ECE435: Network Engineering – Homework 4

DNS, UDP

Due: Thursday, 28 September 2017, 12:30pm

For this homework short answers will suffice.

To submit, create a document with your answers (text, pdf, libreoffice, MS Office if you must) and e-mail them to *vincent.weaver@maine.edu* by the homework deadline. Title your e-mail "ECE435 Homework 4" and be sure your name is included in the document.

1. DNS

   (a) Look up the domain registration info for the **maine.edu** domain. There are various ways to do this; on Linux you can use the `whois` utility: `whois maine.edu`
   (you might need to install it first, `apt-get install whois`)

   i. When was the maine.edu domain *first* created?

   ii. What is the name of the registrar that maine.edu uses?

   (b) Use DNS requests to look up some information on various domains. On Linux you can use a utility named `dig` to do this easily. You might need to install the dnsutils package first `apt-get install dnsutils`. In the examples replace HOSTNAME with the name of the system you are asking about.

   i. What is the IP address of weaver.eece.maine.edu?
   `dig HOSTNAME A`

   ii. What is the IPv6 address of maine.edu?
   `dig HOSTNAME AAAA`

   iii. What is the name of the UMaine nameservers?
   `dig HOSTNAME NS`

   iv. What is the name of the UMaine mailservers?
   `dig HOSTNAME MX`

2. UDP

   (a) You can use the `tcpdump` program to record network packets. The following packet was gathered using the command `sudo tcpdump udp -XX -i eth0`.

   The first lines show a summary of the packet. The rest is a hexdump of the packet. The left column is the offset in hex. The next 8 columns are the hex representation of the bytes. The far right is the contents of the packet in ASCII (unprintable characters are shown as '.').

```
22:20:59.106555 IP macbook-air.43424 >
google-public-dns-a.google.com.domain: 57673+ A? www.adafruit.com. (34)
0x0000:  0013 3b10 667f 0050 b647 1cde 0800 4500  ..;.f..P.G....E.
0x0010:  003e e1ea 4000 4011 7fe6 c0a8 0826 0808  .>..@.@......&..
0x0020:  0808 a9a0 0035 002a 9299 e149 0100 0001  .....5.*...I....
0x0030:  0000 0000 0000 0377 7777 0861 6461 6672  .......www.adafr
0x0040:  7569 7403 636f 6d00 0001 0001            uit.com.....
```

The first part of the packet includes Ethernet and IPv4 headers that we don't know about yet. The UDP fields start at offset 0x22:

```
0x0020:       a9a0 0035 002a 9299 e149 0100 0001  .....5.*...I....
0x0030:  0000 0000 0000 0377 7777 0861 6461 6672  .......www.adafr
0x0040:  7569 7403 636f 6d00 0001 0001            uit.com.....
```

i. What is the source port (in decimal)?

ii. What is the destination port (in decimal)?

iii. What is the size of the UDP packet (in decimal)?

iv. Are checksums enabled? How can you tell?

v. What type of protocol is this / what is the packet doing?

3. General questions:

(a) What is one reason to use UDP over TCP?