Offensive Network Security

Assignment 1
CIS 4930/5930
100 points
Due: Thursday, 06 February 2014 (in-class)

1. The following questions will be regarding Switched Ethernet
    a. What *layer* technology is Ethernet considered? Give layer number and name. Use OSI naming convention for this question.
    b. Does an Ethernet frame need an IP address to send and receive? Why or why not?
    c. When an Ethernet frame travels through an Ethernet switch, what information is stored and/or updated by the switch? Is this information update trustworthy?
    d. Draw a diagram of an Ethernet frame header with the properties provided below. Hex-encode the properties correctly (i.e. A = 0x41): properties: **src**: AA:BB:CC:DD:EE:FF; **dst**: 11:22:33:44:55:66; **type**: ARP; **data**: 'data'; no need to include preamble or crc

2. The following questions will be regarding TCP/IP
    a. What *layers* are IP and TCP? Give layer number and name? Use OSI naming convention for this question.
    b. Does an IP address need to be assigned to a networking adapter for it to receive IP packets from a LAN? Explain your reasoning.
    c. Is it possible to send an Ethernet frame with an *encapsulated* TCP header and data to a receiver without TCP being *encapsulated* in an IP packet? Explain your reasoning.
    d. Draw the TCP threeway handshake between client and server assuming the **client** sequence value is 21312321 and the **server** sequence value is 878665.

3. The follow questions will be regarding UDP
    a. Draw the UDP client-server connection initiation. (Think about this one)
    b. Will a UDP client send it's UDP packet to a UDP receiver even if the UDP receiver is not running? Explain your reasoning.
    c. Could a UDP protocol be built ensuring UDP datagram delivery (ensuring datagrams all arrive correctly)? Assuming the user can not re-code the UDP protocol, where would a user program UDP datagram reliability? Why not

use TCP to for this same reason? Explain your reasoning.

4. Draw an ARP packet with the properties provided below.
    a. Assume encapsulated in Ethernet frame
    b. use hex notation for all values.
    c. All integer values given in decimal notation.
        i. Hardware Type: 20
        ii. Protocol Type: 300
        iii. Hardware Address Length (HAL): 8
        iv. Protocol Address Length (PAL): 16
        v. Operation: 4
        vi. Sender Hardware Address: an address matching HAL size
        vii. Sender Protocol Address: an address matching PAL size
        viii. Destination Hardware Address: an address matching HAL size
        ix. Destination Protocol Address: an address matching PAL size
    d. Is this a valid switched Ethernet ARP packet? If not, what could be the consequences of this packet being sent through a switched Ethernet? Explain your reasoning.