## 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.)

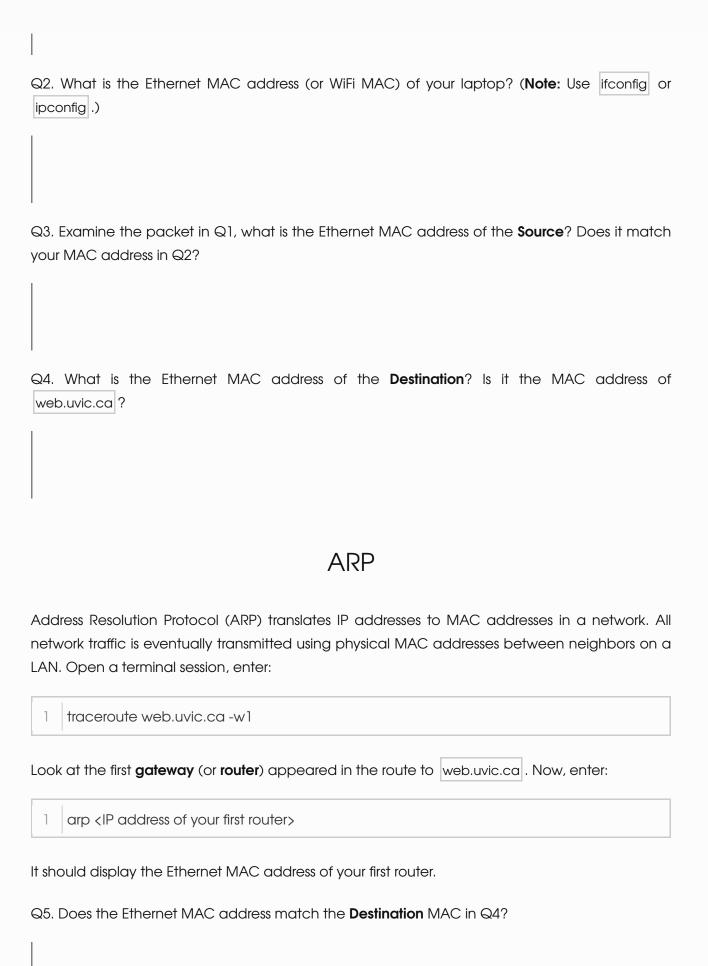
## **CONCEPTS**

- 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?



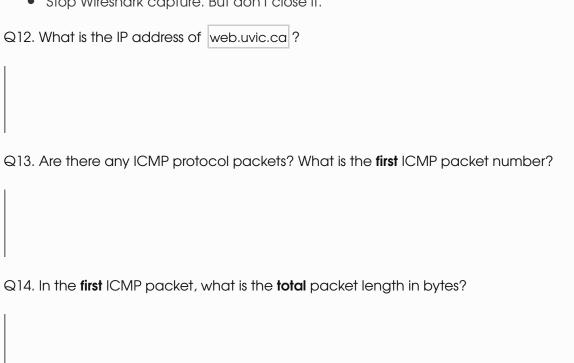
Enter the following command in your terminal:
1 arp-a
it will display all entries in your ARP cache. Enter
1 arp-d
will delete all entries in your ARP cache.
ENCAPSULATION
Each protocol in the upper layer is encapsulated by the protocol used in the lower layer. For example, HTTP is encapsulated by TCP; 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?
Q7. How many bytes are in the TCP header?
Q8. How many bytes are in the IP header?
Q9. How many bytes are in the Ethernet header?

Q10. What is the length in bytes of the first HTTP GET request packet?		
Q11. If you sum up all bytes in Ethernet header + TCP header + IP header + HTTP GET request, does it match the length in Q9?		

## **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.



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

Q16. What is the <b>type</b> of the <b>first</b> ICMP packet, i.e., its request type?	
Q17. What is the packet number of the <b>first</b> ICMP <b>response</b> packet?	
Q18. What is the <b>type</b> of the <b>first</b> ICMP packet <b>response</b> ?	