CSE Network Security Lab 1

Isaac Ashwin Ravindran

1002151

1 Measurement of Round Trip Times using Ping

1.1 Question 1

For each host, record the percentage of packets sent that resulted in a successful response. Record also the minimum, average, and maximum round trip times for the packets that resulted in a response.

Location	Successful Percentage	Min RTT (ms)	Average RTT (ms)	Max RTT (ms)
www.csail.mit.edu	100%	4.039	5.888	10.466
www.berkeley.edu	100%	202.702	294.037	398.142
www.usyd.edu.au	100%	143.507	200.593	305.575
www.kyoto-u.ac.jp	100%	78.128	102.966	201.455

1.2 Question 2

Describe and explain the differences in the minimum round trip time to each of these hosts.

- `www.csail.mit.edu` - MIT makes use of Pantheon to host their website. It provides distributed hosting across the world, therefore giving very low pings from anywhere. Hence, it has the lowest ping of the lot.

- `www.berkeley.edu` - As this university's website is located in the US, the data needs to travel a very long geographical distance to reach Singapore, therefore resulting in very high ping times.

- `www.usyd.edu.au` - This university, being located in Australia, is closer than Berkeley. Therefore, while high, it's ping times are still lower than Berkeley.

- `www.kyoto-u.ac.jp` - Kyoto University is in Japan, which is still in the same continent and therefore is much closer than the previous 2 universities. Therefore it has the shortest time out of the last 3.

1.3 Question 3

Repeat the exercise using packet sizes of 56, 512 and 1024 bytes. Record the minimum, average, and maximum round trip times for each of the packet sizes.

Location	Packet Size (B)	Successful Percentage	Min RTT (ms)	Average RTT (ms)	Max RTT (ms)
www.csail.mit.edu	56	100%	4.039	5.888	10.466
www.csail.mit.edu	512	100%	4.835	12.877	32.240
www.csail.mit.edu	1024	0%	-	-	-
www.berkeley.edu	56	100%	202.702	294.037	398.142
www.berkeley.edu	512	100%	202.565	262.395	327.723
www.berkeley.edu	1024	0%	-	-	-
www.usyd.edu.au	56	100%	143.507	200.593	305.575
www.usyd.edu.au	512	100%	198.095	271.715	362.179
www.usyd.edu.au	1024	0%	-	-	-
www.kyoto-u.ac.jp	56	100%	78.128	102.966	201.455
www.kyoto-u.ac.jp	512	100%	93.773	138.465	220.646
www.kyoto-u.ac.jp	1024	0%	-	-	-

Why are the minimum round-trip times to the same hosts different when using 56, 512, and 1024–byte packets?

The packets take longer to transmit due to the larger size. Therefore the larger the packet, the longer the minimum RTT.

1.4 Question 4

Use ping to send 100 packets to the following host. Each packet should have a size of 56 bytes, and there should be an interval of 5 seconds between each packet sent.

`www.wits.ac.za`

Record the percentage of the packets sent that resulted in a successful response.

0%

What are some possible reasons why you may not have received a response?

It is possible that the sysadmin of the University of Witwatersand blocked ICMP on their routers. Therefore ICMP messages do not get sent out, resulting in no response when performing a `ping`.

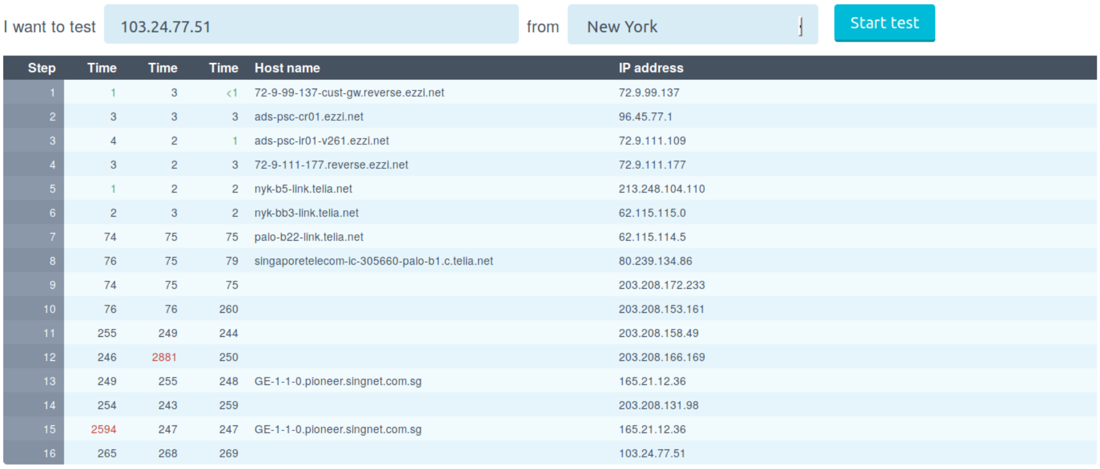
2 Understanding Internet Routes Using Traceroute

2.1 Question 5

Explain how traceroute discovers a path to a remote host.

`traceroute` progressively sends packets with increasing TTLs (starting from 1) until it sends a packet that has a TTL that reaches the intended destination. This way, all intermediate routers/servers/computers will notify the original sender (`traceroute` program) that the TTL has expired, allowing `traceroute` to know all the hops along the way.

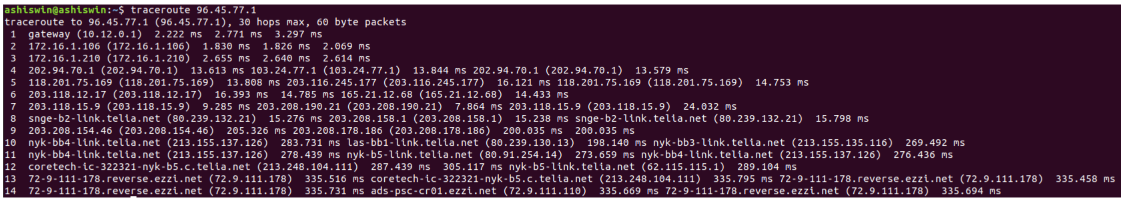
2.2 Question 6



I want to test 103.24.77.51 from New York Start test

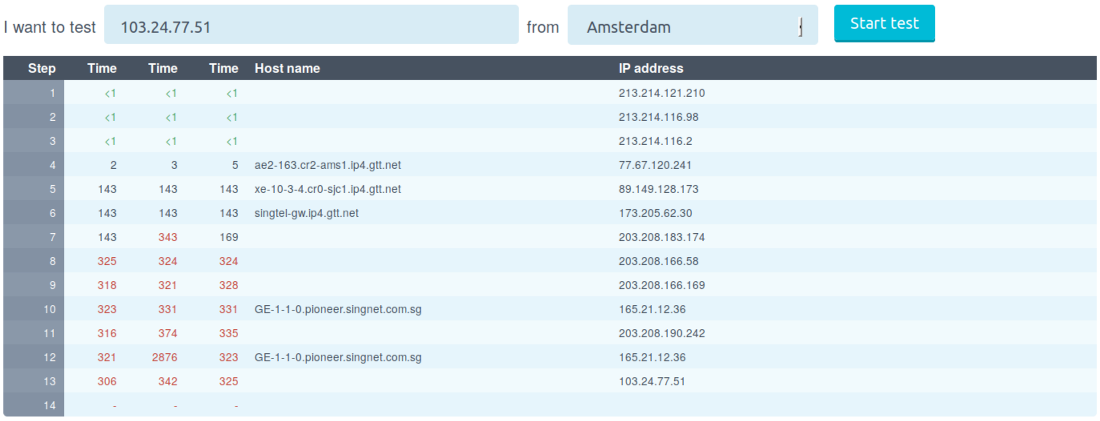
Step	Time	Time	Time	Host name	IP address
1	1	3	<1	72-9-99-137-cust-gw.reverse.ezzi.net	72.9.99.137
2	3	3	3	ads-psc-cr01.ezzi.net	96.45.77.1
3	4	2	1	ads-psc-ir01-v261.ezzi.net	72.9.111.109
4	3	2	3	72-9-111-177.reverse.ezzi.net	72.9.111.177
5	1	2	2	nyk-b5-link.telia.net	213.248.104.110
6	2	3	2	nyk-bb3-link.telia.net	62.115.115.0
7	74	75	75	palo-b22-link.telia.net	62.115.114.5
8	76	75	79	singaporetelecom-ic-305660-palo-b1.c.telia.net	80.239.134.86
9	74	75	75		203.208.172.233
10	76	76	260		203.208.153.161
11	255	249	244		203.208.158.49
12	246	2881	250		203.208.166.169
13	249	255	248	GE-1-1-0.pioneer.singnet.com.sg	165.21.12.36
14	254	243	259		203.208.131.98
15	2594	247	247	GE-1-1-0.pioneer.singnet.com.sg	165.21.12.36
16	265	268	269		103.24.77.51

Figure 1: Traceroute from New York



```
ashiswin@ashiswin:~$ traceroute 96.45.77.1
traceroute to 96.45.77.1 (96.45.77.1), 30 hops max, 60 byte packets
 1  gateway (10.12.0.1)  2.222 ms  2.771 ms  3.297 ms
 2  172.16.1.106 (172.16.1.106)  1.830 ms  1.826 ms  2.069 ms
 3  172.16.1.210 (172.16.1.210)  2.655 ms  2.640 ms  2.614 ms
 4  202.94.70.1 (202.94.70.1)  13.613 ms 103.24.77.1 (103.24.77.1)  13.844 ms 202.94.70.1 (202.94.70.1)  13.579 ms
 5  118.201.75.169 (118.201.75.169)  13.808 ms 203.116.245.177 (203.116.245.177)  16.121 ms 118.201.75.169 (118.201.75.169)  14.753 ms
 6  203.118.12.17 (203.118.12.17)  16.393 ms  14.785 ms 165.21.12.68 (165.21.12.68)  14.433 ms
 7  203.118.15.9 (203.118.15.9)  9.285 ms 203.208.190.21 (203.208.190.21)  7.864 ms 203.118.15.9 (203.118.15.9)  24.032 ms
 8  snge-b2-link.telia.net (80.239.132.21)  15.276 ms 203.208.158.1 (203.208.158.1)  15.238 ms snge-b2-link.telia.net (80.239.132.21)  15.798 ms
 9  203.208.154.46 (203.208.154.46)  205.326 ms 203.208.178.186 (203.208.178.186)  200.035 ms  200.035 ms
10  nyk-bb4-link.telia.net (213.155.137.126)  283.731 ms las-bb1-link.telia.net (80.239.130.13)  198.140 ms nyk-bb3-link.telia.net (213.155.135.116)  269.492 ms
11  nyk-bb4-link.telia.net (213.155.137.126)  278.439 ms nyk-b5-link.telia.net (80.91.254.14)  273.659 ms nyk-bb4-link.telia.net (213.155.137.126)  276.436 ms
12  coretech-ic-322321-nyk-b5.c.telia.net (213.248.104.111)  287.439 ms  305.117 ms nyk-b5-link.telia.net (62.115.115.1)  289.104 ms
13  72-9-111-178.reverse.ezzi.net (72.9.111.178)  335.516 ms coretech-ic-322321-nyk-b5.c.telia.net (213.248.104.111)  335.795 ms 72-9-111-178.reverse.ezzi.net (72.9.111.178)  335.458 ms
14  72-9-111-178.reverse.ezzi.net (72.9.111.178)  335.731 ms ads-psc-cr01.ezzi.net (72.9.111.110)  335.669 ms 72-9-111-178.reverse.ezzi.net (72.9.111.178)  335.694 ms
```

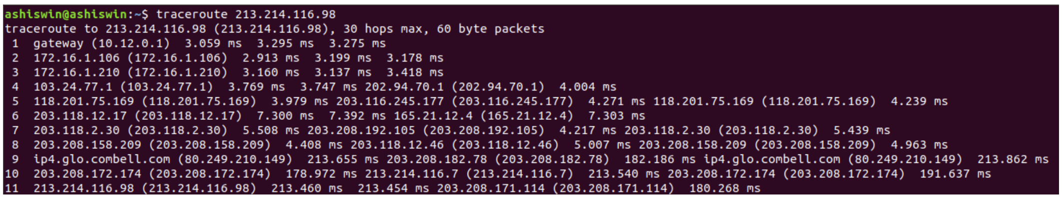
Figure 2: Traceroute to New York



I want to test 103.24.77.51 from Amsterdam

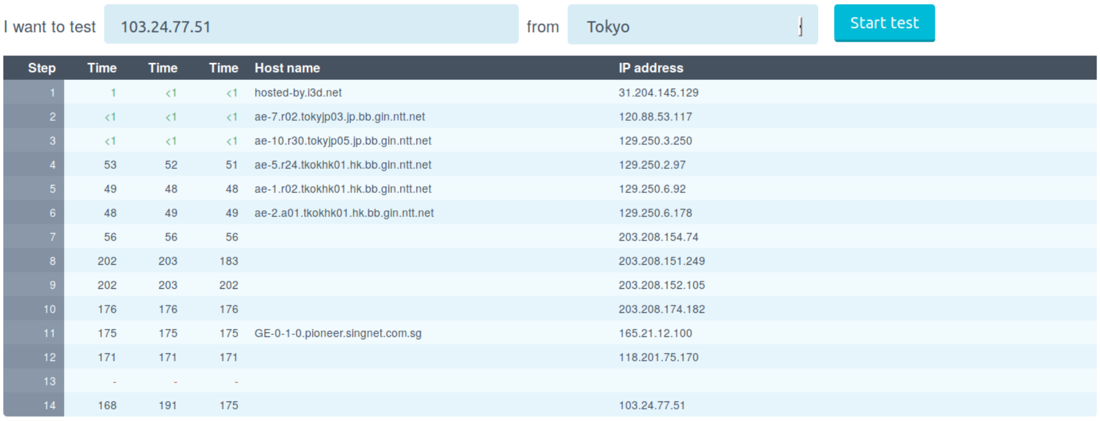
Step	Time	Time	Time	Host name	IP address
1	<1	<1	<1		213.214.121.210
2	<1	<1	<1		213.214.116.98
3	<1	<1	<1		213.214.116.2
4	2	3	5	ae2-163.cr2-ams1.ip4.gtt.net	77.67.120.241
5	143	143	143	xe-10-3-4.cr0-sjc1.ip4.gtt.net	89.149.128.173
6	143	143	143	singtel-gw.ip4.gtt.net	173.205.62.30
7	143	343	169		203.208.183.174
8	325	324	324		203.208.166.58
9	318	321	328		203.208.166.169
10	323	331	331	GE-1-1-0.pioneer.singnet.com.sg	165.21.12.36
11	316	374	335		203.208.190.242
12	321	2876	323	GE-1-1-0.pioneer.singnet.com.sg	165.21.12.36
13	306	342	325		103.24.77.51
14	-	-	-		

Figure 3: Traceroute from Amsterdam



```
ashiswin@ashiswin:~$ traceroute 213.214.116.98
traceroute to 213.214.116.98 (213.214.116.98), 30 hops max, 60 byte packets
 1  gateway (10.12.0.1)  3.059 ms  3.295 ms  3.275 ms
 2  172.16.1.106 (172.16.1.106)  2.913 ms  3.199 ms  3.178 ms
 3  172.16.1.210 (172.16.1.210)  3.160 ms  3.137 ms  3.418 ms
 4  103.24.77.1 (103.24.77.1)  3.769 ms  3.747 ms 202.94.70.1 (202.94.70.1)  4.004 ms
 5  118.201.75.169 (118.201.75.169)  3.979 ms 203.116.245.177 (203.116.245.177)  4.271 ms 118.201.75.169 (118.201.75.169)  4.239 ms
 6  203.118.12.17 (203.118.12.17)  7.300 ms  7.392 ms 165.21.12.4 (165.21.12.4)  7.303 ms
 7  203.118.2.30 (203.118.2.30)  5.508 ms 203.208.192.105 (203.208.192.105)  4.217 ms 203.118.2.30 (203.118.2.30)  5.439 ms
 8  203.208.158.209 (203.208.158.209)  4.408 ms 203.118.12.46 (203.118.12.46)  5.007 ms 203.208.158.209 (203.208.158.209)  4.963 ms
 9  ip4.glo.combell.com (80.249.210.149)  213.655 ms 203.208.182.78 (203.208.182.78)  182.186 ms ip4.glo.combell.com (80.249.210.149)  213.862 ms
10  203.208.172.174 (203.208.172.174)  178.972 ms 213.214.116.7 (213.214.116.7)  213.540 ms 203.208.172.174 (203.208.172.174)  191.637 ms
11  213.214.116.98 (213.214.116.98)  213.460 ms  213.454 ms 203.208.171.114 (203.208.171.114)  180.268 ms
```

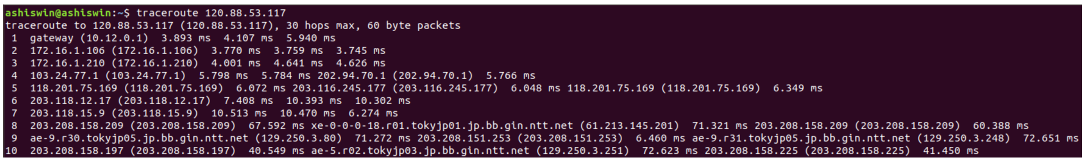
Figure 4: Traceroute to Amsterdam



I want to test 103.24.77.51 from Tokyo

Step	Time	Time	Time	Host name	IP address
1	1	<1	<1	hosted-by.i3d.net	31.204.145.129
2	<1	<1	<1	ae-7.r02.tokyjp03.jp.bb.gin.ntt.net	120.88.53.117
3	<1	<1	<1	ae-10.r30.tokyjp05.jp.bb.gin.ntt.net	129.250.3.250
4	53	52	51	ae-5.r24.tkokhk01.hk.bb.gin.ntt.net	129.250.2.97
5	49	48	48	ae-1.r02.tkokhk01.hk.bb.gin.ntt.net	129.250.6.92
6	48	49	49	ae-2.a01.tkokhk01.hk.bb.gin.ntt.net	129.250.6.178
7	56	56	56		203.208.154.74
8	202	203	183		203.208.151.249
9	202	203	202		203.208.152.105
10	176	176	176		203.208.174.182
11	175	175	175	GE-0-1-0.pioneer.singnet.com.sg	165.21.12.100
12	171	171	171		118.201.75.170
13	-	-	-		
14	168	191	175		103.24.77.51

Figure 5: Traceroute from Tokyo



```
ashiswin@ashiswin:~$ traceroute 120.88.53.117
traceroute to 120.88.53.117 (120.88.53.117), 30 hops max, 60 byte packets
 1  gateway (10.12.0.1)  3.893 ms  4.107 ms  5.940 ms
 2  172.16.1.106 (172.16.1.106)  3.770 ms  3.759 ms  3.745 ms
 3  172.16.1.210 (172.16.1.210)  4.001 ms  4.641 ms  4.626 ms
 4  103.24.77.1 (103.24.77.1)  5.798 ms  5.784 ms 202.94.70.1 (202.94.70.1)  5.766 ms
 5  118.201.75.169 (118.201.75.169)  6.072 ms 203.116.245.177 (203.116.245.177)  6.048 ms 118.201.75.169 (118.201.75.169)  6.349 ms
 6  203.118.12.17 (203.118.12.17)  7.408 ms  10.393 ms  10.302 ms
 7  203.118.15.9 (203.118.15.9)  10.513 ms  10.470 ms  6.274 ms
 8  203.208.158.209 (203.208.158.209)  67.592 ms xe-0-0-0-18.r01.tokyjp01.jp.bb.gin.ntt.net (61.213.145.201)  71.321 ms 203.208.158.209 (203.208.158.209)  60.388 ms
 9  ae-9.r30.tokyjp05.jp.bb.gin.ntt.net (129.250.3.80)  71.272 ms 203.208.151.253 (203.208.151.253)  6.460 ms ae-9.r31.tokyjp05.jp.bb.gin.ntt.net (129.250.3.248)  72.651 ms
10  203.208.158.197 (203.208.158.197)  40.549 ms ae-5.r02.tokyjp03.jp.bb.gin.ntt.net (129.250.3.251)  72.623 ms 203.208.158.225 (203.208.158.225)  41.450 ms
```

Figure 6: Traceroute to Tokyo

2.3 Question 7

Describe anything unusual you might observe about the output. Are the same routers traversed in both directions? If no, why might this be the case?

No, the same routers are not traversed in both directions. Usually, the incoming interface IP address is used in the ICMP error messages, so you see a different IP address while running `traceroute` in different directions.