Homework 4 (ARP, ICMP, IP and Ethernet)

Please complete following questions in the space provided. Submit a modified version to Connex in the submission box.

Consult the files **Wireshark_Ethernet_ARP_v7.0.pdf** and **Wireshark_ICMP_v7.0.pdf** if needed.

(**Note**: You may use the provided `web.uvic.ca.pcap` for this exercise if you can't capture your traffic.)

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?
- What is `ICMP`?

Ethernet MAC Addresses

- Start Firefox browser, and clear its browsing history.
- Start up Wireshark to capture your default network interface, 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.

Q1. What is the packet number of the first HTTP GET request of `csc100.html`?

> *0x0030*

Q2. What is the Ethernet MAC address (or WiFi MAC) of your laptop? (**Note:** Use `ifconfig` or `ipconfig`.)

> *78-0C-B8-EE-2B-22*

Q3. Examine the packet in Q1, what is the Ethernet MAC address of the **Source**? Does it match your MAC address in Q2?

> *78-0C-B8-EE-2B-22 and Yes it matches the MAC addr in Q2*

Q4. What is the Ethernet MAC address of the **Destination**? Is it the MAC address of `web.uvic.ca`?

> *00:00:0c:07:ac:8d*

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.

Q5. Does the Ethernet MAC address match the **Destination** MAC in Q4?

> *00-14-1b-0e-64-00 they dint match*

Enter the following command in your terminal:

```
arp -a
```

it will display all entries in your ARP cache. Enter

```
arp -d
```

will delete all entries in your ARP cache.

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.

Q6. Examine the first HTTP GET request packet. How many bytes used in the HTTP GET request itself, ignoring all lower layer protocols?

> *404*

Q7. How many bytes are in the TCP header?

> *20 bytes*

Q8. How many bytes are in the IP header?

> *20 bytes*

Q9. How many bytes are in the Ethernet header?

> *458 bytes*

Q10. What is the length in bytes of the first HTTP GET request packet?

> *458 bytes*

Q11. If you sum up all bytes in Ethernet header + TCP header + IP header + HTTP GET request, does it match the length in Q9?

<div style=“page-break-after:always;”></div>

ICMP

Internet Control Message Protocol (ICMP) is a meta protocol for controlling and investigating the network layer inside a router.

- Start a terminal session.
- Enter `ping web.uvic.ca`, and you should see responses as follows:

```
PING web.uvic.ca (142.104.193.229) 56(84) bytes of data.
64 bytes from web2.uvic.ca (142.104.193.229): icmp_seq=1 ttl=63 time=16.5 ms
64 bytes from web2.uvic.ca (142.104.193.229): icmp_seq=2 ttl=63 time=17.7 ms
64 bytes from web2.uvic.ca (142.104.193.229): icmp_seq=3 ttl=63 time=18.2 ms
64 bytes from web2.uvic.ca (142.104.193.229): icmp_seq=4 ttl=63 time=16.6 ms
```

- Now, start Wireshark on the default interface with a capture filter `host web.uvic.ca`.
- In your terminal, enter `ping web.uvic.ca` again.
- You should see packets are being captured.
- Kill the `ping` command by entering `ctrl-C`.
- Stop Wireshark capture. But don't close it.

Q12. What is the IP address of `web.uvic.ca`?

> *142.104.197.50*

Q13. Are there any ICMP protocol packets? What is the **first** ICMP packet number?

> *0x0023*

Q14. In the **first** ICMP packet, what is the **total** packet length in bytes?

> *74 bytes*

Q15. What is the length in bytes of the IP packet portion alone in the **first** ICMP packet, not including the Ethernet header?

> *60*

Q16. What is the **type** of the **first** ICMP packet, i.e., its request type?

> *Type: 8 (Echo (ping) request)*

Q17. What is the packet number of the **first** ICMP **response** packet?

> *0x002B*

Q18. What is the **type** of the **first** ICMP packet **response**?

> *Type: 0 (Echo (ping) reply)*