

# 天津大学

## 《计算机网络》



题目：Wireshark Lab: DHCP

学 院 智能与计算学部

专 业 计算机科学与技术

年 级 2019

姓 名 张明君 (2 班)

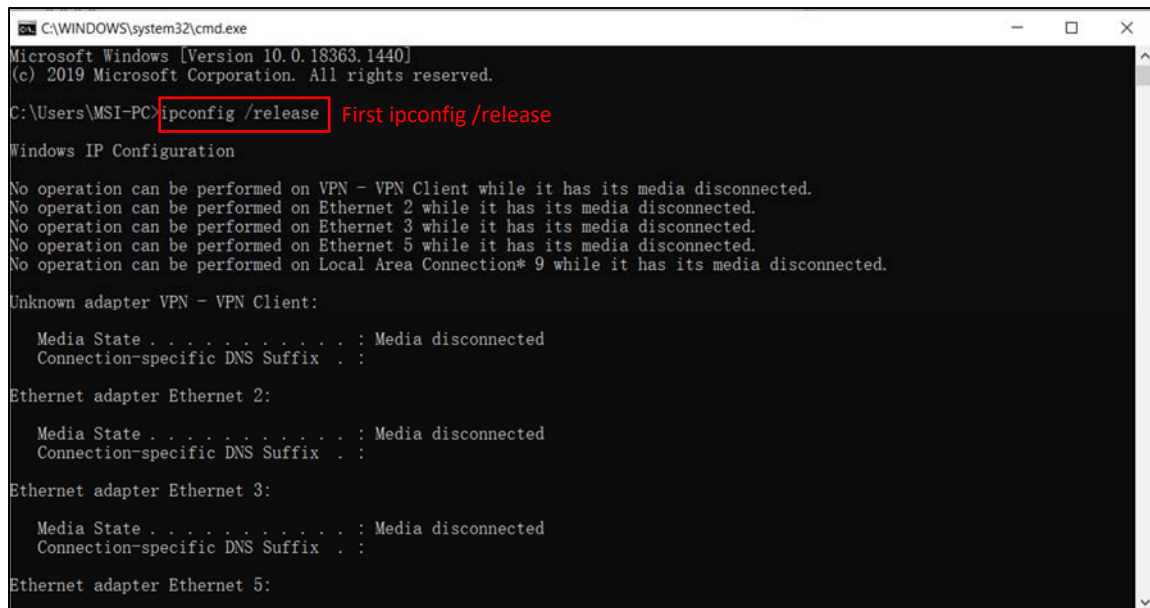
学 号 6319000359

2022年 5 月 12 日

# DHCP Experiment

In order to observe DHCP in action, we'll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following:

1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). As shown in Figure 1, enter "ipconfig /release". The executable for ipconfig is in C:\windows\system32. This command releases your current IP address, so that your host's IP address becomes 0.0.0.0.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.1440]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\MSI-PC>ipconfig /release First ipconfig /release

Windows IP Configuration

No operation can be performed on VPN - VPN Client while it has its media disconnected.
No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Ethernet 3 while it has its media disconnected.
No operation can be performed on Ethernet 5 while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 5:
```

Figure 1:First IP release

2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.

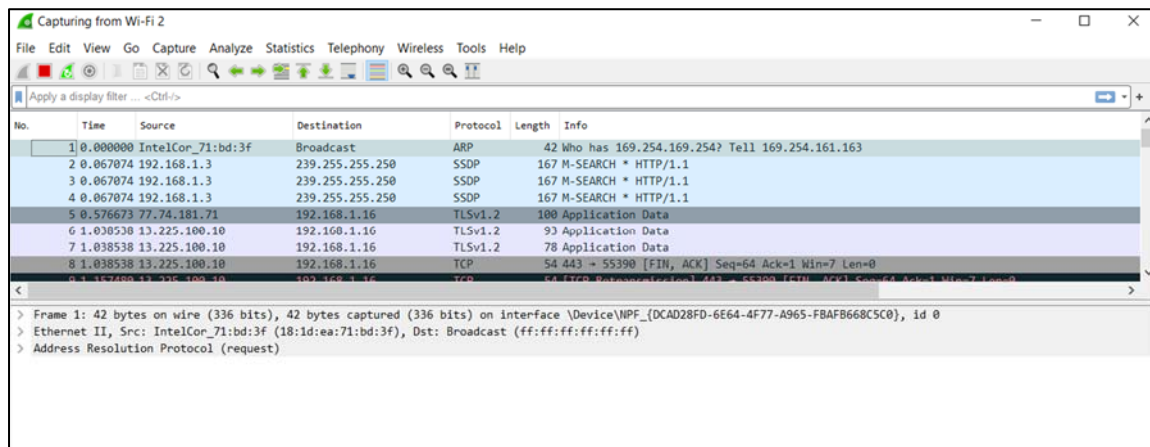
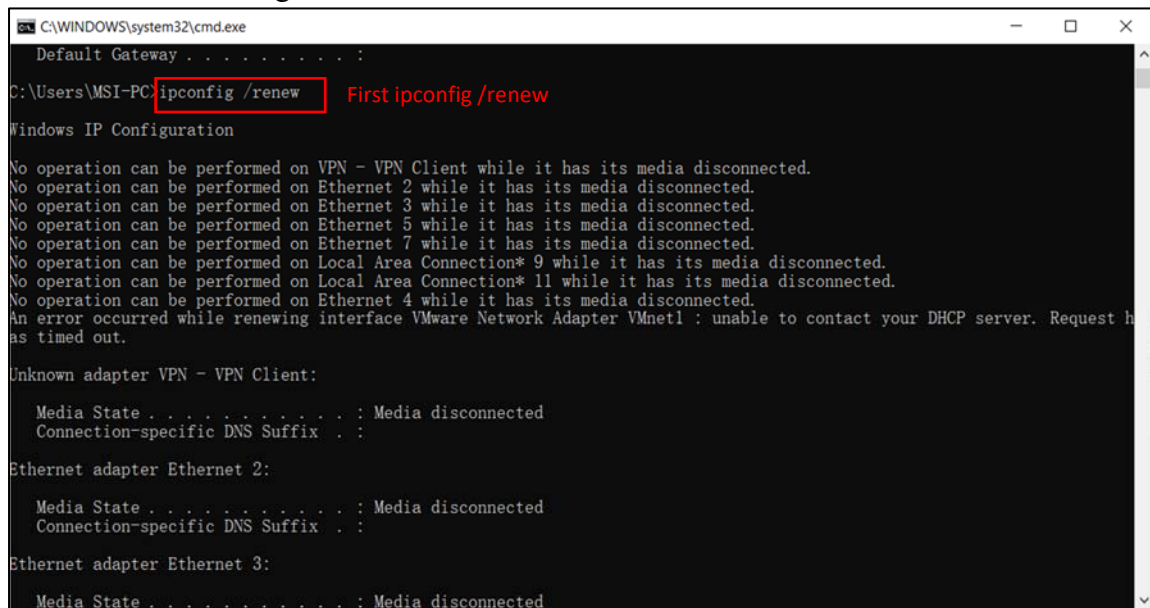


Figure 2:Wireshark Capture

3. Now go back to the Windows Command Prompt and enter “ipconfig /renew”. This instructs your host to obtain a network configuration, including a new IP address. In Figure 1, the host obtains the IP address 192.168.1.108.



```
C:\WINDOWS\system32\cmd.exe
Default Gateway . . . . . :
C:\Users\MSI-PC>ipconfig /renew First ipconfig /renew
Windows IP Configuration

No operation can be performed on VPN - VPN Client while it has its media disconnected.
No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Ethernet 3 while it has its media disconnected.
No operation can be performed on Ethernet 5 while it has its media disconnected.
No operation can be performed on Ethernet 7 while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 11 while it has its media disconnected.
No operation can be performed on Ethernet 4 while it has its media disconnected.
An error occurred while renewing interface VMware Network Adapter VMnet1 : unable to contact your DHCP server. Request has timed out.

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

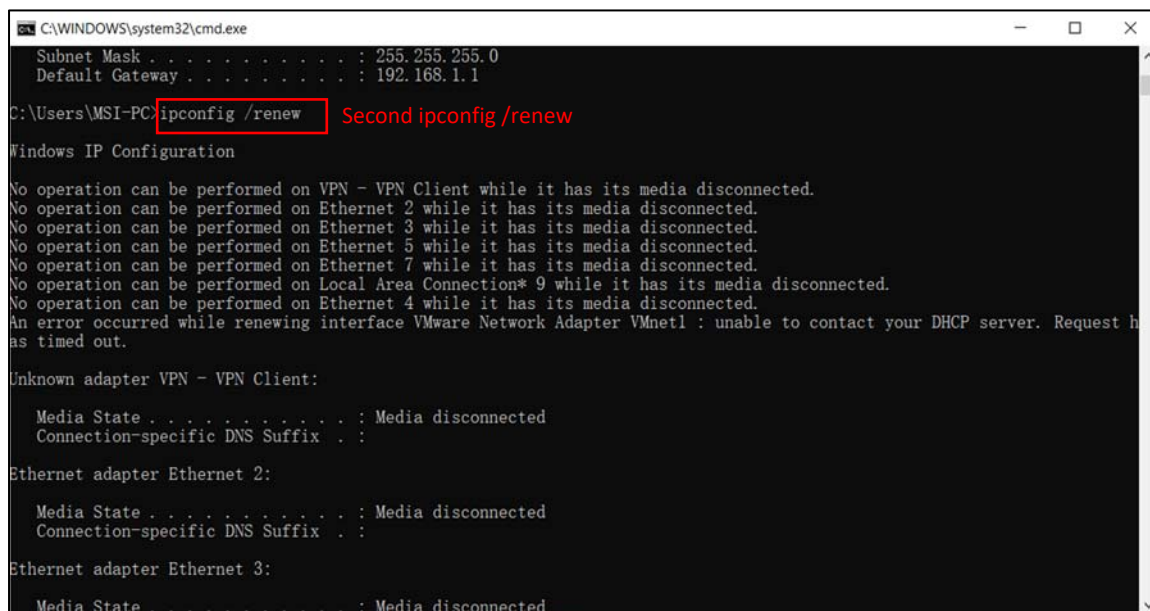
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 3:

    Media State . . . . . : Media disconnected
```

Figure 3:First IP renew

4. Wait until the “ipconfig /renew” has terminated. Then enter the same command “ipconfig /renew” again.



```
C:\WINDOWS\system32\cmd.exe
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Users\MSI-PC>ipconfig /renew Second ipconfig /renew
Windows IP Configuration

No operation can be performed on VPN - VPN Client while it has its media disconnected.
No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Ethernet 3 while it has its media disconnected.
No operation can be performed on Ethernet 5 while it has its media disconnected.
No operation can be performed on Ethernet 7 while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Ethernet 4 while it has its media disconnected.
An error occurred while renewing interface VMware Network Adapter VMnet1 : unable to contact your DHCP server. Request has timed out.

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

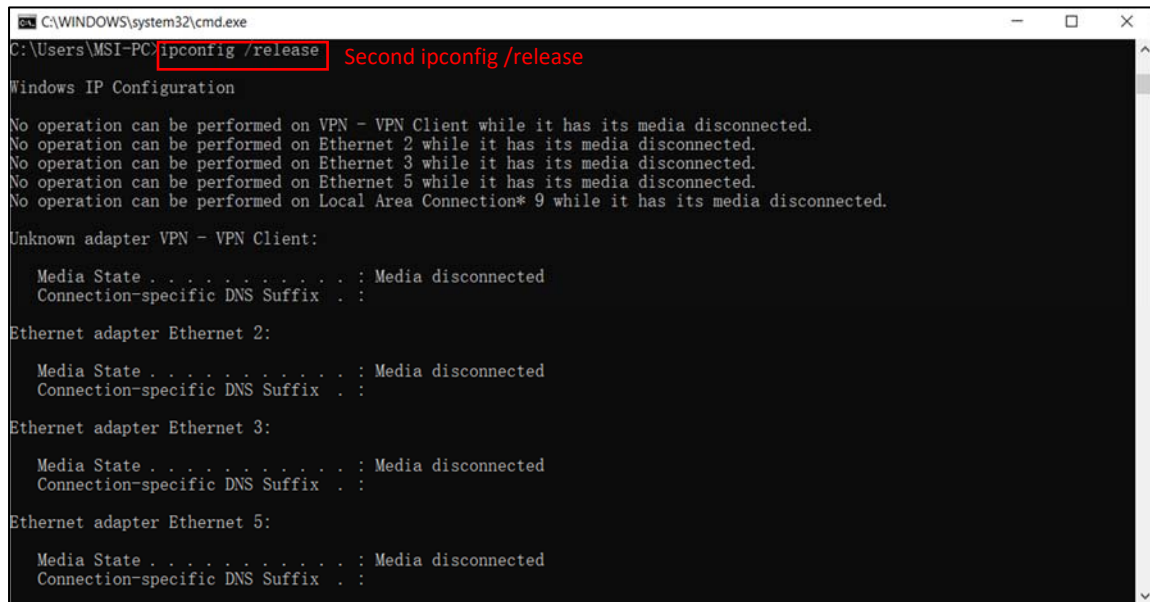
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 3:

    Media State . . . . . : Media disconnected
```

Figure 4:Second IP renew

- When the second “ipconfig /renew” terminates, enter the command “ipconfig/release” to release the previously-allocated IP address to your computer.



```
C:\WINDOWS\system32\cmd.exe
C:\Users\MSI-PC>ipconfig /release Second ipconfig /release

Windows IP Configuration

No operation can be performed on VPN - VPN Client while it has its media disconnected.
No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Ethernet 3 while it has its media disconnected.
No operation can be performed on Ethernet 5 while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

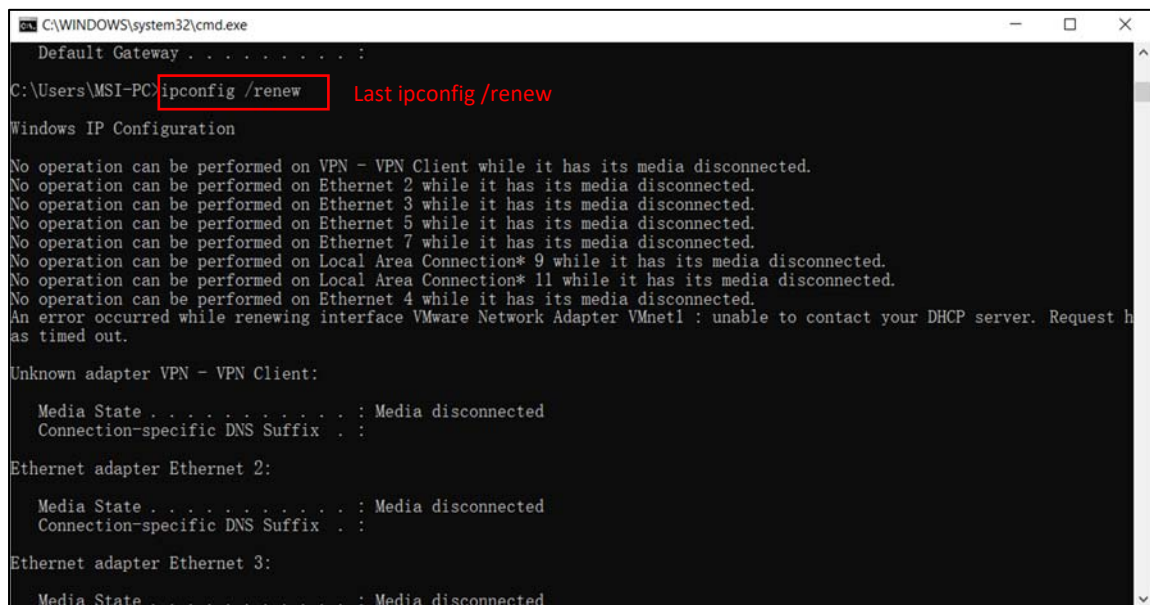
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 5:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

Figure 5:Second IP release

- Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.



```
C:\WINDOWS\system32\cmd.exe
Default Gateway . . . . . :
C:\Users\MSI-PC>ipconfig /renew Last ipconfig /renew

Windows IP Configuration

No operation can be performed on VPN - VPN Client while it has its media disconnected.
No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on Ethernet 3 while it has its media disconnected.
No operation can be performed on Ethernet 5 while it has its media disconnected.
No operation can be performed on Ethernet 7 while it has its media disconnected.
No operation can be performed on Local Area Connection* 9 while it has its media disconnected.
No operation can be performed on Local Area Connection* 11 while it has its media disconnected.
No operation can be performed on Ethernet 4 while it has its media disconnected.
An error occurred while renewing interface VMware Network Adapter VMnet1 : unable to contact your DHCP server. Request has timed out.

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

Figure 6:The last IP renew

- Stop Wireshark packet capture.

Now let's take a look at the resulting Wireshark window. To see only the DHCP packets, enter into the filter field "bootp". (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the current version of Wireshark, you need to enter "bootp" and not "dhcp" in the filter.) We see from Figure 2 that the first ipconfig renew command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.

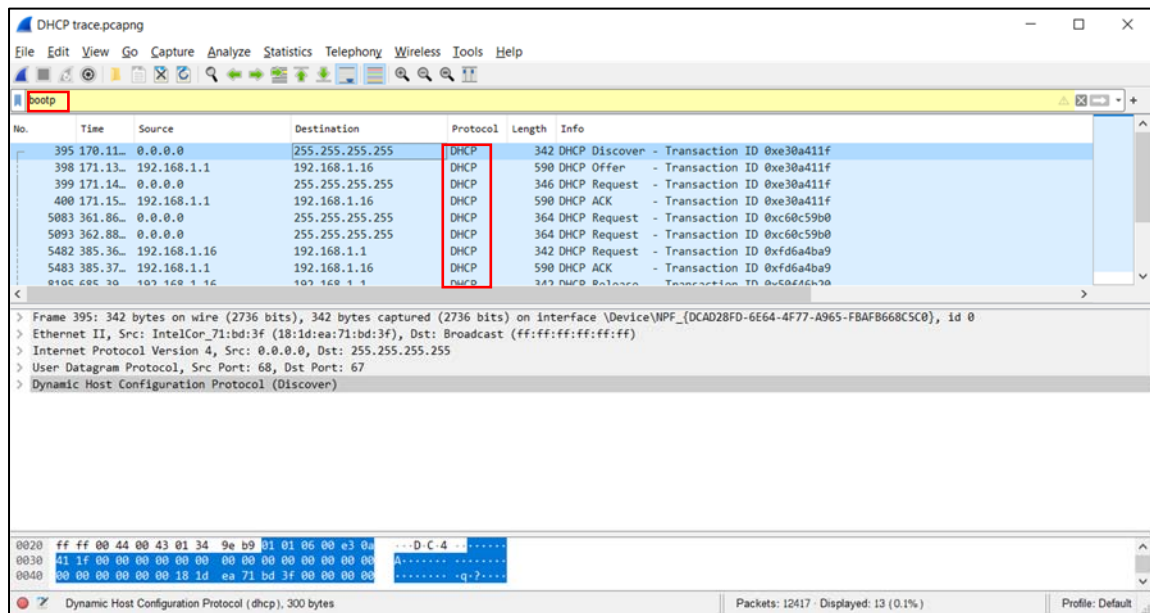


Figure 7:DHCP trace packet



# What to Hand In

Answer the following questions:

- 1) Are DHCP messages sent over UDP or TCP?
  - **DHCP messages are sent over UDP (User Datagram Protocol).**

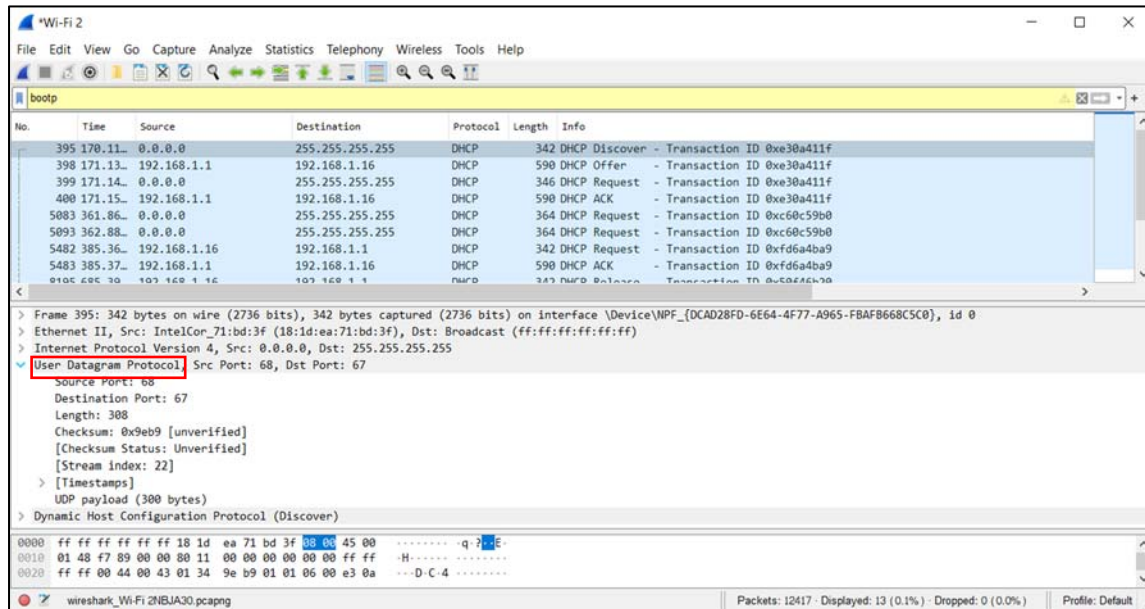


Figure 8:UDP Protocol

- 2) Draw a timing diagram 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?
  - **As we can see the picture below, the port numbers 67 and 68 are the same as in the example given.**

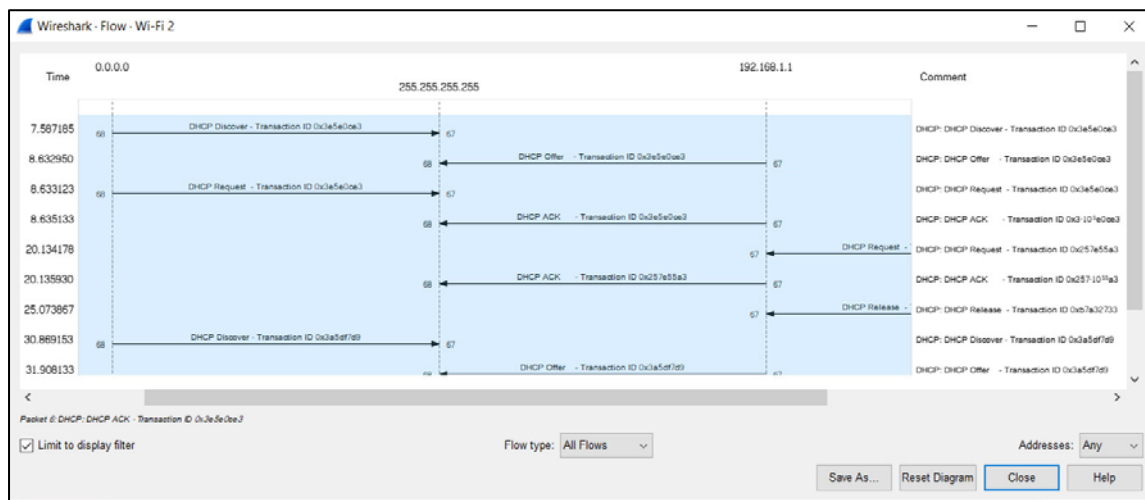


Figure 9:Timing diagram

- 3) What is the link-layer (e.g., Ethernet) address of your host?
- The link-layer address of my host is (18:1d:ea:71:bd:3f).

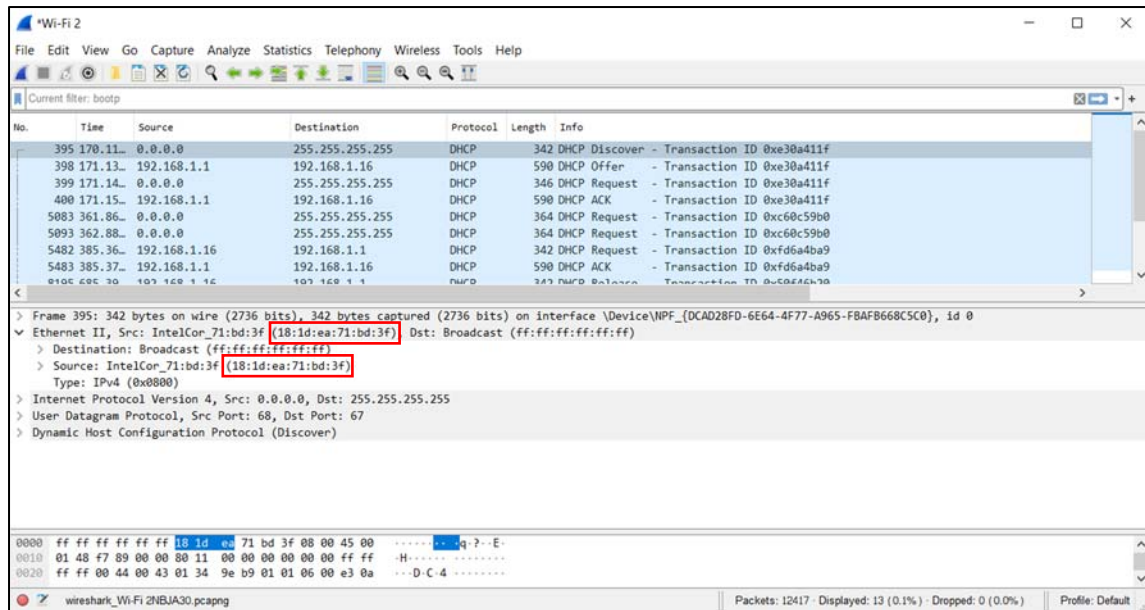


Figure 10: Link layer host

- 4) What values in the DHCP discover message differentiate this message from the DHCP request message?
- The value in the DHCP discover message that differentiates this message from the DHCP request message is Option 53.

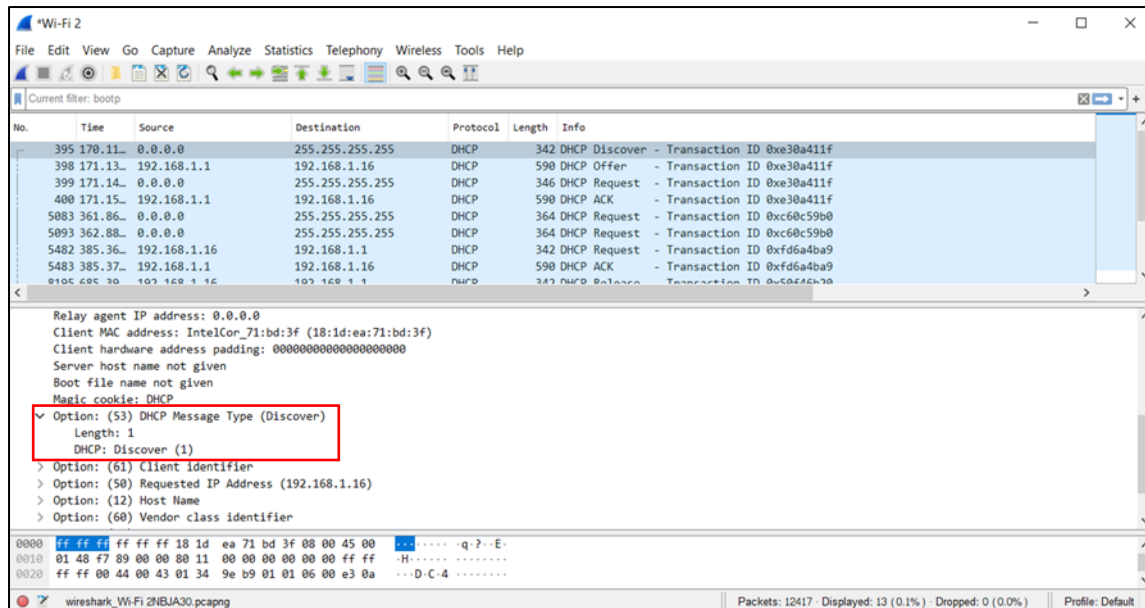


Figure 11: DHCP Discover

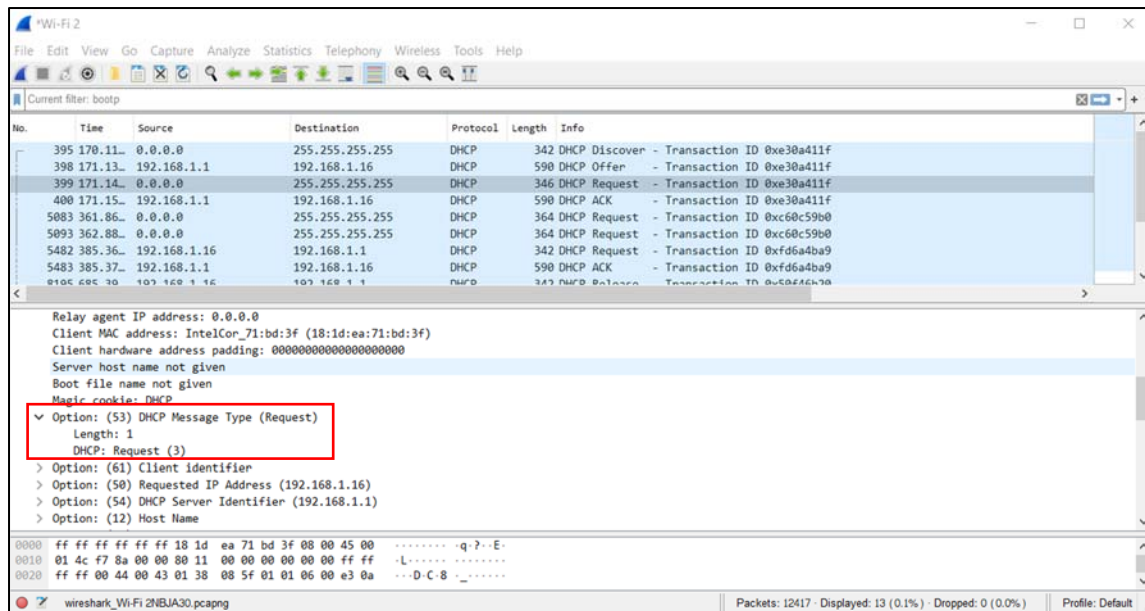


Figure 12:DHCP Request

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?

- The value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages are: 0xe30a411f

The values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages is: 0xfd6a4ba9

The purpose of the transaction ID is so that the DHCP server can differentiate between client requests during the request process.

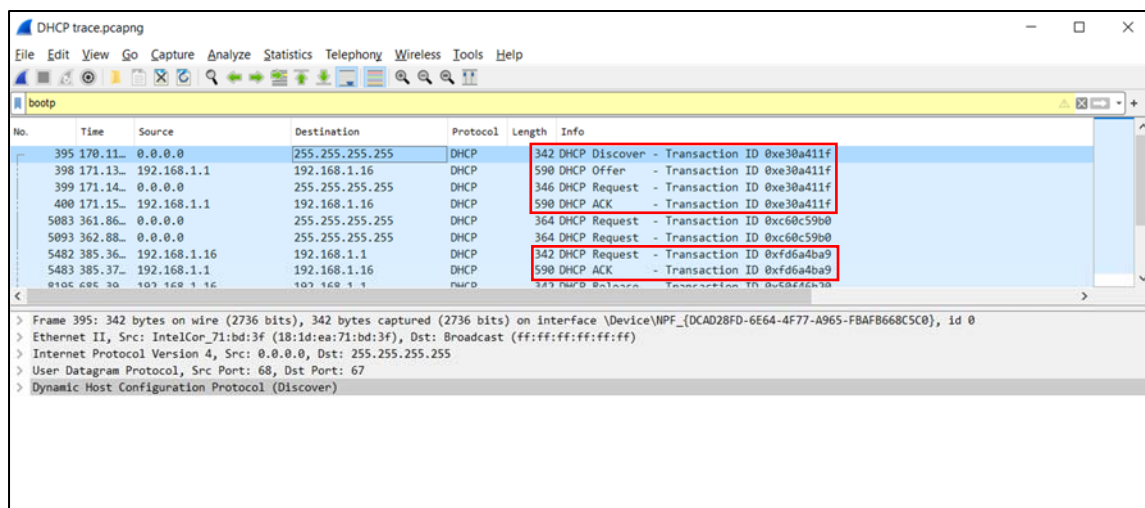


Figure 13:Transaction ID



- 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.

- **Discover IP address = 255.255.255.255**
- **Offer IP address = 192.168.1.16**
- **Request IP address = 255.255.255.255**
- **ACK IP address = 192.168.1.16**

**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**

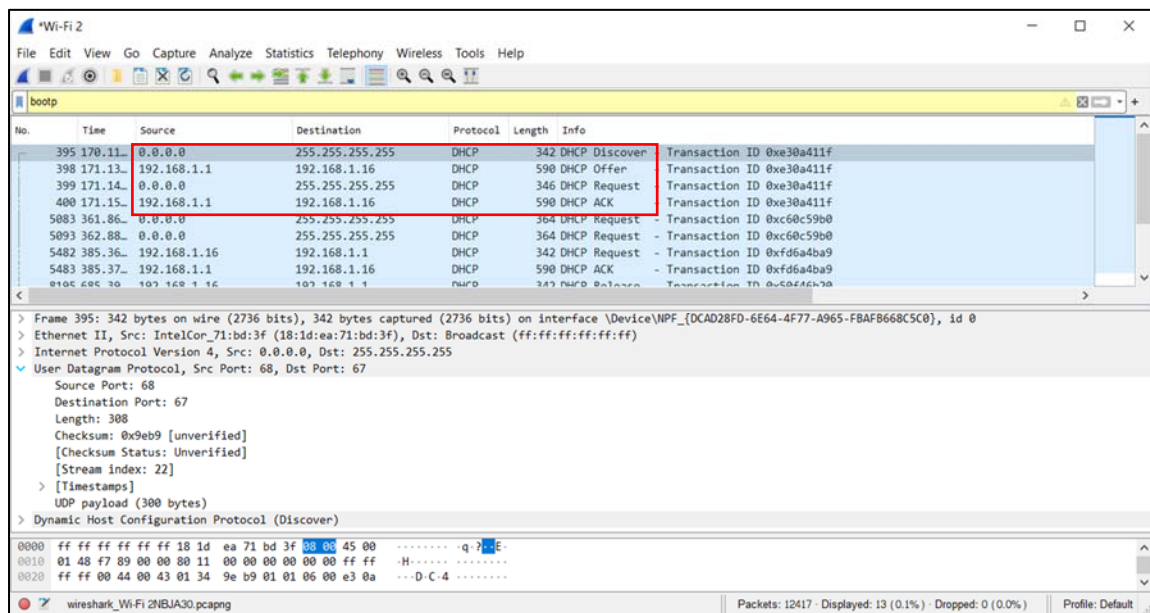


Figure 14: Four DHCP messages IP address

- 7) What is the IP address of your DHCP server?
- **The IP address of my DHCP server is 192.168.1.1.**

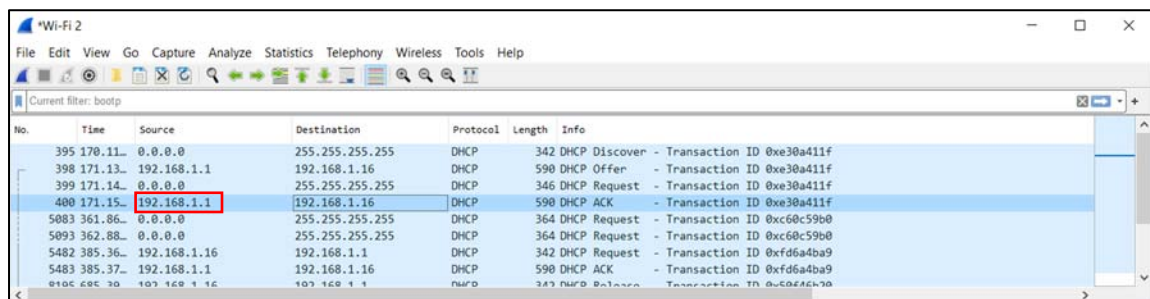


Figure 15: IP address of DHCP server

- 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.
- The IP address in which the DHCP server is offering to my host in the DHCP Offer message is 192.168.1.16.
  - Option 53 contains the DHCP Message type with a length of 1 and the DHCP offer is (2).

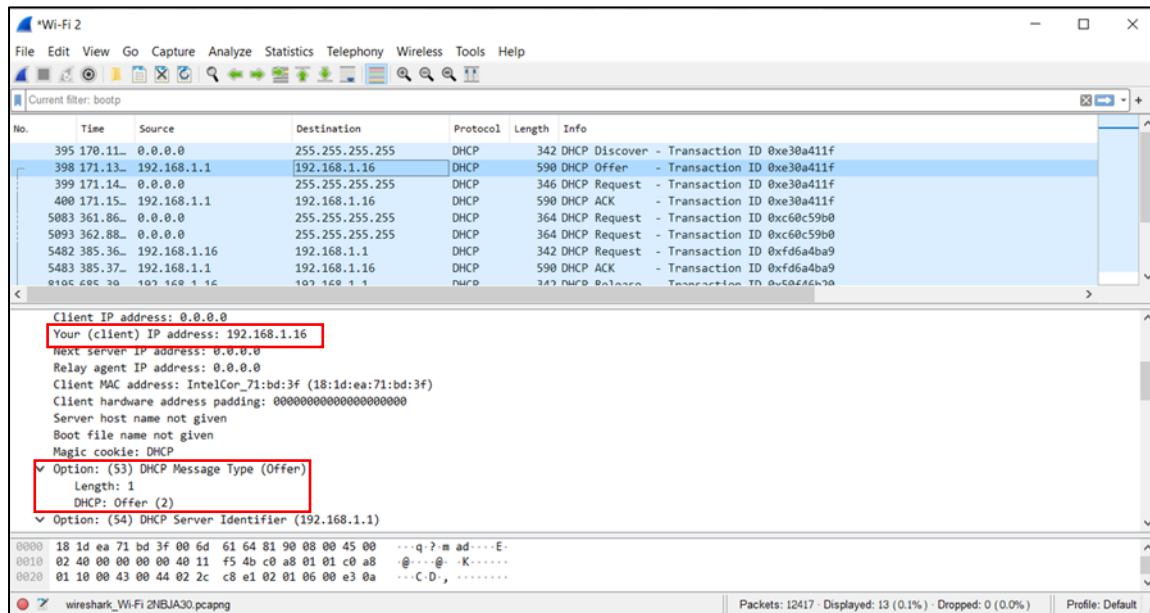


Figure 16:DHCP Offer IP address

- 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?
- The IP address of relay agent is 0.0.0.0 which indicates that there is no DHCP Relay used. There was no Relay Agent used in my experiment.

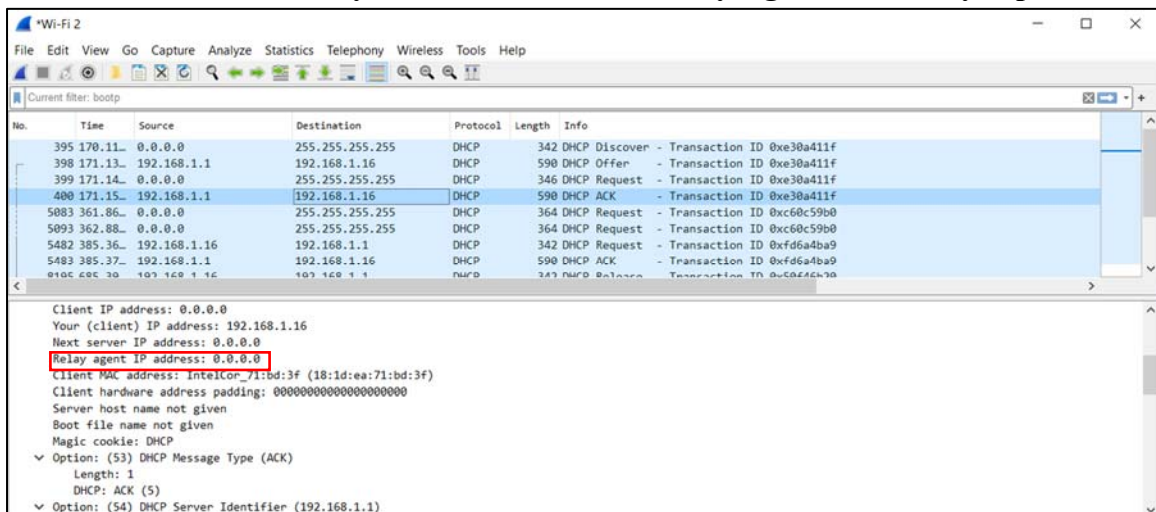


Figure 17:Relay agent IP address

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

- **The router line indicates to the client what its default gateway should be. The subnet mask line tells the client which subnet mask it should use.**

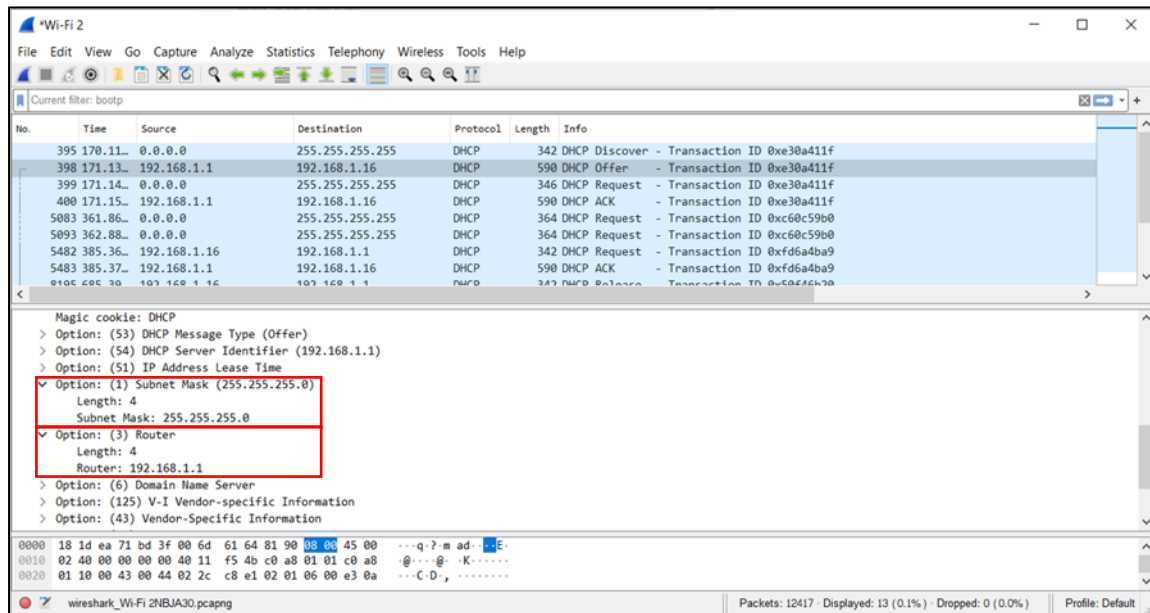


Figure 18: Router and Subnet mask DHCP message

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?

- **The client accepts the IP address offered by the DHCP server. The client's response is in option 50 of the Request message.**

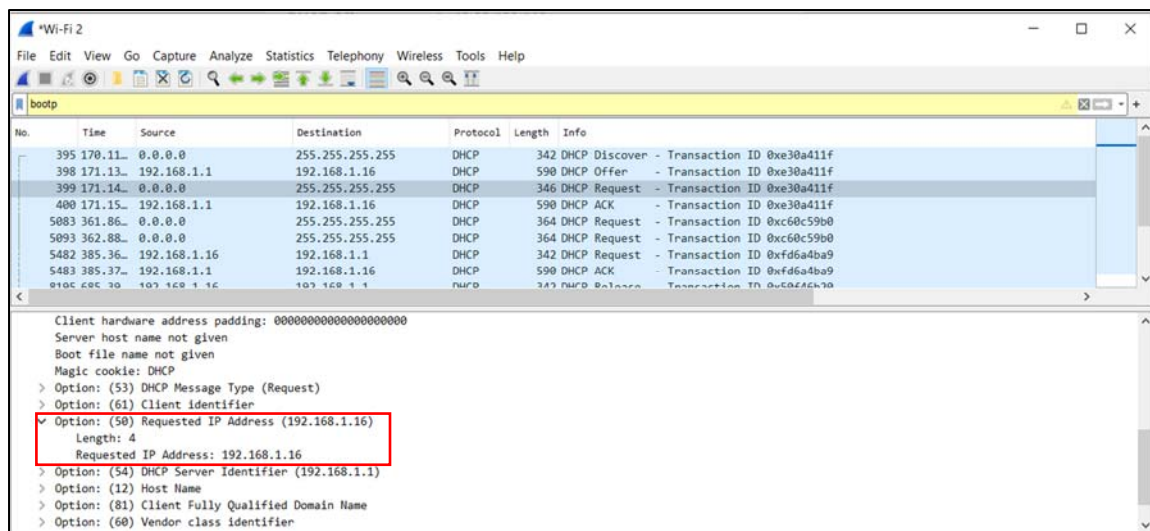


Figure 19: Client IP address accepted by DHCP server

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

- The lease time is the amount of time the DHCP server assigns an IP address to a client. During the lease time, the DHCP server will not assign the IP given to the client to another client, unless it is released by the client. Once the lease time has expired, the IP address can be reused by the DHCP server to give to another client. In my experiment, the lease time is 1 day.

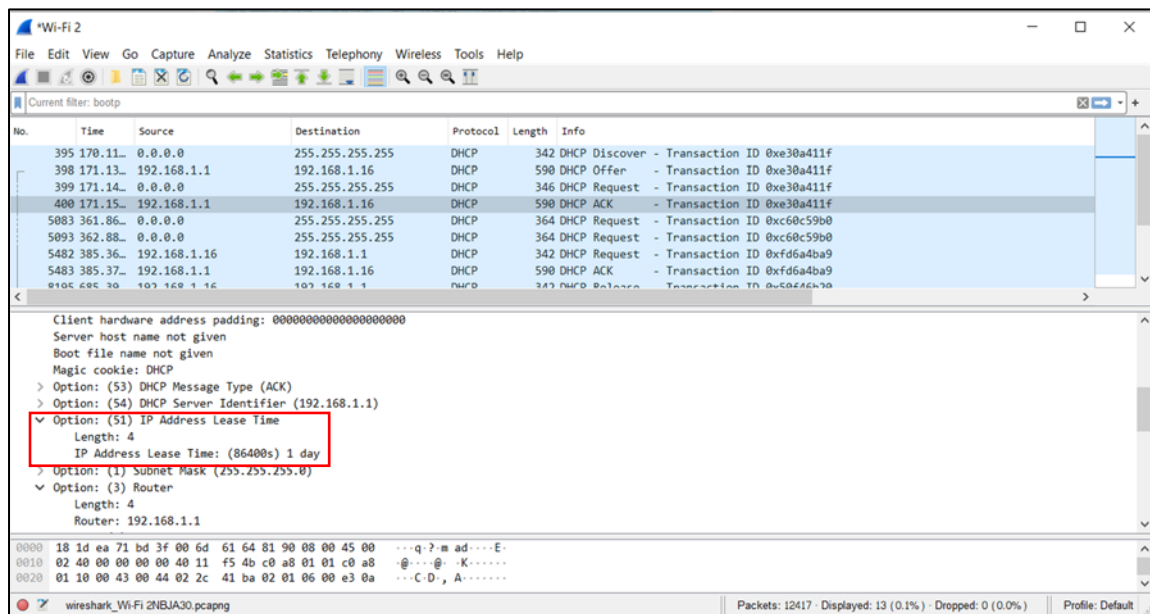


Figure 20: IP address lease time

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?

- The client sends a DHCP Release message to cancel its lease on the IP address given to it by the DHCP server. The DHCP server does not send a message back to the client acknowledging the DHCP Release message. If the DHCP Release message from the client is lost, the DHCP server would have to wait until the lease period is over for that IP address until it could reuse it for another client.

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.

- Yes, there are ARP requests made by the DHCP server. Before offering an IP address to a client, the DHCP server issues an ARP request for the offered IP to make sure the IP address is not already in use by another workstation.

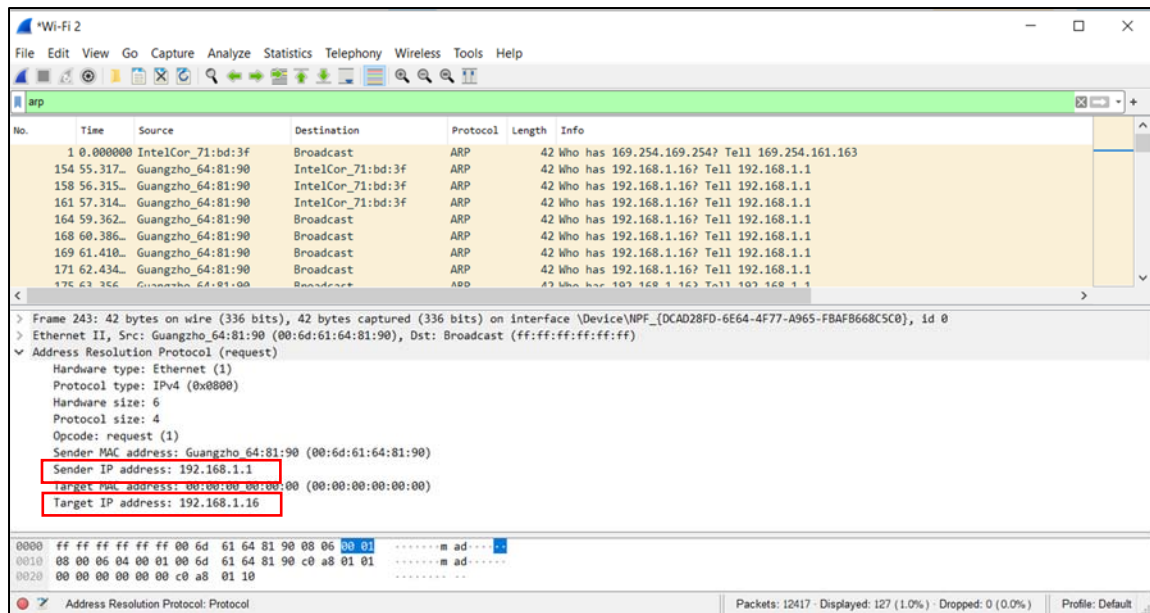


Figure 21:ARP messages

So, The sender IP address is 192.168.1.1 and the Target IP address is 192.168.1.16.