WIRESHARK CA1

Hamidreza Ali-akbar Khoyi – ST ID : 81096514

Contents

Introduction

In this Computer Assignment the goal is to explore 3 important Network Protocols : HTTP in the Application Layer and ARP in the Data link layer DHCP Also running in the Application Layer.

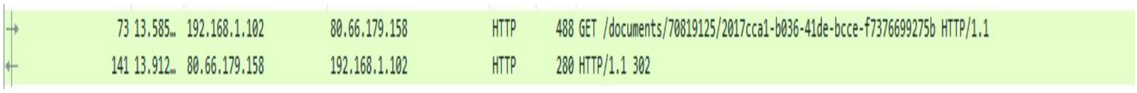
- In Each Part we will analyze the Source and Destination Addresses (MAC, IP), Message Types, headers, timing parameters, etc. Also we ought to explain the way data is being transformed to server and layers It should cross to.

Part1

1.1:

Destination IP address due to figure 1 is 80.66.179.158 and also source IP address is 192.168.1.102

Destination in this part is "ece.ut.ac.ir" as mentioned in project.



```
→   73 13.585…  192.168.1.102   80.66.179.158   HTTP   488 GET /documents/70819125/2017cca1-b036-41de-bcce-f7376699275b HTTP/1.1
←  141 13.912…  80.66.179.158   192.168.1.102   HTTP   280 HTTP/1.1 302
```

Figure 1

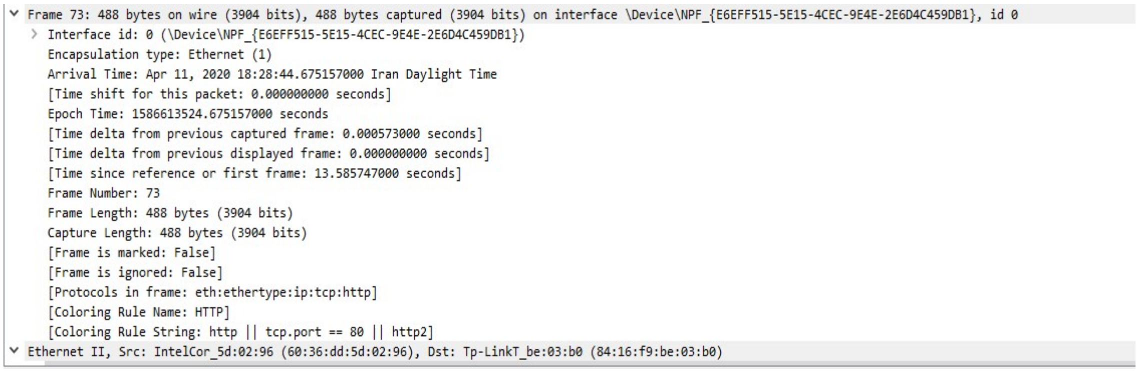
1.2

As shown in figure1 get request and get response packets are 73 and 141.

TTL refers to amount of time that a packet is set to exist inside a network before being discarded by router.

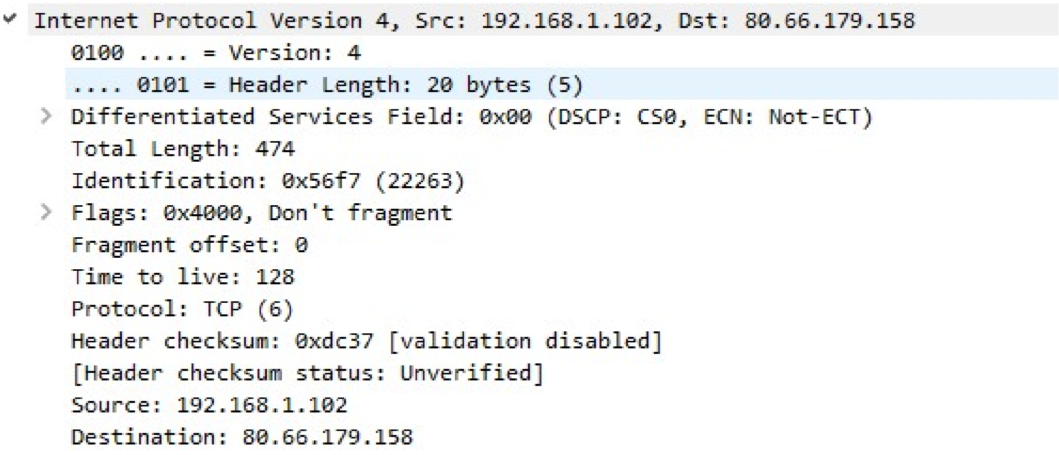
for each switch/router/computer network traffic passes through route to the destination, that counts as 1 hop, and the **TTL** to your destination will decrease by each hop. So, when you **PING** something on your LAN, the **TTL** will be **128**, since all machines on your same subnet (192.168. 1.0/24) are all just 1 hop away.

So for this case time to live is 128 as figure3 shows it.



```
v Frame 73: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface \Device\NPF_{E6EFF515-5E15-4CEC-9E4E-2E6D4C459DB1}, id 0
  > Interface id: 0 (\Device\NPF_{E6EFF515-5E15-4CEC-9E4E-2E6D4C459DB1})
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 11, 2020 18:28:44.675157000 Iran Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1586613524.675157000 seconds
    [Time delta from previous captured frame: 0.000573000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 13.585747000 seconds]
    Frame Number: 73
    Frame Length: 488 bytes (3904 bits)
    Capture Length: 488 bytes (3904 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
v Ethernet II, Src: IntelCor_5d:02:96 (60:36:dd:5d:02:96), Dst: Tp-LinkT_be:03:b0 (84:16:f9:be:03:b0)
```

Figure 2



```
⌄ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 80.66.179.158
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 474
     Identification: 0x56f7 (22263)
   > Flags: 0x4000, Don't fragment
     Fragment offset: 0
     Time to live: 128
     Protocol: TCP (6)
     Header checksum: 0xdc37 [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.102
     Destination: 80.66.179.158
```

Figure 3

1.3

My 48bit address is 60:36:dd:5d:02:96 that shows source as shown in figure 2.

۱/۴

This address as shown in figure 2 is: 84:19:f9:be:03:b0

This is not showing the destination itself but showing my TP Link router address or in other words a gateway to internet.

۱/۵

Header Size : 20 bytes.(shown in figure3)

Both TCP & IP headers are 20 bytes long.

۱/۶

The ASCII “O” appears **52 bytes** from the start of the Ethernet frame. Again, there are **14 bytes** of Ethernet frame, and then **20 bytes** of IP header followed by **20 bytes** of TCP header before the HTTP data is encountered.

Reason for this is it that each packet has two headers and in this case fist letter to transfer in ,is"o".

Part2

ARP protocol consist of two main parts including the part which determines a physical address when a packet is sent, also second part is for answering request from the machines. So ARP provides method for hosts to send message to destination address on a physical network.

Ethernet hosts must convert a 32-bit IP address into a 48-bit Ethernet address. The host checks its ARP cache to see if address mapping from IP to physical address is known:

If mapping is known physical address is placed in frame and sent to recognized destination,

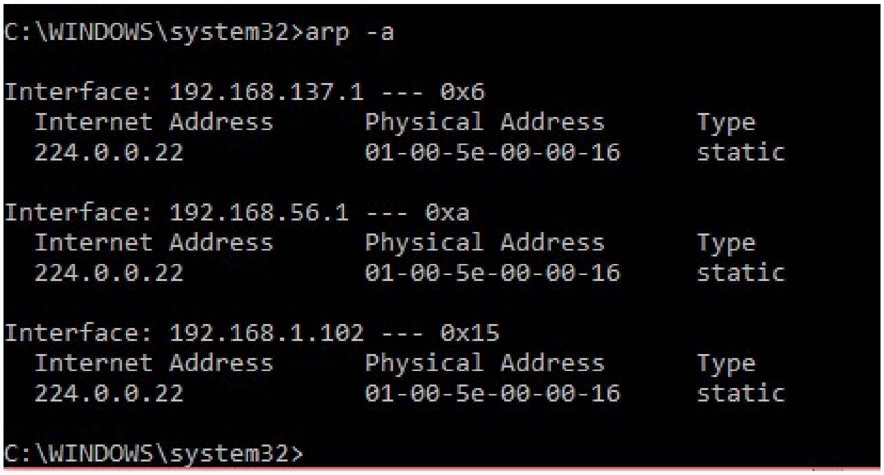
Or,if mapping is unknown,broadcast messages is sent and awaits a reply,else target machine recognizes IP address matches its own and returns answer.

۲/۱

As explained at fisrt of part we know what cache of ARP protocol is.

First column is ip-address and second is for MAC address and third on is showing protocol-type.

Dynamic entry has been learned and is kept on a device for some period of time, as long as it is being used.But static entry could be chose manually or even by your computer programs (in this case these will predefine itself).



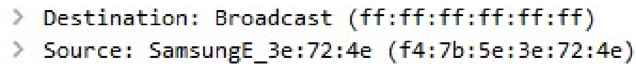
```
C:\WINDOWS\system32>arp -a

Interface: 192.168.137.1 --- 0x6
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.56.1 --- 0xa
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

Interface: 192.168.1.102 --- 0x15
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static

C:\WINDOWS\system32>
```

Figure 4

۲/۲

a)

because of destination we have ff:ff:ff:ff:ff:ff:ff

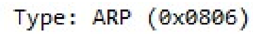


```
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)
> Source: SamsungE_3e:72:4e (f4:7b:5e:3e:72:4e)
```

Figure 5

b)

as hexadecimal value 0806 we know this is our ARP.



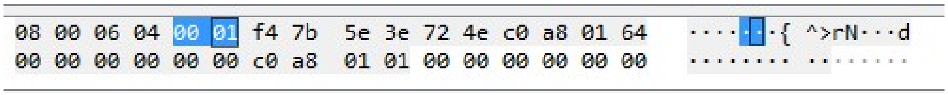
```
Type: ARP (0x0806)
```

Figure 6

c)

answer will be 00 01

reason for it is that it belong to ARP-payload part of Ethernet frame.

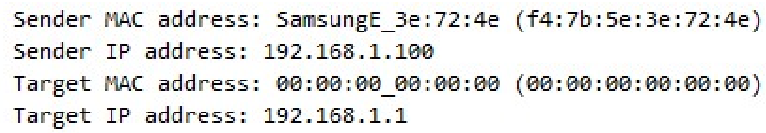


```
08 00 06 04 00 01 f4 7b  5e 3e 72 4e c0 a8 01 64   ·······{ ^>rN···d
00 00 00 00 00 00 c0 a8  01 01 00 00 00 00 00 00   ········ ········
```

Figure 7

d)

yes, it has sender IP address.



```
Sender MAC address: SamsungE_3e:72:4e (f4:7b:5e:3e:72:4e)
Sender IP address: 192.168.1.100
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1
```

Figure 8

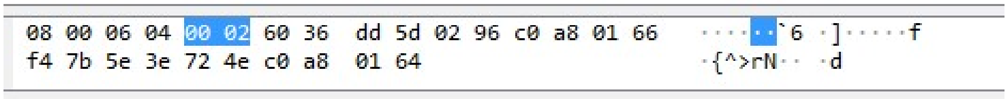
e)

target mac address is being ignored and in packet that a send it outs mac address of gate way and because it doesn’t have the destination mac address so it has to put 0.

So it broadcast its IP address for the whole networks, receiver gives response when he sees his IP and then it puts his MAC address in the response. After Sender has received the MAC address it will be saved in the ARP cache for next communications.

2.3)

a)



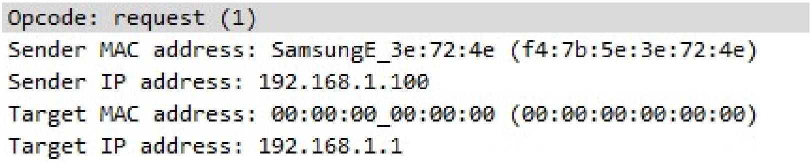
```
08 00 06 04 00 02 60 36  dd 5d 02 96 c0 a8 01 66   ······`6 ·]·····f
f4 7b 5e 3e 72 4e c0 a8  01 64                     ·{^>rN·· ·d
```

Figure 9

Because it is a response in bottom of who in id we should go to reply and click it and because it is response so it is 00 02.

b)

sender mac address (as we are searching in device B)

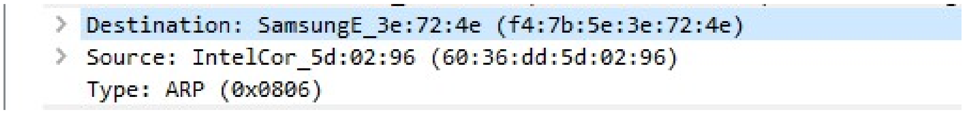


```
Opcode: request (1)
Sender MAC address: SamsungE_3e:72:4e (f4:7b:5e:3e:72:4e)
Sender IP address: 192.168.1.100
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1
```

Figure 10

Sender mac address show the answer that comes.

c)



```
> Destination: SamsungE_3e:72:4e (f4:7b:5e:3e:72:4e)
> Source: IntelCor_5d:02:96 (60:36:dd:5d:02:96)
  Type: ARP (0x0806)
```

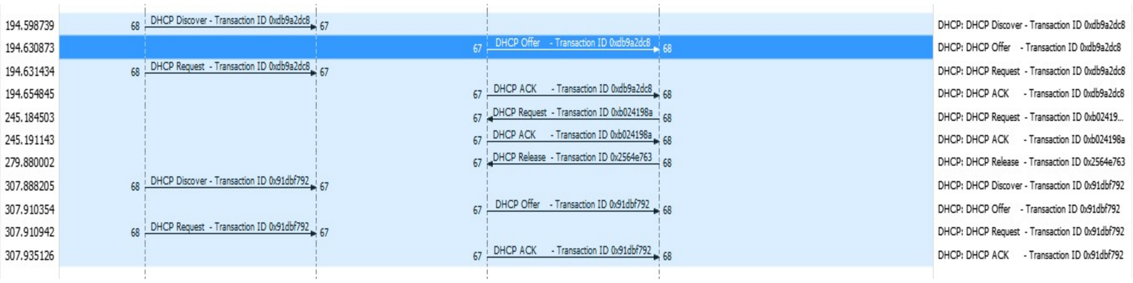
Figure 11

Answer is hexdecimal (f4:7b:5e:3e:72:4e) .

Part3

1)

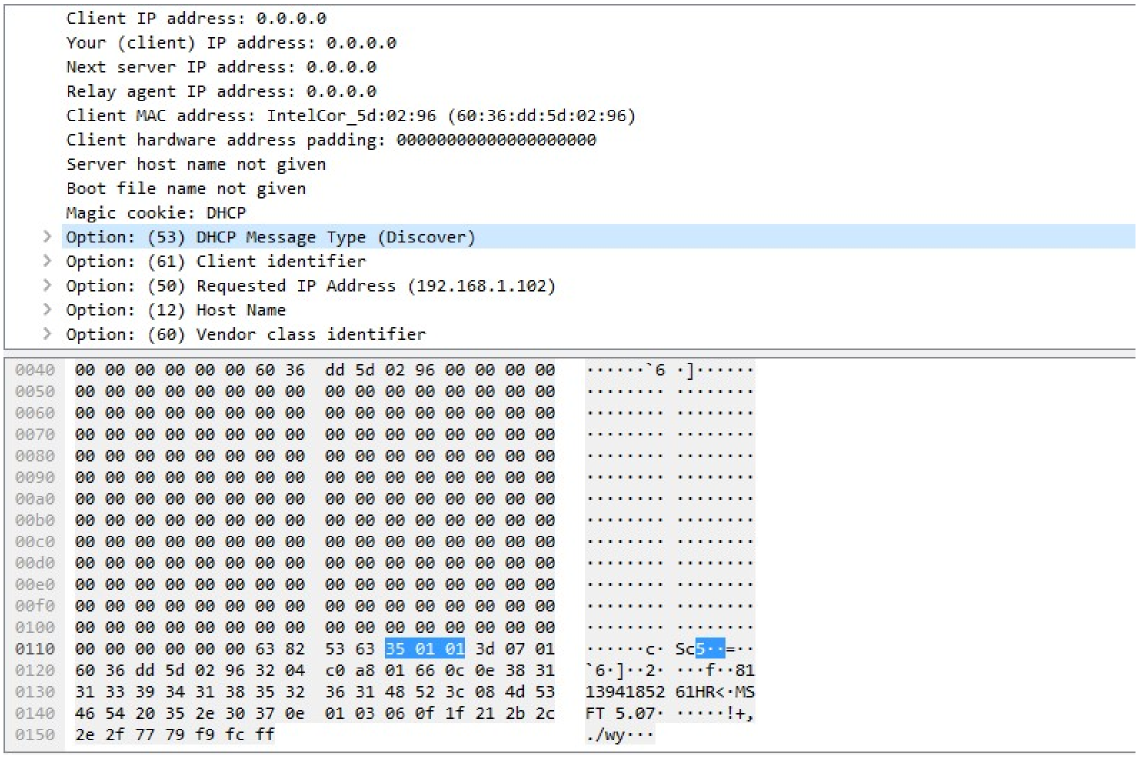
Timing diagram is displayed in Fig.12.



```
194.598739  68 DHCP Discover - Transaction ID 0xdb9a2dc8 67          DHCP: DHCP Discover - Transaction ID 0xdb9a2dc8
194.630873  67 DHCP Offer    - Transaction ID 0xdb9a2dc8 68          DHCP: DHCP Offer    - Transaction ID 0xdb9a2dc8
194.631434  68 DHCP Request  - Transaction ID 0xdb9a2dc8 67          DHCP: DHCP Request  - Transaction ID 0xdb9a2dc8
194.654845  67 DHCP ACK      - Transaction ID 0xdb9a2dc8 68          DHCP: DHCP ACK      - Transaction ID 0xdb9a2dc8
245.184503  67 DHCP Request  - Transaction ID 0xb024198a 68          DHCP: DHCP Request  - Transaction ID 0xb02419...
245.191143  67 DHCP ACK      - Transaction ID 0xb024198a 68          DHCP: DHCP ACK      - Transaction ID 0xb024198a
279.880002  67 DHCP Release  - Transaction ID 0x2564e763 68          DHCP: DHCP Release  - Transaction ID 0x2564e763
307.888205  68 DHCP Discover - Transaction ID 0x91dbf792 67          DHCP: DHCP Discover - Transaction ID 0x91dbf792
307.910354  67 DHCP Offer    - Transaction ID 0x91dbf792 68          DHCP: DHCP Offer    - Transaction ID 0x91dbf792
307.910942  68 DHCP Request  - Transaction ID 0x91dbf792 67          DHCP: DHCP Request  - Transaction ID 0x91dbf792
307.935126  67 DHCP ACK      - Transaction ID 0x91dbf792 68          DHCP: DHCP ACK      - Transaction ID 0x91dbf792
```

Figure 12

2)



```
    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: IntelCor_5d:02:96 (60:36:dd:5d:02:96)
    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 (192.168.1.102)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
```

```
0040  00 00 00 00 00 00 60 36  dd 5d 02 96 00 00 00 00   ······`6 ·]······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d 07 01   ······c· Sc5··=··
0120  60 36 dd 5d 02 96 32 04  c0 a8 01 66 0c 0e 38 31   `6·]··2· ···f··81
0130  31 33 39 34 31 38 35 32  36 31 48 52 3c 08 4d 53   13941852 61HR<·MS
0140  46 54 20 35 2e 30 37 0e  01 03 06 0f 1f 21 2b 2c   FT 5.07· ·····!+,
0150  2e 2f 77 79 f9 fc ff                               ./wy···
```

Figure 13

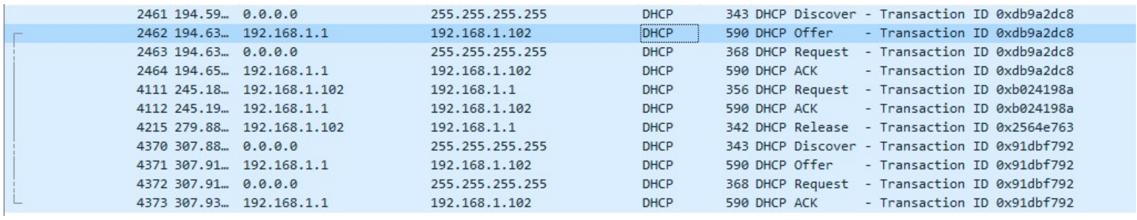
Option 53 is cause of difference.

3)

Purpose is:

For each messages is sent , transaction id will be renewed 'it'll be obtained from different IP addresses)so it causes that requests of variated clients will be different.

4)

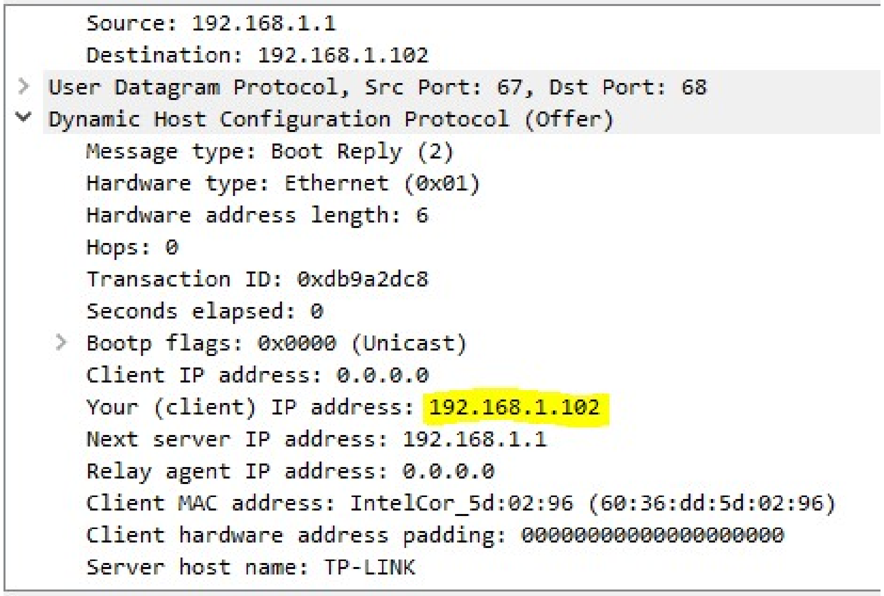


```
2461 194.59…  0.0.0.0        255.255.255.255   DHCP   343 DHCP Discover - Transaction ID 0xdb9a2dc8
2462 194.63…  192.168.1.1    192.168.1.102     DHCP   590 DHCP Offer    - Transaction ID 0xdb9a2dc8
2463 194.63…  0.0.0.0        255.255.255.255   DHCP   368 DHCP Request  - Transaction ID 0xdb9a2dc8
2464 194.65…  192.168.1.1    192.168.1.102     DHCP   590 DHCP ACK      - Transaction ID 0xdb9a2dc8
4111 245.18…  192.168.1.102  192.168.1.1       DHCP   356 DHCP Request  - Transaction ID 0xb024198a
4112 245.19…  192.168.1.1    192.168.1.102     DHCP   590 DHCP ACK      - Transaction ID 0xb024198a
4215 279.88…  192.168.1.102  192.168.1.1       DHCP   342 DHCP Release  - Transaction ID 0x2564e763
4370 307.88…  0.0.0.0        255.255.255.255   DHCP   343 DHCP Discover - Transaction ID 0x91dbf792
4371 307.91…  192.168.1.1    192.168.1.102     DHCP   590 DHCP Offer    - Transaction ID 0x91dbf792
4372 307.91…  0.0.0.0        255.255.255.255   DHCP   368 DHCP Request  - Transaction ID 0x91dbf792
4373 307.93…  192.168.1.1    192.168.1.102     DHCP   590 DHCP ACK      - Transaction ID 0x91dbf792
```

Figure 14

5)

The IP address of the DHCP server is shown in the offer message for the first time



```
    Source: 192.168.1.1
    Destination: 192.168.1.102
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xdb9a2dc8
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.102
    Next server IP address: 192.168.1.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_5d:02:96 (60:36:dd:5d:02:96)
    Client hardware address padding: 00000000000000000000
    Server host name: TP-LINK
```

Figure 15

6)

Your IP(client)address is :192.168.1.102 as shown in figure 15.

7)

The client accepts the offered IP address from the DHCP server :
This IP (192.168.1.102) is shown in the Option 50 of the "Request" message

8)

DHCP Lease Time is the amount of time in minutes or seconds a network device can use an IP Address in a network.
The IP Address is reserved for that device until the reservation expires. The DHCP server is responsible for assigning every device a unique address.