# CS 455: Computer Communications and Networking
# Lab - 4: Ethernet and ARP

**Grading, submission, and late policy:**

- You are expected to complete this lab **on your own** (not with a partner)
- This lab accounts for **4%** of your final grade
- The standard late policy applies - Late penalty for this lab will be 15% for each day. Submissions that are late by 3 days or more will not be accepted
- You will submit your solution via Blackboard

In this lab, we will investigate the Ethernet protocol and the ARP protocol.

## 1. Ethernet protocol

Do the following:

- Start Wireshark capture.
- Open your browser and go to http://www.phpathak.com/CS555/TCP-wireshark.html webpage. You don't have to do anything on this webpage. Simply let the page load on your browser while Wireshark packets are being captured.
- Stop the capture.

Select the packet containing the HTTP GET message from the packet trace. This HTTP GET would correspond to the TCP-wireshark.html object above. Expand the Ethernet II information in the packet details window at the bottom. You might be using WiFi, but Wireshark provides you with a simplified Ethernet frame based on a WiFi header. Answer the following questions and insert a screenshot of the packet detail window:

1. What is the 48 bit Ethernet MAC address of your computer?
2. What is the 48 bit destination MAC address in your Ethernet header? Which device does this MAC address correspond to?
3. Give the hexadecimal value for the two-byte Frame type field.  What upper layer protocol does this correspond to?
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

## 2. ARP protocol

We will first print your existing ARP cache. We will then clear the cache and capture ARP packets in Wireshark.

First, visit https://geekflare.com/check-and-clear-the-arp-cache/ to find your OS-specific command to print the ARP cache. For example, on a Windows machine, running arp -a (on the command line as administrator) gives you the list of cache entries. Answer the following:

5. Print the contents of your computer's ARP cache. You can remove the names of personal devices if they appear in the cache if you want.

Follow the https://geekflare.com/check-and-clear-the-arp-cache/ webpage to remove your ARP cache. The instructions could be different depending on your OS.

6. Show the output of the command that prints the ARP cache to show that it is empty.

Once the cache is clear, do the following again:

- Start Wireshark capture.
- Open your browser and go to http://www.phpathak.com/CS555/TCP-wireshark.html webpage. You don't have to do anything on this webpage. Simply let the page load on your browser while Wireshark packets are being captured.
- Stop the capture.

In your capture, you will now see ARP packets. If you don't, you have to repeat the ARP cache cleanup and Wireshark capture with little time in between so that the cache does not get repopulated. Write "arp" in the display filter to locate an ARP request and response message. Answer the following questions (include Wireshark screenshots for answers below):

7. Include a screenshot of the ARP request and response from your capture.
8. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
9. What are the source and destination MAC addresses for your ARP response?
10. Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
11. Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

## What to submit?

- Submit the two pcap files - one for Ethernet section above and the other for the ARP section.
- Prepare your answers in word/PDF file including the screenshots of packets as asked in the questions above.
- Submit the two pcap files and word/pdf document on blackboard.