Homework 4 (ARP, IP and Ethernet)

Please complete following questions in the space provided. Submit a modified version to Connex in the submission box. Consult the file **Wireshark_Ethernet_ARP_v7.0.pdf** if needed.

Concepts

- What are physical Ethernet **MAC addresses**?
- How **packets/frames** are transmitted over a physical LAN?
- How **logical** IP address are mapped to **physical** MAC addresses?
- What is the purpose of `ARP` and `ARP cache` ?
- What is **protocol encapsulation** in a LAN?

Ethernet MAC Addresses

- Start your CSC361-VM.
- Start Firefox browser, and clear all its browsing history.
- Start up Wireshark to capture your default network interface (`eth0`), using a capture filter `host web.uvic.ca` .
- Enter the URL http://web.uvic.ca/~mcheng/lab1/csc100.html in Firefox.
- Once you see the packets are being captured and stopped, then **reload** the same page again; it will capture more packets.
- Now, stop Wireshark but don't exit.
- In the Display filter, enter `HTTP` . You should only see all `HTTP` protocol packets.
- You may save the packet traces for answering the questions in "Exercise 4" on Connex.

Answer the following questions on Connex under "Tests & Quizzes".

1. What is the packet number of the first HTTP GET request of `csc100.html` ?
2. What is the Ethernet MAC address (or WiFi MAC) of VM's default interface `eth0` ? (**Note:** Use `ifconfig` command.)
3. Examine the packet in question 1, what is the Ethernet MAC address of the **Source**? Does it match your MAC address in question 2?
4. What is the Ethernet MAC address of the **Destination**? Is it the MAC address of `web.uvic.ca` ?

ARP

Address Resolution Protocol (ARP) translates IP addresses to MAC addresses in a network. All network traffic is eventually transmitted using physical MAC addresses between neighbors on a LAN. Open a terminal session, enter:

```
traceroute web.uvic.ca -w1
```

Look at the first **gateway** (or **router**) appeared in the route to `web.uvic.ca` . Now, enter:

```
arp <IP address of your first router>
```

It should display the Ethernet MAC address of your first router.

5. Does this Ethernet MAC address match the **Destination** MAC in question 4?

Enter the following command in your terminal:

```
arp -n
```

it will display all entries in your ARP cache. Enter

```
sudo arp -d <IP address of your first router>
```

will delete the entry in your ARP cache. That is, your network stack no long remembers the MAC address of your first router.

Encapsulation

Each protocol in the upper layer is encapsulated by the protocol used in the lower layer. For example, HTTP is encapsulated by TCP; TCP by IP; IP by Ethernet frame, etc.

6. Examine the first HTTP GET request packet. How many bytes used in the HTTP GET request itself, ignoring all lower layer protocols?
7. How many bytes are in the TCP header? How many bytes are in the IP header?
8. How many bytes are in the Ethernet header? How many bytes are in the entire Ethernet frame, including header and payload?
9. How many bytes are used by the Ethernet header, IP header and TCP header?
10. Does the length of the entire Ethernet frame minus all headers (Ethernet, IP, TCP) match the HTTP GET request length (i.e., question 6)?