Kate Moreland

kem0149

COMP 4320: Lab 4

Computer Network Lab (4)

This lab will go over two parts:

Part 1. Ethernet and ARP

-In this lab, you’ll use Wireshark to examine captured packets from a traceroute execution, then again to examine ARP packets, answering 15 questions as you work through the lab.

Part 2. DCHP

-In this lab, you’ll use Wireshark to capture packets as we force IP address release/renewals with DCHP and answer an additional 12 questions based on the experiment.

What to turn in for this lab:

1. Each part of the lab has a list of questions regarding your work in that part of the lab. You are required to give a report in PDF format including your answer to the questions given in the lab.
2. In addition to your answers, you are required to upload an unlisted video to Youtube (no more than 15 minutes) for each of the 2 parts, of you demoing the lab and demonstrating your knowledge of the material by explaining your answers to the lab questions. You need to provide the Youtube link on your report.

# Part 1: Ethernet and ARP

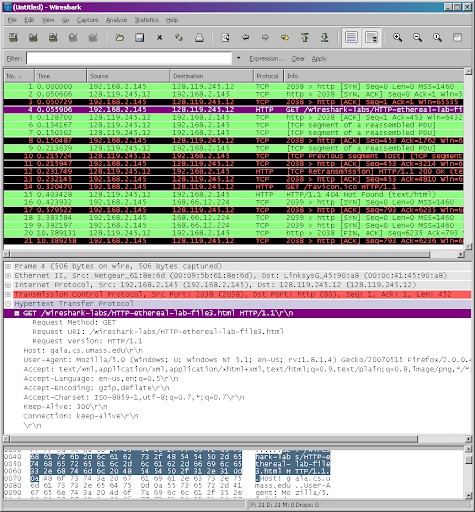
In this lab, we’ll take a quick look at DHCP. Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts (as well as to configure other network configuration information).

## 1. Capturing packets from an execution of traceroute

Let’s begin by capturing a set of Ethernet frames to study. Do the following:

* First, make sure your browser’s cache is empty. To do this under Mozilla Firefox V3, select Tools → Clear Recent History and check the box for Cache. For Internet Explorer, select Tools → Internet Options → Delete Files. Start up the Wireshark packet sniffer.
* Enter the following URL into your browser: [gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html.](http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html) Your browser should display the rather lengthy US Bill of Rights.
* Stop Wireshark packet capture. First, find the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent from your computer to gaia.cs.umass.edu, as well as the beginning of the HTTP response message sent to your computer by gaia.cs.umass.edu. You should see a screen that looks something like the one below (where packet 4 in the screen shot contains the HTTP GET message).

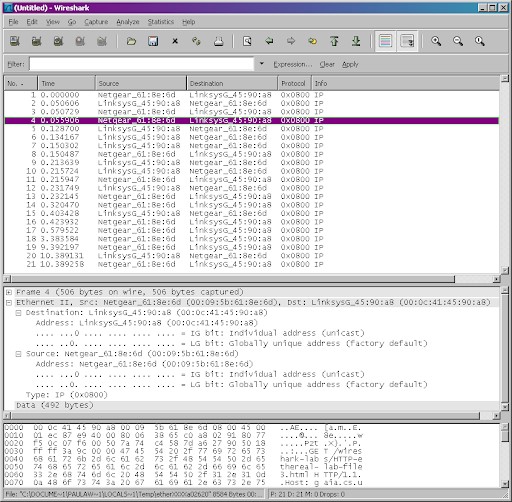
*Dr. K., 2020* 1



* Since this lab is about Ethernet and ARP, we’re not interested in IP or higher-layer protocols. So let’s change Wireshark’s “listing of captured packets” window so that it shows information only about protocols below IP. To have Wireshark do this, select Analyze → Enabled Protocols. Then uncheck the IP box and select OK. You should now see a Wireshark window that looks like (see the screenshot below):

In order to answer the following questions, you’ll need to look into the packet details and packet contents windows (the middle and lower display windows in Wireshark).

Select the Ethernet frame containing the HTTP GET message. (Recall that the HTTP GET message is carried inside of a TCP segment, which is carried inside of an IP datagram, which is carried inside

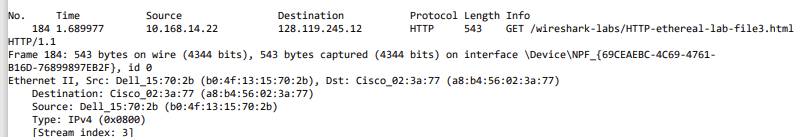


of an Ethernet frame). Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout 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.

1. What is the 48-bit Ethernet address of your computer?

The Ethernet address of my computer is b0:4f:13:15:70:2b.





1. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?

The destination address is a8:b4:56:02:3a:77. This is not the Ethernet address of gaia.cs.umass.edu. Instead, it is the Ethernet address of Cisco\_02:3a:77.

A close-up of a computer screen

AI-generated content may be incorrect.



1. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The frame type field is 0x0800 and it corresponds to IPv4.

A close-up of a computer screen

AI-generated content may be incorrect.



1. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

The G appears at the 54 byte in the Ethernet frame.

A screenshot of a computer

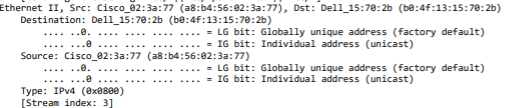
AI-generated content may be incorrect.



Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

1. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

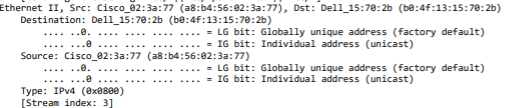
The source address is a8:b4:56:02:3a:77. It is not the address of my computer or gaia.cs.umass.edu. The device is Cisco\_02:3a:77.





1. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

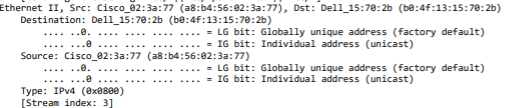
The destination address is b0:4f:13:15:70:2b. It is the address of my computer.





1. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

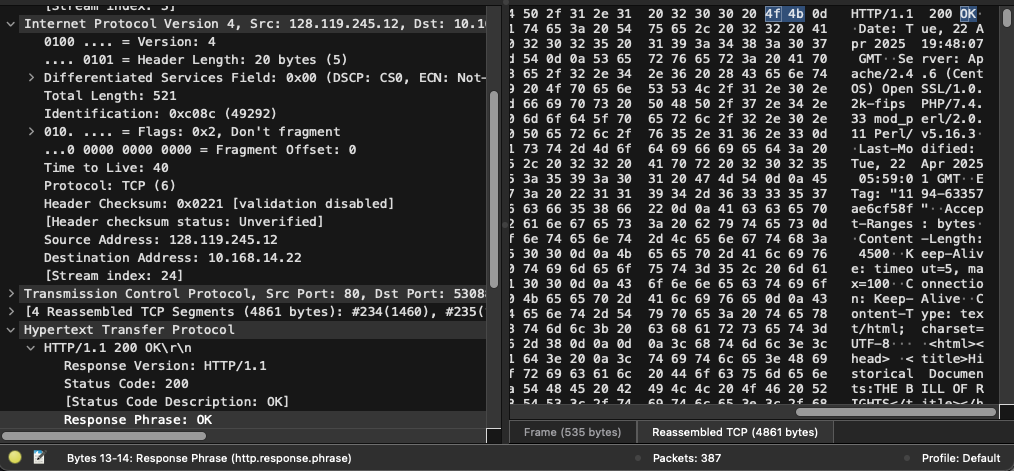
The hexadecimal is 0x0800 and it refers to IPv4.





1. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

The “O” is at byte 13.





## 2. The Address Resolution Protocol

ARP Caching

Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your computer The arp command (in both MSDOS and Linux/Unix) is used to view and manipulate the contents of this cache. Since the arp command and the ARP protocol have the same name, it’s understandably easy to confuse them. But keep in mind that they are different the arp command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on message transmission and receipt.

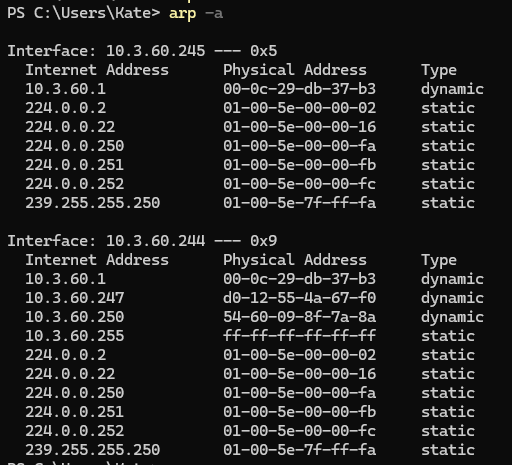
Let’s take a look at the contents of the ARP cache on your computer:

* MS-DOS. The arp command is in c:\windows\system32, so type either “arp” or “c:\windows\system32\arp” in the MS-DOS command line (without quotation marks).
* Linux/Unix/MacOS. The executable for the arp command can be in various places. Popular locations are /sbin/arp (for linux) and /usr/etc/arp (for some Unix variants).

The Windows arp command with no arguments will display the contents of the ARP cache on your computer. Run the arp command.

* Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

This displays and modifies the IP-to-Physical address translation tables. It shows different dynamic and static networks.



In order to observe your computer sending and receiving ARP messages, we’ll need to clear the ARP cache, since otherwise your computer is likely to find a needed IP-Ethernet address translation pair in its cache and consequently not need to send out an ARP message.

* MS-DOS. The MS-DOS arp –d \* command will clear your ARP cache. The –d flag indicates a deletion operation, and the \* is the wildcard that says to delete all table entries.
* Linux/Unix/MacOS. The arp –d \* will clear your ARP cache. In order to run this command you’ll need root privileges. If you don’t have root privileges and can’t run Wireshark on a Windows machine, you can skip the trace collection part of this lab and just use the trace given [here.](http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip)

Observing ARP in action Do the following:

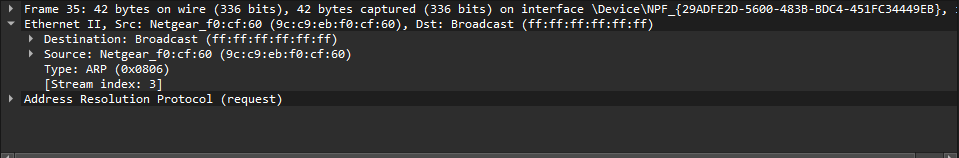
* Clear your ARP cache, as described above.
* Next, make sure your browser’s cache is empty. To do this under Mozilla Firefox V3, select Tools → Clear Recent History and check the box for Cache. For Internet Explorer, select Tools → Internet Options → Delete Files.
* Start up the Wireshark packet sniffer
* Enter the following URL into your browser [gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html) Your browser should again display the rather lengthy US Bill of Rights.
* Stop Wireshark packet capture. Again, we’re not interested in IP or higher-layer protocols, so change Wireshark’s “listing of captured packets” window so that it shows information only about protocols below IP. To have Wireshark do this, select Analyze-¿Enabled Protocols. Then uncheck the IP box and select OK. You should now see an Wireshark window that looks like the screenshot below:

In the example below, the first two frames in the trace contain ARP messages (as does the 6th message).

Answer the following questions:

* What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

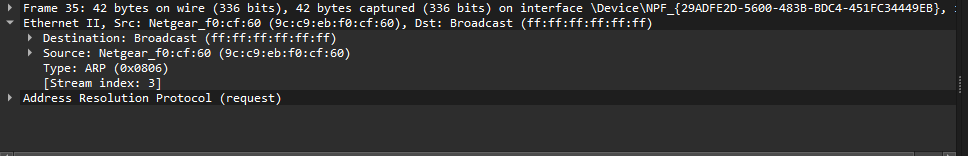
The source address is 9c:c9:eb:f0:cf:60 and the destination address is ff:ff:ff:ff:ff:ff.





* Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

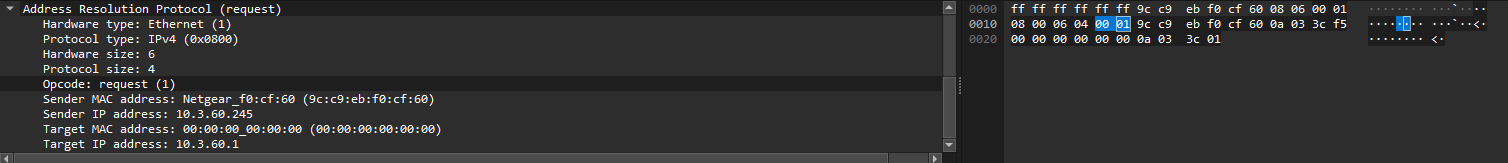
The type is 0x0806. It refers to ARP.

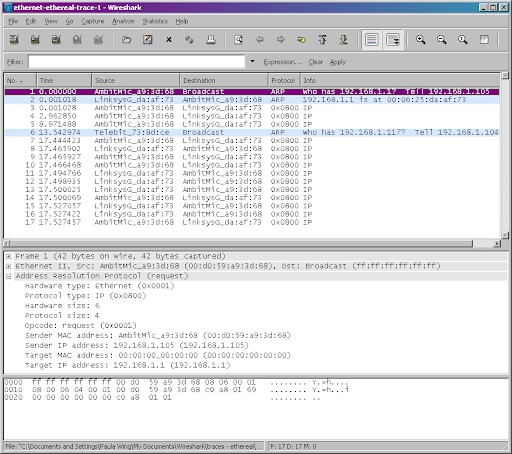




* Download the ARP specification from [ftp://ftp.rfc-editor.org/in-notes/std/std37.txt.](ftp://ftp.rfc-editor.org/in-notes/std/std37.txt) A readable, detailed discussion of ARP is also at [erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.](http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html)
  1. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

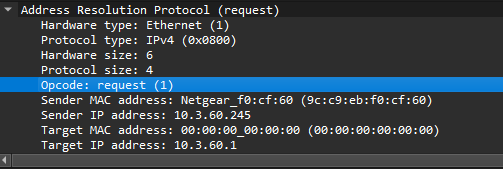
It starts at 20 bytes from the beginning.





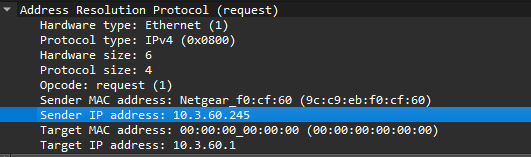
* 1. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The value of the field is 1 which means request.



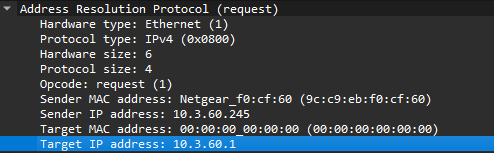
* 1. Does the ARP message contain the IP address of the sender?

Yes, the ARP message does contain the IP address of the sender which is 10.3.60.245.



* 1. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

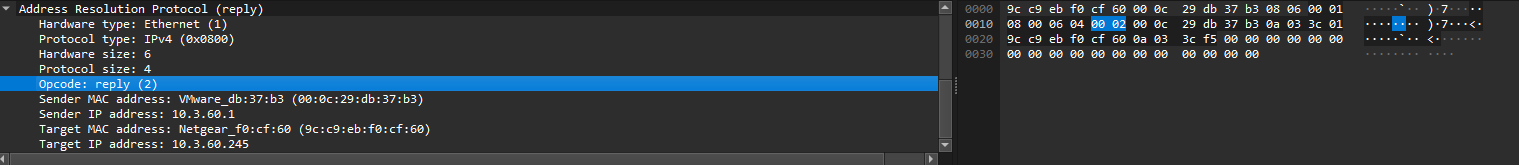
That will be shown under the target IP address which is 10.3.60.1.



* Now find the ARP reply that was sent in response to the ARP request.

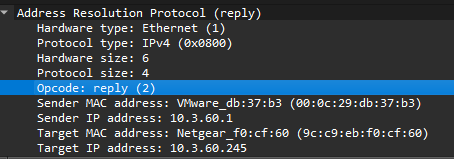
1. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

It begins 20 bytes from the beginning.



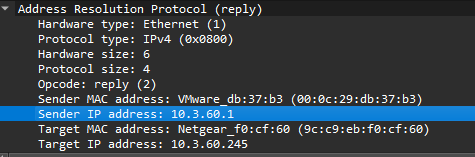
1. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of the opcode is 2 which means reply.



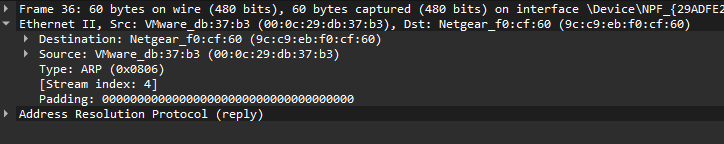
1. Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

It appears in the ARP under Sender IP address. It is 10.3.60.1.



1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

The source address is 00:0c:29:db:37:b3 and the destination address is 9c:c9:eb:f0:cf:60.



1. Open the ethernet-ethereal-trace-1 trace file provided [here.](http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip) The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

This indicates that there is no device with that IP that is active on that network.

# Part 2: DHCP

-In this lab, we’ll take a quick look at DHCP. 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.

\*\*\*For Linux and OSX users, we have added links and additional notes to these instructions showing the appropriate commands: [Linux](https://www.cyberciti.biz/faq/howto-linux-renew-dhcp-client-ip-address/) [Mac OS](https://osxdaily.com/2015/07/30/release-renew-dhcp-command-line-ipconfig/)

## 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:

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

\*\*\*Linux: the appropriate command for releasing your IP address is:

$ sudo dhclient -r

You can also use the -v to option show information on screen about dhcp server and obtained lease.Additionally, you can provide the specific interface you wish to release (eth0, wlp59s0, etc), which can be obtained using the command:

$ ip a

\*\*\*Mac OS: the appropriate command for releasing and renewing your IP address is:

$ sudo ipconfig set en0 DHCP where en0 is the name of your specific interface

* Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
* 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 the following figure, the host obtains the IP address 192.168.1.108.

\*\*\*Linux: the command to renew your IP address is:

$ sudo dhclient

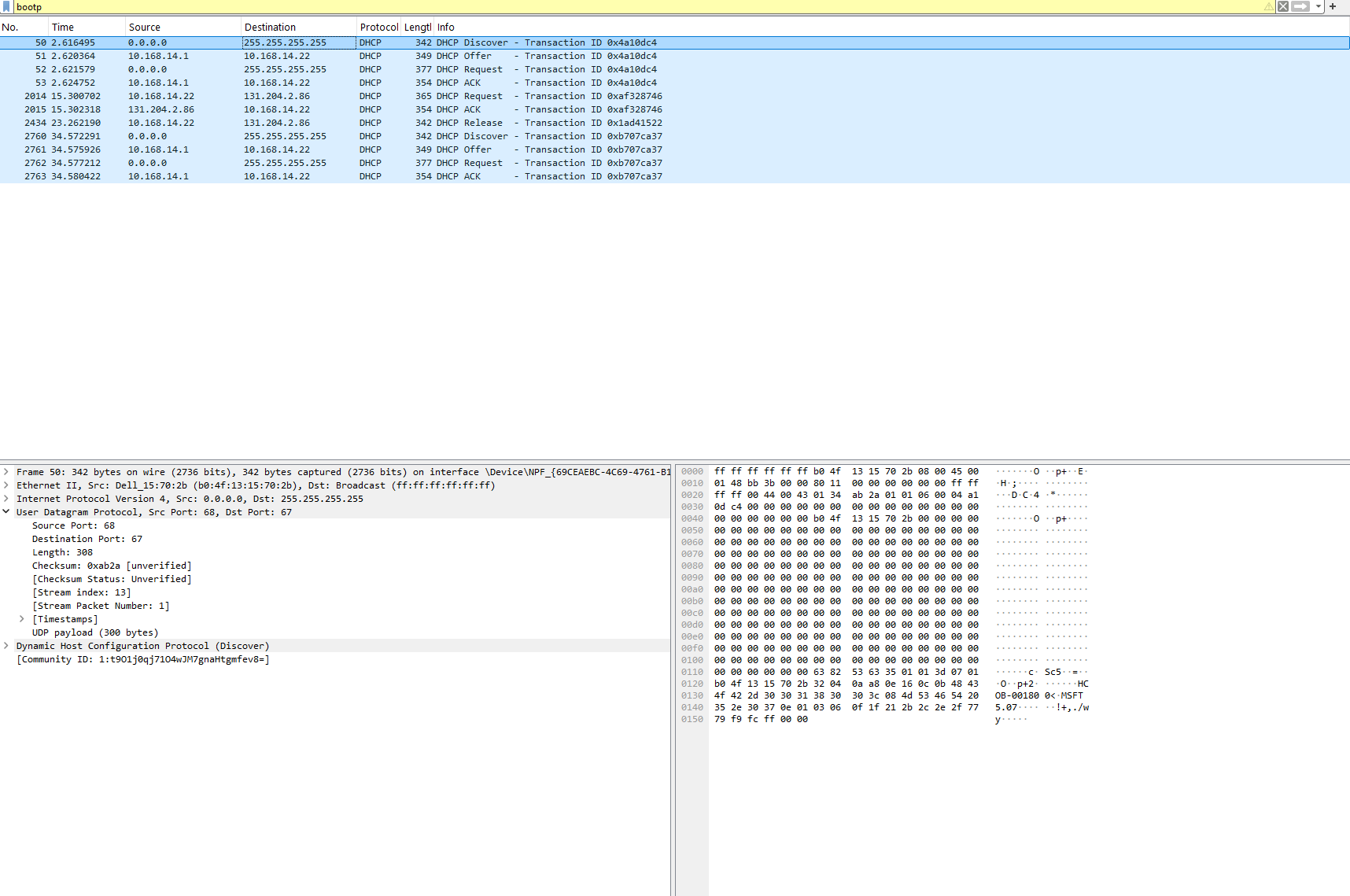
Here you also have the option to specify an interface or use -v to show information about the dhcp server and obtained lease.

* Wait until the “ipconfig /renew” has terminated. Then enter the same command “ipconfig /renew” again.
* When the second “ipconfig /renew” terminates, enter the command “ipconfig/release” to release the previously-allocated IP address to your computer.
* Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.
* 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. Answer the following questions:

1. Are DHCP messages sent over UDP or TCP?

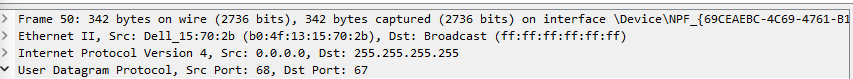
DHCP messages are sent over UDP.





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

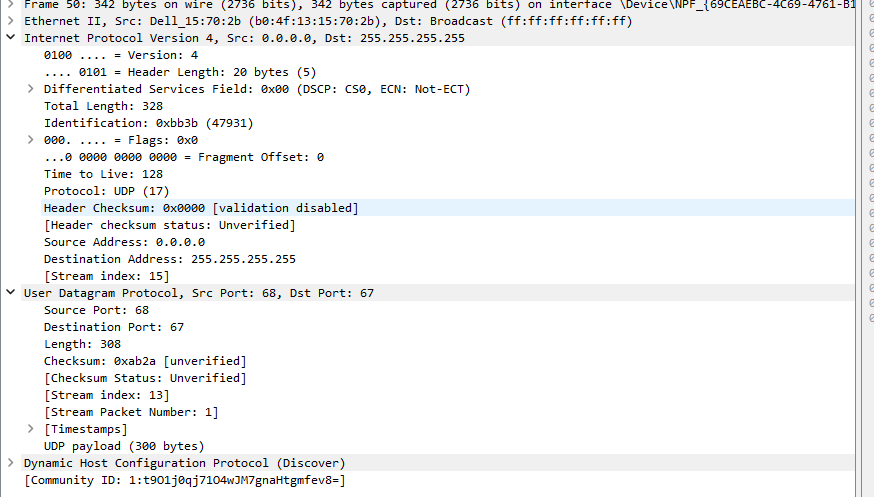
The link-layer address of the host is b0:4f:13:15:70:2b.

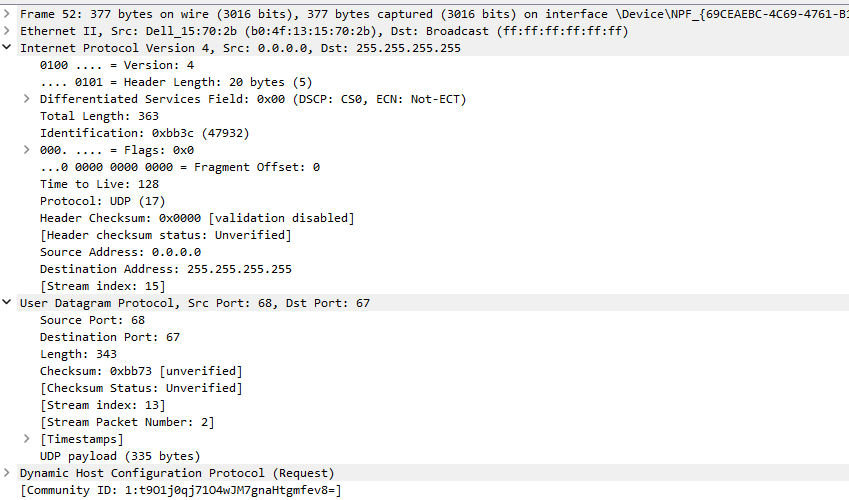




1. What values in the DHCP discover message differentiate this message from the DHCP request message?

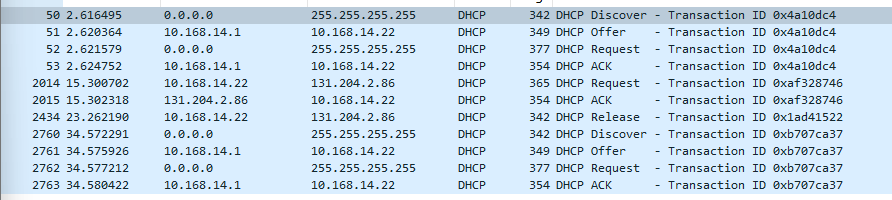
The length of the discover message is 342 and the length of the request message is 377. The UDP payload for discover is 300 bytes and the UDP payload for request is 335 bytes. The checksums are different as well.





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?

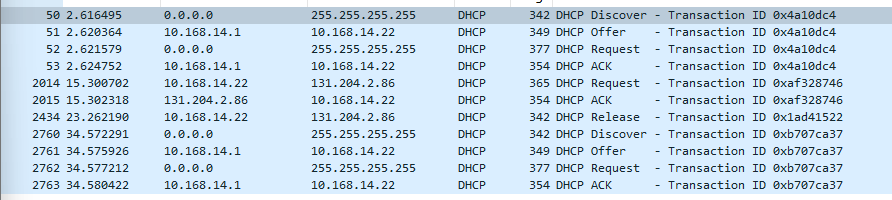
The Transaction-ID in each of the four messages are 0x4a10dc4. The values in the second set are 0xaf328746. The purpose of a Transaction-ID field is to make sure to group the replies and requests together to not get them mixed up. It makes sure that ACKs are sent in the correct session.





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.

In discover the source is 0.0.0.0 and the destination is 255.255.255.255. In offer the source is 10.168.14.1 and the destination is 10.168.14.22. In request the source is 0.0.0.0 and the destination is 255.255.255.255. In ACK the source is 10.168.14.1 and the destination is 10.168.14.22.





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

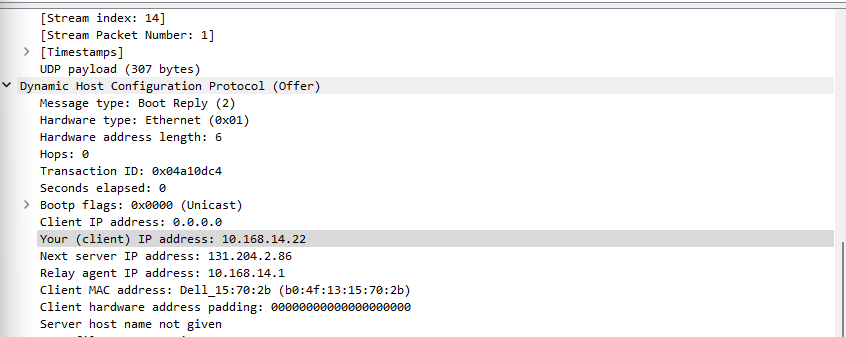
The IP address of the DHCP server is 131.204.2.86.





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.

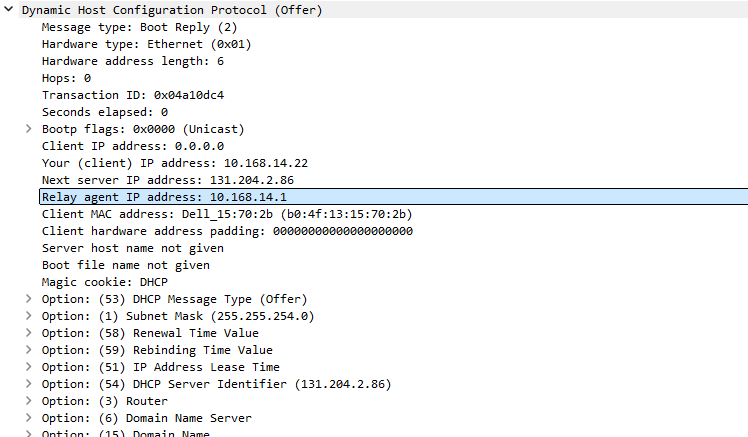
The IP address the DHCP server is offering is 10.168.14.22. This is found within the DHCP offer message.





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?

Yes, there is a relay agent. The IP of the agent is 10.168.14.1. To find the agent look in relay agent IP address.



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

The router line in the DHCP offer message shows the default gateway IP address. This is used by the client to deliver packets that are meant for networks outside its local subnet. The subnet mask line shows the size of the local network. This helps the client identify devices on the same network and ones on a different network.

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

Lease time shows the amount of time a client can use an IP that is assigned to them. This makes sure that there is no overlap in IP usage. The lease time in my experiment is 5 days.

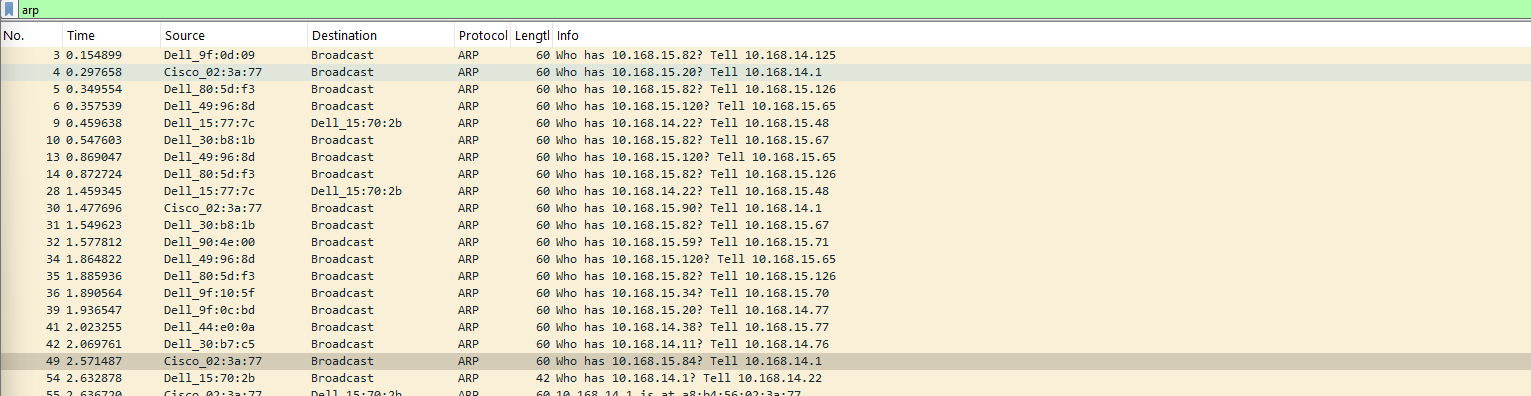


1. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

The request message is sent by the client to tell the DHCP server that it does not need the IP address anymore. This allows for another client to use it. There is no acknowledgement for a release message it will just automatically remove the IP. If the message gets lost then the server cannot mark the IP as available. This can lead to issue with getting the IP back in the server’s control.

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 packets sent during the exchange. After the client is able to get an IP then it will send an ARP message for its own IP. It double checks if anyone else on the network is currently using that IP. Also, other clients are updating their ARP tables.



End of Lab (4)

YouTube Link:

<https://youtu.be/eSw4wFeb1FA>

