ECE435: Network Engineering – Homework 7

Internet Protocol v4 / v6

Due: Friday, 8 March 2024, 5:00pm

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 7" and be sure your name is included in the document.

1. If you recall from previous homeworks we looked at a packet similar to this:

```
0x0000:  0013 3b10 667f b827 ebaf 3711 0800 4500  ..;.f..'..7...E.
0x0010:  0038 572a 4000 4006 69cc c0a8 0833 826f  .8W*@.@.i....3.o
0x0020:  2e7f bda5 0050 cdc4 6a49 3c7b 6ca5 8018  .....P..jI<{l...
0x0030:  00e5 79f4 0000 0101 080a 0104 3e58 34a8  ..y.........>X4.
0x0040:  7bc3 4745 540a                           {.GET.
```

   The IPv4 header begins at offset 0xe.
   Fill in the table with the name of the field as well as the decoded value. Use decimal when decoding if it makes sense, provide units if necessary, and if the value decoded has a meaning (such as a flag of pre-defined value) say what it means. Give sizes in bytes if possible, and any IPv4 addreses show in dotted decimal.
   For help decoding the IPv4 header see the class notes or else RFC791.

BEGIN IPv4 HEADER	Name of Field	Decoded Value
0x000e: 4		
0x000e: 5		
0x000f: 00		
0x0010: 0038		
0x0012: 572a		
0x0014: 4000		
0x0016: 40		
0x0017: 06		
0x0018: 69cc		
0x001a: c0a8 0833		
0x001e: 826f 2e7f		
END IPv4 HEADER		

2. Which of the following are valid IPv4 addresses?

   (a) 123.267.67.44

   (b) 1.1.1.1

   (c) 3232237569

   (d) 0xc0a80801

3. Early internet adopters got large IPv4 allocations. For example Ford (the car company) owned all of 19.0.0.0/8. What percentage of the entire IPv4 space is that? (Somewhat related, this old xkcd comic gives an interesting map of the IPv4 situation at the time: `https://xkcd.com/195/`)

4. A network is described as 192.168.13.0/24.

   (a) What would be the subnet mask for this subnet?

   (b) What would be the lowest IP address you could assign on this subnet?

   (c) What would be the highest IP address you could assign on this subnet?

5. Traditionally on Linux you could use the `route` command to find out the IP routing information for a system. Here are the results from a Raspberry Pi on one of my networks.

```
pi3:~$ /sbin/route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.8.2     0.0.0.0         UG    0      0        0 eth0
192.168.8.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

   The `route` command is now considered deprecated and you can now find the same info with the `ip route` command

```
pi3:~$ ip route
default via 192.168.8.2 dev eth0 proto dhcp src 192.168.8.138 metric 202
192.168.8.0/24 dev eth0 proto dhcp scope link src 192.168.8.138 metric 202
```

   (a) If a packet is sent to 216.58.192.132, what is its first "hop" on the way?

   (b) If a packet is sent to 192.168.8.50 what is its first "hop" on the way?

6. Use the "ping" command on a network connected machine to `ping www.google.com`. (If you don't have access to a machine with ping on traceroute available, let me know and I can provide access)

   (a) What is the round-trip packet time?

   (b) Do you notice anything odd about the hostname that responds?

7. Use the "traceroute" command. It's tracert on Windows.

   (a) `traceroute www.maine.edu`.
   How many hops away is it? Do you recognize any of the names in the hops along the way?

   (b) `traceroute www.facebook.com`.
   How many hops away is it? Do the response times gradually go up for each further hop?

8. **Network Address Translation**

   (a) You use tcpdump to monitor your network and see packets such as this go by:

   ```
   16:58:49.108396 00:13:3b:10:66:7f (oui Unknown) >
   00:50:b6:47:1c:de (oui Unknown), ethertype IPv4 (0x0800),
   length 141: google-public-dns-a.google.com.domain >
   macbook-air.51415: 30858 2/0/0
   CNAME pagead46.l.doubleclick.net., A 172.217.7.130 (99)
   ```

   where macbook-air has the address 192.168.8.38 and it is connecting to IP 8.8.8.8.

   Is it normal for an address like 192.168.8.38 to be able to connect directly to 8.8.8.8? Why or why not?

   What is the likely reason this is working?

   (b) You can use the `netstat-nat` command on a Linux machine doing NAT to see all of the nat connections. Some sample output is below.

   ```
   Proto NATed Address              Destination Address             State
   tcp   macbook-air:51908          49.246.178.107.bc.google:https ESTABLISHED
   tcp   macbook-air:55194          iad23s63-in-f19.1e100.ne:https ESTABLISHED
   tcp   macbook-air:42334          206-140.amazon.com:https       TIME_WAIT
   tcp   macbook-air:52930          104.16.78.166:https            ESTABLISHED
   tcp   macbook-air:57928          akamai-1-s.net.maine.edu:http  ESTABLISHED
   udp   macbook-air:58903          google-public-dns-a.goo:domain ASSURED
   udp   macbook-air:49779          google-public-dns-a.goo:domain ASSURED
   udp   macbook-air:44416          google-public-dns-a.goo:domain UNREPLIED
   udp   pi2:ntp                    clock.xmission.com:ntp         ASSURED
   udp   pi2:ntp                    38.88.18.251:ntp               ASSURED
   udp   pi2:ntp                    tock.no-such-agency.net:ntp    ASSURED
   ```

   One of the UDP connections is listed as UNREPLIED. Why might the NAT firewall track whether a UDP packet has been replied to or not?

9. **IPv6**

(a) Which of the following are valid IPv6 addresses?

i. 2607:f8b0:4009:0801:0000:0000:0000:200e

ii. 2607:f8b0:4009:801::200e

iii. 2607:f8b0::4009:801::200e

iv. 123.45.67.189

(b) We used tcpdump to gather the following network frame.

```
tcpdump port 53 -xe -i eth1 -XX
```

```
0x0000:  8875 563d 2a80 0030 18ab 1c39 86dd 6002  .uV=*..0...9..`.
0x0010:  2618 0031 1140 2610 0048 0100 08da 0230  &..1.@&..H.....0
0x0020:  18ff feab 1c39 2001 4860 4860 0000 0000  .....9..H`H`....
0x0030:  0000 0000 8844 e239 0035 0031 9c0e 8657  .....D.9.5.1...W
0x0040:  0120 0001 0000 0000 0001 0377 7777 0465  ...........www.e
0x0050:  7370 6e03 636f 6d00 0001 0001 0000 2910  spn.com.......).
0x0060:  0000 0000 0000 00
```

The IP header starts at address 0xe. From the value found there you suspect this is an IPv6 packet, so use the class notes or RFC2460 to decode the various fields. Decode to decimal if it makes sense, report what fields or flags stand for, be sure to report units if necessary, report addresses in hex with colons.

BEGIN IPv6 HEADER			Name of Field	Decoded Value
0x000e:	6			
0x000f:	00			
0x0010:	2	2618		
0x0012:	0031			
0x0014:	11			
0x0015:	40			
0x0016:	2610 0048	0100 08da		
	0230 18ff	feab 1c39		
0x0026:	2001 4860	4860 0000		
	0000 0000	0000 8844		
END IPv6 HEADER				

10. **Traceroute and Routing**

(a) You `traceroute www.cam.ac.uk` which is at Cambridge University in England. And get the following:

```
 1  bobcat.deaternet.vmw (192.168.8.1)  0.531 ms  0.455 ms  0.375 ms
 2  VL218.gw-um-pri.net.maine.edu (130.111.218.2)  0.567 ms  0.517 ms  0.506 ms
 3  be11.gw-oro.net.maine.edu (130.111.0.4)  1.200 ms  0.891 ms  0.914 ms
 4  * * *
 5  fourhundredge-0-0-0-0.4079.core1.hart2.net.internet2.edu (163.253.1.11)  19.283 ms  19.211 ms  19.152 m
 6  fourhundredge-0-0-0-0.4079.core1.newy32aoa.net.internet2.edu (163.253.1.229)  17.844 ms  17.833 ms  17.
 7  198.71.45.237 (198.71.45.237)  89.834 ms  89.682 ms  89.562 ms
 8  ae8.mx1.lon2.uk.geant.net (62.40.98.106)  101.424 ms  101.796 ms  101.597 ms
 9  janet-bckp-gw.mx1.lon2.uk.geant.net (62.40.125.58)  101.884 ms  101.794 ms  101.675 ms
10  ae31.erdiss-sbr2.ja.net (146.97.33.22)  105.984 ms  105.843 ms  105.626 ms
11  ae30.lowdss-sbr1.ja.net (146.97.33.26)  107.500 ms  107.941 ms  107.787 ms
12  ae26.lowdss-ban1.ja.net (146.97.35.246)  109.668 ms  107.610 ms  107.309 ms
13  uoc.ja.net (146.97.41.38)  109.475 ms  109.465 ms  109.345 ms
14  c-mi.b-jc.net.cam.ac.uk (131.111.6.182)  109.512 ms  110.400 ms  110.222 ms
15  d-dw.s-dw.net.cam.ac.uk (193.60.88.2)  110.916 ms  110.822 ms  110.754 ms
16  d-dw.s-dw.net.cam.ac.uk (193.60.88.2)  110.580 ms  110.489 ms  110.243 ms
17  s-dw.f-sv-net.net.cam.ac.uk (128.232.128.2)  110.032 ms  109.873 ms  109.747 ms
```

i. Can you tell which hop takes you across the Atlantic Ocean?

ii. Can you guess what city this happens in based on the hostnames?

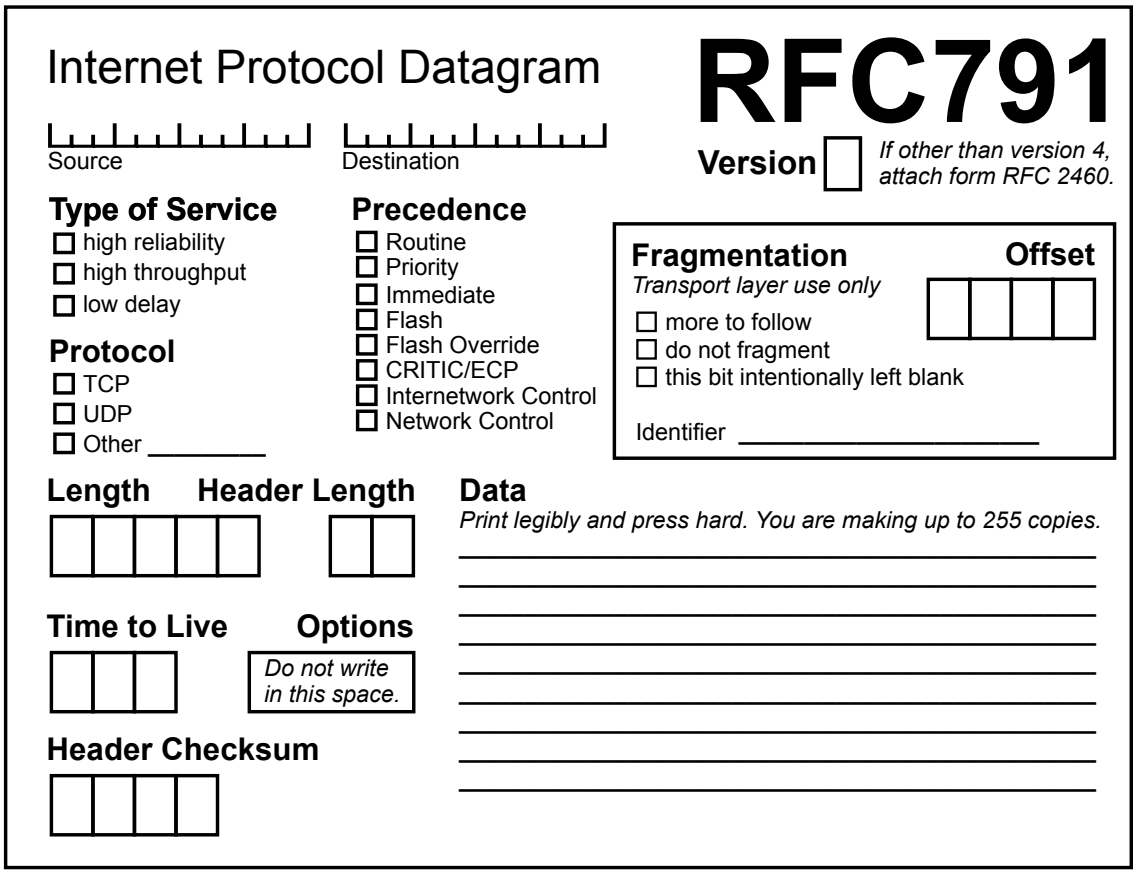
(b) Back in 2018 you ran `traceroute6 www.cam.ac.uk` which traces the same connection, but with IPv6, and you get the following (for some reason IPv6 doesn't seem to be working from my office anymore and I never got around to researching why):

```
 1  vl218.gw-o-neville.net.maine.edu (2610:48:100:8da::1)  1.957 ms  1.908 ms  2.068 ms
 2  gi7-2.gw-orono.net.maine.edu (2610:48::25)  0.769 ms  0.680 ms  0.836 ms
 3  2610:48:0:a::9 (2610:48:0:a::9)  0.774 ms  1.004 ms  0.943 ms
 4  2610:48:0:a::2 (2610:48:0:a::2)  21.907 ms  21.967 ms  21.878 ms
 5  et-4-1-0.4072.rtsw.wash.net.internet2.edu (2001:468:ff:a02::2)  30.120 ms  30.076 ms  29.928 ms
 6  abilene-wash.mx1.fra.de.geant2.net (2001:798:14:10aa::11)  126.785 ms  130.140 ms  126.743 ms
 7  ae1.mx1.ams.nl.geant.net (2001:798:cc:1401:2201::a)  120.872 ms  124.076 ms  120.840 ms
 8  ae2.mx1.lon.uk.geant.net (2001:798:cc:2801:2201::1)  119.811 ms  116.640 ms  119.732 ms
 9  janet-gw.mx1.lon.uk.geant2.net (2001:798:28:10aa::2)  129.290 ms  116.694 ms  129.300 ms
10  ae29.londpg-sbr2.ja.net (2001:630:0:10::1ca)  120.310 ms  117.270 ms  117.199 ms
11  ae30.londtw-sbr2.ja.net (2001:630:0:10::1ce)  120.909 ms  139.899 ms  139.835 ms
12  2001:630:0:10::17e (2001:630:0:10::17e)  120.647 ms  123.732 ms  133.303 ms
13  2001:630:0:1000:10::75 (2001:630:0:1000:10::75)  120.475 ms  120.632 ms  120.669 ms
14  2001:630:0:9000::2 (2001:630:0:9000::2)  123.632 ms  120.554 ms  120.494 ms
15  b-ec.c-ce.net.cam.ac.uk (2001:630:210:3::1)  133.603 ms  133.565 ms  133.567 ms
16  c-ce.d-dr.net.cam.ac.uk (2001:630:210:19::2)  124.555 ms  124.511 ms  133.799 ms
17  d-dr.s-dw.net.cam.ac.uk (2001:630:210:2002::2)  133.760 ms  121.897 ms d-dr.s-dr.net.cam.ac.uk (2001:63
18  mws-83481.mws3.csx.cam.ac.uk (2001:630:212:8::8c:90)  133.478 ms  133.416 ms  133.175 ms
```

i. Why are there be a different number of hops compared to IPv4?

ii. Is the latency better or worse when using IPv6? Why might this be?

Not a question, but you might know enough about IP networking now to find this novelty notepad amusing:



for more info, check IPv4 specifications at http://www.ietf.org/rfc/rfc0791.txt