CSCI 450: Lab 1

Session 3

DHCP

Tushar Tiwari

Abstract

To illustrate and observe the process of an host acquiring an IP address from a DHCP server with the help of Wireshark.

Snapshots

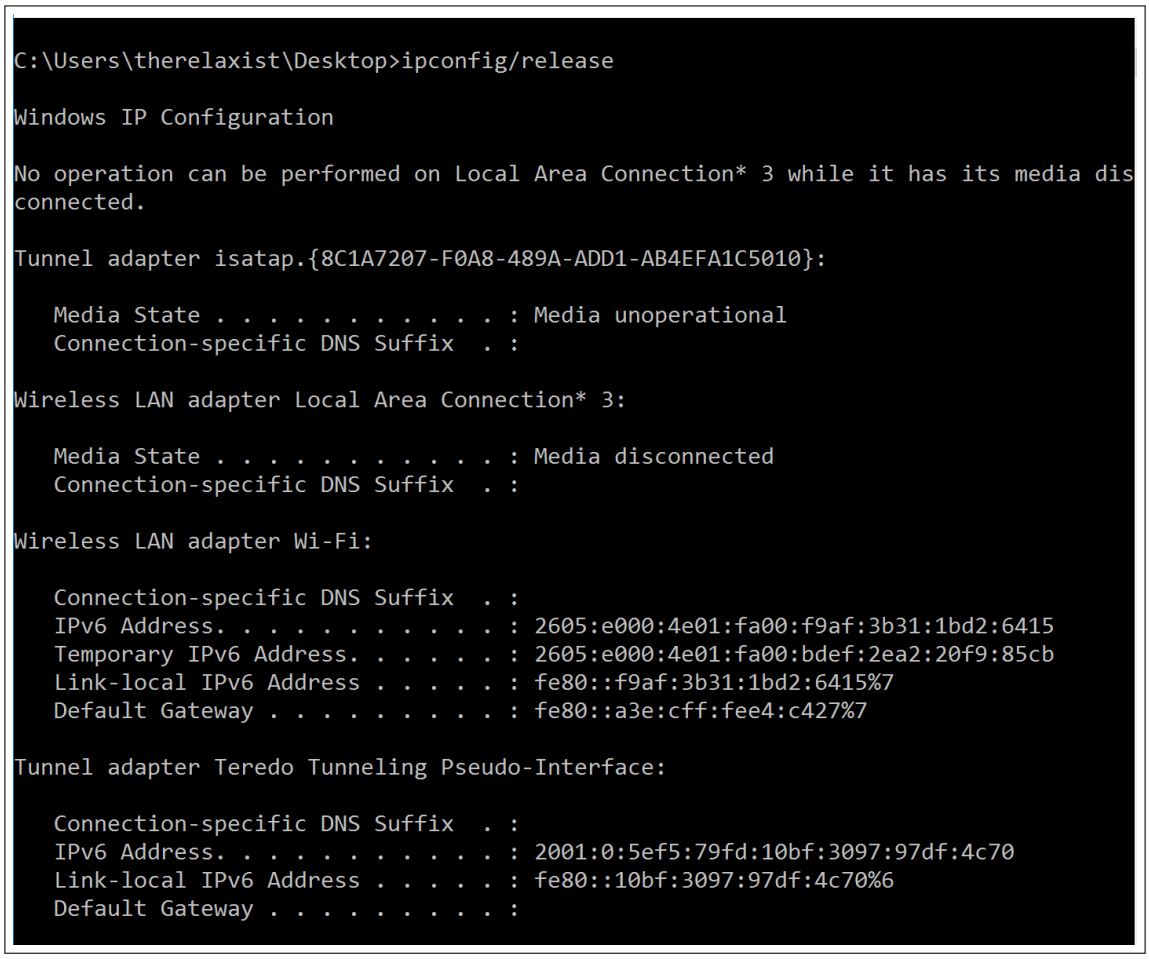


Figure 1: The WiFi config doesn't have an IPv4 address.

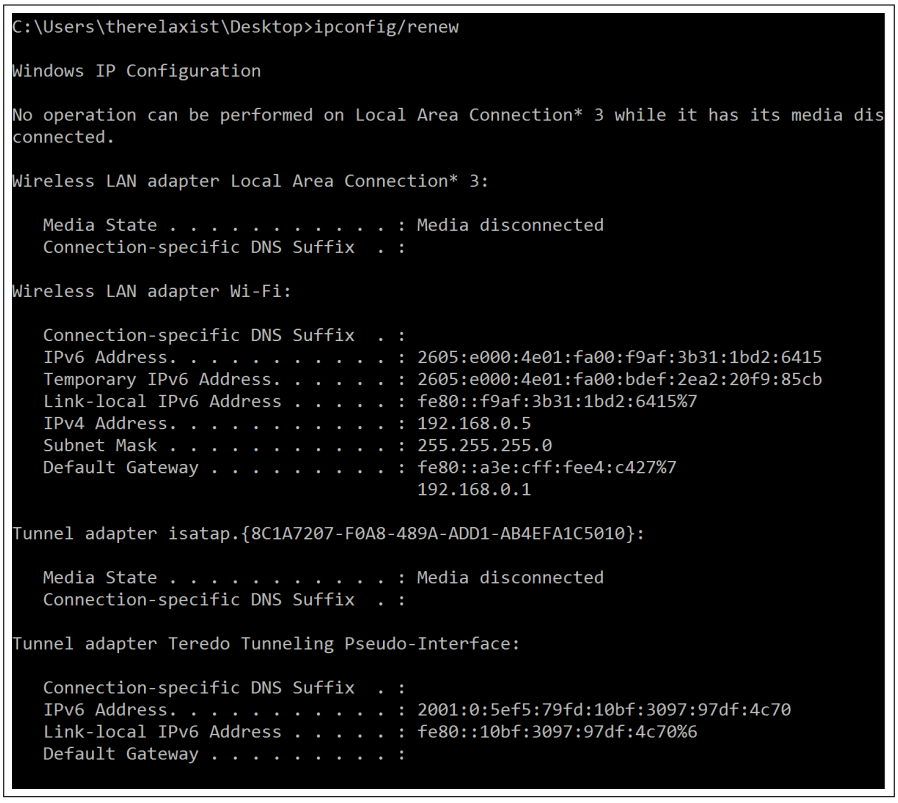
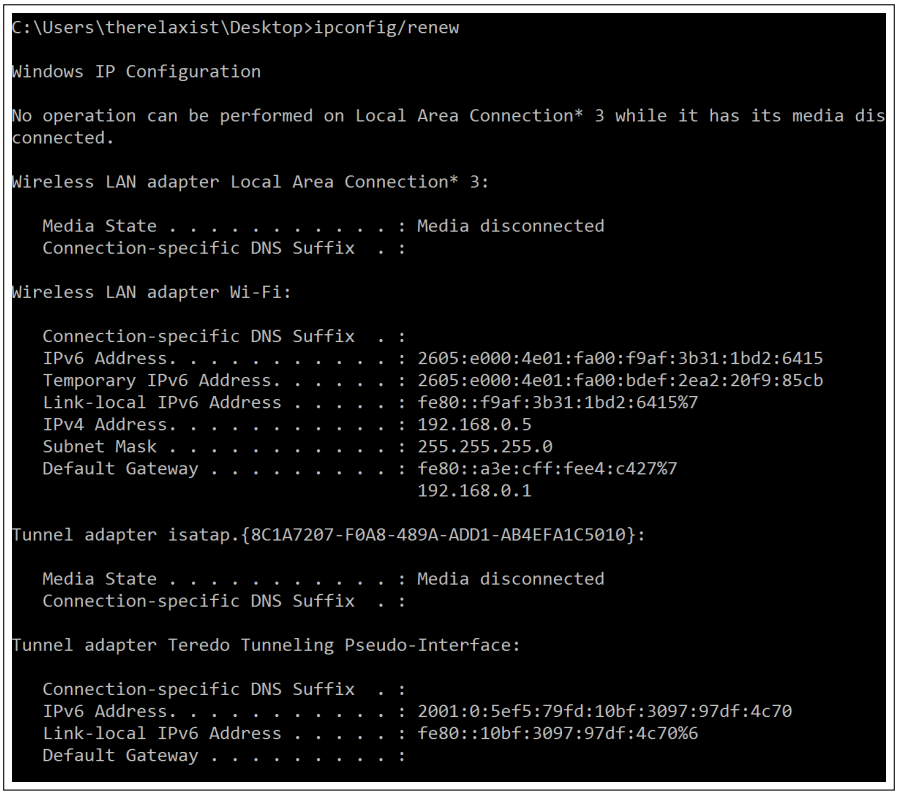


Figure 2: The IP address **192.168.0.5** can now be seen in the IPv4 config.



```
C:\Users\therelaxist\Desktop>ipconfig/release

Windows IP Configuration

No operation can be performed on Local Area Connection* 3 while it has its media dis
connected.

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2605:e000:4e01:fa00:f9af:3b31:1bd2:6415
   Temporary IPv6 Address. . . . . . : 2605:e000:4e01:fa00:bdef:2ea2:20f9:85cb
   Link-local IPv6 Address . . . . . : fe80::f9af:3b31:1bd2:6415%7
   Default Gateway . . . . . . . . . : fe80::a3e:cff:fee4:c427%7

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fd:10bf:3097:97df:4c70
   Link-local IPv6 Address . . . . . : fe80::10bf:3097:97df:4c70%6
   Default Gateway . . . . . . . . . :
```

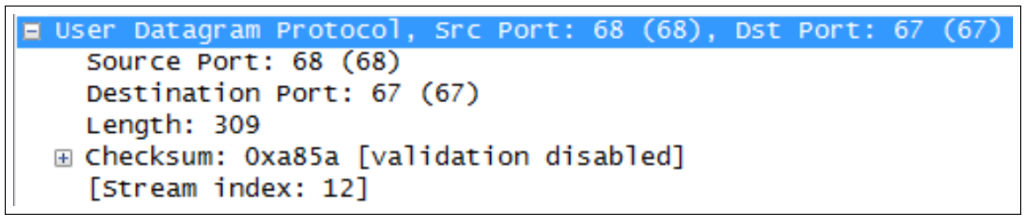
```
C:\Users\therelaxist\Desktop>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 3 while it has its media dis
connected.

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2605:e000:4e01:fa00:f9af:3b31:1bd2:6415
   Temporary IPv6 Address. . . . . . : 2605:e000:4e01:fa00:bdef:2ea2:20f9:85cb
   Link-local IPv6 Address . . . . . : fe80::f9af:3b31:1bd2:6415%7
   IPv4 Address. . . . . . . . . . . : 192.168.0.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::a3e:cff:fee4:c427%7
                                       192.168.0.1

Tunnel adapter isatap.{8C1A7207-F0A8-489A-ADD1-AB4EFA1C5010}:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

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

Problem 1

Are DHCP messages sent over UDP or TCP?

Solution

DHCP messages are sent over UDP (User Datagram Protocol).

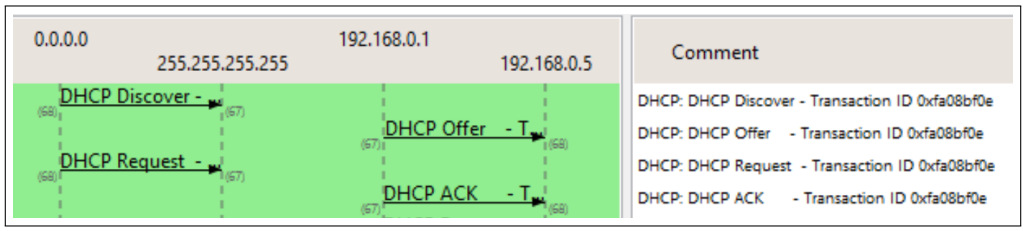


Problem 2

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?

Solution

Please note that the DHCP server does not send a broadcast message because it uses the IP address that was previously assigned to my computer before the IP release.



Message Type	Source Port	Destination Port
Discover	68	67
Offer	67	68
Request	68	67
ACK	67	68

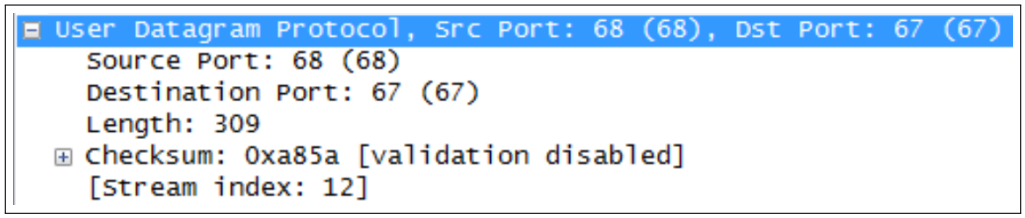


Figure 3: The DHCP Discover message. The port numbers are the same as in the example.

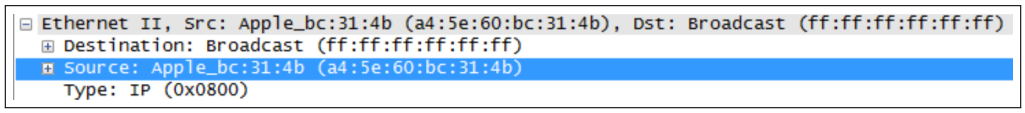
Problem 2 continued on next page...

Problem 3

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

Solution

The Link Layer address of my workstation is a4:5e:60:bc:31:4b.



Problem 4

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

Solution

They are different in the message type (Option 53).

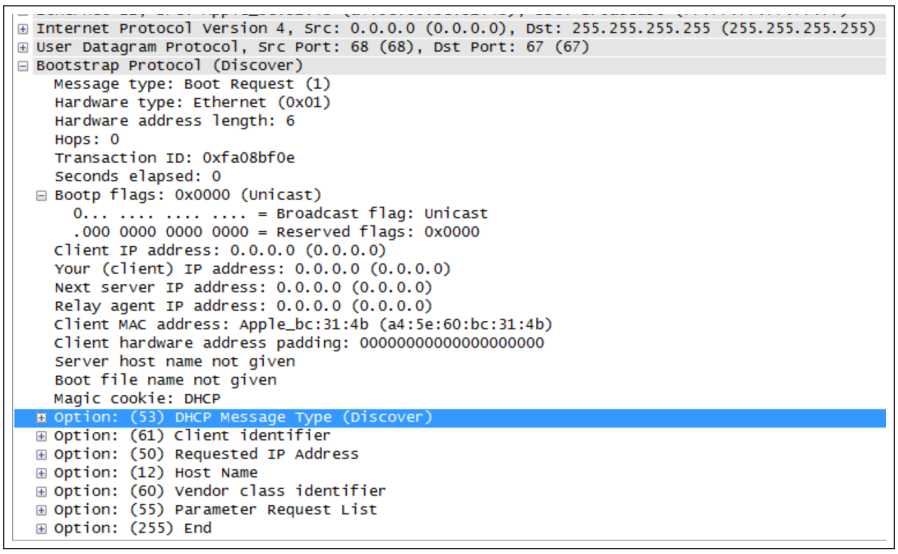


Figure 4: The DHCP Discover Message

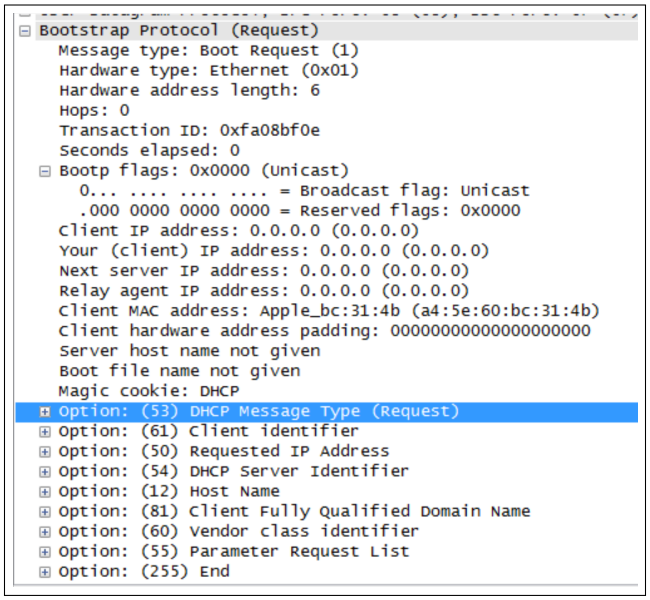


Figure 5: The DHCP Request Message

Problem 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?

Solution

The first line and fifth line specify the two transaction addresses **0xfa08bf0e** and **0xa90b00da**. Their purpose is to differentiate the transactions when multiple clients are performing DHCP requests.

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xfa08bf0e
192.168.0.1	192.168.0.5	DHCP	590	DHCP Offer - Transaction ID 0xfa08bf0e
0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xfa08bf0e
192.168.0.1	192.168.0.5	DHCP	590	DHCP ACK - Transaction ID 0xfa08bf0e
192.168.0.5	192.168.0.1	DHCP	357	DHCP Request - Transaction ID 0xa90b00da
192.168.0.1	192.168.0.5	DHCP	590	DHCP ACK - Transaction ID 0xa90b00da

Figure 6: The two DHCP transactions

Problem 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.

Solution

The client uses **0.0.0.0** and the DHCP server uses its actual IP address. Also the DHCP Offer and ACK messages are not broadcast because the router knows the previous IP address associated with my MAC address. This IP addresses lease is not expired yet, hence no other computer will be using that IP. Hence, it is not a broadcast to 255.255.255.255. The IP addresses are:

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Transaction ID 0xfa08bf0e
192.168.0.1	192.168.0.5	DHCP	590	DHCP Offer - Transaction ID 0xfa08bf0e
0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Transaction ID 0xfa08bf0e
192.168.0.1	192.168.0.5	DHCP	590	DHCP ACK - Transaction ID 0xfa08bf0e

Figure 7: The source and destination IP addresses are in the first two columns.

Problem 7

What is the IP address of your DHCP server?

Solution

The router at my home itself acts as a DHCP server.

Source	Destination	Protocol	Length	Info
192.168.0.1	192.168.0.5	DHCP	590	DHCP ACK - Transaction ID 0xfa08bf0e

Figure 8: IP address of DHCP server

Problem 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.

Solution

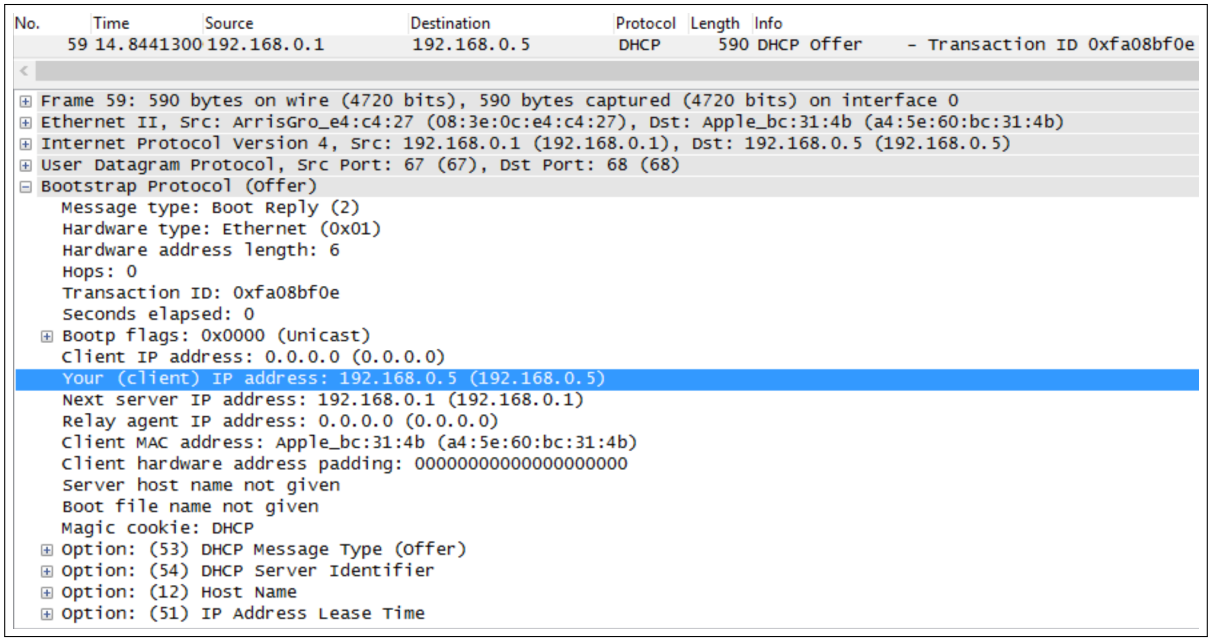


Figure 9: The DHCP message of type **"Offer" (Option 53)** offers the IP address **192.168.0.5**

Problem 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?

Solution

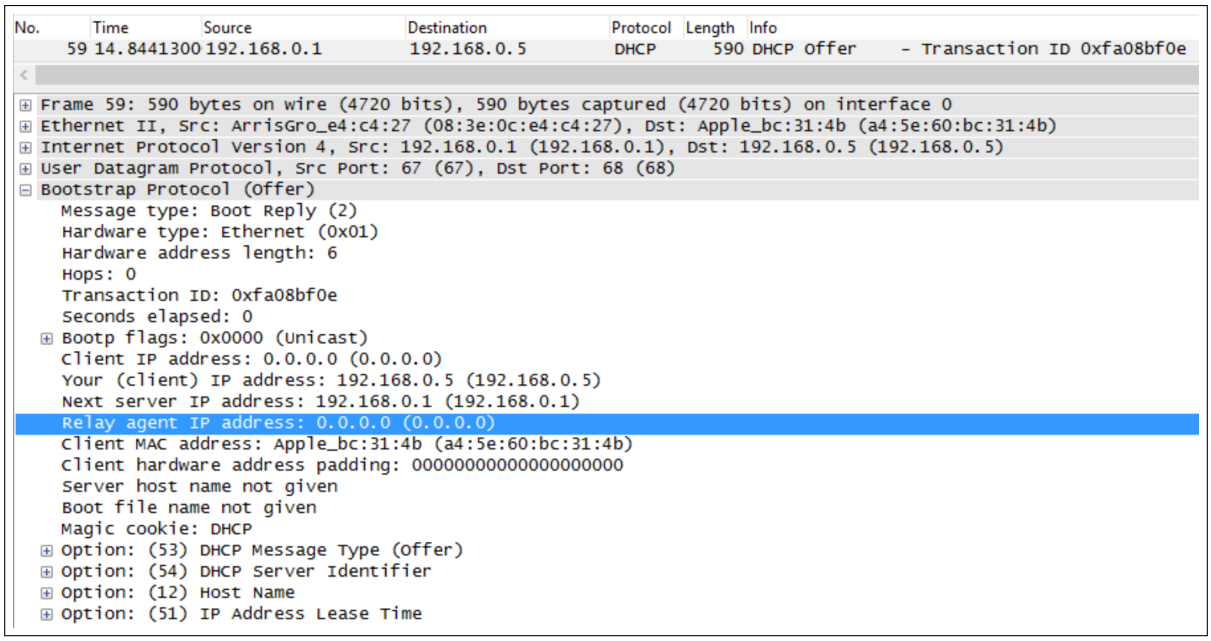


Figure 10: The relay agent address is 0.0.0.0 which means it doesn't exist.

Problem 10

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

Solution

They are given to the client so it can start communicating via the router. The router indicates to the client the default gateway. The subnet mask helps the host identify the network address of the IP address. In my example the DHCP server itself acts as the router, but this can be different.

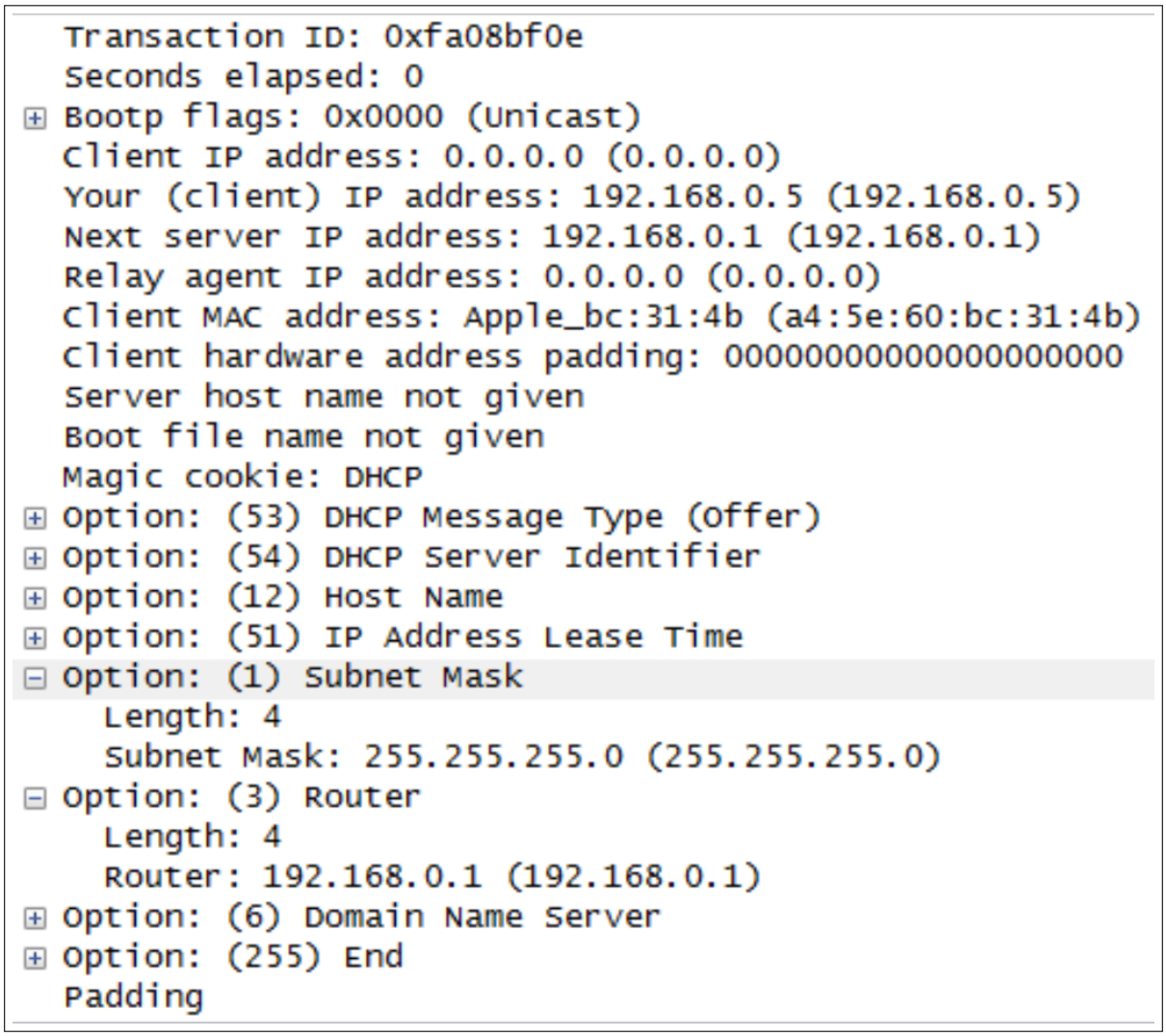


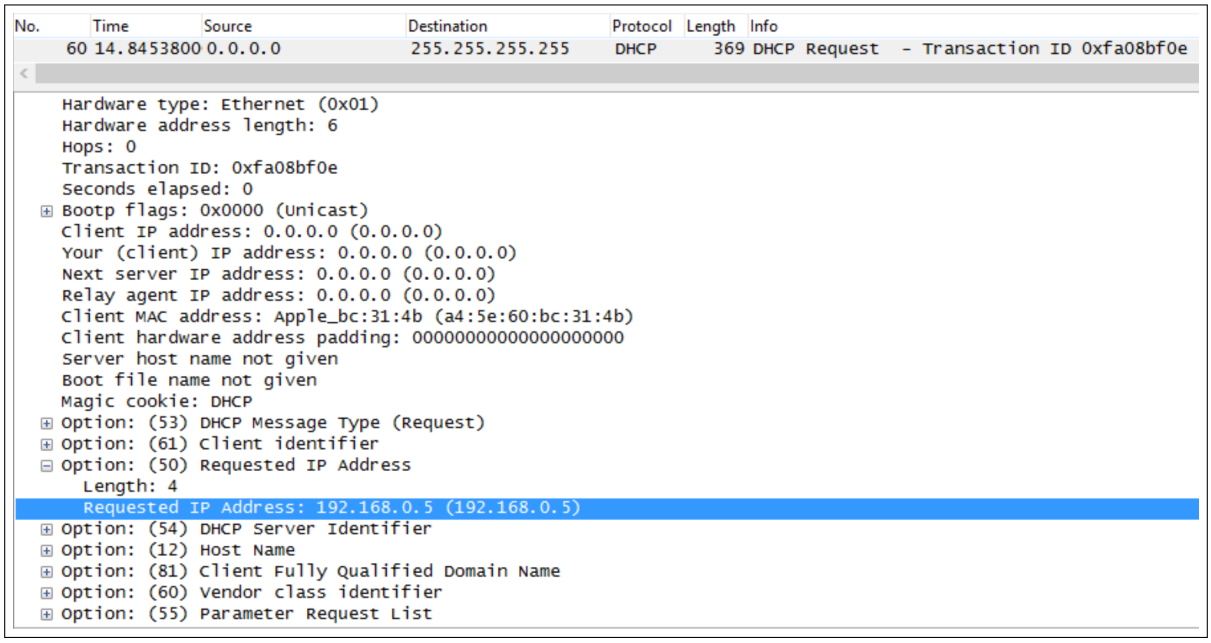
Figure 11: Option 1 indicates the subnet mask and Option 3 indicates the router

Problem 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?

Solution

My computer requests, in the DHCP Request message, the IP address that was offered by the DHCP server. So it is fine with the offered IP address, but cannot yet start using the IP address unless the DHCP server responds with a positive acknowledgement to the DHCP Request message.



Problem 12

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

Solution

The lease time is the amount of time the IP address is assigned to the host. No other host can use this IP address. After lease time expires the IP can be given to another host.

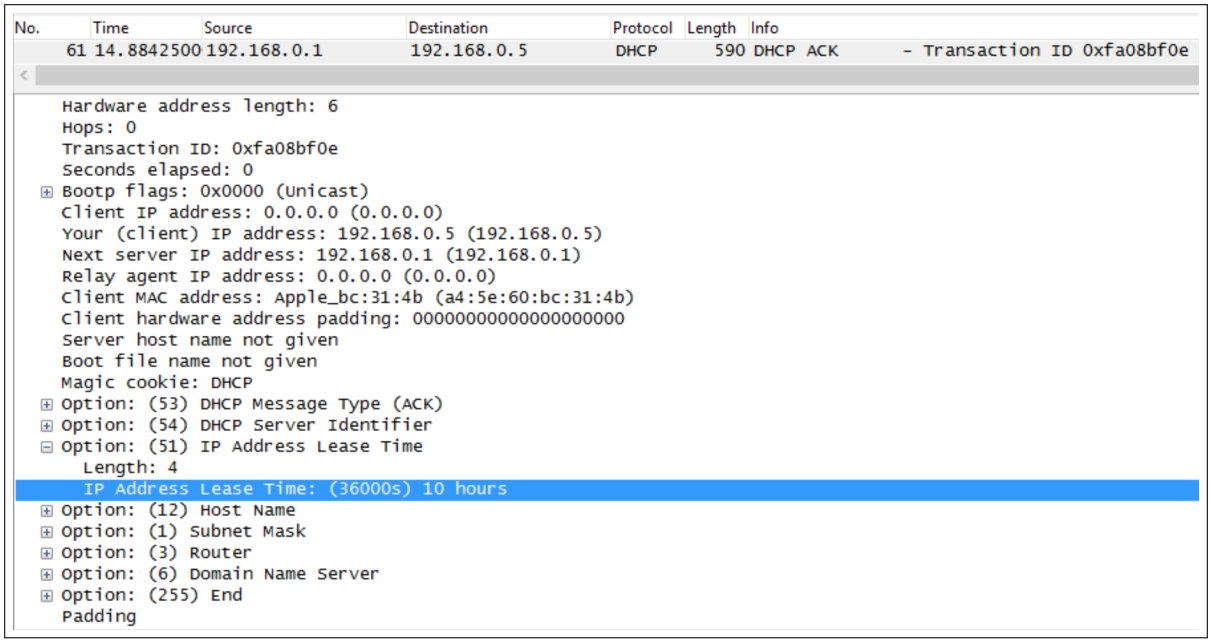


Figure 12: The lease time is 10 hours.

Problem 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?

Solution

The purpose of the release message is to tell the DHCP server to delete the association of the IP address from the requesting host. The lease is terminated by the host and the IP address can be assigned to another host. No acknowledgement is issued by the DHCP server. If the DHCP release message is lost the DHCP server can only release the IP address after it's lease time has expired.

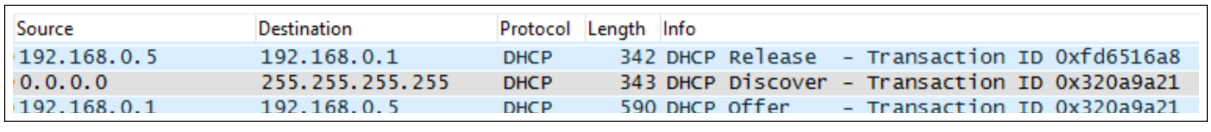


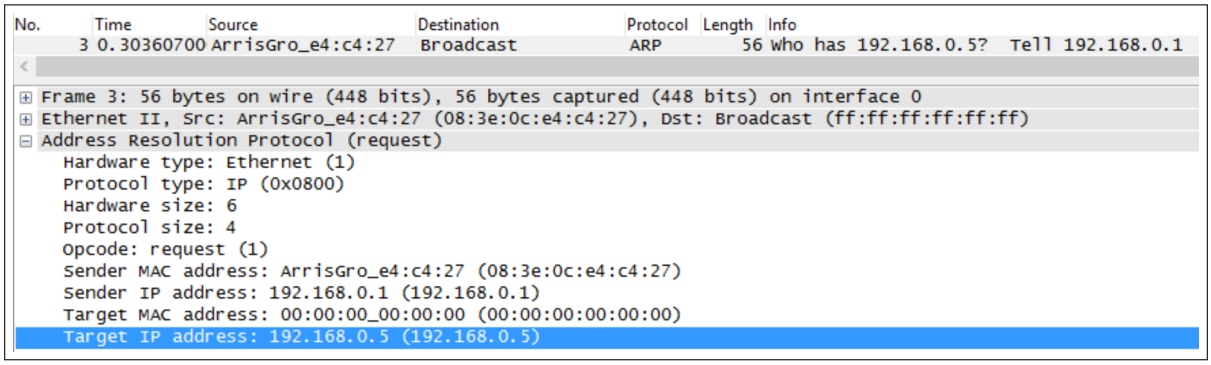
Figure 13: No acknowledgement is seen to the DHCP release message.

Problem 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.

Solution

Yes, there were ARP requests made by the DHCP server as shown here. They are made to check if anybody is using the IP address that will be offered to the requesting host. That is why the destination mac address is broadcast while destination IP is the IP in question.



Conclusion

To findings indicate that DHCP runs over UDP that is without handshaking. The host requests an IP address over a series of DHCP messages namely Discover, Offer, Request & Offer. Wireshark is an excellent tool that helps look into the structure of the datagram/segment, packet & frame. It also shows the data in hexadecimal form. With Wireshark all the DHCP packets were examined.