CS 145 Lab Exercise 2
Wireshark Lab: Layer 2 Addresses
A.Y. 2016-2017, 2nd Semester

1 Introduction

In this laboratory exercise you are going to explore the role played by the Data Link Layer (Layer 2) and Media Access Control (MAC) addresses in computer networks. As such, it would be helpful for you to review Lectures 5A and 5B (as well as Laboratory Exercise 1) before doing the laboratory exercise.

2 Restrictions

There are no restrictions for this laboratory exercise - you can use whatever computer, operating system, or network connection that you want. However, certain network connections or network setups will generate trace files that will complicate our discussion of this laboratory exercise. In other words, some network connections will generate "invalid" trace files. You will know whether your trace file is valid or not while in the process of answering the questions for the laboratory report. If you are not able to find a network connection that generates valid trace files, you can use the trace file that we will provide through the course webpage (UVLE) when working on your laboratory report. In your laboratory report, specify the computer and network setup that you used (laptop, DSL connection, etc.) - in the same manner, specify whether you used the trace file that we provided.

3 Instructions: Trace Generation

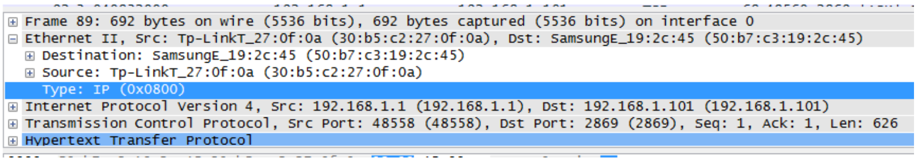
1. Start up a web browser, which will display your selected homepage.
2. Clear the memory/cache/history of your web browser. Throughout the exercise also avoid using multiple tabs, even if your browser is capable of tabbed browsing. That is, while doing the laboratory exercise, do **not** surf any other websites, as that would affect the trace that you would generate.
3. Start up the Wireshark software.

4. Select the appropriate interface and begin packet capture.
5. While Wireshark is running, enter the URL `http://www.cbtl.com.ph/` and have the web page displayed in your web browser. Wait for the entire web page to load completely before proceeding to the next step.
6. Enter the URL `http://www.philstar.com/` and have the web page displayed in your web browser. Wait for the entire web page to load completely before proceeding to the next step.
7. Stop packet capture.
8. Save the packet trace file as `labexercise2.pcapng`. You can use this if you wish to work on the laboratory report at a later time.
9. Open up the terminal.
10. In the terminal, type and execute the command `ifconfig eth0` (if you are using a laboratory computer or a computer with a wired connection). Take note of the results, or take a screenshot.
11. At this stage, you are now ready to work on the laboratory report.

4 What to hand in

Answer the following questions in the laboratory report, based on your Wireshark experimentation:

1. Filter (remove) all non-HTTP message packets in the packet-listing window. Identify the packet with the *first* HTTP GET message associated with the web page hosted by `cbtl.com.ph`. Include a screenshot or image of the packet, with an annotation showing why you think it is the packet we are looking for.
2. Repeat (1) for the web page hosted by `philstar.com`.
   - At this step, we can now determine whether your trace can be used for this exercise. Compare the addresses under the Destination column of the two GET messages (one from (1), one from (2)). If they are the *same*, then you can *not* use the trace file for this exercise. Either use another network for generating your trace file, or use `cbtlphilstar.pcapng`, which will be made available in the course webpage. Of course, when you change tracefiles, you would have to repeat (1) and (2).
3. Focus on the packet with the HTTP GET message associated with the web page hosted by `cbtl.com.ph`. In the packet details window, expand the second section (called "Ethernet II", between "Frame" and "Internet Protocol", see Figure 1). In the expansion of this section you find two fields: Source and Destination, containing the source and destination addresses, respectively. What is the source address associated with the packet? What is the destination address associated with the packet? Include an annotated image of the packet supporting your answer. **IMPORTANT**



```
⊞ Frame 89: 692 bytes on wire (5536 bits), 692 bytes captured (5536 bits) on interface 0
⊟ Ethernet II, Src: Tp-LinkT_27:0f:0a (30:b5:c2:27:0f:0a), Dst: SamsungE_19:2c:45 (50:b7:c3:19:2c:45)
  ⊞ Destination: SamsungE_19:2c:45 (50:b7:c3:19:2c:45)
  ⊞ Source: Tp-LinkT_27:0f:0a (30:b5:c2:27:0f:0a)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.101 (192.168.1.101)
⊞ Transmission Control Protocol, Src Port: 48558 (48558), Dst Port: 2869 (2869), Seq: 1, Ack: 1, Len: 626
⊞ Hypertext Transfer Protocol
```

Figure 1: Layer 2 addresses of a packet displayed by Wireshark.

NOTE: In this document, all references to "source address" and "destination address" should be taken to mean the source address and destination address at Layer 2. A packet contains other source and destination addresses that you will learn more about in later lectures.

4. Repeat (3) for the web page hosted by `philstar.com`.

5. For the packets with the HTTP GET messages you examined, what exactly does the source address signify? It is the address of what?

6. For the packets with the HTTP GET messages you examined, what exactly does the destination address signify? It is the address of what? Is it the address of the HTTP server hosting the web page you loaded?

7. Compare the source address of the packet with the HTTP GET message associated with the web page hosted by `cbtl.com.ph` with the source address of the packet with the HTTP GET message associated with the web page hosted by `philstar.com`. Are the two addresses the same? Does this make sense? Why?

8. Compare the destination address of the packet with the HTTP GET message associated with the web page hosted by `cbtl.com.ph` with the destination address of the packet with the HTTP GET message associated with the web page hosted by `philstar.com`. Are the two addresses the same? Does this make sense? Why?

9. What is the command `ifconfig` for? Look this up in the Internet or in books, but do not forget to cite your reference(s). Consider the values returned by `ifconfig`: are they consistent with the values you saw in the Wireshark packet trace? Justify, and include annotated screenshots or images supporting your answer.

Note: If you have not done so, exit the Wireshark software.

5 Submission

The laboratory report is due on Sunday, February 12, 2016, 2359 hours. You can submit the laboratory report via UVLE.