Lab 2: Ethernet and ARP

Hide Assignment Information

Instructions

Lab 2: Ethernet and ARP

Instructions:

- Support all answers by a screenshot of your Wireshark and Command Prompt windows. Annotate screenshots to explain your answer.
- Submissions must be through Brightspace.
- There is a 24-hour grace period after the due date without a penalty. Late submissions will not be accepted.

Note: This lab is mostly adapted from materials provided by the authors of *Computer Networking: A Top-Down Approach*.

Introduction

In this lab, you will investigate the Ethernet protocol and the ARP protocol. Before beginning this lab, you will probably want to review Link-layer addressing and ARP and Ethernet. RFC 826 (ftp://ftp.rfc-editor.org/in-notes/std/std37.txt) contains details of the ARP protocol, which is used by an IP device to determine the IP address of a remote interface whose Ethernet address is known.

Capturing and Analyzing Ethernet Frames

To capture a set of Ethernet frames, you will need access to a wired Ethernet connection for your PC or Mac - not necessarily a common scenario these days, given the popularity of wireless WiFi and cellular access.

Do the following:

- First, make sure to empty your browser's cache of previously downloaded documents. Instructions to clear your cache can be found here:

  https://www.uwindsor.ca/aipabuseresearchgroup/328/clearing-your-browser-cache

- Start up Wireshark and enter the following URL into your browser. Your browser should display the rather lengthy US Bill of Rights.

  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

Cancel

- Stop Wireshark packet capture.

In case you do not have access to a wired Ethernet connection, download the zip file here and extract the file *ethernet-wireshark-trace1.pcapng*. This trace file can be used to answer this Wireshark lab without capturing packets on your own. This trace was made using Wireshark running on one of the author's computers, while performing the steps indicated in this Wireshark lab. Once you have downloaded a trace file, you can load it into Wireshark and view the trace using the File pull down menu, choosing Open, and then selecting the trace file name.

Since this lab is about Ethernet and ARP, we are not interested in high-level protocols like IP, TCP or HTTP. We are interested in Ethernet frames and ARP messages.

Let's start by looking at 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. Your display should look similar to that shown in Figure 1.

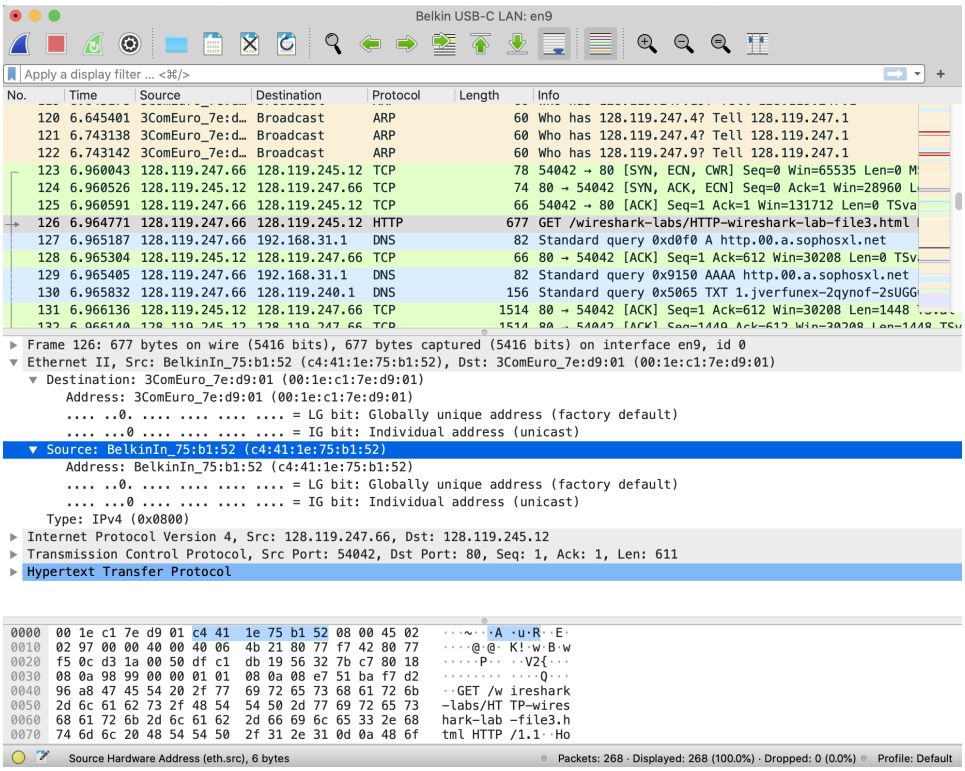

Figure 1: Wireshark display showing details of the Ethernet frame containing the HTTP GET request.

Questions

Now answer the following questions:

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 gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address?

3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request?

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

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

5. 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?

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

7. What is the hexadecimal value for the two-byte Frame type field?

8. 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? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

9. How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP "OK 200 ..." reply message?

The Address Resolution Protocol

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

Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your computer. The `arp` command (in Windows, MacOS and Linux) is used to view and manipulate the contents of this cache. Since the `arp` command and the ARP protocol have the same name, it is 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 ARP message transmission and receipt.

Let's take a look at the contents of the ARP cache on your computer. In Windows, MacOS, and Linux, the `arp -a` command will display the contents of the ARP cache on your computer. So, at a command line, type `arp -a`.

Questions

10. How many entries are stored in your ARP cache?

11. What is contained in each displayed entry of the ARP cache?

Observing ARP in action

To observe your computer sending and receiving ARP messages, you will 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. The `arp --d` command will clear your ARP cache using the command line. To run this command on a Mac or Linux machine you will need root privileges or use `sudo`. To run it on a Windows machine you will need to run as an administrator.

Do the following:

- Clear your ARP cache, as described above and make sure your browser's cache is cleared of previously downloaded documents.
- Start up the Wireshark packet sniffer.
- Enter the following URL into your browser:

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 are not interested in IP or higher-layer protocols, so let'sjust look at ARP packets. Your display should look similar to thatshown in Figure 2 (note we have entered "arp" into the display filterwindow at the top of the Wireshark screen).

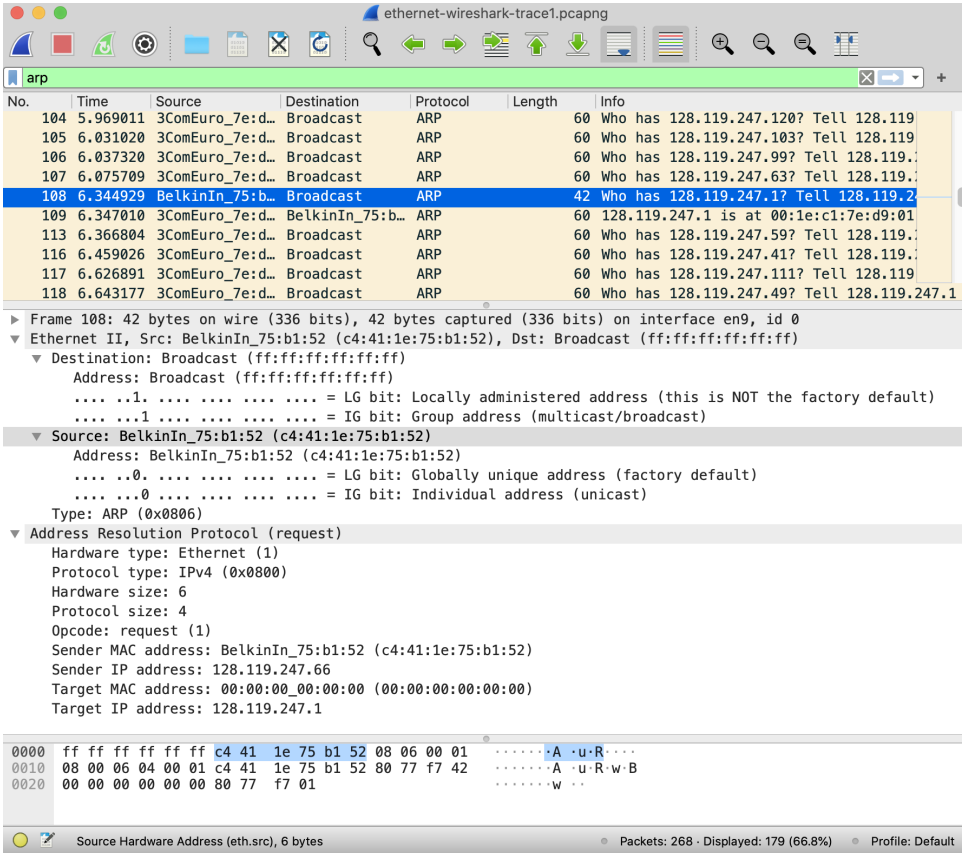

Figure 2: An ARP query being broadcast from the computer of one of the authors'

Questions

Let's start by looking at the Ethernet frames containing ARP messages. Answer the following questions:

12. What is the hexadecimal value of the source address in the Ethernet frame containing the ARP request message sent out by your computer?

13. What is the hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message sent out by your computer? And what device (if any) corresponds to that address (e.g., client, server, router, switch or otherwise...)?

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

Due on Oct 6, 2023 11:59 PM

Available on Oct 3, 2023 12:01 AM. **Access restricted before availability starts.**

Available until Oct 7, 2023 11:59 PM. **Submission restricted after availability ends.**

Submit Assignment

Submission is restricted outside of availability dates.