Part 1:

1.1 Source: 134.190.137.5 destination: 172.217.13.174

1.2 type: 8 code: 0. Type 8 means echo request, 0 means network is unreachable.

1.3 because ICMP is “designed to communicate using network layer information between hosts and routers, not between application layer processes”.
http://www.cs.toronto.edu/~ahchinaei/teaching/2016jan/csc358/Assignment4wSol.pdf

1.4 checksum: 0x4d41, Identifier (BE): 26 , Identifier (LE): 256, Sequence Number (BE): 26, Sequence Number (LE): 6656.

1.5 type 0, code 0

1.6 checksum: 0x5541, Identifier (BE): 1, Identifier (LE): 256 , Sequence Number (BE): 26, Sequence Number (LE): 6656.

```
C:\Users\alkin>ping -n 10 youtube.com

Pinging youtube.com [172.217.13.174] with 32 bytes of data:
Reply from 172.217.13.174: bytes=32 time=107ms TTL=117
Reply from 172.217.13.174: bytes=32 time=111ms TTL=117
Reply from 172.217.13.174: bytes=32 time=127ms TTL=117
Reply from 172.217.13.174: bytes=32 time=135ms TTL=117
Reply from 172.217.13.174: bytes=32 time=42ms TTL=117
Reply from 172.217.13.174: bytes=32 time=43ms TTL=117
Reply from 172.217.13.174: bytes=32 time=53ms TTL=117
Reply from 172.217.13.174: bytes=32 time=56ms TTL=117
Reply from 172.217.13.174: bytes=32 time=53ms TTL=117
Request timed out.

Ping statistics for 172.217.13.174:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 135ms, Average = 80ms
```

4225	259.246280	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 4226)
4226	259.354009	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=117 (request in 4225)
4230	260.265809	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 4231)
4231	260.377559	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=117 (request in 4230)
4232	261.274288	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 4233)
4233	261.401474	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=117 (request in 4232)
4234	262.290203	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 4235)
4235	262.425746	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=117 (request in 4234)
4236	263.304711	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 4237)
4237	263.347518	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=117 (request in 4236)
4238	264.327768	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 4239)
4239	264.371304	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=117 (request in 4238)
4240	265.342595	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 4241)
4241	265.395455	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=117 (request in 4240)
4242	266.362638	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 4243)
4243	266.419383	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=117 (request in 4242)
4244	267.389675	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 4245)
4245	267.443243	172.217.13.174	134.190.137.5	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=117 (request in 4244)
4246	268.405365	134.190.137.5	172.217.13.174	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (no response found!)

Part 2:

2.1: 1472 bytes.

```
C:\Users\alkin>ping -l 1473 youtube.com

Pinging youtube.com [172.217.13.174] with 1473 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.217.13.174:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\alkin>ping -l 1472 youtube.com

Pinging youtube.com [172.217.13.174] with 1472 bytes of data:
Reply from 172.217.13.174: bytes=68 (sent 1472) time=134ms TTL=117
Reply from 172.217.13.174: bytes=68 (sent 1472) time=127ms TTL=117
Reply from 172.217.13.174: bytes=68 (sent 1472) time=131ms TTL=117
Reply from 172.217.13.174: bytes=68 (sent 1472) time=129ms TTL=117

Ping statistics for 172.217.13.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 127ms, Maximum = 134ms, Average = 130ms
```

2.2

```
C:\Users\alkin>ping -l 1472 youtube.com

Pinging youtube.com [172.217.13.174] with 1472 bytes of data:
Reply from 172.217.13.174: bytes=68 (sent 1472) time=171ms TTL=117
Reply from 172.217.13.174: bytes=68 (sent 1472) time=180ms TTL=117
Reply from 172.217.13.174: bytes=68 (sent 1472) time=85ms TTL=117
Reply from 172.217.13.174: bytes=68 (sent 1472) time=86ms TTL=117

Ping statistics for 172.217.13.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 85ms, Maximum = 180ms, Average = 130ms
```

v

```
154 129.330315   172.217.13.174   134.190.137.5    ICMP   110 Echo (ping) reply    id=0x0001, seq=119/30464, ttl=117
155 130.173785   134.190.137.5    172.217.13.174   ICMP  1514 Echo (ping) request  id=0x0001, seq=120/30720, ttl=128 (no response found!)
156 130.354426   172.217.13.174   134.190.137.5    ICMP   110 Echo (ping) reply    id=0x0001, seq=120/30720, ttl=117
157 131.192029   134.190.137.5    172.217.13.174   ICMP  1514 Echo (ping) request  id=0x0001, seq=121/30976, ttl=128 (no response found!)
158 131.277717   172.217.13.174   134.190.137.5    ICMP   110 Echo (ping) reply    id=0x0001, seq=121/30976, ttl=117
159 132.214353   134.190.137.5    172.217.13.174   ICMP  1514 Echo (ping) request  id=0x0001, seq=122/31232, ttl=128 (no response found!)
160 132.300358   172.217.13.174   134.190.137.5    ICMP   110 Echo (ping) reply    id=0x0001, seq=122/31232, ttl=117
```

No response found:

```
C:\Users\alkin>ping -l 1474 youtube.com

Pinging youtube.com [172.217.13.174] with 1474 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.217.13.174:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

icmp

No.	Time	Source	Destination	Protocol	Length	Info
9	7.397709	134.190.137.5	172.217.13.174	ICMP	36	Echo (ping) request id=0x0001, seq=115/29440, ttl=128 (no response found!)
16	12.255745	134.190.137.5	172.217.13.174	ICMP	36	Echo (ping) request id=0x0001, seq=116/29696, ttl=128 (no response found!)
18	17.276002	134.190.137.5	172.217.13.174	ICMP	36	Echo (ping) request id=0x0001, seq=117/29952, ttl=128 (no response found!)
45	22.261613	134.190.137.5	172.217.13.174	ICMP	36	Echo (ping) request id=0x0001, seq=118/30208, ttl=128 (no response found!)

```
C:\Users\alkin>ping -l 65000 youtube.com

Pinging youtube.com [142.251.40.110] with 65000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 142.251.40.110:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

icmp

No.	Time	Source	Destination	Protocol	Length	Info
126	12.856474	192.168.2.13	142.251.40.110	ICMP	1402	Echo (ping) request id=0x0001, seq=227/5811
188	17.609331	192.168.2.13	142.251.40.110	ICMP	1402	Echo (ping) request id=0x0001, seq=228/5836
282	22.612707	192.168.2.13	142.251.40.110	ICMP	1402	Echo (ping) request id=0x0001, seq=229/5862
366	27.612725	192.168.2.13	142.251.40.110	ICMP	1402	Echo (ping) request id=0x0001, seq=230/5888

Because I'm using windows, it won't show the message is too big error.

3. to prevent attackers from abusing ping requests by overflowing servers with large sized requests.

Part 3:

1. First, the total length of the traceroute packet is bigger than the ping packet . Second, each ping packet ICMP request had the same time to live value, which is 8 (no of hops to the final network). Whereas the traceroute packet requests had increasing values starting from 1 to 8 capture the time to get to each node in the route to the final network. The checksum, Sequence Number (BE) and (LE), Identifier (BE) and (LE) were different.

2.

```
C:\Users\alkin>tracert omantel.om

Tracing route to omantel.om [212.72.10.211]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  mynetwork.home [192.168.2.1]
  2     9 ms     1 ms     2 ms  loop0.6cw.ba17.hlfx.ns.aliant.net [142.176.50.10]
  3     2 ms     3 ms     1 ms  be14-181.cr01.hlfx.ns.aliant.net [142.166.181.125]
  4     5 ms     4 ms     4 ms  be16.cr01.stjh.nb.aliant.net [142.166.185.65]
  5     5 ms     5 ms     6 ms  ae3-50.cr02.stjh.nb.aliant.net [142.166.181.110]
  6    23 ms    22 ms    22 ms  ae0.bx01.toro.on.aliant.net [207.231.227.53]
  7    25 ms    22 ms    22 ms  bx3-torontoxn_be8.net.bell.ca [184.150.187.56]
  8    26 ms    28 ms    37 ms  100ge0-78.core2.tor1.he.net [184.104.196.178]
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12   107 ms   106 ms   106 ms  omantel.10gigabitethernet3-1.core1.mrs1.he.net [216.66.85.170]
 13     *        *        *     Request timed out.
 14   200 ms   200 ms   200 ms  134.0.217.238
 15   200 ms   199 ms   200 ms  82.178.159.2
 16   204 ms   203 ms   203 ms  as22-6.omantel.net.om [212.72.10.133]
 17   202 ms   201 ms   201 ms  as22-7.omantel.net.om [212.72.10.134]
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
```

In the error packets, there is no response seen and It is written that security level is high.

```
    Destination Address: 129.173.31.187
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf681 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 381 (0x017d)
    Sequence Number (LE): 32001 (0x7d01)
  ▾ [No response seen]
    › [Expert Info (Warning/Sequence): No response seen to ICMP request]
  › Data (64 bytes)
```

3.

```
kindi@timberlea:~$ traceroute -T youtube.com
You do not have enough privileges to use this traceroute method.
socket: Operation not permitted
```

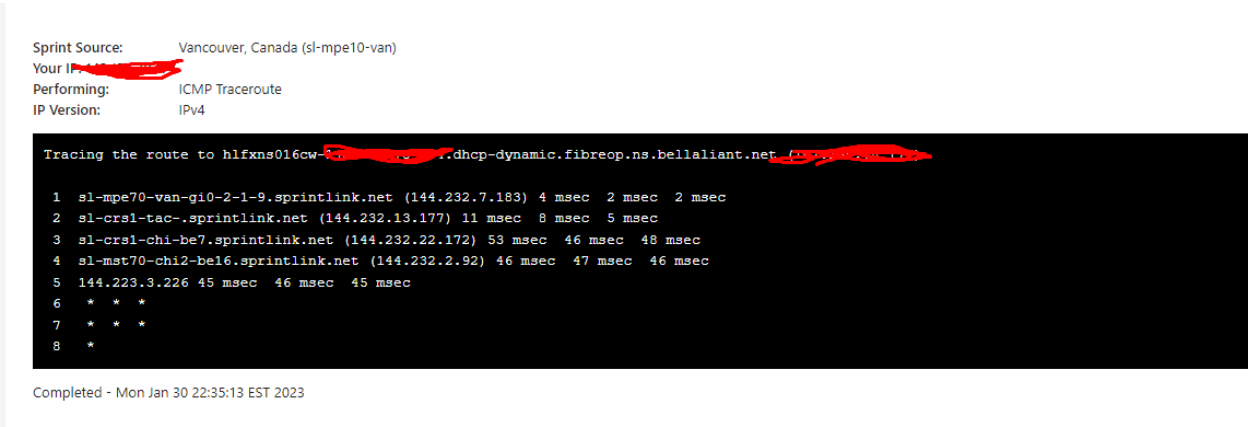
```
kindi@timberlea:~$ traceroute -d youtube.com
traceroute to youtube.com (172.217.13.110), 30 hops max, 60 byte packets
setsockopt SO_DEBUG: Permission denied
```

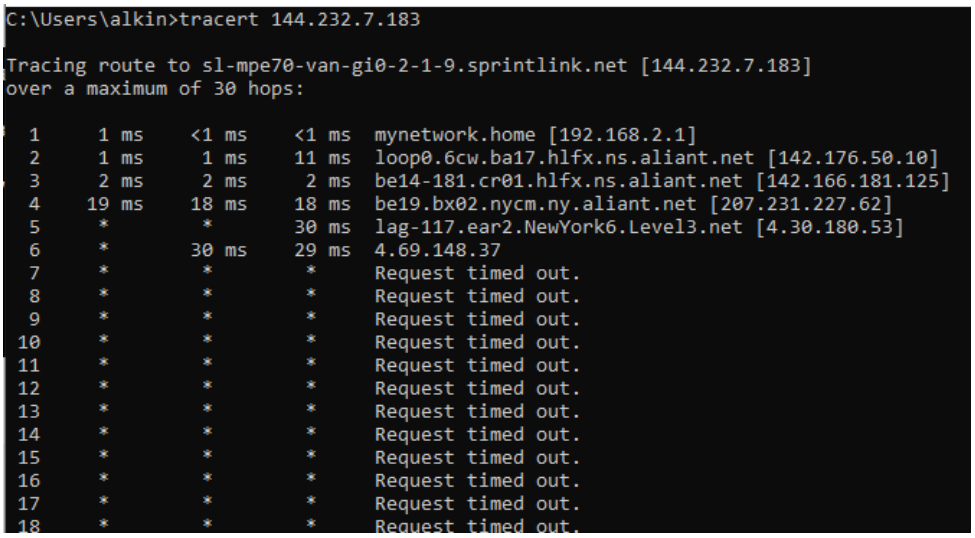
Using -T, which is to use port 80 to establish connections to the server was not permitted because I don't have the privileges to do so. Also, -d, which is used to allow for have more access to the packets sent is not permitted.

4. -s allows editing the ip address that sends the request. This can be a huge security issue because allowing people to edit the ip gives attackers the opportunity to hide behind other ips and create attacks from different IP addresses.

Part 4:

Experiment 1:





Experiment 2:

Sprint Source: Sao Paulo, Brazil (sl-mpe02-spb)
Your IP: [redacted]
Performing: ICMP Traceroute
IP Version: IPv4

```
Tracing the route to hlfxns016cw-[redacted].dhcp-dynamic.fibreop.ns.bellaliant.net [redacted]

 1  sl-mpe01-spb-te0-0-2-0.sprintlink.net (144.223.192.98) 6 msec  4 msec  1 msec
 2  sl-mpe01-nyc-gi0-0-0-6.sprintlink.net (144.232.4.32) 110 msec  110 msec  110 msec
 3  sl-crs1-nyc-lc2-.sprintlink.net (144.232.21.141) 110 msec  112 msec
    sl-crs2-nyc-lc2-.sprintlink.net (144.232.21.143) 113 msec
 4  sl-crs1-akr-be21.sprintlink.net (144.232.22.64) 126 msec
    sl-crs2-akr-be21.sprintlink.net (144.232.22.66) 127 msec  128 msec
 5  sl-crs2-chi-be2.sprintlink.net (144.232.18.7) 128 msec
    sl-crs1-chi-be2.sprintlink.net (144.232.18.5) 128 msec
    sl-crs2-chi-be2.sprintlink.net (144.232.18.7) 128 msec
 6  sl-mst70-chi2-be17.sprintlink.net (144.232.2.94) 130 msec
    sl-mst70-chi2-be16.sprintlink.net (144.232.2.92) 130 msec
    sl-mst70-chi2-be17.sprintlink.net (144.232.2.94) 130 msec
 7  144.223.3.226 128 msec  128 msec  128 msec
 8   *  *  *
 9   *  *  *
10  *
```

```
C:\Users\alkin>tracert 144.223.192.98

Tracing route to sl-mpe01-spb-te0-0-2-0.sprintlink.net [144.223.192.98]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  mynetwork.home [192.168.2.1]
  2     2 ms     2 ms     2 ms  loop0.6cw.ba17.hlfx.ns.aliant.net [142.176.50.10]
  3     1 ms     1 ms     2 ms  be14-181.cr01.hlfx.ns.aliant.net [142.166.181.125]
  4    20 ms    20 ms    20 ms  be19.bx02.nycm.ny.aliant.net [207.231.227.62]
  5     *        *       31 ms  lag-117.ear2.NewYork6.Level3.net [4.30.180.53]
  6     *       30 ms    30 ms  4.69.148.33
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *
```

Experiment 3:

Sprint Source: Frankfurt, Germany (sl-mpe71-fra)
Your IP: [redacted]
Performing: ICMP Traceroute
IP Version: IPv4

```
Tracing the route to hlfxns016cw-[redacted].dhcp-dynamic.fibreop.ns.bellaliant.net [redacted]

 1  sl-mpe71-ams-hu0-0-0-1.sprintlink.net (213.206.129.27) 8 msec  7 msec  7 msec
 2  sl-mpe70-ams-be10.sprintlink.net (217.149.32.42) 6 msec  7 msec  6 msec
 3  sl-mpe70-lon-be3.sprintlink.net (213.206.129.15) 11 msec  12 msec  12 msec
 4  sl-mpe75-lon2-be5.sprintlink.net (213.206.129.1) 12 msec  12 msec  12 msec
 5  sl-crs1-spr-be10.sprintlink.net (144.232.9.109) 74 msec  79 msec  79 msec
 6  sl-crs1-akr-be7.sprintlink.net (144.232.10.240) 85 msec  89 msec  85 msec
 7  sl-crs1-chi-be2.sprintlink.net (144.232.18.5) 93 msec  96 msec  92 msec
 8  sl-mst70-chi2-be16.sprintlink.net (144.232.2.92) 90 msec  90 msec  89 msec
 9  144.223.3.226 90 msec  89 msec  90 msec
10  *  *  *
11  *  *  *
12  *
```

```
C:\Users\alkin>tracert 213.206.129.27

Tracing route to sl-mpe71-ams-hu0-0-0-1.sprintlink.net [213.206.129.27]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  mynetwork.home [192.168.2.1]
  2     1 ms    <1 ms     1 ms  loop0.6cw.ba17.hlfx.ns.aliant.net [142.176.50.10]
  3     1 ms    <1 ms     1 ms  ae15-182.cr02.hlfx.ns.aliant.net [142.166.181.141]
  4     2 ms     1 ms     2 ms  hg-0-2-0-0-50.cr01.hlfx.ns.aliant.net [142.166.149.93]
  5    20 ms    19 ms    19 ms  be19.bx02.nycm.ny.aliant.net [207.231.227.62]
  6     *        *        *     Request timed out.
  7     *        *       30 ms  4.69.148.33
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *
```

Experiment 4:

Sprint Source: Dubai, UAE (sl-mpe02-dbi)
[redacted]
Performing: ICMP Ping
IP Version: IPv4

```
Sending 5, 100-byte ICMP Echos to [redacted], timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

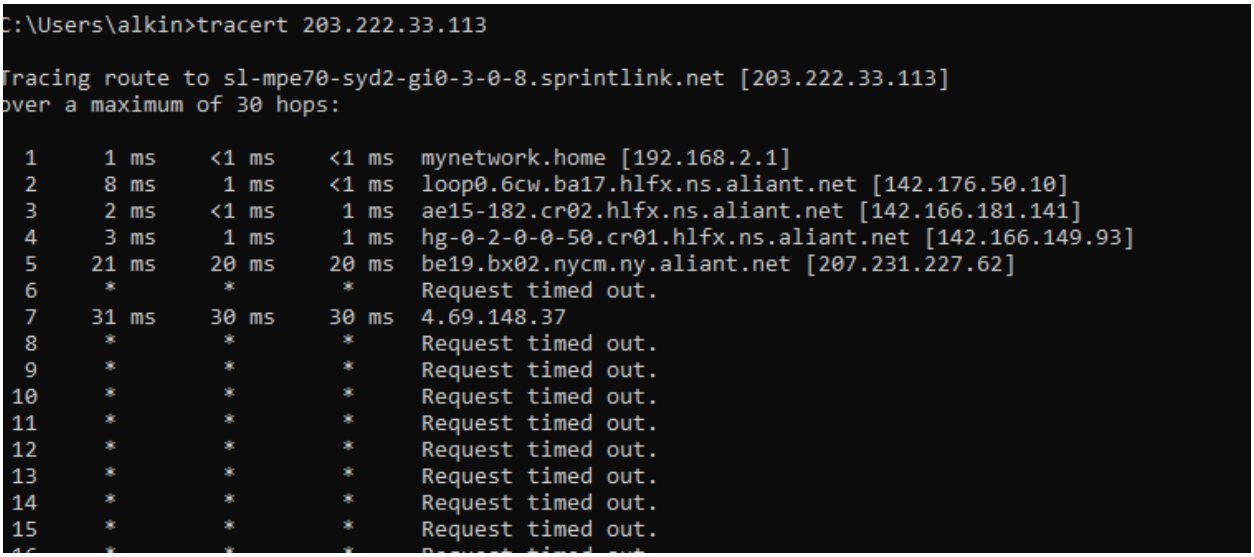
Completed - Mon Jan 30 22:52:22 EST 2023

Experiment 5:

Sprint Source: Perth, Australia (sl-mpe01-per)
[redacted]
Performing: ICMP Traceroute
IP Version: IPv4

```
Tracing the route to hlfxns016cw-[redacted].dhcp-dynamic.fibreop.ns.bellaliant.net ([redacted])

 1  sl-mpe70-syd2-gi0-3-0-8.sprintlink.net (203.222.33.113) 53 msec  52 msec  51 msec
 2  sl-mpe02-ana-gi0-0-0-0.sprintlink.net (203.222.33.20) 189 msec  189 msec  189 msec
 3  sl-crs1-ana-te1-2-0-29.sprintlink.net (144.232.16.157) 196 msec
    sl-crs2-ana-te1-2-0-29.sprintlink.net (144.232.16.159) 192 msec  191 msec
 4  sl-crs1-sj-be7.sprintlink.net (144.232.17.27) 200 msec
    sl-crs2-sj-be7.sprintlink.net (144.232.17.29) 201 msec
    sl-crs1-sj-be7.sprintlink.net (144.232.17.27) 200 msec
 5  sl-crs2-stk-be3.sprintlink.net (144.232.22.179) 199 msec
    sl-crs1-stk-be3.sprintlink.net (144.232.22.177) 200 msec
    sl-crs2-stk-be11.sprintlink.net (144.232.22.95) 198 msec
 6  sl-crs1-oro-be2.sprintlink.net (144.232.15.236) 208 msec
    sl-crs2-oro-be2.sprintlink.net (144.232.15.238) 205 msec  200 msec
 7  sl-crs1-oma-be7.sprintlink.net (144.232.15.164) 236 msec
    sl-crs2-oma-be7.sprintlink.net (144.232.15.166) 236 msec
    sl-crs1-oma-be7.sprintlink.net (144.232.15.164) 232 msec
 8  sl-crs1-chi-be4.sprintlink.net (144.232.22.72) 245 msec
    sl-crs2-chi-be4.sprintlink.net (144.232.22.74) 241 msec
    sl-crs1-chi-be4.sprintlink.net (144.232.22.72) 239 msec
 9  sl-mst70-chi2-be17.sprintlink.net (144.232.2.94) 238 msec  238 msec
    sl-mst70-chi2-be16.sprintlink.net (144.232.2.92) 238 msec
10 144.223.3.226 238 msec  257 msec  238 msec
11  *  *  *
12  *  *  *
```



Conclusion: For my host to the server's closest link, it seems like once the packet gets the server in New York, the packet returns ** errors. So, it was hard to determine whether the packets followed the same path or not. However, I think that even if the packets were shown, generally, each network provider has its own best cost route. For example, Eastlink might have direct connection to London, so when connecting to a server in Frankfurt, it would use that link. Whereas when the Frankfurt server connects to Eastlink server, it might use its own best connection that might go through New York or Toronto. So, this means that each server when connected might use different routes to get packets to each other. It was hard to determine because my packets gave an error when reaching New York.