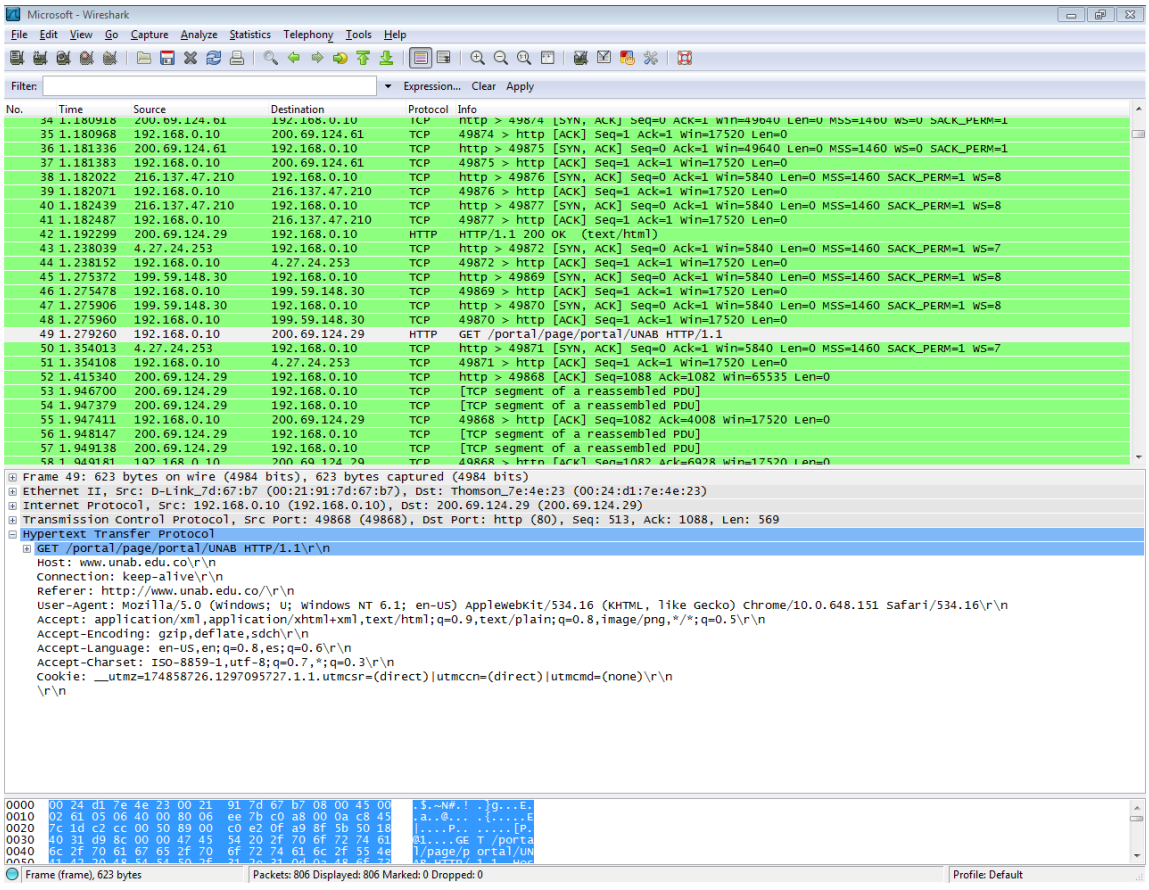
Wireshark Lab: Ethernet and ARP[1]

1. Capturing and analyzing Ethernet frames

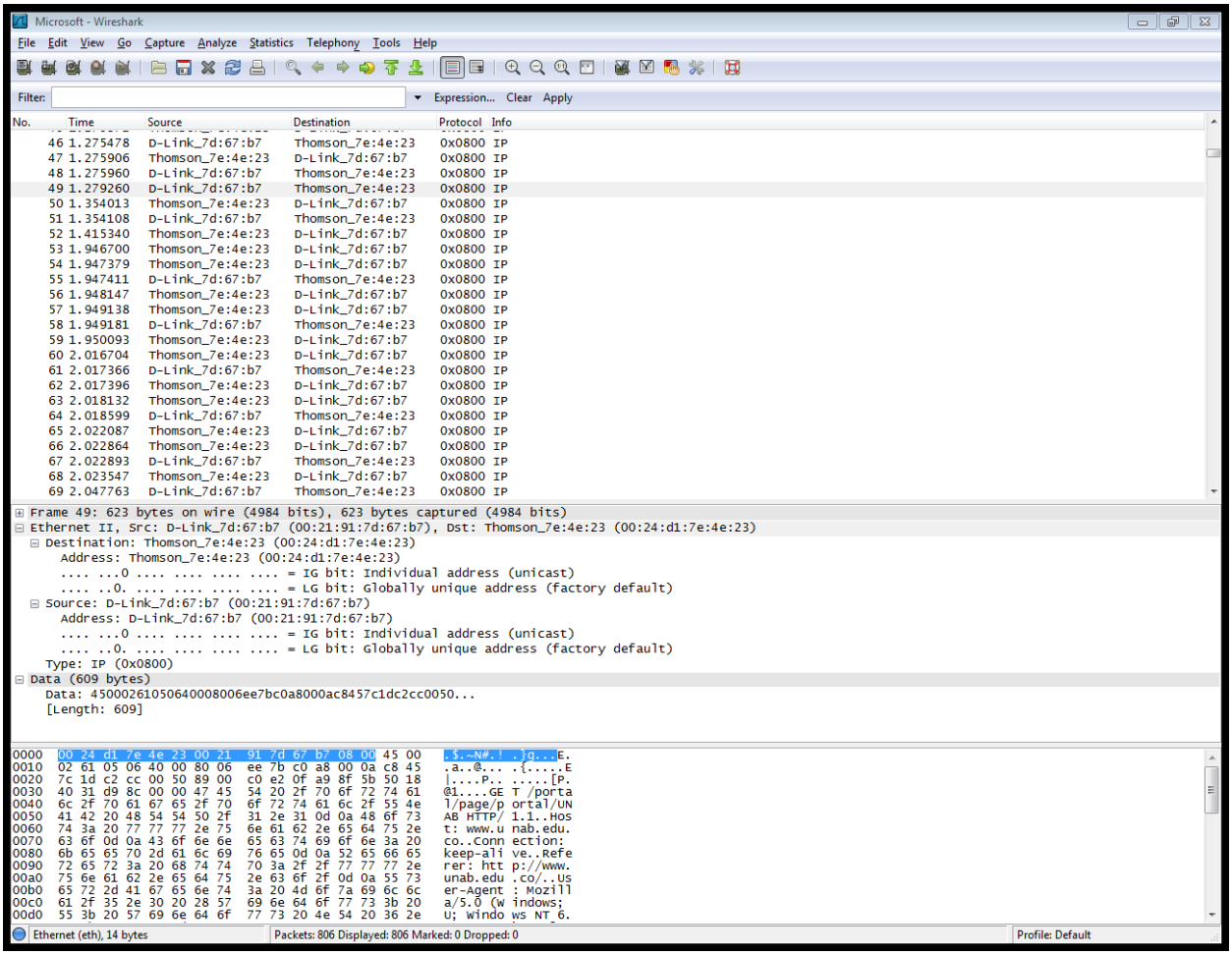
Let's begin by capturing a set of Ethernet frames to study. Do the following:

- First, make sure your browser's cache is empty. (To do this under Netscape 7.0, select Edit -> Preferences -> Advanced -> Cache and clear the memory and disk cache. For Internet Explorer, select Tools -> Internet Options -> Delete Files. For Firefox select Tools -> Clear Private Data.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser: http://www.unab.edu.co
- 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 www.unab.edu.co, as well as the beginning of the HTTP response message sent to your computer by www.unab.edu.co. You should see a screen that looks something like this (where packet 49 in the screen shot below contains the HTTP GET message)



[1] Lab modified version from Computer Networking: A Top down Approach, 4th edition by J.F. Kurose and K.W. Ross.

- Since this lab is about Ethernet and ARP, we're not interested in IP or higherlayer 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 an Wireshark window that looks like:



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. 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?

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of www.unab.edu.co? (Hint: the answer is no). What device has this as its Ethernet address?
3. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?
5. What is the hexadecimal value of the CRC field in this Ethernet frame?

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

6. What is the value of the Ethernet source address? Is this the address of your computer, or of www.unab.edu.co (Hint: the answer is no). What device has this as its Ethernet address?
7. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
8. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?
9. 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?
10. What is the hexadecimal value of the CRC field in this Ethernet frame?

2. The Address Resolution Protocol

In this section, we'll observe the ARP protocol in action.

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

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

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.

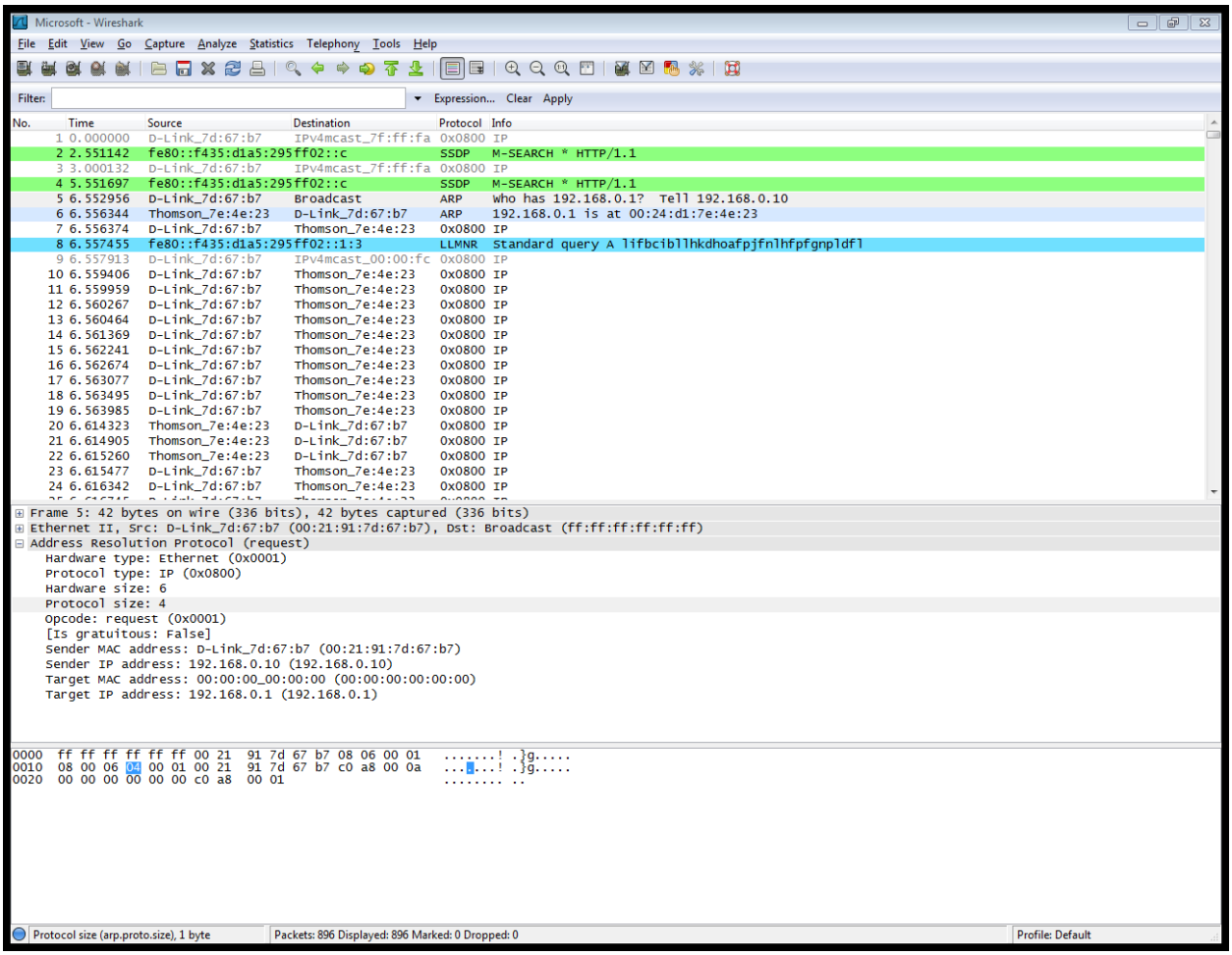
- MS-DOS. The MS-DOS arp –d * command will clear your ARP cache. The –d flag indicates a deletion operation, and the * is the wildcard that says to delete all table entries. You will need to run it as administrator.
- Linux/Unix. The arp –d * will clear your ARP cache. In order to run this command you'll need root privileges.

Observing ARP in action

Do the following

- Clear your ARP cache, as described above.
- Next, make sure your browser's cache is empty.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser: www.unab.edu.co
- 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 a Wireshark window that looks like:



In the example above, frames 5 and 6 in the trace contain ARP messages.

Answer the following questions:

12. Locate the ARP request message.
    a. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
    b. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?
    c. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
    d. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
    e. Does the ARP message contain the IP address of the sender?
    f. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?
13. Now find the ARP reply that was sent in response to the ARP request.

a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
b. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
c. 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?
d. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?