University of Tehran
College of Engineering
School of Electrical and Computer Engineering

Computer Networks

Dr.Shah-Mansouri

Wireshark Lab 1

Soroush Mesforush Mashhad

SN:810198472

Ordibehesht 01

Contents

Abstract

In this assignment, our goal is to get familiar with Ethernet and ARP(address resolution protocol).

In the first part, we shall attempt to capture and analyze the IP headers as instructed in the assignment description using Wireshark.

In the next section we go on to observe the ARP protocol in action, we pay attention that the ARP protocol normally maintains a cache of IP-to-Ethernet address translation pairs in out computer. We then go on to satisfy the assignment's requirements.

In the final part we shall observe the DHCP protocol, we need to carry out this part in a place where we have a dynamically assigned IP address.

1 Capturing and analyzing Ethernet and IP headers

1.1 GET request and respond frames

The frame numbers of the GET request and response are as follows.

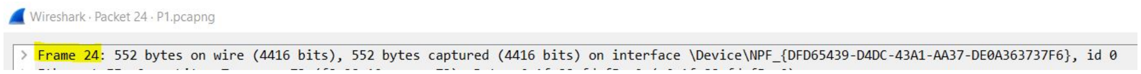


Figure 1: GET request frame

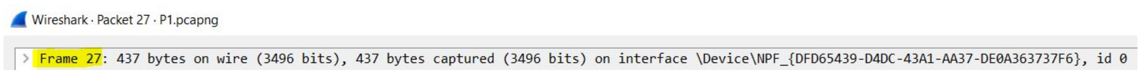


Figure 2: GET response frame

Hence the frame numbers are:

$$GET\ Request\ NO = 24, \quad GET\ Response\ NO = 27$$

1.2 Q1

First of all, a screenshot of the packet sniffer containing the IP of the destination and source is included.

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
…	3.560360	192.168.43.244	80.66.177.54	HTTP	552	GET / HTTP/1.1
…	3.607702	80.66.177.54	192.168.43.244	HTTP	437	HTTP/1.1 301 Moved Permanently (text/html)

Figure 3: Filtered HTTP packets

So we have the following

$$Source\ IP : 192.168.43.244 \quad Destination\ IP : 80.66.177.54$$

Now we go on to locate the MAC address of the source and destination.

I have included the following pictures of the properties of the send and receive frames.

```
Ethernet II, Src: LiteonTe_ae:ea:73 (f8:28:19:ae:ea:73), Dst: e6:1f:88:fd:f5:a0 (e6:1f:88:fd:f5:a0)
  Destination: e6:1f:88:fd:f5:a0 (e6:1f:88:fd:f5:a0)
  Source: LiteonTe_ae:ea:73 (f8:28:19:ae:ea:73)
  Type: IPv4 (0x0800)
```

Figure 4: Send frame

```
Ethernet II, Src: e6:1f:88:fd:f5:a0 (e6:1f:88:fd:f5:a0), Dst: LiteonTe_ae:ea:73 (f8:28:19:ae:ea:73)
  Destination: LiteonTe_ae:ea:73 (f8:28:19:ae:ea:73)
  Source: e6:1f:88:fd:f5:a0 (e6:1f:88:fd:f5:a0)
  Type: IPv4 (0x0800)
```

Figure 5: Get frame

Hence we conclude that.

$$Source\ MAC\ Address : f8 : 28 : 19 : ae : ea : 73$$

$$Destination\ MAC\ Address : e6 : 1f : 88 : fd : f5 : a0$$

1.3 Q2

The IP address of my computer shall be the same as the source which is:

$$PC\ IP : 192.168.43.244$$

1.4 Q3

First we define the time to live of a packet.

Time to Live(TTL)(Hop limit)

The TTL of a packet is an amount or value for the period of time that a packet should exist on a computer or a network before being discarded.

Now we observe the TTL for the send and receive packets.

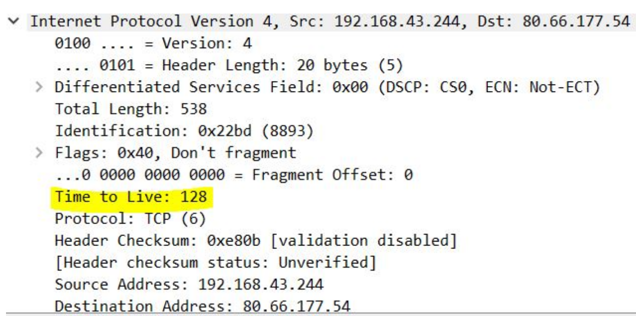


Figure 6: Send frame TTL

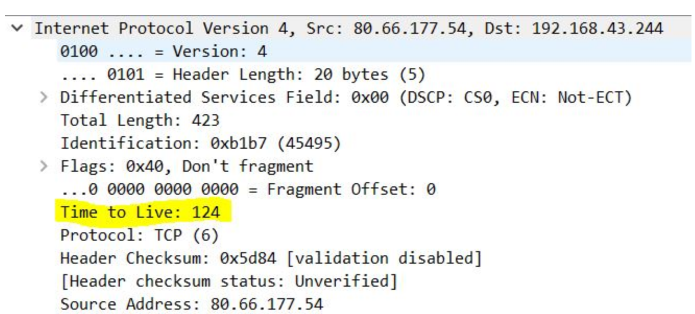


Figure 7: Get frame TTL

So we have:

$$TTL_{Send} = 128, \quad TTL_{Receive} = 124$$

It is useful to mention that the TTL is given in seconds.

TTL Purpose:

The TTL prevents a packet from circulating indefinitely in our network, also TTL is most commonly used to improve the performance and manage the catching of data.

1.5 Q4

The header length for the IP layer is as follows.

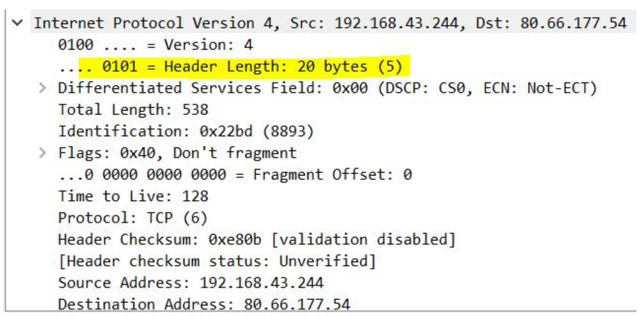


Figure 8: IP layer header length

The MAC layer size is the same as the Ethernet layer which is 14 bytes.

For insurance, I have included the header length of the Transmission control protocol (TCP).

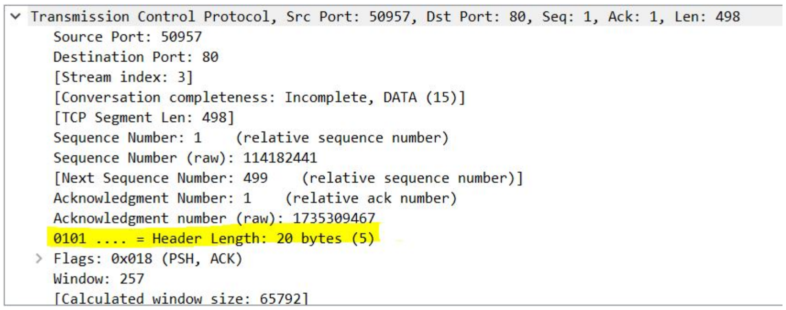


Figure 9: TCP header length

Now we go on to explain the next part of the question.

The 'O' in ASCII appears 52 bytes from the start of the Ethernet frame, then again we have 14 bytes of the Ethernet frame, followed by 20 bytes of the IP layer header which is followed by 20 bytes of the TCP header, then the HTTP data is encountered.

1.6 Q5

The answer is positive, the IP has provision for header fields identified by an option type field.

Due to the possibility of the IP datagram might contain different number of options, the total length of the option field shall be variable in the IPv4(IPv6) header, these options are multiple bytes in length, this is because each option needs to convey different lengths of information, when we have more than one option they are concatenated and form the option field in unison, this field is optional and all datagrams don't have it.

Figure 10: TCP header length

2 The Address Resolution Protocol

2.1 Q1

The ARP table is as follows.

```
C:\Users\Soroush>arp -a

Interface: 192.168.56.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.43.244 --- 0x10
  Internet Address      Physical Address      Type
  192.168.43.1          e6-1f-88-fd-f5-a0     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 11: ARP table

The first column from the left AKA the internet address column contains the IP address, the second column AKA the physical address column contains the MAC addresses, and the third column AKA the type column shows the protocol type.

2.2 Q2

2.2.1 a

The hexadecimal values for the source and destination are as follows.

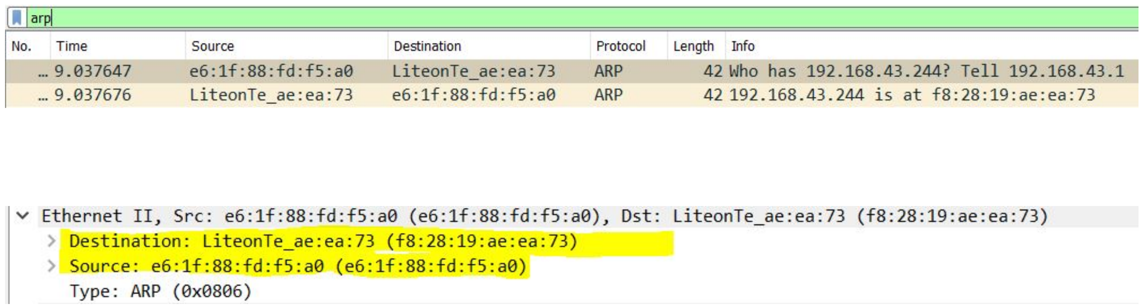


Figure 12: Source and destination Hexadecimal

2.2.2 b

We know that the ARP belongs to the DLL layer, and what it does is save the mappings of the IP address which is in the network layer to the MAC address which is in the physical layer which is beneath the network layer and DLL layer, hence ARP corresponds to IP protocols.

2.2.3 c

The value of the opcode field can be seen as below.

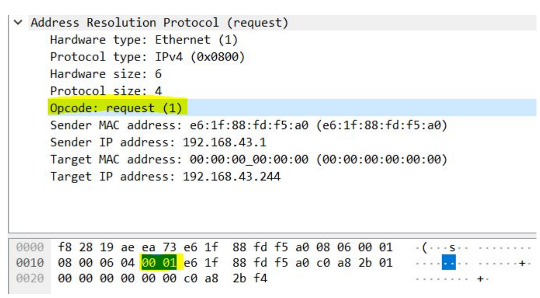
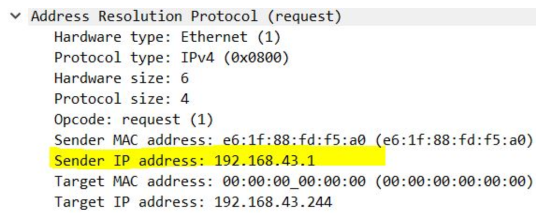


Figure 13: Opcode value

$$Opcode = 0001$$

2.2.4 d

The ARP message contains the sender IP, I have highlighted it in the following screenshot.



```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: e6:1f:88:fd:f5:a0 (e6:1f:88:fd:f5:a0)
    Sender IP address: 192.168.43.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.43.244
```

Figure 14: Opcode value

$$Sender\ IP = 192.168.43.1$$

2.2.5 e

The target MAC address is set to zero, because the source sure of its destination, hence broadcasting occurs, this is the meaning of the MAC address being set to zero, the IP address is broadcasted for the whole network and the destination gives a response when it sees the IP and puts the corresponding MAC address in response, in short the IP address 192.168.43.244 is being queried.

2.3 Q3

2.3.1 a

The value of the opcode field can be seen as below.

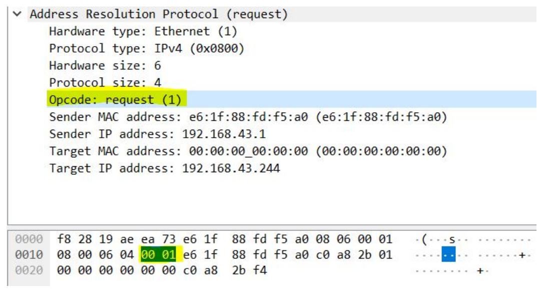


Figure 15: Opcode value

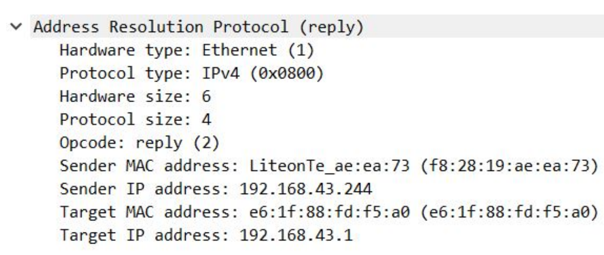
$$Opcode = 0002$$

2.3.2 b

The answer for the earlier ARP request is located in the **Sender MAC address** in which contains the IP and MAC address of the sender.

2.3.3 c

The hexadecimal values can be seen as follows.



$$Sender_{IP} : 192.168.43.244, \quad Sender_{MAC} : f8 : 28 : 19 : ae : ea : 73$$
$$Target_{IP} : 192.168.43.1, \quad Target_{MAC} : e6 : 1f : 88 : fd : f5 : a0$$

3 DHCP

We pay attention that our IP address is dynamic, then we complete the instructions.

3.1 Q1

The packet sniffer is as follows.

bootp

No.	Time	Source	Destination	Protocol	Length	Info
…	11.374702	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xd9cde183
…	11.386267	192.168.1.1	192.168.1.116	DHCP	328	DHCP Offer - Transaction ID 0xd9cde183
…	11.386824	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xd9cde183
…	11.410530	192.168.1.1	192.168.1.116	DHCP	378	DHCP ACK - Transaction ID 0xd9cde183
…	19.650005	192.168.1.116	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x7f93add2
…	30.190902	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xbd86c4df
…	30.201585	192.168.1.1	192.168.1.116	DHCP	328	DHCP Offer - Transaction ID 0xbd86c4df
…	30.202283	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xbd86c4df
…	30.229997	192.168.1.1	192.168.1.116	DHCP	378	DHCP ACK - Transaction ID 0xbd86c4df

Figure 16: Packet sniffer

The timing diagram(flow graph) is displayed below.

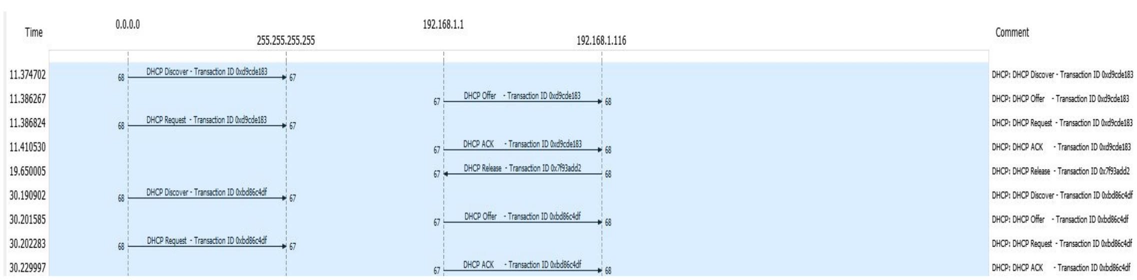


Figure 17: Timing diagram

3.2 Q2

As it is depicted in the picture below, option number **53**(DHCP message type) contains the values which differentiate the discover message from the request message.

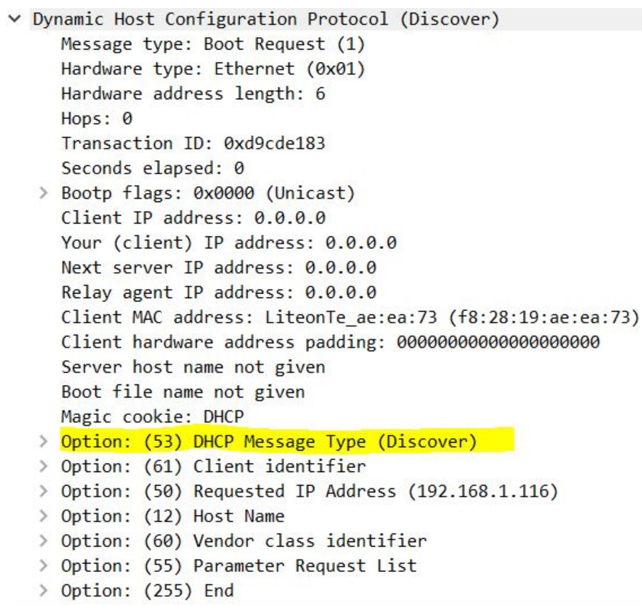


Figure 18: Option 53

3.3 Q3

First, we give a brief explanation about the purpose of the transaction ID.

3.3.1 Transaction ID purpose

We know that the client picks the transaction ID, this normally happens randomly, the server goes to copy this ID in the response, this ID is used to differentiate between different clients in the network, to put in simply, the transaction ID is used to identify if a message is part of a set related to one transaction.

3.3.2 First four DHCP messages

The transaction ID can be seen as follows.

Figure 19: Transaction ID(Discover,Request)

Figure 20: Transaction ID(Offer,ACK)

$$Transaction\ ID : 0xd9cde183$$

3.3.3 Second four DHCP messages

The transaction ID can be seen as follows.

Figure 21: Transaction ID(Discover,Request)

Figure 22: Transaction ID(Offer,ACK)

$$Transaction\ ID : 0xbd86c4df$$

As expected in each set these values are the same for Discover,Request,Offer and ACK.

3.4 Q4

The source and destination IP for the different DHCP messages are shown below.

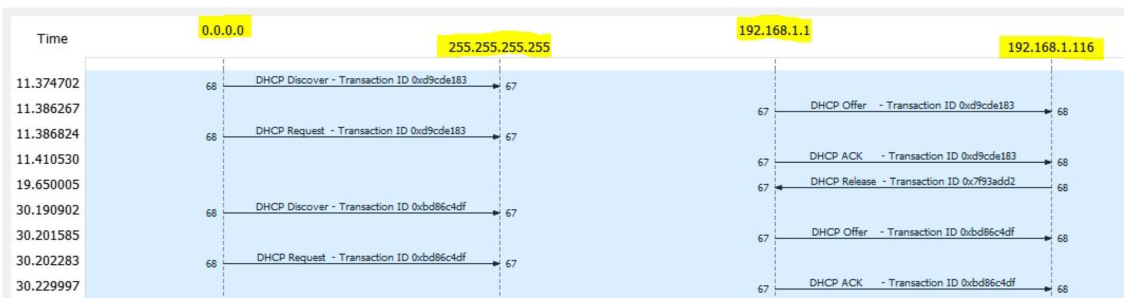


Figure 23: Ips for DHCP messages

3.4.1 Discover and Request

$$Source : 0.0.0.0 \quad Destination : 255.255.255.255$$

3.4.2 Offer and ACK

$$Source : 192.168.1.1 \quad Destination : 192.168.1.116$$

We must pay attention that **255.255.255.255** implies that the message is being broadcasted.

3.5 Q5

The IP address of our DHCP server is shown in the offer message for the first time as follows.

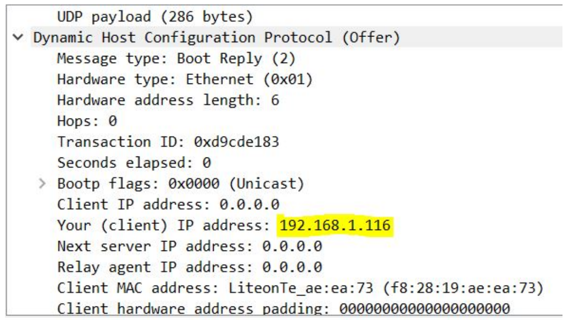
… 11.374702	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xd9cde183
… 11.386267	192.168.1.1	192.168.1.116	DHCP	328	DHCP Offer - Transaction ID 0xd9cde183
… 11.386824	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xd9cde183
… 11.410530	192.168.1.1	192.168.1.116	DHCP	378	DHCP ACK - Transaction ID 0xd9cde183
… 19.650005	192.168.1.116	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x7f93add2
… 30.190902	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xbd86c4df
… 30.201585	192.168.1.1	192.168.1.116	DHCP	328	DHCP Offer - Transaction ID 0xbd86c4df
… 30.202283	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xbd86c4df
… 30.229997	192.168.1.1	192.168.1.116	DHCP	378	DHCP ACK - Transaction ID 0xbd86c4df

Figure 24: DHCP IP

$$DHCP_{IP} = 192.168.1.1$$

3.6 Q6

Our computer's IP is set at **0.0.0.0** at the moment, hence the DHCP server offers the client an IP address, this address may be observed in the offer message which is:



```
    UDP payload (286 bytes)
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd9cde183
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.1.116
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_ae:ea:73 (f8:28:19:ae:ea:73)
    Client hardware address padding: 00000000000000000000
```

Figure 25: Client IP

$$Client_{IP} = 192.168.1.116$$

3.7 Q7

The DHCP server offers the client a certain IP as shown in the previous question, this IP is accepted by the client and the client's requested IP address can be seen in option 50 of the request message as follows.

Figure 26: Requested IP address

$$Requested_{IP} = 192.168.1.116$$

3.8 Q8

The DHCP lease time, is the time assigned by the DHCP server for an IP address to a client, in other words it is the time a client can use an IP address in the network without the IP being reassigned to another client. After the expiration of the lease time the IP may be assigned to new clients by the DHCP server.

3.8.1 DHCP lease time in our case

This time is depicted as follows.

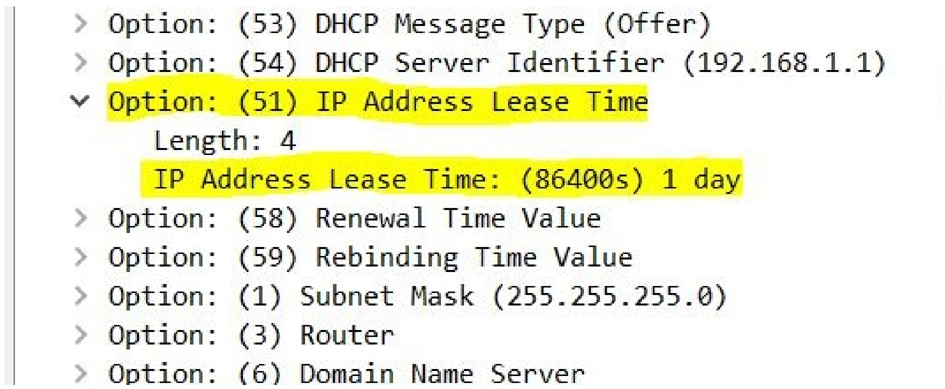


Figure 27: DHCP lease time

$$Lease\,Time = 86400s = 1Day$$