# Hands-on 3: Traceroute

Michael Plasmeier

1. Results are below
	1. Ping www.csail.mit.edu

6 packets transmitted, 6 received, 0% packet loss, time 5000ms

rtt min/avg/max/mdev = 0.293/0.313/0.373/0.032 ms

* 1. Ping www.berkeley.edu

6 packets transmitted, 6 received, 0% packet loss, time 5000ms

rtt min/avg/max/mdev = 92.620/93.224/95.324/0.984 ms

* 1. Ping www.usyd.edu.au

6 packets transmitted, 0 received, 100% packet loss, time 5003ms

* 1. Ping www.kyoto-u.ac.jp

6 packets transmitted, 6 received, 0% packet loss, time 5005ms

rtt min/avg/max/mdev = 209.480/209.742/210.801/0.710 ms

1. The network latency to server in Japan is much higher than the server in California, which is much higher than a server down the street in CSAIL.
2. Results are below
	1. Ping www.csail.mit.edu with 56 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5000ms

rtt min/avg/max/mdev = 0.308/0.400/0.541/0.082 ms

* 1. Ping www.csail.mit.edu with 512 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5004ms

rtt min/avg/max/mdev = 0.352/0.388/0.423/0.035 ms

* 1. Ping www.csail.mit.edu with 1024 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5003ms

rtt min/avg/max/mdev = 0.445/0.492/0.560/0.043 ms

* 1. Ping www.berkeley.edu with 56 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5002ms

rtt min/avg/max/mdev = 92.680/92.821/93.125/0.161 ms

* 1. Ping www.berkeley.edu with 512 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5005ms

rtt min/avg/max/mdev = 92.748/92.942/93.222/0.286 ms

* 1. Ping www.berkeley.edu with 1024 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5005ms

rtt min/avg/max/mdev = 92.994/93.101/93.429/0.382 ms

* 1. Ping www.usyd.edu.au with 56 bytes

6 packets transmitted, 0 received, 100% packet loss, time 5003ms

* 1. Ping www.csail.mit.edu with 512 bytes

6 packets transmitted, 0 received, 100% packet loss, time 5002ms

* 1. Ping www.csail.mit.edu with 1024 bytes

6 packets transmitted, 0 received, 100% packet loss, time 5017ms

* 1. Ping www. www.kyoto-u.ac.jp with 56 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5001ms

rtt min/avg/max/mdev = 209.510/215.836/241.162/11.545 ms

* 1. Ping www.kyoto-u.ac.jp with 512 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5000ms

rtt min/avg/max/mdev = 209.601/209.871/210.705/0.594 ms

* 1. Ping www.kyoto-u.ac.jp with 1024 bytes

6 packets transmitted, 6 received, 0% packet loss, time 5002ms

rtt min/avg/max/mdev = 209.691/209.958/210.779/0.702 ms

* 1. The response times are higher because larger packets take longer to transmit.
1. Servers may choose not to respond to a ping for security reasons. Pings could be used to flood the server. There could be a bug in the server’s handling of ICMP messages so those are blocked. Finally it has become good practice to “stealth” a computer – not return a response on any port. However, this arguably should not apply to public web servers.
2. Traceroute works by sending a sequence of ICMP echo requests (pings) to servers on the route to the destination. Traceroute sends a packet addressed to the ultimate destination, but with a time-to-live (TTL) of 1 – which causes the first server to return a response. Traceroute than increments the TTL by 1, until the destination responds.
3. Athena Dialup to Stanford Server:

theplaz@dr-wily:~$ traceroute www.slac.stanford.edu

traceroute to www.slac.stanford.edu (134.79.18.188), 30 hops max, 60 byte packets

 1 \* \* \*

 2 BACKBONE-RTR-1.MIT.EDU (18.168.1.1) 0.386 ms 0.421 ms 0.499 ms

 3 DMZ-RTR-1-BACKBONE-RTR-1.MIT.EDU (18.168.5.2) 2.067 ms 2.079 ms 2.042 ms

 4 NY32-RTR-1-DMZ-RTR-1.MIT.EDU (18.192.5.2) 7.423 ms 7.428 ms 7.409 ms

 5 tge-0-2-0-3.4006.newy.layer3.nlr.net (216.24.184.101) 7.417 ms 7.498 ms 7.418 ms

 6 vlan-59.phil.layer2.nlr.net (216.24.186.85) 83.319 ms 83.092 ms 83.087 ms

 7 vlan-58.wash.layer2.nlr.net (216.24.186.87) 83.020 ms 82.449 ms 82.461 ms

 8 vlan-55.rale.layer2.nlr.net (216.24.186.90) 82.655 ms 82.507 ms 82.520 ms

 9 vlan-54.atla.layer2.nlr.net (216.24.186.52) 83.053 ms 83.040 ms 83.073 ms

10 vlan-53.jack.layer2.nlr.net (216.24.186.55) 83.029 ms 82.496 ms 82.495 ms

11 vlan-51.hous.layer2.nlr.net (216.24.186.78) 82.701 ms 82.710 ms 82.384 ms

12 vlan-47.elpa.layer2.nlr.net (216.24.186.74) 82.552 ms 82.426 ms 82.516 ms

13 vlan-43.losa.layer2.nlr.net (216.24.186.73) 82.705 ms 82.379 ms 82.455 ms

14 hpr-lax-hpr2--nlr-pn.cenic.net (137.164.26.25) 82.699 ms 82.778 ms 82.384 ms

15 svl-hpr2--lax-hpr2-10g.cenic.net (137.164.25.38) 91.146 ms 91.022 ms 91.062 ms

16 hpr-stanford--svl-hpr2-10ge.cenic.net (137.164.27.62) 91.199 ms 91.006 ms 91.294 ms

17 boundarya-rtr.Stanford.EDU (171.66.0.34) 91.694 ms 91.466 ms 91.717 ms

18 rtr-border1-p2p-stanford-west-ech.slac.stanford.edu (192.68.191.242) 83.306 ms 83.177 ms 83.125 ms

19 \* \* \*

20 \* \* \*

21 \* \* \*

22 \* \* \*

23 \* rtr-border1-p2p-stanford-west-ech.slac.stanford.edu (192.68.191.242) 83.328 ms !X \*

Stanford Server to Athena Dialup:

Executing exec(traceroute, -m 30 -q 1 -w 3, 18.181.0.233)

traceroute to 18.181.0.233 (18.181.0.233), 30 hops max, 40 byte packets

 1 rtr-servcore1-nethub.slac.stanford.edu (134.79.19.4) 0.599 ms

 2 rtr-core1-p2p-servcore1.slac.stanford.edu (134.79.252.166) 0.531 ms

 3 rtr-border1-p2p-core1.slac.stanford.edu (134.79.252.133) 0.674 ms

 4 slac-mr2-p2p-rtr-border1.slac.stanford.edu (192.68.191.245) 0.395 ms

 5 sunnsdn2-ip-slacmr2.es.net (134.55.217.2) 0.817 ms

 6 sunncr1-sunnsdn2.es.net (134.55.209.98) 0.816 ms

 7 denvcr2-sunncr1.es.net (134.55.220.49) 27.861 ms

 8 kanscr1-ip-denvcr2.es.net (134.55.209.46) 40.953 ms

 9 chiccr1-ip-kanscr1.es.net (134.55.221.58) 53.343 ms

10 clevcr1-ip-chiccr1.es.net (134.55.217.53) 60.665 ms

11 bostcr1-ip-clevcr1.es.net (134.55.41.146) 73.759 ms

12 \*

13 DMZ-RTR-1-EXTERNAL-RTR-1.MIT.EDU (18.192.9.1) 83.154 ms

14 BACKBONE-RTR-1-DMZ-RTR-1.MIT.EDU (18.168.5.1) 83.044 ms

15 \*

16 DR-WILY.MIT.EDU (18.181.0.233) 83.070 ms

1. The routes are not symmetrical. On the way to Stanford, we used nlr.net. On the way back, a network operated by es.net was taken. This is because nothing in BGP requires a route to be symmetrical. Each BGP table was created separately.
2. Traceroute to a dead address produces the following output: Four servers attempt to route the request until trantor decides that the computer cannot be found. (Or perhaps it’s a later server that does not respond to pings) . The \* \* \* line means no response. It’s possible to have such a line and then continue getting data if the server does not respond to pings. For example, server 1 below.

traceroute to 18.31.0.200 (18.31.0.200), 30 hops max, 60 byte packets

 1 \* \* \*

 2 B24-RTR-2-BACKBONE.MIT.EDU (18.168.0.23) 0.515 ms 0.614 ms 0.740 ms

 3 MITNET.TRANTOR.CSAIL.MIT.EDU (18.4.7.65) 0.571 ms 0.682 ms 0.792 ms

 4 trantor.helicon.csail.mit.edu (128.30.0.246) 2.614 ms 3.448 ms 3.569 ms

 5 \* \* \*

 6 \* \* \*

 7 \* \* \*

 8 \* \* \*

 9 \* \* \*

10 \* \* \*

11 \* \* \*

12 \* \* \*

13 \* \* \*

14 \* \* \*

15 \* \* \*

16 \* \* \*

17 \* \* \*

18 \* \* \*

19 \* \* \*

20 \* \* \*

21 \* \* \*

22 \* \* \*

23 \* \* \*

24 \* \* \*

25 \* \* \*

26 \* \* \*

27 \* \* \*

28 \* \* \*

29 \* \* \*

30 \* \* \*

1. MIT is AS number 3.
2. ASes with a link to MIT are:
	1. 3356 (Level 3)
	2. 10578 (Harvard)
	3. 16631 (Cogent)