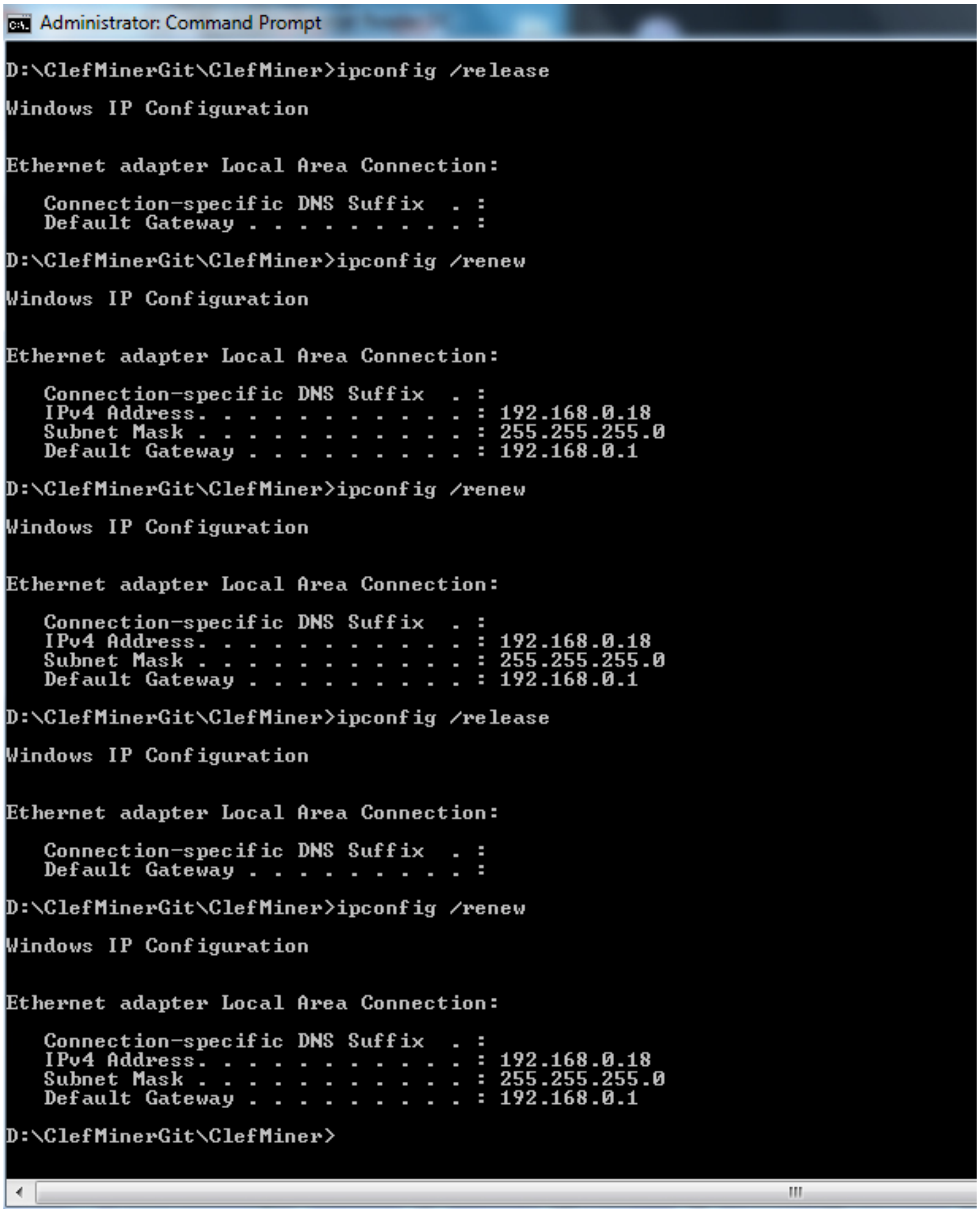
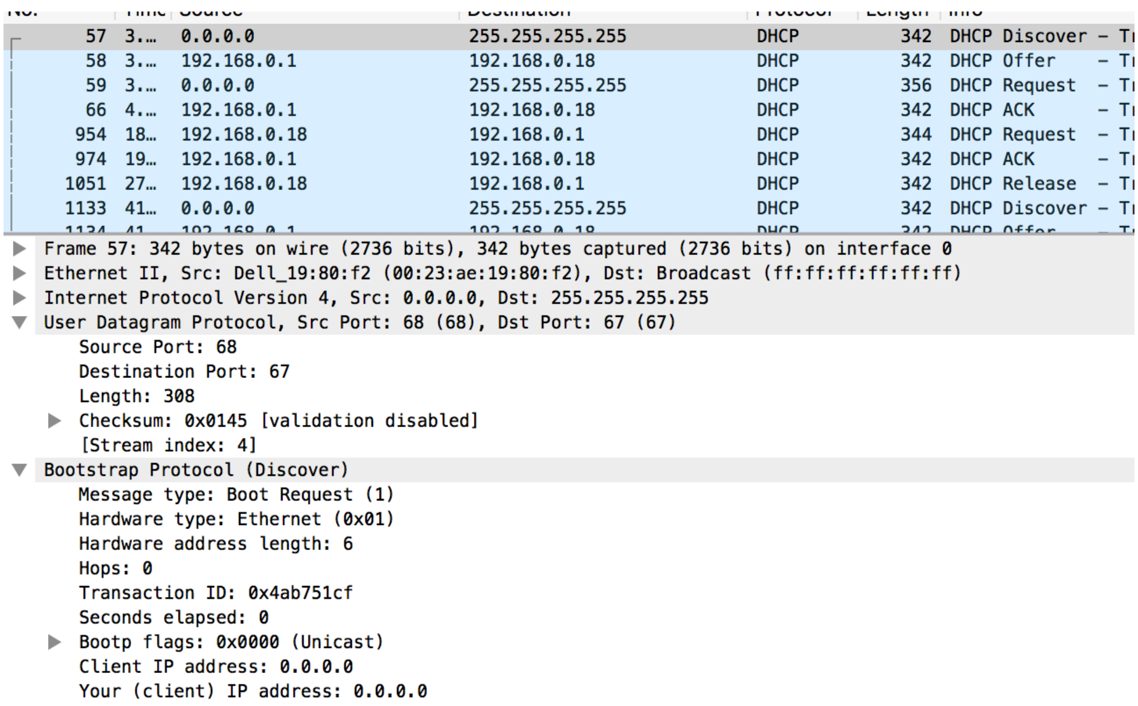
Course: Computer Networks(ECE/CSC 570)
Instructor: Mihail L. Sichitiu
Description: Spring 2016, Wireshark Assignment 4(DHCP) Solutions.
Student Name: Himangshu Ranjan Borah
Student ID: 200105222
Unity ID: hborah

__The Snapshot of the command prompt:__



```
D:\ClefMinerGit\ClefMiner>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Default Gateway . . . . . . . . . :

D:\ClefMinerGit\ClefMiner>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

D:\ClefMinerGit\ClefMiner>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

D:\ClefMinerGit\ClefMiner>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Default Gateway . . . . . . . . . :

D:\ClefMinerGit\ClefMiner>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.18
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

D:\ClefMinerGit\ClefMiner>
```

Answer No 1:

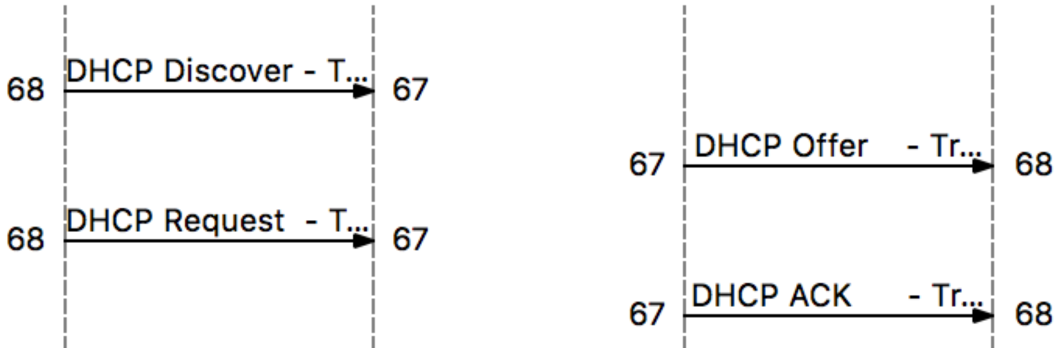


```
   57  3…   0.0.0.0          255.255.255.255   DHCP       342  DHCP Discover – Tı
   58  3…   192.168.0.1      192.168.0.18      DHCP       342  DHCP Offer    – Tı
   59  3…   0.0.0.0          255.255.255.255   DHCP       356  DHCP Request  – Tı
   66  4…   192.168.0.1      192.168.0.18      DHCP       342  DHCP ACK      – Tı
  954  18…  192.168.0.18     192.168.0.1       DHCP       344  DHCP Request  – Tı
  974  19…  192.168.0.1      192.168.0.18      DHCP       342  DHCP ACK      – Tı
 1051  27…  192.168.0.18     192.168.0.1       DHCP       342  DHCP Release  – Tı
 1133  41…  0.0.0.0          255.255.255.255   DHCP       342  DHCP Discover – Tı
 1134  41…  192.168.0.1      192.168.0.18      DHCP       342  DHCP Offer    – Tı
▶ Frame 57: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Dell_19:80:f2 (00:23:ae:19:80:f2), 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 (68), Dst Port: 67 (67)
    Source Port: 68
    Destination Port: 67
    Length: 308
  ▶ Checksum: 0x0145 [validation disabled]
    [Stream index: 4]
▼ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4ab751cf
    Seconds elapsed: 0
  ▶ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
```

As we can see above, the messages are being sent over **UDP (User Datagram Protocol)**

Answer No 2:

The timing diagram of my pc:

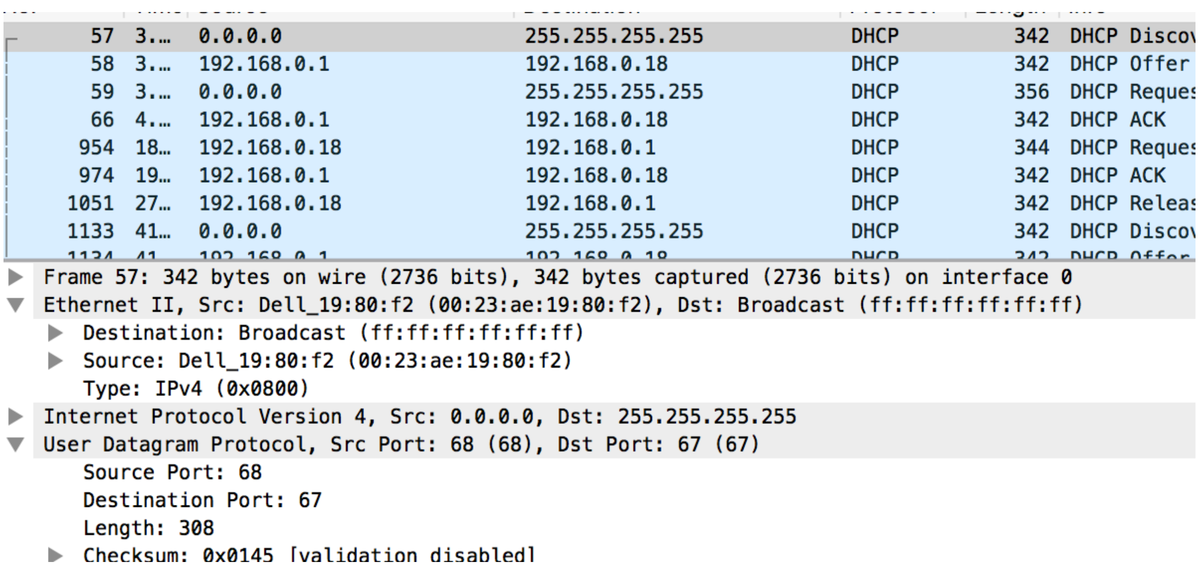


1. Discover Packet : Source port => 68, Destination Port => 67
2. Offer Packet : Source port => 67, Destination Port => 68

3. Request Packet : Source port => 68, Destination Port => 67
4. ACK Packet : Source port => 67, Destination Port => 68
5.

The timing diagram from the traces shared by author are same as this one and the corresponding port numbers are also **same**.

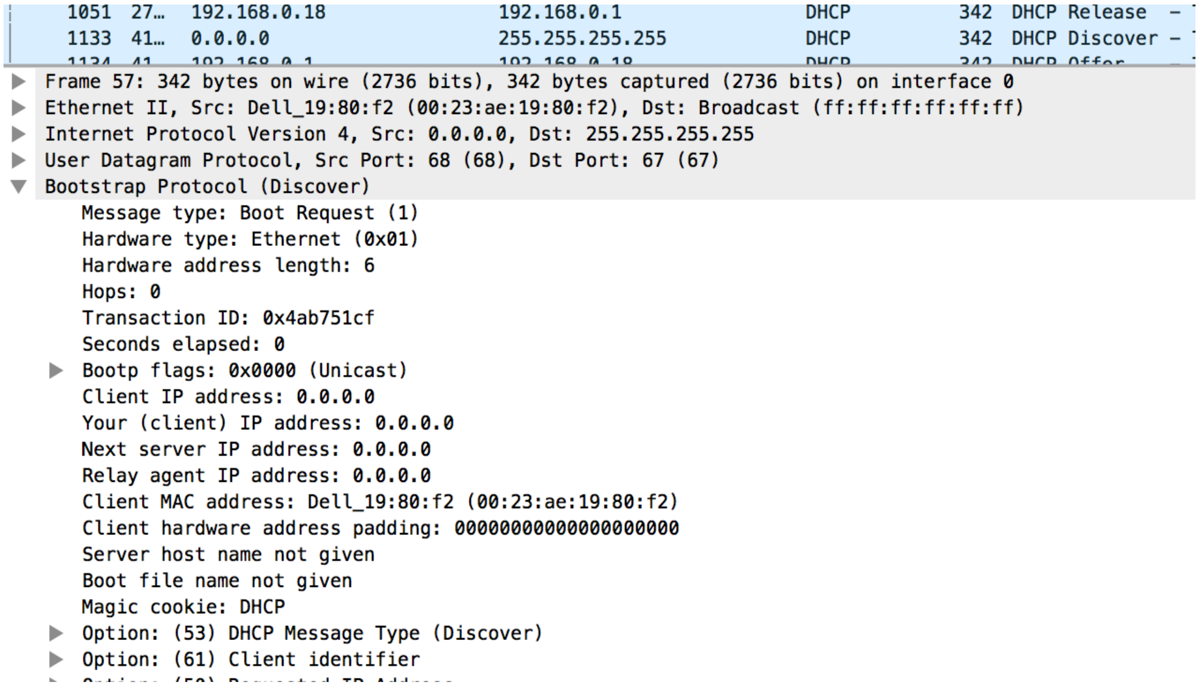
Answer No 3:



```
   57  3.…  0.0.0.0        255.255.255.255  DHCP   342  DHCP Discov
   58  3.…  192.168.0.1    192.168.0.18     DHCP   342  DHCP Offer
   59  3.…  0.0.0.0        255.255.255.255  DHCP   356  DHCP Reques
   66  4.…  192.168.0.1    192.168.0.18     DHCP   342  DHCP ACK
  954  18…  192.168.0.18   192.168.0.1      DHCP   344  DHCP Reques
  974  19…  192.168.0.1    192.168.0.18     DHCP   342  DHCP ACK
 1051  27…  192.168.0.18   192.168.0.1      DHCP   342  DHCP Releas
 1133  41…  0.0.0.0        255.255.255.255  DHCP   342  DHCP Discov
 1134  41…  192.168.0.1    192.168.0.18     DHCP   342  DHCP Offer
▶ Frame 57: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▼ Ethernet II, Src: Dell_19:80:f2 (00:23:ae:19:80:f2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   ▶ Source: Dell_19:80:f2 (00:23:ae:19:80:f2)
     Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▼ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
     Source Port: 68
     Destination Port: 67
     Length: 308
   ▶ Checksum: 0x0145 [validation disabled]
```

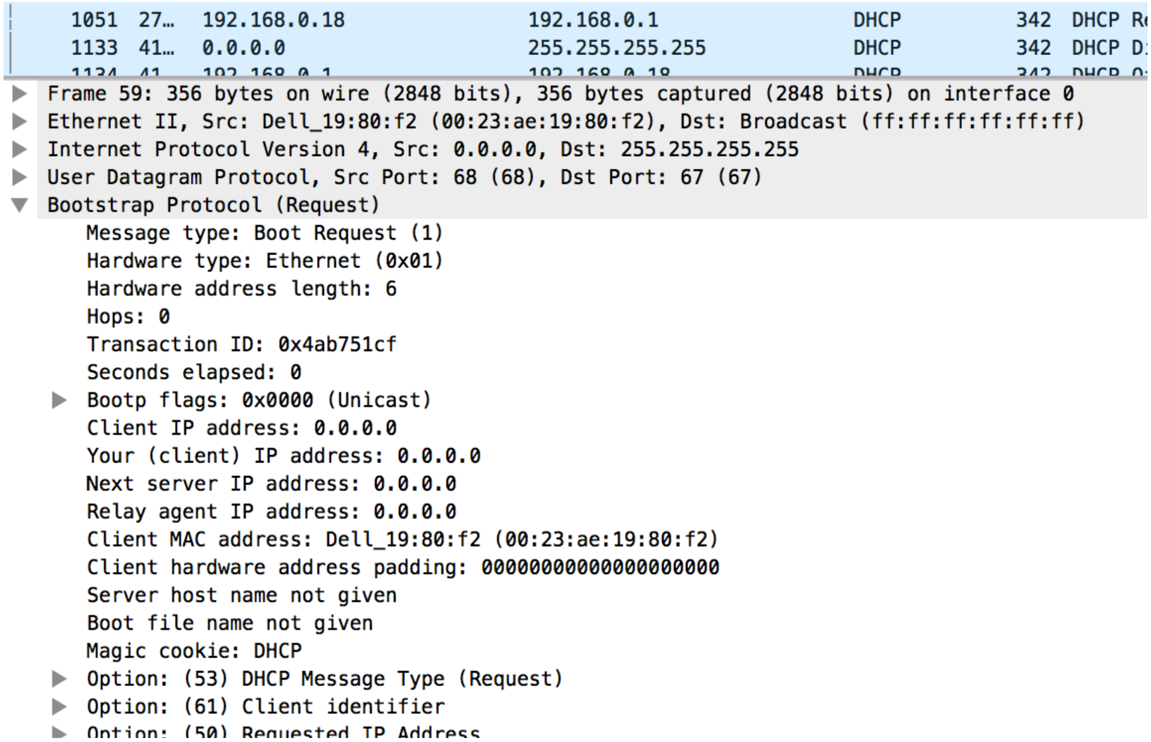
The Link Layer Address is : **00:23:ae:19:80:f2**

Answer No 4:
Discover Packet:



```
 1051  27…  192.168.0.18   192.168.0.1      DHCP   342  DHCP Release  -
 1133  41…  0.0.0.0        255.255.255.255  DHCP   342  DHCP Discover -
 1134  41…  192.168.0.1    192.168.0.18     DHCP   342  DHCP Offer    -
▶ Frame 57: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Dell_19:80:f2 (00:23:ae:19:80:f2), 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 (68), Dst Port: 67 (67)
▼ Bootstrap Protocol (Discover)
     Message type: Boot Request (1)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
     Hops: 0
     Transaction ID: 0x4ab751cf
     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_19:80:f2 (00:23:ae:19:80:f2)
     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: (61) Client identifier
   ▶ Option: (50) Requested IP Address
```

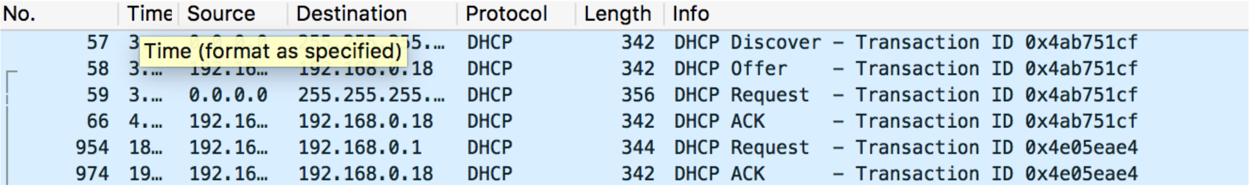
Request Packet:



```
   1051  27…   192.168.0.18             192.168.0.1              DHCP          342  DHCP R
   1133  41…   0.0.0.0                  255.255.255.255          DHCP          342  DHCP D
▶ Frame 59: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface 0
▶ Ethernet II, Src: Dell_19:80:f2 (00:23:ae:19:80:f2), 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 (68), Dst Port: 67 (67)
▼ Bootstrap Protocol (Request)
     Message type: Boot Request (1)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
     Hops: 0
     Transaction ID: 0x4ab751cf
     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_19:80:f2 (00:23:ae:19:80:f2)
     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
```

Inside the Bootstrap Protocol header, we see a field called **Option :(53): DHCP Message Type.** This field is **Discover** is case of Discover messages and **Request** in case of request messages as seen in the above two snapshots. Hence, we can differentiate them with this field.

Answer No 5:

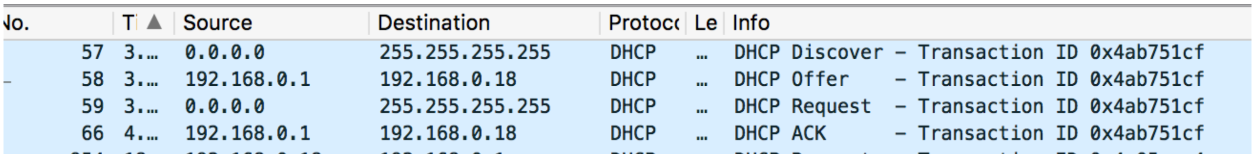


```
No.       Time  Source    Destination     Protocol  Length  Info
      57  3 Time (format as specified) 5.…  DHCP       342  DHCP Discover  – Transaction ID 0x4ab751cf
      58  3.…   192.16…   192.168.0.18    DHCP       342  DHCP Offer     – Transaction ID 0x4ab751cf
      59  3.…   0.0.0.0   255.255.255.…   DHCP       356  DHCP Request   – Transaction ID 0x4ab751cf
      66  4.…   192.16…   192.168.0.18    DHCP       342  DHCP ACK       – Transaction ID 0x4ab751cf
     954  18…   192.16…   192.168.0.1     DHCP       344  DHCP Request   – Transaction ID 0x4e05eae4
     974  19…   192.16…   192.168.0.18    DHCP       342  DHCP ACK       – Transaction ID 0x4e05eae4
```

Transaction ID for the first set of messages = **0x4ab751cf**
Transaction ID for the second set of messages = **0x4e05eae4**

This field is used to distinguish between different client requests during the process. One particular sequence for a full DHCP cycle has same transaction IDs for all it's corresponding messages.

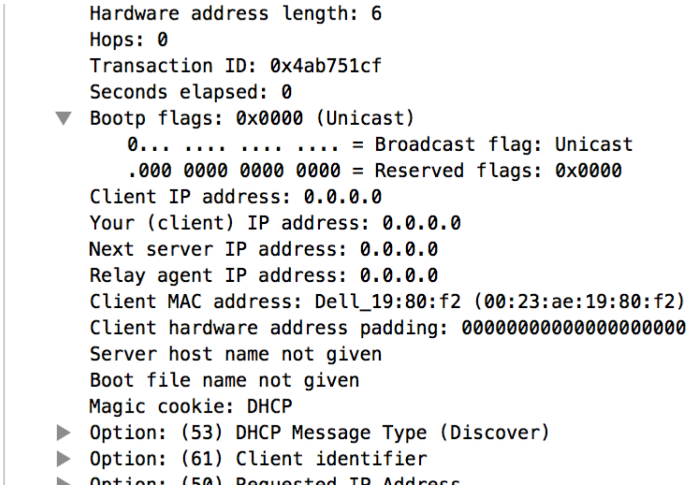
Answer No 6:



No.	T	Source	Destination	Protoco	Le	Info
57	3.…	0.0.0.0	255.255.255.255	DHCP	…	DHCP Discover - Transaction ID 0x4ab751cf
58	3.…	192.168.0.1	192.168.0.18	DHCP	…	DHCP Offer - Transaction ID 0x4ab751cf
59	3.…	0.0.0.0	255.255.255.255	DHCP	…	DHCP Request - Transaction ID 0x4ab751cf
66	4.…	192.168.0.1	192.168.0.18	DHCP	…	DHCP ACK - Transaction ID 0x4ab751cf

Discover Packet : source => 0.0.0.0 , Destination => 255.255.255.255
Offer packet : source => 192.168.0.1, Destination => 192.168.0.18
Request Packet : source => 0.0.0.0, Destination => 255.255.255.255
Ack Packet : source => 192.168.0.1, Destination => 192.168.0.18

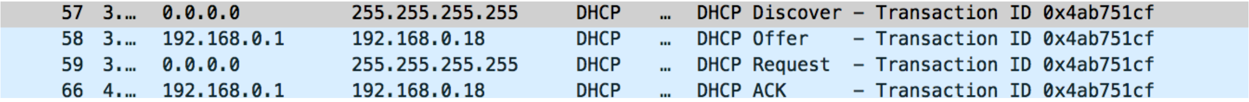
So we can see that initially the client sends a broadcast message for the discovery. Then the DHCP server(in my case, it is the router in my home settings) offers an IP address and directs it as a unicast to the IP message that the client requested. This is a different process than typical DHCP and is used in small networks like home setups. The clients can set the broadcast bit to false so that the Offer packets are unicast instead of board cast, also the client's request an IP to be assigned(RFC 2131). The snapshot below shows how the client requested unicast in the discovery message(Broadcast Flag):



```
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4ab751cf
    Seconds elapsed: 0
  ▼ Bootp flags: 0x0000 (Unicast)
       0... .... .... .... = Broadcast flag: Unicast
       .000 0000 0000 0000 = Reserved flags: 0x0000
    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_19:80:f2 (00:23:ae:19:80:f2)
    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: (61) Client identifier
  ▶ Option: (50) Requested IP Address
```

The request message is again sent as a broadcast from the client and finally the router sends back the acknowledgment as an unicast to the client with his requested IP as the assigned new IP address. This way the full cycle is completed.

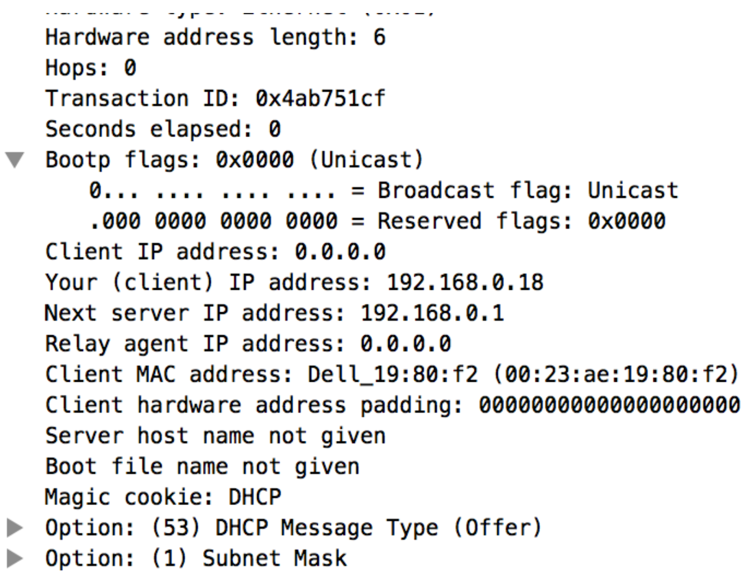
Answer No 7:



```
57  3.…  0.0.0.0        255.255.255.255   DHCP   …  DHCP Discover - Transaction ID 0x4ab751cf
58  3.…  192.168.0.1    192.168.0.18      DHCP   …  DHCP Offer    - Transaction ID 0x4ab751cf
59  3.…  0.0.0.0        255.255.255.255   DHCP   …  DHCP Request  - Transaction ID 0x4ab751cf
66  4.…  192.168.0.1    192.168.0.18      DHCP   …  DHCP ACK      - Transaction ID 0x4ab751cf
```

IP address of the DHCP server : **192.168.0.1**

Answer No 8:

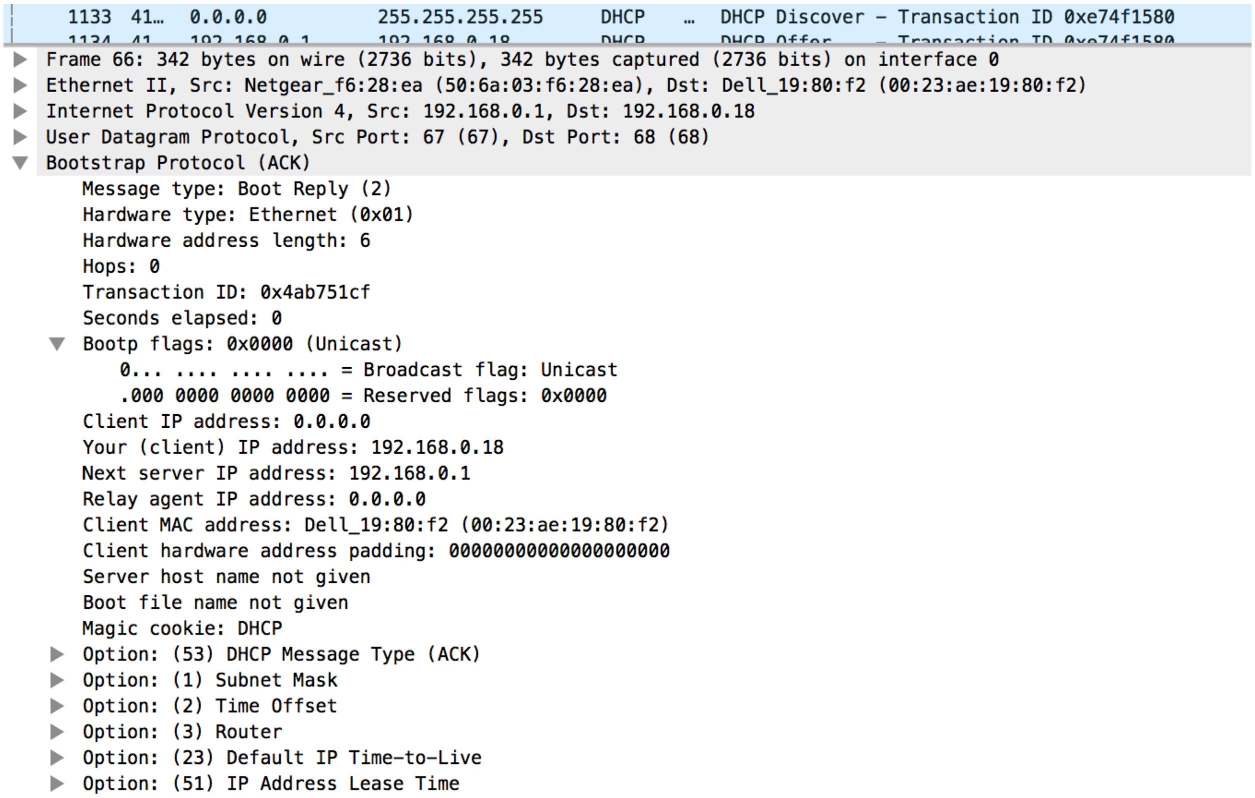


```
   Hardware type: Ethernet (0x01)
   Hardware address length: 6
   Hops: 0
   Transaction ID: 0x4ab751cf
   Seconds elapsed: 0
▼  Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
   Client IP address: 0.0.0.0
   Your (client) IP address: 192.168.0.18
   Next server IP address: 192.168.0.1
   Relay agent IP address: 0.0.0.0
   Client MAC address: Dell_19:80:f2 (00:23:ae:19:80:f2)
   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
```

The offered IP : **192.168.0.18**
The DHCP message **OFFER** contains this IP which can be seen above.(DHCP Message Type : Offer)

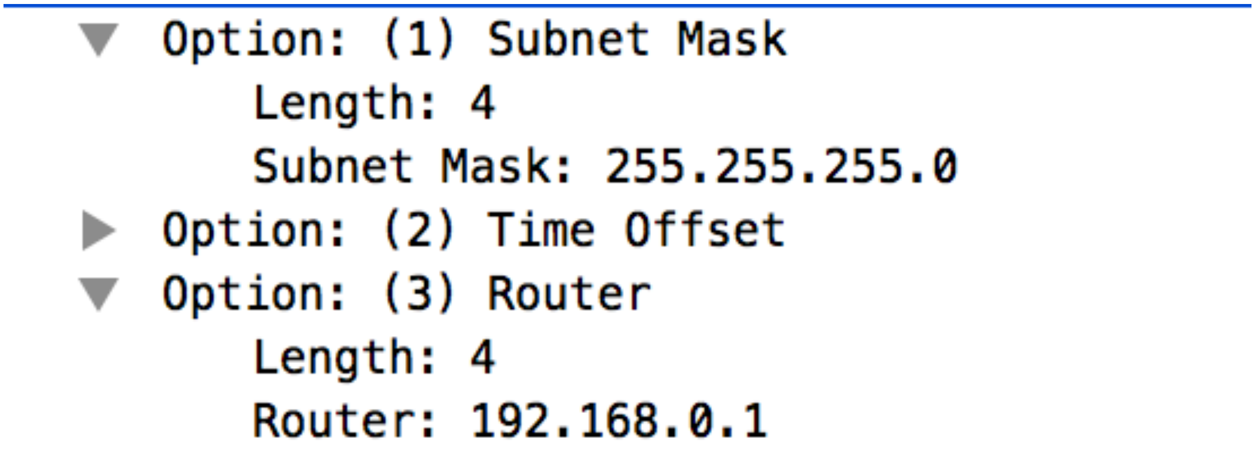
Answer No 9:

There is a field is the Bootstrap header which is called “**Relay Agent IP address**”. The value of this field is **0.0.0.0** in my experiment. This indicates that there was no Relay agent used. The snapshot below shows it.



```
  1133  41…  0.0.0.0          255.255.255.255     DHCP    …  DHCP Discover – Transaction ID 0xe74f1580
  1134  41   192.168.0.1      192.168.0.18        DHCP       DHCP Offer     – Transaction ID 0xe74f1580
▶ Frame 66: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Netgear_f6:28:ea (50:6a:03:f6:28:ea), Dst: Dell_19:80:f2 (00:23:ae:19:80:f2)
▶ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.18
▶ User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
▼ Bootstrap Protocol (ACK)
     Message type: Boot Reply (2)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
     Hops: 0
     Transaction ID: 0x4ab751cf
     Seconds elapsed: 0
  ▼  Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
     Client IP address: 0.0.0.0
     Your (client) IP address: 192.168.0.18
     Next server IP address: 192.168.0.1
     Relay agent IP address: 0.0.0.0
     Client MAC address: Dell_19:80:f2 (00:23:ae:19:80:f2)
     Client hardware address padding: 00000000000000000000
     Server host name not given
     Boot file name not given
     Magic cookie: DHCP
  ▶  Option: (53) DHCP Message Type (ACK)
  ▶  Option: (1) Subnet Mask
  ▶  Option: (2) Time Offset
  ▶  Option: (3) Router
  ▶  Option: (23) Default IP Time-to-Live
  ▶  Option: (51) IP Address Lease Time
```

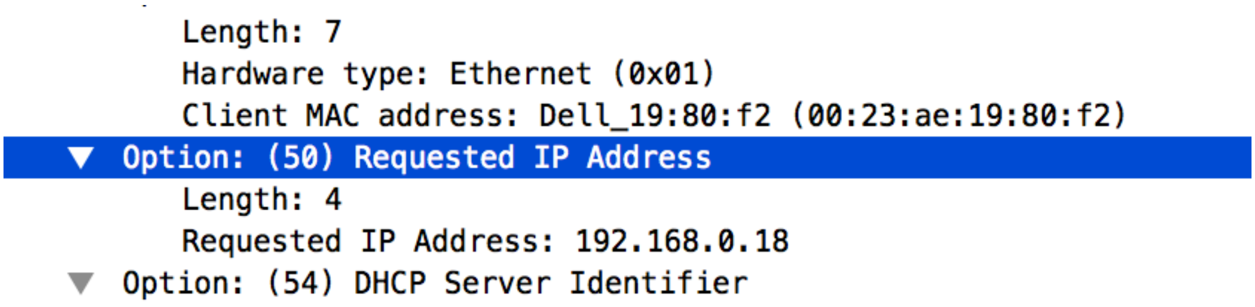
Answer No 10:



```
  ▼  Option: (1) Subnet Mask
          Length: 4
          Subnet Mask: 255.255.255.0
  ▶  Option: (2) Time Offset
  ▼  Option: (3) Router
          Length: 4
          Router: 192.168.0.1
```

1. The **Router** field informs the client what default gateway it should use.
2. The **Subnet** Mask field similarly tells the client which subnet mask it should use.

Answer No 11:

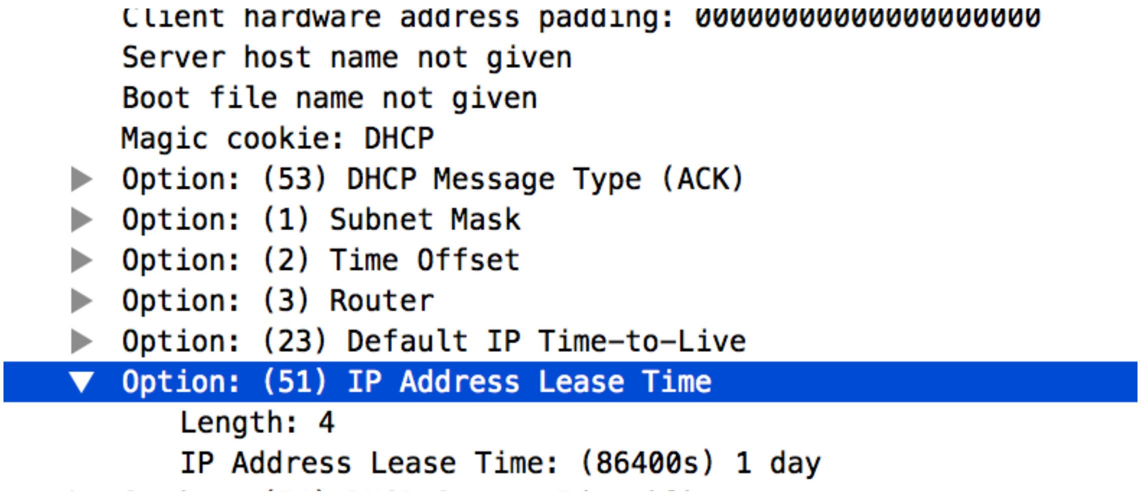


```
         Length: 7
         Hardware type: Ethernet (0x01)
         Client MAC address: Dell_19:80:f2 (00:23:ae:19:80:f2)
   ▼ Option: (50) Requested IP Address
         Length: 4
         Requested IP Address: 192.168.0.18
   ▼ Option: (54) DHCP Server Identifier
```

Similar to the given traces, in my experiment also, the client requests the offered IP address in the **DHCP REQUEST** packet.

Answer No 12:

The Lease Time is the time for which the DHCP server allocates an IP address to the Client requesting for it. It means that during the lease time, the DHCP server will refrain from assigning that IP to anyone else, unless released by the client. But after the Lease time is over , the IP can be assigned to any other system by the DHCP server. This facilitates the reuse of unused IP addresses from a small pool of addresses. In my experiment, the lease time was 1 day as seen below.



```
       Client hardware address padding: 00000000000000000000
       Server host name not given
       Boot file name not given
       Magic cookie: DHCP
   ▶ Option: (53) DHCP Message Type (ACK)
   ▶ Option: (1) Subnet Mask
   ▶ Option: (2) Time Offset
   ▶ Option: (3) Router
   ▶ Option: (23) Default IP Time-to-Live
   ▼ Option: (51) IP Address Lease Time
          Length: 4
          IP Address Lease Time: (86400s) 1 day
```

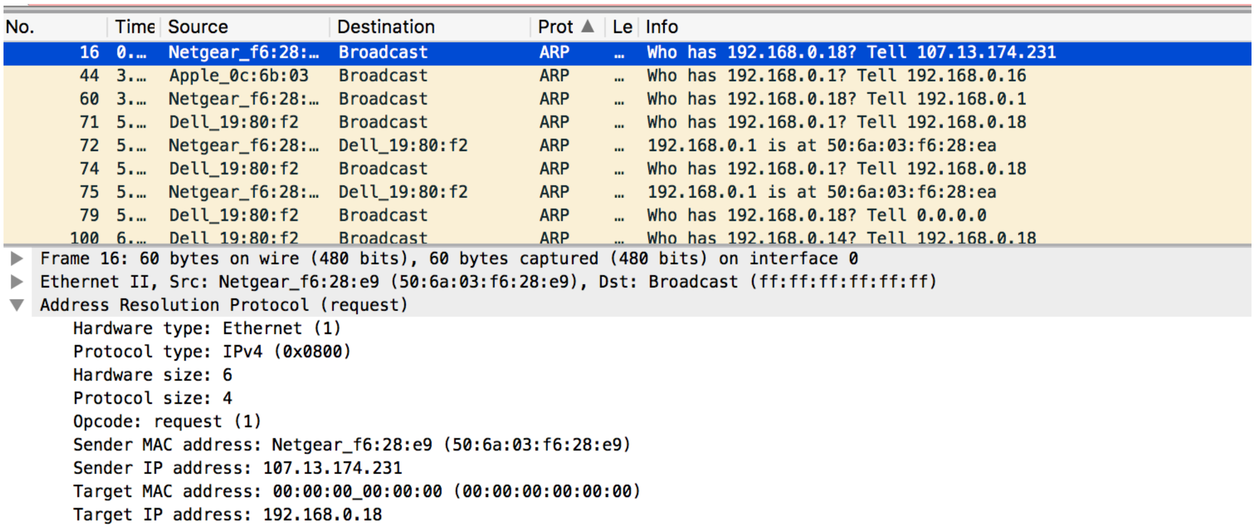
Answer No 13:

The purpose of the DHCP release message is to tell the DHCP server that the client has released the IP address assigned and the server can use it for other systems in the network.

The server doesn’t send any acknowledgement back to the client.

If the release messages get lost, then the server does’t know abut the release and it waits till the lease period is over just like the normal flow.

Answer No 14:



```
No.    Time  Source            Destination     Prot ▲  Le  Info
    16 0.…   Netgear_f6:28:…   Broadcast       ARP     …   Who has 192.168.0.18? Tell 107.13.174.231
    44 3.…   Apple_0c:6b:03    Broadcast       ARP     …   Who has 192.168.0.1? Tell 192.168.0.16
    60 3.…   Netgear_f6:28:…   Broadcast       ARP     …   Who has 192.168.0.18? Tell 192.168.0.1
    71 5.…   Dell_19:80:f2     Broadcast       ARP     …   Who has 192.168.0.1? Tell 192.168.0.18
    72 5.…   Netgear_f6:28:…   Dell_19:80:f2   ARP     …   192.168.0.1 is at 50:6a:03:f6:28:ea
    74 5.…   Dell_19:80:f2     Broadcast       ARP     …   Who has 192.168.0.1? Tell 192.168.0.18
    75 5.…   Netgear_f6:28:…   Dell_19:80:f2   ARP     …   192.168.0.1 is at 50:6a:03:f6:28:ea
    79 5.…   Dell_19:80:f2     Broadcast       ARP     …   Who has 192.168.0.18? Tell 0.0.0.0
   100 6.…   Dell_19:80:f2     Broadcast       ARP     …   Who has 192.168.0.14? Tell 192.168.0.18
▶ Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▶ Ethernet II, Src: Netgear_f6:28:e9 (50:6a:03:f6:28:e9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: Netgear_f6:28:e9 (50:6a:03:f6:28:e9)
      Sender IP address: 107.13.174.231
      Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Target IP address: 192.168.0.18
```

YES, there were ARP packets issued by the DHCP server as shown above. This is done just before assigning the IP address to the client to check if anyone has already taken that IP address corresponding to a hardware address.