# CSCI 466 Homework 3

Due Friday December 2nd at 11:59 PM

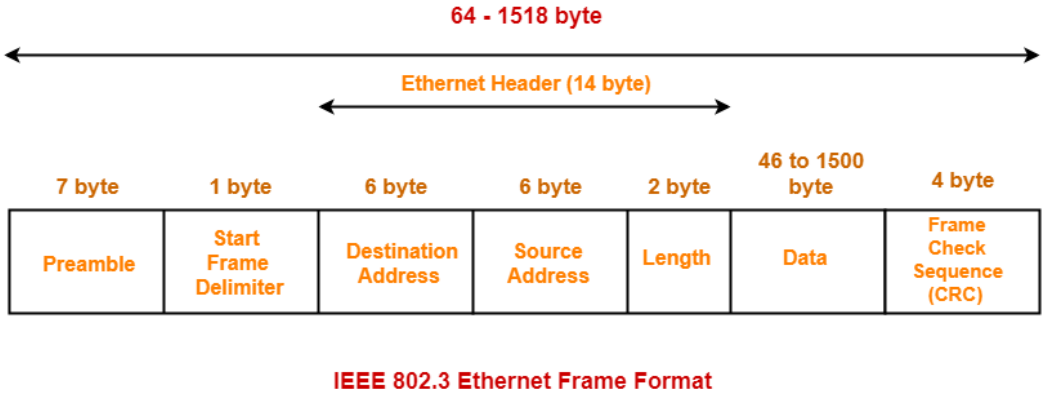
Please submit your **typed** answers as a PDF to the correct D2L dropbox

**Problem 1.** What is a MAC address? Why do we need one if IP addresses already exist?

**Problem 2.** In the link layer, a collision will occur if a receiver gets two frames at the same time. Describe one multiple access protocol we discussed in class, how it works, and how it prevents collisions.

**Problem 3.** What is the ARP protocol? When is it used, and how does it work?

**Problem 4.** Picture below is the format of a standard Ethernet frame in the link layer:




IEEE 802.3 Ethernet Frame Format

(a) What is the preamble field of an Ethernet frame? What is it used for?

(b) What is the CRC field of an Ethernet frame? What is it used for?

(c) What can you typically find in the Data field of an Ethernet frame? Hint: Think about the OSI layer above

**Problem 5.** What is the difference between symmetric and asymmetric cryptography? Why don't we just use asymmetric cryptography (such as RSA) for everything?

**Problem 6.** In RSA, what is the difference between the public key, and the private key? When is each one used?

**Problem 7.** TLS/SSL are very important protocols for providing confidentially and message integrity in network communications. **Digital Signatures** are used to verify the sender of a message. Describe the process of sending/creating a digital signature **and** the process for verifying a signed message.

**Problem 8.** In class we talked about 5 different network attacks: **TCP Flooding, TCP Reset, TCP Hijack, DNS Poisoning, and BGP Hijacking**. Provide a description of *three* of those attacks and a brief explanation of how they work.