Wireshark Lab:

DHCP

v

8

.0

Supplement to

*Computer Networking: A Top*

*-*

*Down*

*Approach,*

*8*

*th*

*ed.*

*,*

J.F. Kurose and K.W. Ross

*“Tell me and I forget. Show me and I remember. Involve me*

*and I understand.”*

Chinese proverb

©

2005

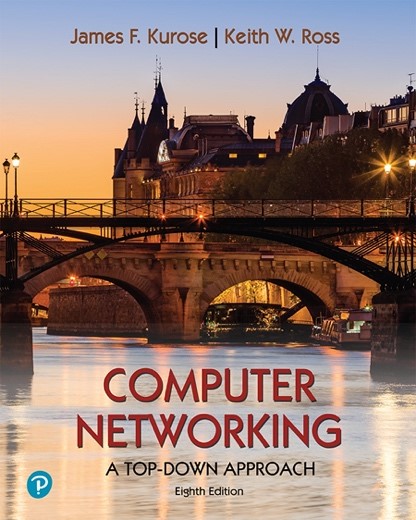
-

20

20

, J.F Kurose and K.W. Ross, All

Rights Reserved



In this lab, we’ll take a quick look at DHCP. DHCP is covered in Section 4.4.3 of the text[[1]](#footnote-1). Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts (as well as to configure other network configuration information).

This lab is brief, as we’ll only examine the DHCP packets captured by a host. If you also have administrative access to your DHCP server, you may want to repeat this lab after making some configuration changes (such as the lease time). If you have a router at home, you most likely can configure your DHCP server. Because many linux/Unix machines (especially those that serve many users) have a static IP address and because manipulating DHCP on such machines typically requires super-user privileges, we’ll only present a Windows version of this lab below.

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[[2]](#footnote-2):

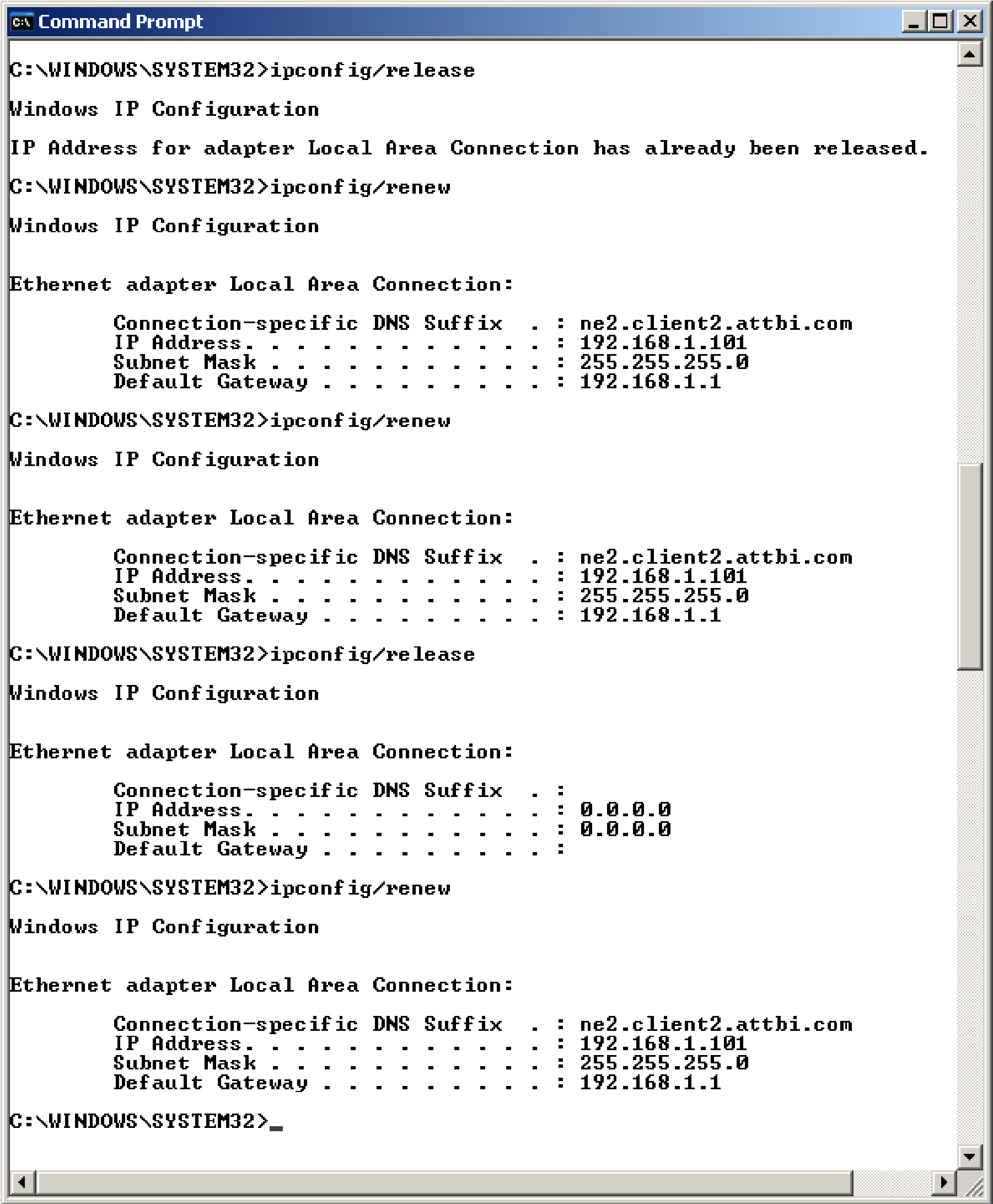
1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). As shown in Figure 1, enter

“*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.

1. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
2. 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
3. Wait until the “*ipconfig /renew*” has terminated. Then enter the same command “*ipconfig /renew*” again.
4. When the second *“ipconfig /renew”* terminates, enter the command

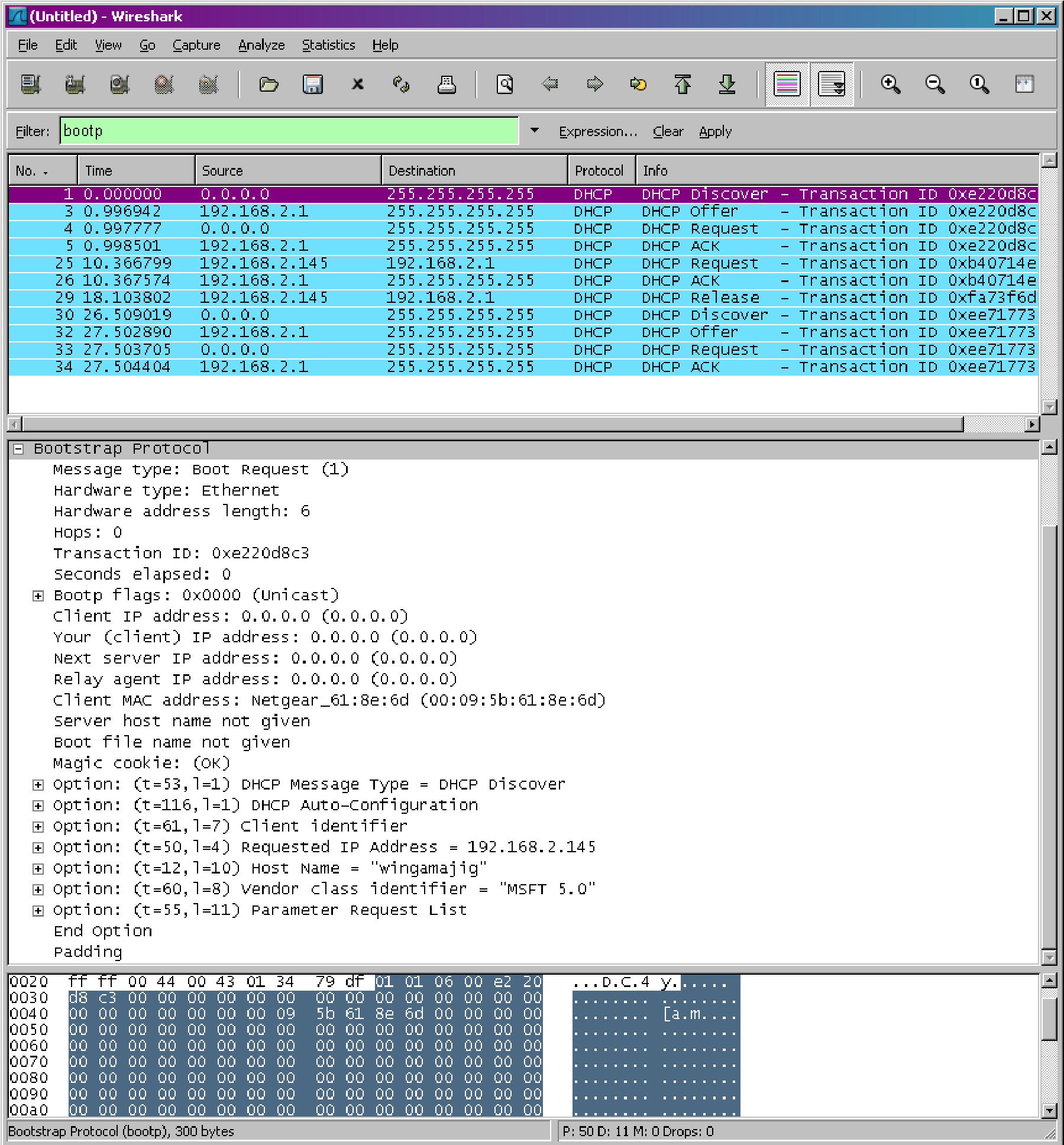
“ipconfig/release” to release the previously-allocated IP address to your computer.

1. Finally, enter “*ipconfig /renew*” to again be allocated an IP address for your computer.
2. Stop Wireshark packet capture.



**Figure 1** Command Prompt window showing sequence of *ipconfig* commands that you should enter.

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.



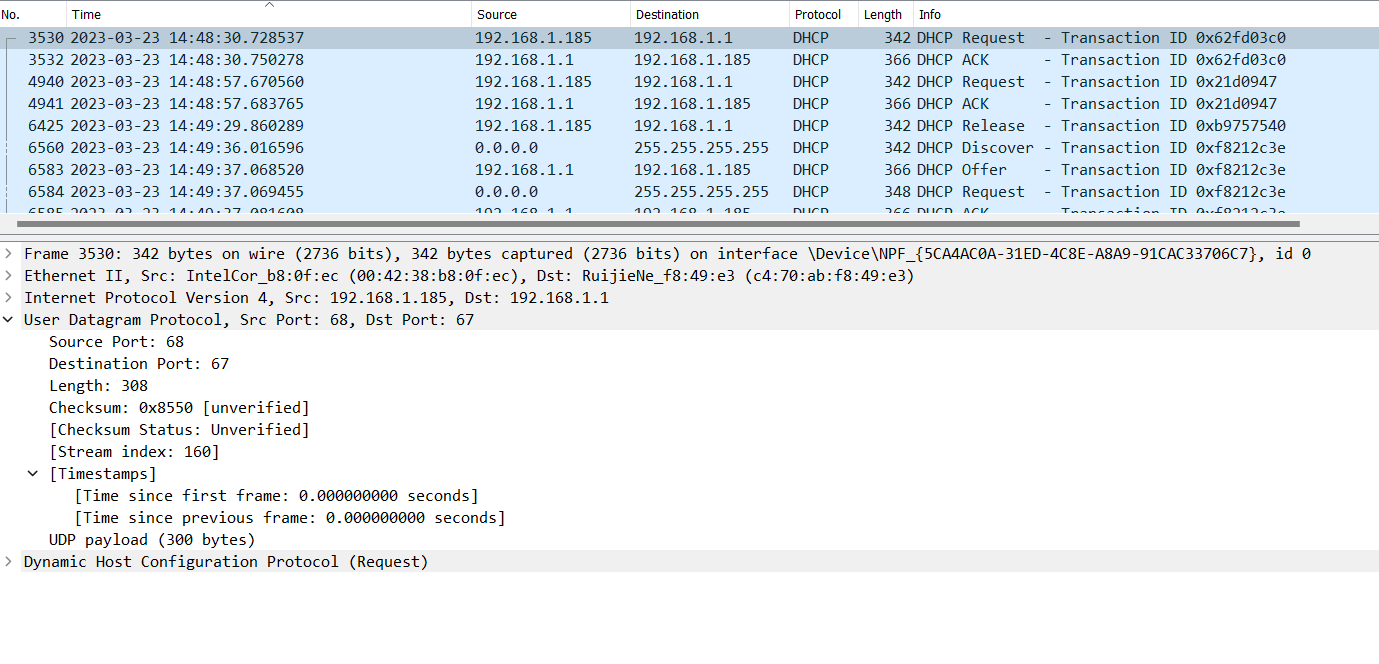
**Figure 2** Wireshark window with first DHCP packet – the DHCP Discover packet – expanded.

What to Hand In:

You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[[3]](#footnote-3) to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?



They sent by UDP

1. 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?

Table

Description automatically generated

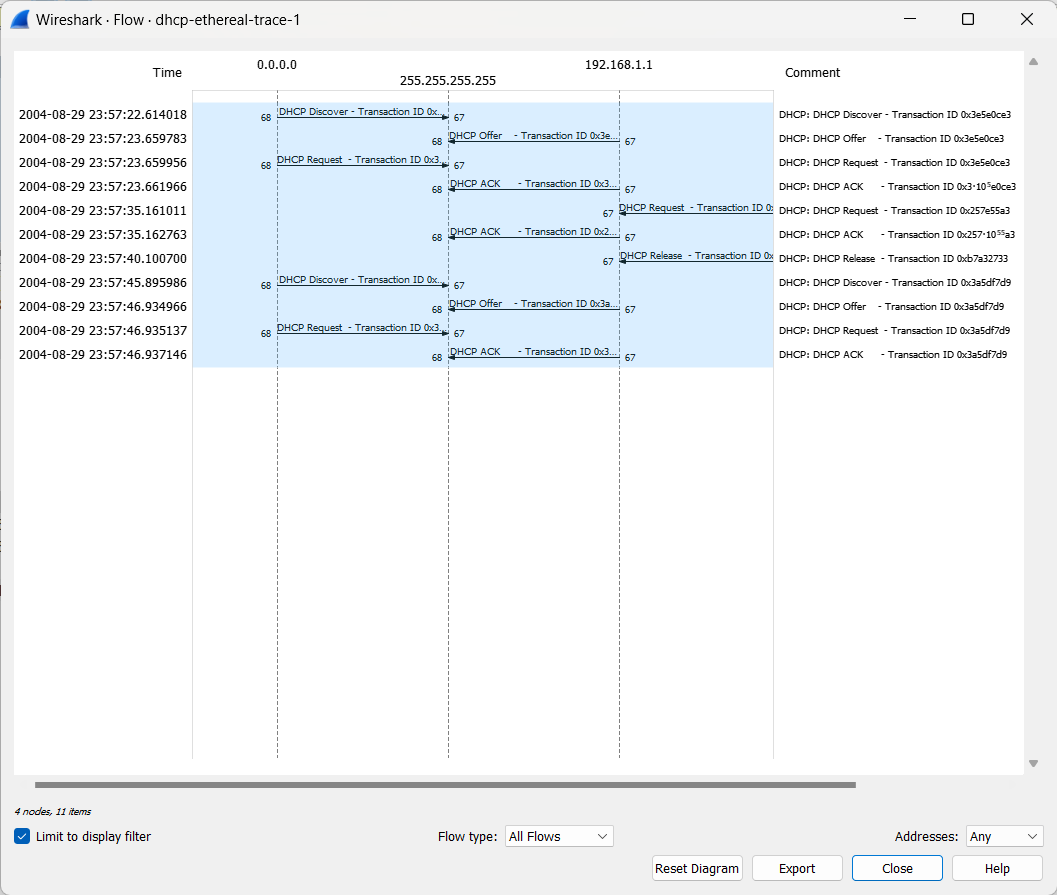
The Discover packet has a source port of 68 and destination port of 67

The Offer packet has a source port of 67 and a destination port of 68

The Request packet has a source port of 68 and a destination of 67

The ACK packet has a source port of 67 and a destination of 68

All of this corresponds to the example given in the lab.



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

Graphical user interface, application

Description automatically generated

the link-layer (e.g., Ethernet) address of my host is

Client MAC address: IntelCor\_b8:0f:ec (00:42:38:b8:0f:ec)

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

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated

The discover message has type value 1 and the request message has a type value of a 3

1. 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 DHCP messages is 0x5cf0dd80

The value of the Transaction-ID in each of the second DHCP messages is 0xeb5ee96b

The transaction ID identifies if a message is part of a set of messages related to one transaction

1. 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.

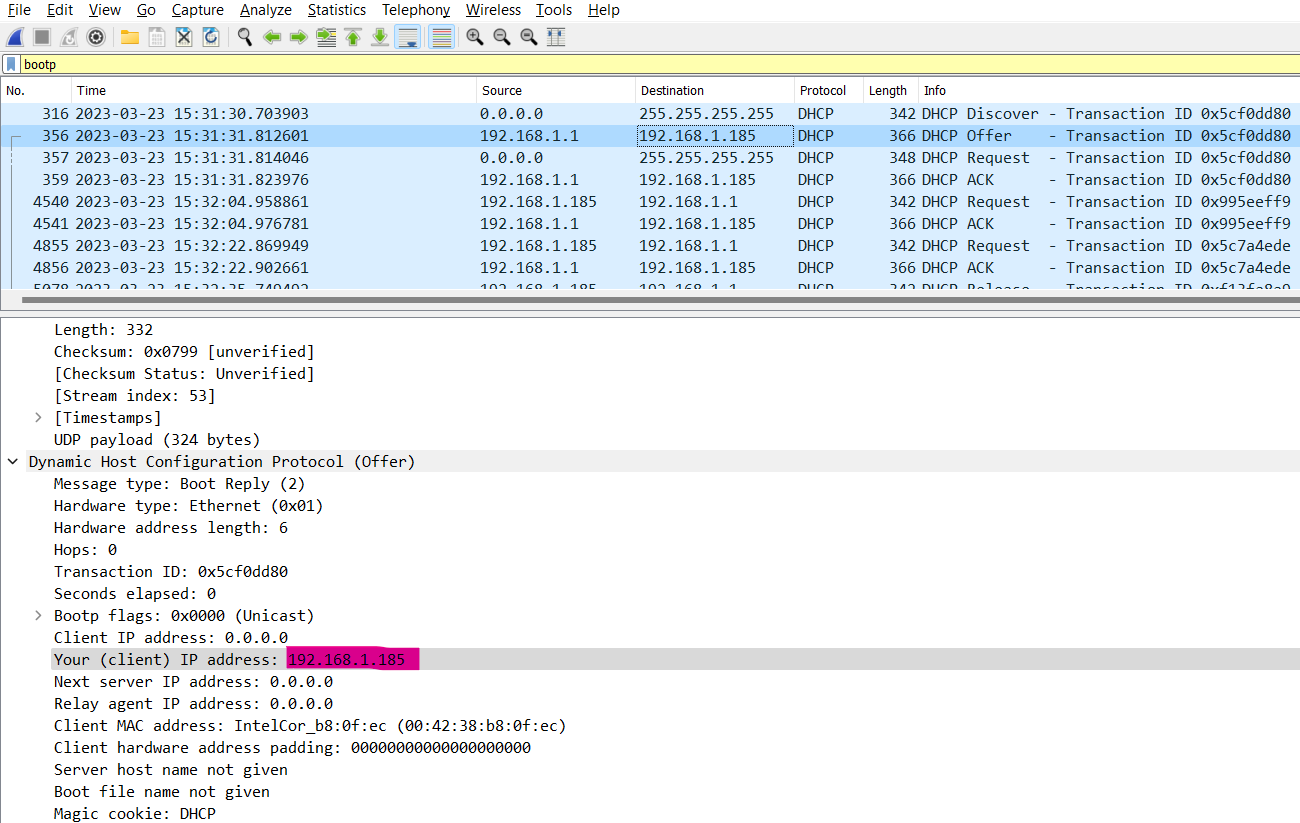
Note : I use the file *dhcp-ethereal-trace-1* to answer this question.

Discover source 0.0.0.0 Destination 255.255.255.255  
Offer source 192.168.1.1 Destination 255.255.255.255  
Request source 0.0.0.0 Destination 255.255.255.255  
Ack DHCP 192.168.1.1 Destination 255.255.255.255

Table

Description automatically generated

1. What is the IP address of your DHCP server?



The IP address of my DHCP server is 192.168.1.185

1. 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.

Graphical user interface

Description automatically generated with medium confidence

The DHCP server offers 192.168.1.1 as the ip address in the DHCP offer message.

1. 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 being 0.0.0.0 indicates the absence of a relay agent. There is no relay agent in my experiment.

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

The IP address for the router identifies the default  internet gateway. The subnet mask defines the subnet that is available.

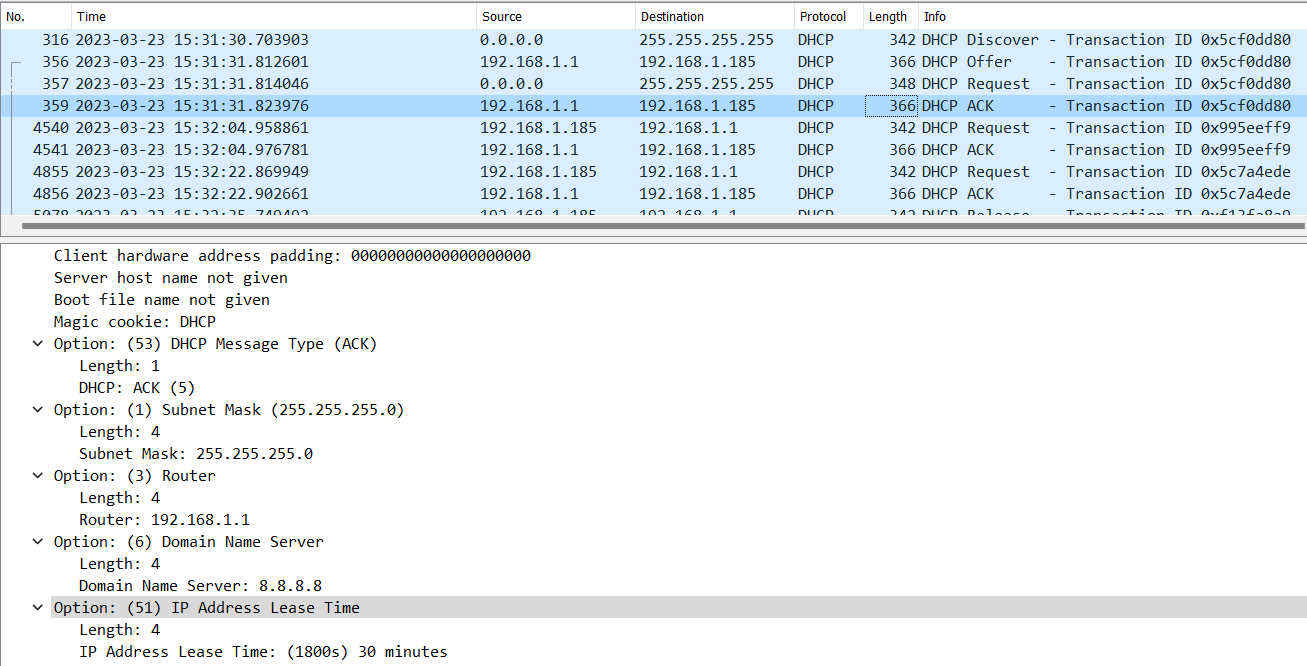
Graphical user interface, application

Description automatically generated

1. 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 same thing occurs the host requests the offered ip address.  
Option: (50) Requested IP Address (192.168.1.185)

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



The lease time is the amount of the time the user is aloud connection to the router

Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: (1800s) 30 minutes

1. 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 DHCP release message tells the dhcp server that you want to cancel the ip address offered. The DHCP server will not issue an ack of recipt of the client’s DHCP request. If the release message is lost then the dhcp server retains the ip address until the lease time expires.

1. 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 were arp packets sent and received to map the mac address with the ip addres (192.168.1.185)

1. References to figures and sections are for the 8th edition of our text, *Computer Networks, A Top-down Approach, 8th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2020.*  [↑](#footnote-ref-1)
2. If you are unable to run Wireshark live on a computer, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file *dhcp-ethereal-trace-1*. The traces in this zip file were collected by Wireshark running on one of the author’s computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the dhcp-ethereal-trace-1 trace file. You can then use this trace file to answer the questions below. [↑](#footnote-ref-2)
3. What do we mean by “annotate”? If you hand in a paper copy, please highlight where in the printout you’ve found the answer and add some text (preferably with a colored pen) noting what you found in what you ‘ve highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate. [↑](#footnote-ref-3)