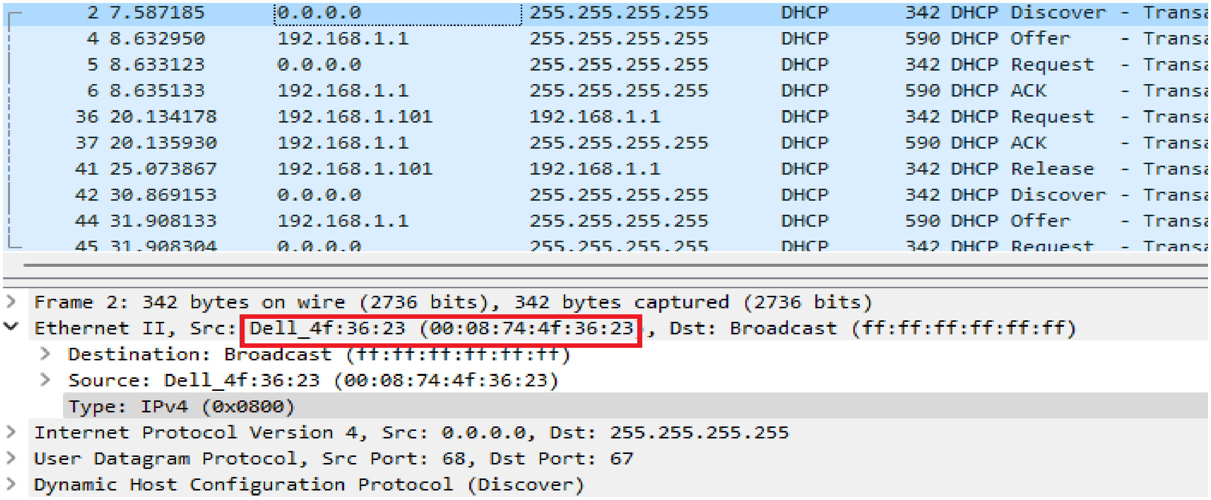
Time
0.0.0.0
255.255.255.255
192.168.1.1
192.168.1.101
Comment
68 DHCP Discover - Transaction ID 0x3e5e0ce3 67
68 DHCP Offer - Transaction ID 0x3e5e0ce3 67
68 DHCP Request - Transaction ID 0x3e5e0ce3 67
68 DHCP ACK - Transaction ID 0x3e5e0ce3 67
67 DHCP Request - Transaction ID 0x257e55a3 68
68 DHCP 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
7.587185   DHCP: DHCP Discover - Transaction ID 0x3e5e0ce3
8.632950   DHCP: DHCP Offer    - Transaction ID 0x3e5e0ce3
8.633123   DHCP: DHCP Request  - Transaction ID 0x3e5e0ce3
8.635133   DHCP: DHCP ACK      - Transaction ID 0x3·10⁵e0ce3
20.134178  DHCP: DHCP Request  - Transaction ID 0x257e55...
20.135930  DHCP: DHCP ACK      - Transaction ID 0x257·10⁵⁵a3
25.073867  DHCP: DHCP Release  - Transaction ID 0xb7a32733
30.869153  DHCP: DHCP Discover - Transaction ID 0x3a5df7d9
31.908133  DHCP: DHCP Offer    - Transaction ID 0x3a5df7d9
31.908304  DHCP: DHCP Request  - Transaction ID 0x3a5df7d9
31.910313  DHCP: DHCP ACK      - Transaction ID 0x3a5df7d9
```

Also, the port numbers are the same as in the example given.

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

Answer:



```
    2 7.587185   0.0.0.0         255.255.255.255   DHCP    342 DHCP Discover - Transa
    4 8.632950   192.168.1.1     255.255.255.255   DHCP    590 DHCP Offer    - Transa
    5 8.633123   0.0.0.0         255.255.255.255   DHCP    342 DHCP Request  - Transa
    6 8.635133   192.168.1.1     255.255.255.255   DHCP    590 DHCP ACK      - Transa
   36 20.134178  192.168.1.101   192.168.1.1       DHCP    342 DHCP Request  - Transa
   37 20.135930  192.168.1.1     255.255.255.255   DHCP    590 DHCP ACK      - Transa
   41 25.073867  192.168.1.101   192.168.1.1       DHCP    342 DHCP Release  - Transa
   42 30.869153  0.0.0.0         255.255.255.255   DHCP    342 DHCP Discover - Transa
   44 31.908133  192.168.1.1     255.255.255.255   DHCP    590 DHCP Offer    - Transa
   45 31.908304  0.0.0.0         255.255.255.255   DHCP    342 DHCP Request  - Transa

› Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⌄ 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)
› Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
› User Datagram Protocol, Src Port: 68, Dst Port: 67
› Dynamic Host Configuration Protocol (Discover)
```

00:08:74:4f:36:23

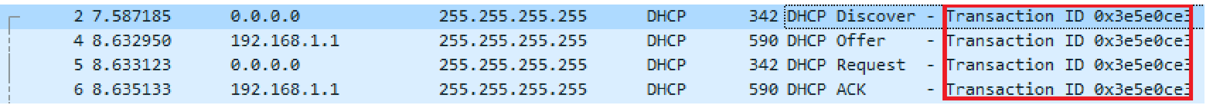
4. What values in the DHCP discover message differentiate this message from the DHCP request message?

Answer:

DHCP Message Type
Request includes a server identifier field

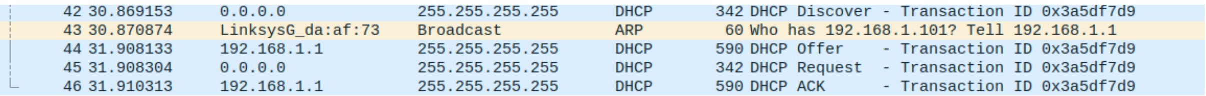
5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

Answer:



```
  2 7.587185    0.0.0.0          255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0x3e5e0ce3
  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
```

First four (Discover/Offer/Request/ACK) DHCP messages : 0x3e5e0ce3



```
42 30.869153   0.0.0.0             255.255.255.255    DHCP     342 DHCP Discover - Transaction ID 0x3a5df7d9
43 30.870874   LinksysG_da:af:73   Broadcast          ARP       60 Who has 192.168.1.101? Tell 192.168.1.1
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
46 31.910313   192.168.1.1         255.255.255.255    DHCP     590 DHCP ACK      - Transaction ID 0x3a5df7d9
```

2nd Set of messages: 0x3a5df7d9
=> Differentiate between different requests made by the user.

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.

Answer:

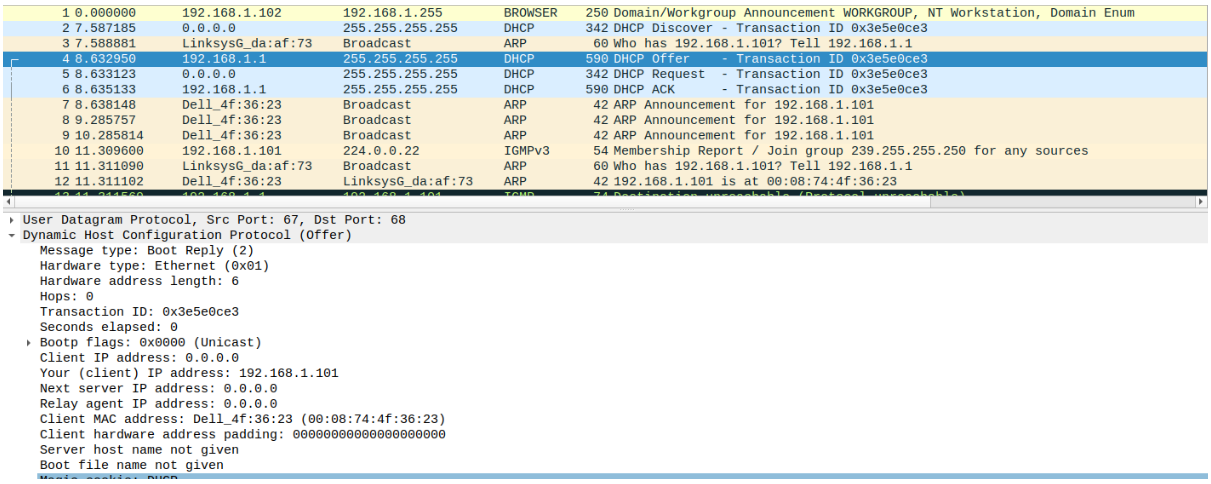
- Discover: source 0.0.0.0 Destination 255.255.255.255
- Offer: source 192.168.1.1 Destination 255.255.255.255
- Request: source 0.0.0.0 Destination 255.255.255.255
- Ack: source 192.168.1.1 Destination 255.255.255.255

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

Answer: The IP address of my 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.

Answer:



```
 1 0.000000    192.168.1.102      192.168.1.255      BROWSER   250 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
 2 7.587185    0.0.0.0            255.255.255.255    DHCP      342 DHCP Discover - Transaction ID 0x3e5e0ce3
 3 7.588881    LinksysG_da:af:73  Broadcast          ARP        60 Who has 192.168.1.101? Tell 192.168.1.1
 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
 7 8.638148    Dell_4f:36:23      Broadcast          ARP        42 ARP Announcement for 192.168.1.101
 8 9.285757    Dell_4f:36:23      Broadcast          ARP        42 ARP Announcement for 192.168.1.101
 9 10.285814   Dell_4f:36:23      Broadcast          ARP        42 ARP Announcement for 192.168.1.101
10 11.309600   192.168.1.101      224.0.0.22         IGMPv3     54 Membership Report / Join group 239.255.255.250 for any sources
11 11.311090   LinksysG_da:af:73  Broadcast          ARP        60 Who has 192.168.1.101? Tell 192.168.1.1
12 11.311102   Dell_4f:36:23      LinksysG_da:af:73  ARP        42 192.168.1.101 is at 00:08:74:4f:36:23
```

```
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration 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
    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
```

My client is offered 192.168.1.10 by the DHCP server. The offer message contains the DHCP address offered by the server

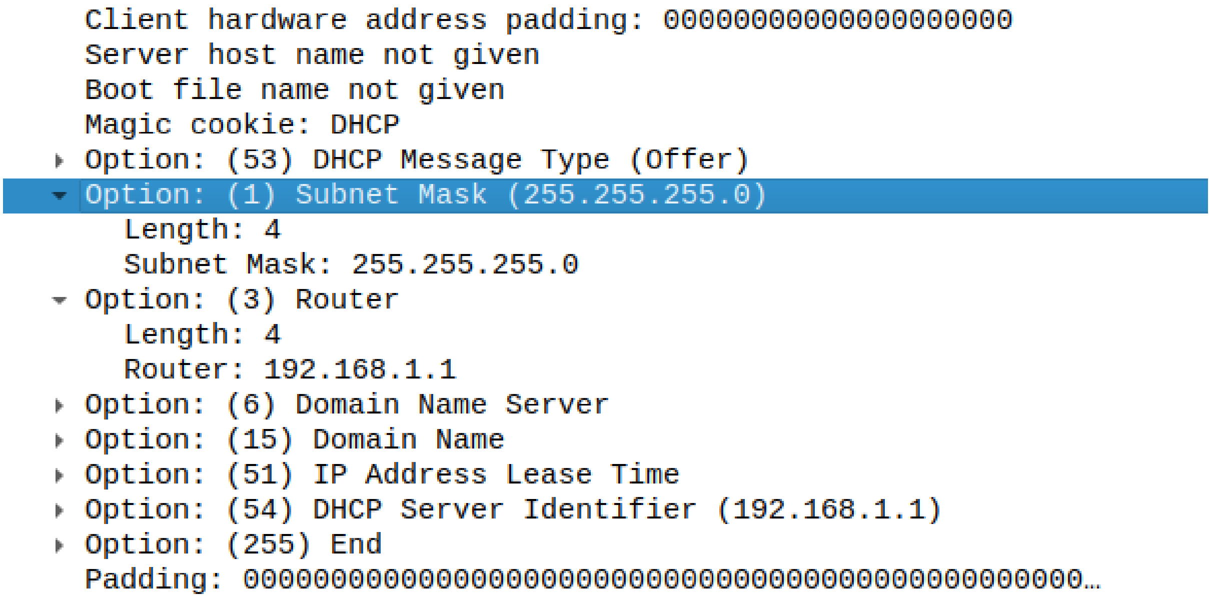
9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent? 10. Explain the purpose of the router and subnet mask lines in the DHCP offer message

Answer:

In the example given, the value that indicates there is no relay agent is 0.0.0.0, in the case of my capture, I also have a value for the relay agent of 0.0.0.0 indicating that I too did not have a relay agent.

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

Answer:

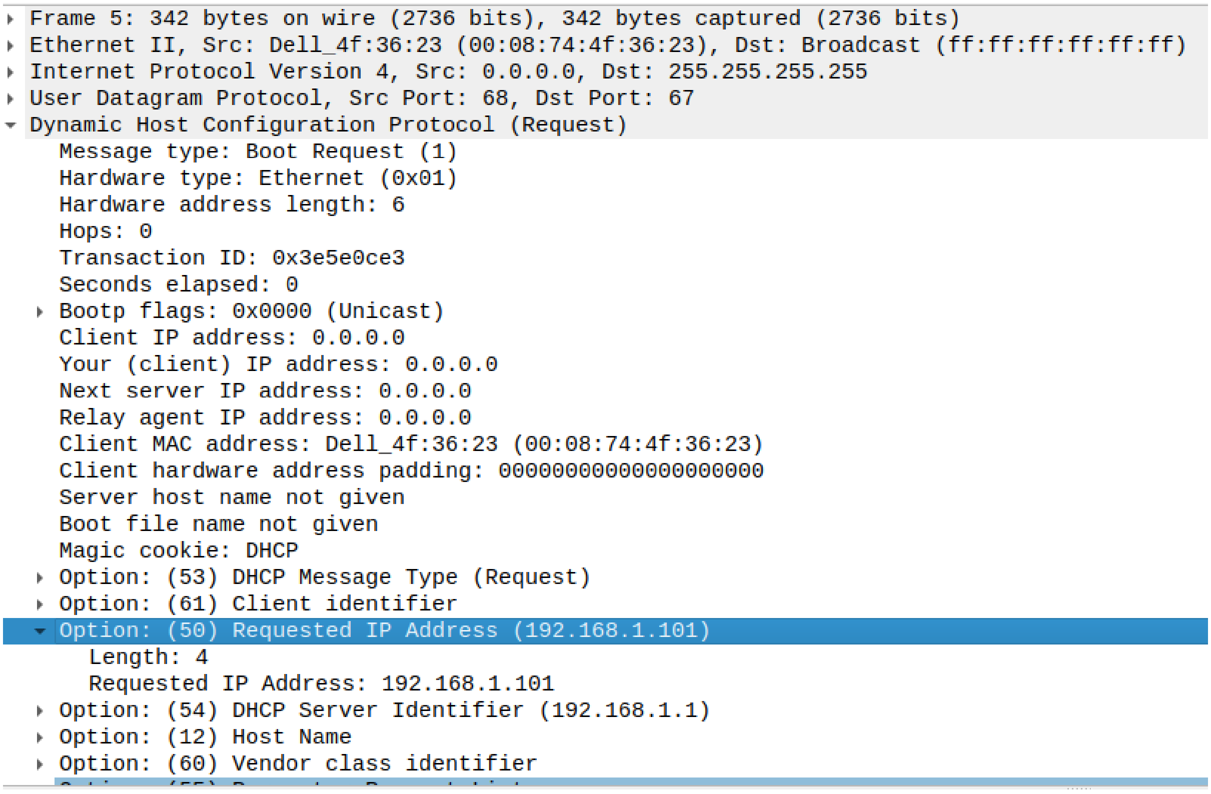


```
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▸ Option: (53) DHCP Message Type (Offer)
  ▾ Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
  ▾ Option: (3) Router
      Length: 4
      Router: 192.168.1.1
  ▸ Option: (6) Domain Name Server
  ▸ Option: (15) Domain Name
  ▸ Option: (51) IP Address Lease Time
  ▸ Option: (54) DHCP Server Identifier (192.168.1.1)
  ▸ Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000…
```

- The router IP address is the way to identify the default internet entrance.
- The subnet mask is the way to show that a subnet is available.

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 address?

Answer:

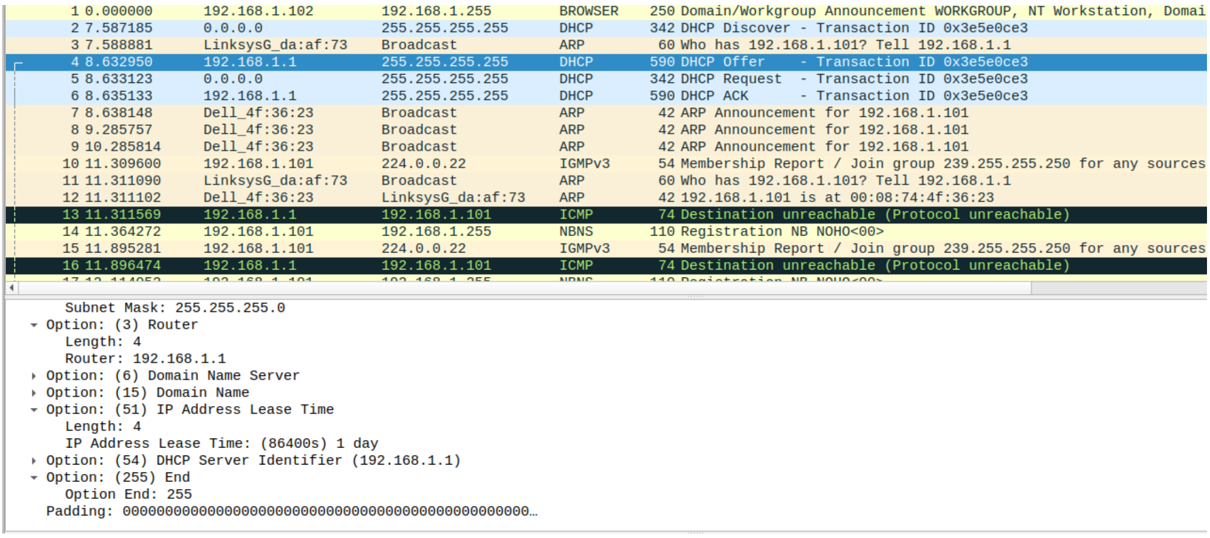


```
▸ Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▸ User Datagram Protocol, Src Port: 68, Dst Port: 67
▾ Dynamic Host Configuration 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 (192.168.1.101)
      Length: 4
      Requested IP Address: 192.168.1.101
  ▸ Option: (54) DHCP Server Identifier (192.168.1.1)
  ▸ Option: (12) Host Name
  ▸ Option: (60) Vendor class identifier
```

- The same thing occurs the host requests the offered ip address.
- Option: (t=50,l=4) Requested IP Address = 192.168.1.101 (of the Request message.)

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

Answer:



```
  1 0.000000    192.168.1.102       192.168.1.255       BROWSER   250 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domai
  2 7.587185    0.0.0.0             255.255.255.255     DHCP      342 DHCP Discover - Transaction ID 0x3e5e0ce3
  3 7.588881    LinksysG_da:af:73   Broadcast           ARP        60 Who has 192.168.1.101? Tell 192.168.1.1
  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
  7 8.638148    Dell_4f:36:23       Broadcast           ARP        42 ARP Announcement for 192.168.1.101
  8 9.285757    Dell_4f:36:23       Broadcast           ARP        42 ARP Announcement for 192.168.1.101
  9 10.285814   Dell_4f:36:23       Broadcast           ARP        42 ARP Announcement for 192.168.1.101
 10 11.309600   192.168.1.101       224.0.0.22          IGMPv3     54 Membership Report / Join group 239.255.255.250 for any sources
 11 11.311090   LinksysG_da:af:73   Broadcast           ARP        60 Who has 192.168.1.101? Tell 192.168.1.1
 12 11.311102   Dell_4f:36:23       LinksysG_da:af:73   ARP        42 192.168.1.101 is at 00:08:74:4f:36:23
 13 11.311569   192.168.1.1         192.168.1.101       ICMP       74 Destination unreachable (Protocol unreachable)
 14 11.364272   192.168.1.101       192.168.1.255       NBNS      110 Registration NB NOHO<00>
 15 11.895281   192.168.1.101       224.0.0.22          IGMPv3     54 Membership Report / Join group 239.255.255.250 for any sources
 16 11.896474   192.168.1.1         192.168.1.101       ICMP       74 Destination unreachable (Protocol unreachable)

      Subnet Mask: 255.255.255.0
  ▾ Option: (3) Router
      Length: 4
      Router: 192.168.1.1
  ▸ Option: (6) Domain Name Server
  ▸ Option: (15) Domain Name
  ▾ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (86400s) 1 day
  ▸ Option: (54) DHCP Server Identifier (192.168.1.1)
  ▾ Option: (255) End
      Option End: 255
    Padding: 000000000000000000000000000000000000000000000000…
```

- The lease time is the amount of the time the user is aloud connection to the router
- Option: (t=51,l=4) IP Address Lease Time = 1 day

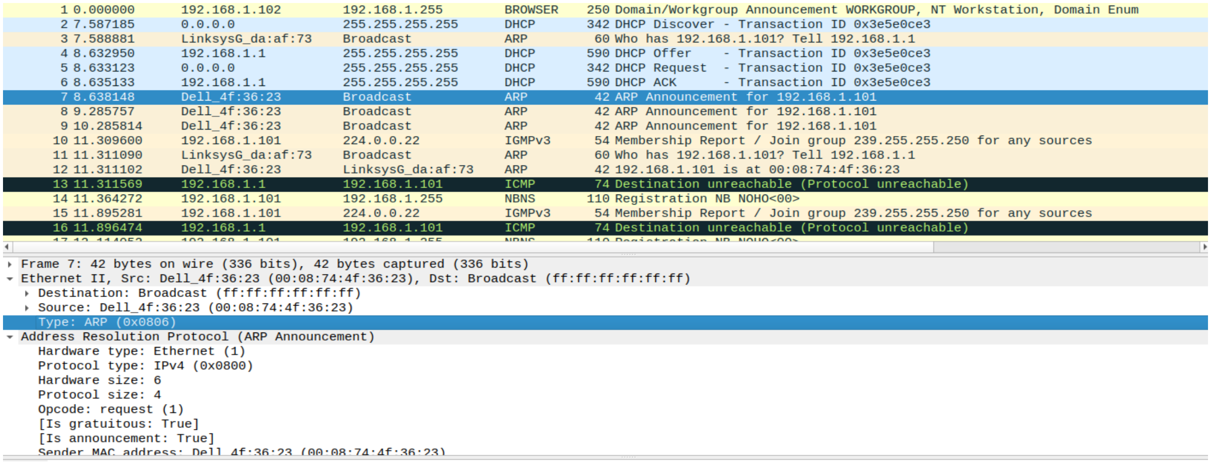
13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

Answer:

- The DHCP release message tells the dhcp server that you want to cancel the IP address offered.
- The DHCP server will not issue an ack of receipt of the client’s DHCP request.
- If the release message is lost then the DHCP server retains the IP address until the lease time expires.

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:



```
  1 0.000000    192.168.1.102       192.168.1.255       BROWSER   250 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
  2 7.587185    0.0.0.0             255.255.255.255     DHCP      342 DHCP Discover - Transaction ID 0x3e5e0ce3
  3 7.588881    LinksysG_da:af:73   Broadcast           ARP        60 Who has 192.168.1.101? Tell 192.168.1.1
  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
  7 8.638148    Dell_4f:36:23       Broadcast           ARP        42 ARP Announcement for 192.168.1.101
  8 9.285757    Dell_4f:36:23       Broadcast           ARP        42 ARP Announcement for 192.168.1.101
  9 10.285814   Dell_4f:36:23       Broadcast           ARP        42 ARP Announcement for 192.168.1.101
 10 11.309600   192.168.1.101       224.0.0.22          IGMPv3     54 Membership Report / Join group 239.255.255.250 for any sources
 11 11.311090   LinksysG_da:af:73   Broadcast           ARP        60 Who has 192.168.1.101? Tell 192.168.1.1
 12 11.311102   Dell_4f:36:23       LinksysG_da:af:73   ARP        42 192.168.1.101 is at 00:08:74:4f:36:23
 13 11.311569   192.168.1.1         192.168.1.101       ICMP       74 Destination unreachable (Protocol unreachable)
 14 11.364272   192.168.1.101       192.168.1.255       NBNS      110 Registration NB NOHO<00>
 15 11.895281   192.168.1.101       224.0.0.22          IGMPv3     54 Membership Report / Join group 239.255.255.250 for any sources
 16 11.896474   192.168.1.1         192.168.1.101       ICMP       74 Destination unreachable (Protocol unreachable)

▸ Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▾ 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: ARP (0x0806)
▾ Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
```

Yes, they appear to be broadcasts sent out by the network to build up the known IP addresses by the clients network.