Exercises for Hands-on 5: Traceroute

Make sure to fill in questions in the space provided underneath the question text.

Round Trip Times

In the following questions, you are asked to use the `ping` utility to measure the round trip times to several hosts on the Internet.

For the following hosts, send 10 packets, each with a length of 56 data bytes. *Note*: You may find that the packet responses are 64 bytes instead of 56 bytes. Look at RFC 792 to find out the reason. (Hint: read what the `-c` flag does on `ping` man page)

```
lids.mit.edu
stanford.edu
www.sydney.edu.au
www.aoyama.ac.jp
```

Question 1: Indicate what percentage of packets sent resulted in a successful response. For the packets from which you received a response, write down the minimum, average, and maximum round trip times in milliseconds. Note that ping reports these times to you if you tell it how many packets to send on the command line.

Question 2: Explain the differences in minimum round trip time to each of these hosts.

---

1) (done from ssh to athena)

URL	**response%**	**min/avg/max/mdev**
`lids.mit.edu`	100%	8.046/9.020/14.452/1.845 ms
`stanford.edu`	100%	95.500/95.862/96.082/0.419 ms
`www.sydney.edu.au`	100%	222.045/222.388/222.735/0.472 ms
`www.aoyama.ac.jp`	100%	210.150/210.401/211.489/0.627 ms

2) Intuitively, it makes sense that sending pings to australia and japan would take longer than to somewhere on campus. More in depth, the packets to lids.mit.edu were routed inside of our own AS (AS3). Packet sent to stanford have to be routed from our AS to theirs, most likely through a lower tier ISP or peering. The packets sent to australia/japan have to be sent through huge cables that go across the pacific ocean floor, traveling over 10,000 miles and probably through a peered tier 1 ISP.

Question 3: Now send pings with 56, 512, 1024 and 2056 byte packets to `lids.mit.edu`. (Hint: read about the `-s` flag on the ping man page.) Write down the average round trip times in milliseconds for each of the four groups. Do the same for `www.aoyama.ac.jp`. Explain the changes in round-trip times that you observed (or didn't observe) in both cases.

---

3) (done from ssh to athena machine)

size	avg(lids.mit.edu)	avg(www.aoyama.ac.jp)	www.aoyama.ac.jp from local machine (just curious)
56	8.228	210.372	262.462
512	8.413	210.423	247.505
1024	8.432	210.479	277.558
2056	8.878	211.473	276.789

As we can see, the there is a slight general trend of increasing time with size, but not much. Most of the overhead for transmitting a packet is just for sending the packet. The extra time for an extra kilobyte of data is marginally small compared to the overhead.

Unanswered Pings

For the following hosts, send 50 packets that have a length of 128 data bytes. Indicate what percentage of the packets resulted in a successful response.

`www.wits.ac.za` (University of the Witwatersrand, Johannesburg)
www.apple.com

Question 4: For some of the hosts, you may not have received any responses for the packets you sent. What are some reasons as to why you might have not gotten a response? (Be sure to check the hosts in a web browser.)

---

4)
www.wits.ac.za ⇒ 50 packets transmitted, 0 received, 100% packet loss
www.apple.com ⇒ 50 packets transmitted, 49 received, 2% packet loss,

- For the server in Africa, packets were not replied to at all. This could be because they have their firewall configured to not accept pings for security reasons, or that their server may be mis-configured. Since the server didn't time out, and the host is accessible from the web browser, we can rule out that the host has completely failed.
- As for Apple, we just lost one packet. Somewhere, in routing from MIT to Apple a buffer was full, and the packet was dropped. As the majority of packets get through, it most likely is not a hardware or configuration issue.

Understanding Internet routes using traceroute

As the name implies, `traceroute` essentially allows you to trace the entire route from your machine to a remote machine. The remote machine can be specified either as a name or as an IP address.

We include a sample output of an execution of traceroute and explain the salient features. The command:

```
> traceroute www.google.com
```

tries to determine the path from the source machine to `www.google.com`. The machine encountered on the path after the first hop is `NW12-RTR-2-SIPB.MIT.EDU` , the next is `EXTERNAL-RTR-1-BACKBONE-2.MIT.EDU` , and so on. In all, it takes 13 hops to reach `py-in-f99.google.com` . The man page for traceroute contains explanations for the remaining fields on each line.

```
> traceroute www.google.com
traceroute: Warning: www.google.com has multiple addresses; using 64.233.167.99
traceroute to www.l.google.com (64.233.167.99), 30 hops max, 40 byte packets
 1  NW12-RTR-2-SIPB.MIT.EDU (18.181.0.1)  0.476 ms  0.318 ms  0.237 ms
 2  EXTERNAL-RTR-1-BACKBONE-2.MIT.EDU (18.168.1.18)  0.827 ms  0.624 ms  0.753 ms
 3  EXTERNAL-RTR-2-BACKBONE.MIT.EDU (18.168.0.27)  1.097 ms  0.772 ms  0.887 ms
 4  207.210.142.233 (207.210.142.233)  0.578 ms  0.549 ms  0.713 ms
 5  207.210.142.1 (207.210.142.1)  0.750 ms  2.530 ms  1.178 ms
 6  207.210.142.2 (207.210.142.2)  5.886 ms  15.387 ms  5.762 ms
 7  64.57.29.21 (64.57.29.21)  24.732 ms  24.693 ms  24.695 ms
 8  72.14.236.215 (72.14.236.215)  31.733 ms  27.588 ms 216.239.49.34 (216.239.49.34)  27.810
ms
 9  66.249.94.235 (66.249.94.235)  12.495 ms 209.85.252.166 (209.85.252.166)  36.961 ms
26.459 ms
10  216.239.46.224 (216.239.46.224)  33.736 ms  33.396 ms 209.85.248.221 (209.85.248.221)
26.130 ms
11  66.249.94.133 (66.249.94.133)  26.126 ms 72.14.232.53 (72.14.232.53)  25.744 ms  25.611 ms
12  66.249.94.133 (66.249.94.133)  26.183 ms  27.460 ms 72.14.232.70 (72.14.232.70)  37.800 ms
13  py-in-f99.google.com (64.233.167.99)  28.249 ms  26.050 ms  26.398 ms
```

(No questions on this page)

Question 5: In at most 50 words, explain how `traceroute` discovers a path to a remote host. The man page might be useful in answering this question.

---

5) Traceroute exploits the TTL parameter. Every packet has a lifespan (number of hops) specified by TTL, and when it is exceeded the current host will reply saying that time has been exceeded. Traceroute sends out many packets with artificially low lifespans in order to get a lot of ‘time exceeded’ responses from the hosts along the route.

Routine Asymmetries

For this exercise, you need to use the traceroute server at http://www.slac.stanford.edu/cgi-bin/nph-traceroute.pl. You'll use this server to execute a traceroute to your own machine.

To figure out your machine's IP address, run /sbin/ifconfig. You'll get a lot of information, including its IP:

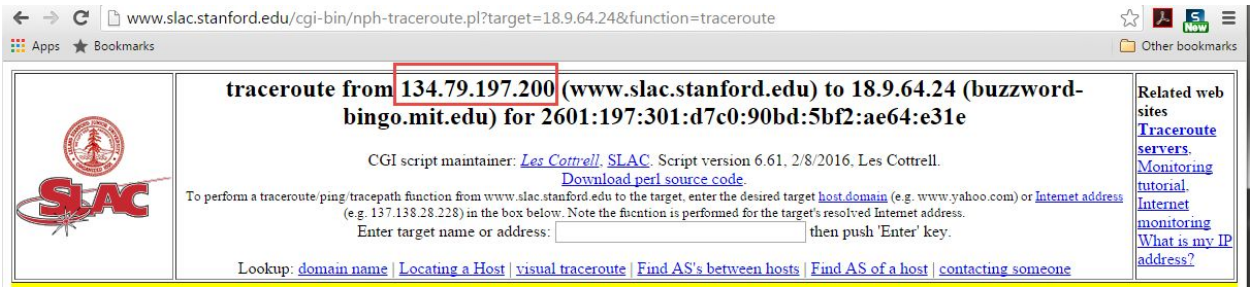
```
krebecca@buzzword-bingo:~$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:89:1a:f1
          inet addr:18.9.64.24  Bcast:18.9.64.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe89:1af1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:513562680 errors:0 dropped:206 overruns:0 frame:0
          TX packets:601861257 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:187171624575 (187.1 GB)  TX bytes:652372056999 (652.3 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:62618453 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62618453 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33902208037 (33.9 GB)  TX bytes:33902208037 (33.9 GB)
```

Once you have your IP, use Stanford's server to execute a traceroute to it.
Then run your own traceroute to Stanford's server, via

```
> traceroute [IP ADDRESS FROM STANFORD]
```

You can get Stanford's IP address from the website:



Note: It is important to run this on an Athena machine. If the Stanford traceroute does not work, or if you get no reply after 2--3 minutes, you should try one of the other looking glass servers on this page. *No questions on this page*

If you use a different server, make sure that you note in your hands-on that you used a different server than the question asked for.

Question 6: Show the output of traceroute from each direction above.

Write or type your answers to questions 6 below on the next two pages (if you don't need the second, just leave it blank).

---

traceroute to 18.9.64.21 (18.9.64.21), 30 hops max, 40 byte packets
1 134.79.197.131 (134.79.197.131) 11.672 ms 0.760 ms 0.678 ms
2 rtr-core2-p2p-serv01-02.slac.stanford.edu (134.79.253.253) 0.647 ms 0.658 ms 0.686 ms
3 rtr-fwcore2-trust-p2p-core2.slac.stanford.edu (134.79.254.146) 0.845 ms 0.867 ms 0.819 ms
4 rtr-core2-p2p-fwcore2-untrust.slac.stanford.edu (134.79.254.149) 1.191 ms 1.162 ms 1.103 ms
5 rtr-border1-p2p-core2.slac.stanford.edu (134.79.252.137) 0.989 ms 1.175 ms 0.960 ms
6 rtr-border2-p2p-border1.slac.stanford.edu (192.68.191.253) 1.651 ms 1.500 ms 1.381 ms
7 sacrcr5-ip-a-sunncr5.es.net (134.55.40.5) 4.195 ms 4.265 ms 4.204 ms
8 denvcr5-ip-a-sacrcr5.es.net (134.55.50.202) 25.170 ms 25.187 ms 25.179 ms
9 kanscr5-ip-a-denvcr5.es.net (134.55.49.58) 35.726 ms denvcr5-ip-a-sacrcr5.es.net (134.55.50.202) 25.271 ms kanscr5-ip-a-denvcr5.es.net (134.55.49.58) 35.748 ms
10 chiccr5-ip-a-kanscr5.es.net (134.55.43.81) 46.745 ms 46.842 ms 46.780 ms
11 washcr5-ip-a-chiccr5.es.net (134.55.36.46) 63.922 ms 63.877 ms 63.577 ms
12 * washcr5-ip-a-chiccr5.es.net (134.55.36.46) 64.493 ms 63.969 ms
13 * * 198.124.216.98 (198.124.216.98) 69.364 ms
14 198.124.216.98 (198.124.216.98) 69.224 ms 69.114 ms *
15 backbone-rtr-1-dmz-rtr-1.mit.edu (18.192.1.2) 75.553 ms * *
16 backbone-rtr-1-dmz-rtr-1.mit.edu (18.192.1.2) 75.447 ms oc11-rtr-1-backbone-rtr-1.mit.edu (18.168.69.2) 75.362 ms backbone-rtr-1-dmz-rtr-1.mit.edu (18.192.1.2) 75.804 ms
17 oc11-rtr-1-backbone-rtr-1.mit.edu (18.168.69.2) 76.613 ms 75.884 ms 76.039 ms
18 mint-square.mit.edu (18.9.64.21) 83.004 ms 82.921 ms 83.299 ms
traceroute -m 30 -q 3 18.9.64.21 took 32secs. Total time=32secs. user=nobody

---

traceroute to 134.79.197.200 (134.79.197.200), 30 hops max, 60 byte packets
1 18.9.64.3 (18.9.64.3) 8.443 ms 8.677 ms 8.463 ms
2 BACKBONE-RTR-1-OC11-RTR-1.MIT.EDU (18.168.69.1) 8.335 ms 8.234 ms 8.435 ms
3 DMZ-RTR-1-BACKBONE-RTR-1.MIT.EDU (18.192.1.1) 10.325 ms 10.311 ms 10.730 ms
4 NY32-RTR-1-DMZ-RTR-1.MIT.EDU (18.192.5.2) 15.016 ms 14.864 ms 15.011 ms
5 aofasdn1-mit.es.net (198.124.216.97) 15.986 ms 15.046 ms 15.595 ms
6 washcr5-ip-a-aofacr5.es.net (134.55.36.34) 20.303 ms 20.197 ms 19.688 ms
7 chiccr5-ip-a-washcr5.es.net (134.55.36.45) 36.731 ms 37.045 ms 37.097 ms
8 kanscr5-ip-a-chiccr5.es.net (134.55.43.82) 47.932 ms 47.826 ms 48.021 ms

```
 9  denvcr5-ip-a-kanscr5.es.net (134.55.49.57)  58.470 ms  58.342 ms  58.601 ms
10  sacrcr5-ip-a-denvcr5.es.net (134.55.50.201)  79.310 ms  79.415 ms  79.598 ms
11  sunncr5-ip-a-sacrcr5.es.net (134.55.40.6)  82.201 ms  82.231 ms  82.112 ms
12  rtr-border2-p2p-sunn-cr5.slac.stanford.edu (192.68.191.234)  82.798 ms  82.777 ms  82.775
ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Question 7: Describe anything unusual about the output. Are the same routers traversed in both directions? If not, why might this happen?

Black holes

At the command prompt, type:

```
> traceroute 18.31.0.200
```

Question 8: Show the output of the above command. Describe what is strange about the observed output, and why `traceroute` gives you such an output. Refer to the `traceroute` man page for useful hints.

---

7) The trace from Stanford ⇒ MIT went fine, and took 18 hops. From MIT ⇒ Stanford, the trace made it to Stanford's network, but fails to reach target host, as shown by the '***' lines. The asterisks mean that the probes failed to reach any router within their lifespan. This is because after reaching Stanford's network, the specified host was unreachable. This is because it could be disabled for security reasons, or could be taken as port scanning. This could be an example of a network "black hole."

8)

```
 1  18.9.64.3 (18.9.64.3)  8.396 ms  8.328 ms  8.582 ms
 2  BACKBONE-RTR-1-OC11-RTR-1.MIT.EDU (18.168.69.1)  8.877 ms  8.875 ms  8.870 ms
 3  DMZ-RTR-1-BACKBONE-RTR-1.MIT.EDU (18.192.1.1)  10.048 ms  10.044 ms  10.255 ms
 4  DMZ-RTR-2-DMZ-RTR-1-2.MIT.EDU (18.192.3.2)  8.950 ms  8.949 ms  8.834 ms
 5  * * *
 6  DMZ-RTR-2-CSAIL.MIT.EDU (18.4.7.1)  10.808 ms  10.081 ms  10.729 ms
 7  * * *
 8  DMZ-RTR-2-CSAIL.MIT.EDU (18.4.7.1)  10.519 ms  10.943 ms  10.741 ms
 9  * * *
(Repeat 5 and 6 until try 30)
```

Since the behavior alternates, it seems likely that there is a loop in the network rather than a black hole. It appears that the packets enter a loop with (18.4.7.1) followed by a timeout.

Border Gateway Protocol (BGP)

For this last question on the topic of Internet routing, you need to refer to the BGP routing table data below. This table shows all of the BGP routing entries that a particular router (near the University of Oregon) refers to when forwarding any packets to MIT (IP Address 18.*.*.*).
As described in the Internet routing paper, recall that BGP is a path vector protocol. Each line of this table lists a distinct path from this router to MIT, from which it will choose one to use. The Next Hop field is the IP address of the router that forwards packets for each path listed in the table. The Path field is the list of autonomous systems the path traverses on its way to MIT. The other fields (Metric, LocPrf, Weight) may be used by the router to decide which one of the possible paths to use.

```
BGP table version is 9993576, local router ID is 198.32.162.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	18.0.0.0	216.140.8.59	413		0	6395 3356 3 i
*		216.140.2.59	982		0	6395 3356 3 i
*		141.142.12.1			0	1224 22335 11537 10578 3 i
*		209.249.254.19	125		0	6461 3356 3 i
*		202.232.0.2			0	2497 3356 3 i
*		209.10.12.125	8204		0	4513 3356 3 i
*		208.51.113.253			0	3549 174 16631 3 3 3 i
*		209.123.12.51			0	8001 1784 10578 3 i
*		209.10.12.156	0		0	4513 3356 3 i
*		195.66.224.82			0	4513 3356 3 i
*		209.10.12.28	8203		0	4513 3356 3 i
*		203.181.248.233			0	7660 11537 10578 3 i
*		64.50.230.2			0	4181 174 174 174 16631 3 3 3 i
*		195.66.232.254			0	5459 2649 174 174 174 16631 3 3 3 i
*		195.66.232.239			0	5459 2649 174 174 174 16631 3 3 3 i
*		64.50.230.1			0	4181 174 174 174 16631 3 3 3 i
*		194.85.4.55			0	3277 8482 29281 702 701 3356 3 i
*		207.172.6.227	83		0	6079 10578 3 i
*		207.172.6.162	62		0	6079 10578 3 i
*		129.250.0.85	11		0	2914 174 16631 3 3 3 i
*		206.220.240.95			0	10764 11537 10578 3 i
*		217.75.96.60			0	16150 8434 3257 3356 3 i
*		66.185.128.48	514		0	1668 3356 3 i
*		206.24.210.26			0	3561 3356 3 i
*		216.191.65.118			0	15290 174 16631 3 3 3 i
*		216.191.65.126			0	15290 174 16631 3 3 3 i
*		209.161.175.4			0	14608 19029 3356 3 i
*		202.249.2.86			0	7500 2497 3356 3 i
*		208.186.154.35	0		0	5650 3356 3 i

```
*                 167.142.3.6                          0 5056 1239 3356 3 i
*                 64.200.151.12                        0 7911 3356 3 i
*                 195.219.96.239                       0 6453 3356 3 i
*                 208.186.154.36           0           0 5650 3356 3 i
*                 203.194.0.12                         0 9942 16631 174 174 174 16631 3 3 3 i
*                 213.200.87.254          40           0 3257 3356 3 i
*                 216.218.252.145                      0 6939 3356 3 i
*                 216.18.63.137                        0 6539 174 16631 3 3 3 i
*                 216.218.252.152                      0 6939 3356 3 i
*                 195.249.0.135                        0 3292 3356 3 i
*                 65.106.7.139             3           0 2828 174 16631 3 3 3 i
*                 207.45.223.244                       0 6453 3356 3 i
*                 207.246.129.14                       0 11608 6461 3356 3 i
*                 207.46.32.32                         0 8075 174 16631 3 3 3 i
*                 129.250.0.11             0           0 2914 174 16631 3 3 3 i
*                 134.55.200.1                         0 293 11537 10578 3 i
*                 193.0.0.56                           0 3333 3356 3 i
*                 216.140.14.186           3           0 6395 3356 3 i
*                 198.32.8.196           960           0 11537 10578 3 i
*                 64.200.95.239                        0 7911 3356 3 i
*                 196.7.106.245                        0 2905 701 3356 3 i
*                 154.11.63.86                         0 852 174 16631 3 3 3 i
*                 134.222.85.45            0           0 286 209 3356 3 i
*                 213.140.32.146                       0 12956 174 16631 3 3 3 i
*                 164.128.32.11                        0 3303 3356 3 i
*                 213.248.83.240                       0 1299 3356 3 i
*                 154.11.98.18                         0 852 174 16631 3 3 3 i
*>                4.68.0.243               0           0 3356 3 i
*                 204.42.253.253           0           0 267 2914 174 16631 3 3 3 i
*                 206.186.255.223                      0 2493 3602 174 16631 3 3 3 i
*                 193.251.128.22                       0 5511 3356 3 i
*                 203.62.252.26                        0 1221 4637 3356 3 i
*                 12.0.1.63                            0 7018 3356 3 i
*                 144.228.241.81  4294967294           0 1239 3356 3 i
```

(No questions on this page)

Question 9: From the path entry data, which Autonomous System (AS) number corresponds to MIT?

Question 10: What are the Autonomous System (AS) numbers of each AS which advertises a direct link to MIT?

Question 11: How long did it take you to complete this hands-on?

---

9) 3. Looking at the table above, each path (e.g. ` `7911 3356 3``) ends in AS3. As MIT is our target host, it follows that it is in AS3.

10) If by direct link, it is meant that from source to target there is only one intermediary, that would be `3356` . Though, if by direct link, it is meant all ASs which directly connect to AS3, there are a few additional: `16631 , 10578`.

11) 4.5 hours.