Barret Jackson
66122573
November 27, 2020

COSC 328 Lab 7

Part 1: ICMP and Ping

```
bearitt ~ $ ping -c 10 ox.ac.uk
PING ox.ac.uk (151.101.66.133) 56(84) bytes of data.
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=1 ttl=60 time=15.5 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=2 ttl=60 time=15.1 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=3 ttl=60 time=15.4 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=4 ttl=60 time=15.4 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=5 ttl=60 time=15.5 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=6 ttl=60 time=15.5 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=7 ttl=60 time=15.4 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=8 ttl=60 time=15.5 ms
64 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=9 ttl=60 time=14.9 ms
64 bytes from 151.101.66.133: icmp_seq=10 ttl=60 time=15.6 ms

--- ox.ac.uk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 45302ms
rtt min/avg/max/mdev = 14.872/15.375/15.573/0.207 ms
```

Note: The URL "www.ust.hk" resulted in only dropped packets (not sure why since I was able to access it in my browser), so I used the Oxford University's homepage instead

9	1.054822801	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=1/256, ttl=64 (reply in 10)
10	1.070265581	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=1/256, ttl=60 (request in 9)
31	6.106237227	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=2/512, ttl=64 (reply in 32)
32	6.121334152	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=2/512, ttl=60 (request in 31)
46	11.132879887	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=3/768, ttl=64 (reply in 47)
47	11.148280849	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=3/768, ttl=60 (request in 46)
76	16.156986952	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=4/1024, ttl=64 (reply in 77)
77	16.172377125	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=4/1024, ttl=60 (request in 76)
104	21.182844885	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=5/1280, ttl=64 (reply in 105)
105	21.198377865	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=5/1280, ttl=60 (request in 104)
124	26.210895797	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=6/1536, ttl=64 (reply in 125)
125	26.226416945	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=6/1536, ttl=60 (request in 124)
138	31.235933234	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=7/1792, ttl=64 (reply in 139)
139	31.251326912	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=7/1792, ttl=60 (request in 138)
167	36.262919404	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=8/2048, ttl=64 (reply in 168)
168	36.278371523	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=8/2048, ttl=60 (request in 167)
191	41.333461835	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=9/2304, ttl=64 (reply in 192)
192	41.348320647	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=9/2304, ttl=60 (request in 191)
231	46.356972085	192.168.1.71	151.101.66.133	ICMP	98 Echo (ping) request	id=0x000a, seq=10/2560, ttl=64 (reply in 232)
232	46.372531899	151.101.66.133	192.168.1.71	ICMP	98 Echo (ping) reply	id=0x000a, seq=10/2560, ttl=60 (request in 231)

1) The IP address of my host is 192.168.1.71 (although this a a private address, so this is clearly behind a NAT). The IP address of the destination host is 151.101.66.133.

2) ICMP is primarily (but not exclusively) used for error messages; all ICMP messages are handled directly by the operating system of the source and destination hosts. Since port numbers are used by the operating system to forward datagrams to a specific process, ICMP does not require port numbers for either the source or destination because the data will not be forwarded to any processes in the OS. More specifically, TCP/IP usually implements the ping server directly in the operating system (Kurose and Ross 7th Edition, pg. 472).

3) Packet information from first packet sent from my host to destination:

```
No.     Time           Source                Destination           Protocol Length Info
      9 1.054822801    192.168.1.71          151.101.66.133        ICMP     98     Echo (ping) request  id=0x000a,
seq=1/256, ttl=64 (reply in 10)
Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp4s0, id 0
Ethernet II, Src: ASUSTekC_de:7c:0a (24:4b:fe:de:7c:0a), Dst: Actionte_f6:8c:80 (fc:2b:b2:f6:8c:80)
Internet Protocol Version 4, Src: 192.168.1.71, Dst: 151.101.66.133
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x820a (33290)
    Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x1cc5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.71
    Destination Address: 151.101.66.133
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x6012 [correct]
    [Checksum Status: Good]
    Identifier (BE): 10 (0x000a)
    Identifier (LE): 2560 (0x0a00)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 10]
    Timestamp from icmp data: Nov 27, 2020 18:00:48.000000000 PST
    [Timestamp from icmp data (relative): 0.262346473 seconds]
    Data (48 bytes)
0000  c3 00 04 00 00 00 00 00 10 11 12 13 14 15 16 17   ................
0010  18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27   ........ !"#$%&'
0020  28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37   ()*+,-./01234567
```

The ICMP is of type 8 and code 0, which is a “echo request” packet. The packet also has a checksum, identifiers (BE and LE), a timestamp, and lastly, the data being sent (randomized data 56 bytes long, https://linux.die.net/man/8/ping). The checksum, sequence number, and identifier fields are all identified by a four digit hex number, meaning they are (4 bits per hex digit) * (4 hex digits) = 16 bits = 2 bytes long each.

4) The ICMP packet is of type 0 and code 0, also known as an “echo reply” packet. This packet also has a checksum, an identifier, a sequence number, timestamp, and the data from the request packet. As in the request packet, the checksum, identifier, and sequence number fields are all 2 bytes long. (see next page for screenshot).

```
No.     Time           Source                Destination           Protocol Length Info
     10 1.070265581    151.101.66.133        192.168.1.71          ICMP     98     Echo (ping) reply    id=0x000a,
seq=1/256, ttl=60 (request in 9)
Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp4s0, id 0
Ethernet II, Src: Actionte_f6:8c:80 (fc:2b:b2:f6:8c:80), Dst: ASUSTekC_de:7c:0a (24:4b:fe:de:7c:0a)
Internet Protocol Version 4, Src: 151.101.66.133, Dst: 192.168.1.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xd4e5 (54501)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 60
    Protocol: ICMP (1)
    Header Checksum: 0x0dea [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 151.101.66.133
    Destination Address: 192.168.1.71
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x6812 [correct]
    [Checksum Status: Good]
    Identifier (BE): 10 (0x000a)
    Identifier (LE): 2560 (0x0a00)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 9]
    [Response time: 15.443 ms]
    Timestamp from icmp data: Nov 27, 2020 18:00:48.000000000 PST
    [Timestamp from icmp data (relative): 0.277789253 seconds]
    Data (48 bytes)
0000  c3 00 04 00 00 00 00 00 10 11 12 13 14 15 16 17   ................
0010  18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27   ........ !"#$%&'
0020  28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37   ()*+,-./01234567
```

Part 1 question 4) screenshot

Part 2: ICMP and Traceroute

(note that I use Linux, however from the man page for traceroute, the -I flag forces traceroute to use ICMP ECHO for probes. Therefore, this is what I used)

```
traceroute to inria.fr (128.93.162.63), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.254)  13.321 ms  13.322 ms  13.317 ms
 2  10.29.152.1 (10.29.152.1)  14.925 ms  14.934 ms  14.927 ms
 3  154.11.15.111 (154.11.15.111)  28.588 ms  28.599 ms  28.594 ms
 4  ae55.edge6.Seattle1.Level3.net (4.35.244.229)  33.773 ms  33.777 ms  33.779 ms
 5  * * *
 6  ae17.cr4-sea2.ip4.gtt.net (173.205.57.37)  52.343 ms  25.351 ms  25.328 ms
 7  et-3-3-0.cr4-par7.ip4.gtt.net (213.200.119.214)  162.704 ms  170.426 ms  170.416 ms
 8  renater-gw-ix1.gtt.net (77.67.123.206)  186.845 ms  188.382 ms  188.387 ms
 9  te1-1-inria-rtr-021.noc.renater.fr (193.51.177.107)  186.788 ms  186.795 ms  186.792 ms
10  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr (193.51.184.177)  186.799 ms  186.803 ms  186.808 ms
11  unit240-reth1-vfw-ext-dc1.inria.fr (192.93.122.19)  183.137 ms  183.134 ms  172.095 ms
12  inria-cms.inria.fr (128.93.162.63)  173.719 ms  173.718 ms  187.575 ms
```

5) As in Part 1, the IP for my source host remains 192.168.1.71 (hidden behind a NAT. However, the IP 192.168.1.254 is frequently seen, as in hop 1 from traceroute. This is the internal IP address for my router, confirmed in the browser as it navigates to the settings page for my router). The destination host's IP is 128.93.162.63.

6) No, if ICMP sent UDP packets instead, the IP protocol would be 17 since this is the protocol number for UDP (Kurose and Ross 7th Edition, pg. 377. Verified by running traceroute without -I flag)

7)

```
No.     Time           Source                Destination           Protocol Length Info
    479 51.478864598   192.168.1.71          128.93.162.63         ICMP     74     Echo (ping) request  id=0x000c,
seq=48/12288, ttl=16 (reply in 496)
Frame 479: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp4s0, id 0
Ethernet II, Src: ASUSTekC_de:7c:0a (24:4b:fe:de:7c:0a), Dst: Actionte_f6:8c:80 (fc:2b:b2:f6:8c:80)
Internet Protocol Version 4, Src: 192.168.1.71, Dst: 128.93.162.63
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8fcb (36811)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 16
    Protocol: ICMP (1)
    Header Checksum: 0x366a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.71
    Destination Address: 128.93.162.63
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x823e [correct]
    [Checksum Status: Good]
    Identifier (BE): 12 (0x000c)
    Identifier (LE): 3072 (0x0c00)
    Sequence Number (BE): 48 (0x0030)
    Sequence Number (LE): 12288 (0x3000)
    [Response frame: 496]
    Data (32 bytes)
0000  48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57   HIJKLMNOPQRSTUVW
0010  58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67   XYZ[\]^_`abcdefg
```

This packet appears to be the same format as the one from part 1. The packet is a type 8, code 0 packet (echo request) and it has a 2 byte checksum, identifier, and sequence number (albeit the values are different than the packet from part 1). One noticeable difference is that the length of the payload is only 32 bytes, compared to 48 bytes in the ping packet, and rather than being randomized, the payload is part of the alphabet in upper case, which starts again in lower case after what I’m assuming would be a carriage return or maybe line feed character (looking at the hex values, it’s merely increasing by 1 at each character).

8)

```
No.     Time           Source                Destination           Protocol Length Info
     24 0.333249504    10.29.152.1           192.168.1.71          ICMP     102    Time-to-live exceeded (Time to
live exceeded in transit)
Frame 24: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface enp4s0, id 0
Ethernet II, Src: Actionte_f6:8c:80 (fc:2b:b2:f6:8c:80), Dst: ASUSTekC_de:7c:0a (24:4b:fe:de:7c:0a)
Internet Protocol Version 4, Src: 10.29.152.1, Dst: 192.168.1.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 88
    Identification: 0x589e (22686)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0xbef9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.29.152.1
    Destination Address: 192.168.1.71
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
    Internet Protocol Version 4, Src: 192.168.1.71, Dst: 128.93.162.63
        0100 .... = Version: 4
        .... 0101 = Header Length: 20 bytes (5)
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 60
        Identification: 0x7ba3 (31651)
        Flags: 0x00
        Fragment Offset: 0
        Time to Live: 1
        Protocol: ICMP (1)
        Header Checksum: 0x5992 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 192.168.1.71
        Destination Address: 128.93.162.63
    Internet Control Message Protocol
        Type: 8 (Echo (ping) request)
        Code: 0
        Checksum: 0x826a [unverified] [in ICMP error packet]
        [Checksum Status: Unverified]
        Identifier (BE): 12 (0x000c)
        Identifier (LE): 3072 (0x0c00)
        Sequence Number (BE): 4 (0x0004)
        Sequence Number (LE): 1024 (0x0400)
        Data (32 bytes)
0000  48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57   HIJKLMNOPQRSTUVW
0010  58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67   XYZ[\]^_`abcdefg
```

In the ICMP header, we have a type 11 code 0 packet, indicating the TTL was exceeded (exactly the behaviour we're looking for). We also have a checksum (2 bytes), an unused part of the header, then what looks like the header from the packet that was rejected. Distinctly missing here are the identifier and sequence number header fields.

9) (screenshots on following pages, answer to question 9 after)

```
No.     Time           Source                Destination           Protocol Length Info
    494 51.667941041   128.93.162.63         192.168.1.71          ICMP     74     Echo (ping) reply    id=0x000c,
seq=45/11520, ttl=43 (request in 476)
Frame 494: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp4s0, id 0
Ethernet II, Src: Actionte_f6:8c:80 (fc:2b:b2:f6:8c:80), Dst: ASUSTekC_de:7c:0a (24:4b:fe:de:7c:0a)
Internet Protocol Version 4, Src: 128.93.162.63, Dst: 192.168.1.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x659a (26010)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 43
    Protocol: ICMP (1)
    Header Checksum: 0x4573 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.93.162.63
    Destination Address: 192.168.1.71
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8a41 [correct]
    [Checksum Status: Good]
    Identifier (BE): 12 (0x000c)
    Identifier (LE): 3072 (0x0c00)
    Sequence Number (BE): 45 (0x002d)
    Sequence Number (LE): 11520 (0x2d00)
    [Request frame: 476]
    [Response time: 189.095 ms]
    Data (32 bytes)
0000  48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57   HIJKLMNOPQRSTUVW
0010  58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67   XYZ[\]^_`abcdefg
```

```
No.     Time           Source                Destination           Protocol Length Info
    495 51.667948876   128.93.162.63         192.168.1.71          ICMP     74     Echo (ping) reply    id=0x000c,
seq=46/11776, ttl=43 (request in 477)
Frame 495: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp4s0, id 0
Ethernet II, Src: Actionte_f6:8c:80 (fc:2b:b2:f6:8c:80), Dst: ASUSTekC_de:7c:0a (24:4b:fe:de:7c:0a)
Internet Protocol Version 4, Src: 128.93.162.63, Dst: 192.168.1.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x659b (26011)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 43
    Protocol: ICMP (1)
    Header Checksum: 0x4572 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.93.162.63
    Destination Address: 192.168.1.71
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8a40 [correct]
    [Checksum Status: Good]
    Identifier (BE): 12 (0x000c)
    Identifier (LE): 3072 (0x0c00)
    Sequence Number (BE): 46 (0x002e)
    Sequence Number (LE): 11776 (0x2e00)
    [Request frame: 477]
    [Response time: 189.100 ms]
    Data (32 bytes)
0000  48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57   HIJKLMNOPQRSTUVW
0010  58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67   XYZ[\]^_`abcdefg
```

```
No.     Time           Source                Destination           Protocol Length Info
    496 51.667956520   128.93.162.63         192.168.1.71          ICMP     74     Echo (ping) reply    id=0x000c,
seq=48/12288, ttl=43 (request in 479)
Frame 496: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp4s0, id 0
Ethernet II, Src: Actionte_f6:8c:80 (fc:2b:b2:f6:8c:80), Dst: ASUSTekC_de:7c:0a (24:4b:fe:de:7c:0a)
Internet Protocol Version 4, Src: 128.93.162.63, Dst: 192.168.1.71
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x659c (26012)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 43
    Protocol: ICMP (1)
    Header Checksum: 0x4571 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.93.162.63
    Destination Address: 192.168.1.71
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x8a3e [correct]
    [Checksum Status: Good]
    Identifier (BE): 12 (0x000c)
    Identifier (LE): 3072 (0x0c00)
    Sequence Number (BE): 48 (0x0030)
    Sequence Number (LE): 12288 (0x3000)
    [Request frame: 479]
    [Response time: 189.092 ms]
    Data (32 bytes)
0000  48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57   HIJKLMNOPQRSTUVW
0010  58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67   XYZ[\]^_`abcdefg
```

These packets are all type 0 code 0 (echo reply) ICMP packets. They each have a checksum, an identifier, and a sequence number, but are lacking a timestamp like in part 1. They are different than the other ICMP error packets because once the destination has been reached, the source host sends three ICMP echo request packets and waits to receive ICMP echo reply packets in order to obtain an average RTT from the source host to the destination host.

10) On my screenshot, the link between routers 6 and 7 seems to incur the longest delay, and on the screenshot in figure 4 of the assignment, the link between routers 9 and 10 seems to incur the longest delay. My screenshot is a little less obvious on the router names, although looking at router 4 with the name ‘Seattle’ in it and router 6 with sea2, we can guess that the packets depart from Seattle at router 6. The next router isn’t very obvious at all, with cr4-par7.gtt.net at the end. GTT is a multinational ISP, so not a lot to go on there. Router 8 though contains renater which looks like a French name, so we can assume the link between routers 6 and 7 crosses the Atlantic Ocean.
Figure 4 on the assignment is a lot more obvious: router 9 contains ‘nyc’ (New York City), and router 10 contains ‘Pastourelle’, which I would bet $1000 is located in France. So clearly, link 9-10 crosses the Atlantic.

Note: sure enough, using iplocation.net/ip-lookup, router 6 on my example is located in Seattle and router 7 is located in France. How a packet can travel directly from Seattle to France without any intermediate links is beyond me though (some sort of satellite transmission?). By the same method, routers 9 and 10 in the assignment are located in the US (although somehow in California?) and Paris, France respectively.