Member: 張凱華、林晨煦、沈韋辰、葉彥東

## **Environment**

OS: Ubuntu 16.04 @ Virtual Box 6.1.18

Language: C

## How to detect and defend traceroute?

Detect:

When the router continuously receiving ICMP requests from the same IP address with incremental TTL (plus 1 every time).

Defend:

Router can use firewall to filter the ICMP requests by the IP address we just detect.

# Why traceroute cannot show the full route?

Some routers will block ICMP requests because security issues or don't want to waste bandwidth and time on dealing them.

# Why the result may not always be the same?

The path to the destination may be multiple. Each traceroute command can have different path, it depends on the design of routing algorithm, bandwidth or other facts.

## Compare the results between local and foreign

Local example: www.ntu.edu.tw (140.112.8.116) @ Taipei, Taiwan

```
root)~/CNLab-Ass01$ ./traceroute www.ntu.edu.tw
traceroute to www.ntu.edu.tw (140.112.8.116), 64 hops max
                                                          3.270ms
1 10.118.0.253
                                    2.786ms
                                               2.581ms
                                               4.295ms
2.723ms
2 192.168.203.229
                                    2.652ms
                                                          2.005ms
                                    3.180ms
                                                          4.373ms
  wl127.cc.ntu.edu.tw
                                    8.453ms
                                               6.702ms
4 www.ntu.edu.tw
                                                          2.731ms
```

Foreign example: www.hku.hk (147.8.2.58) @ Hongkong

```
root)~/CNLab-Ass01$ ./traceroute www.hku.hk
2.831ms
  10.118.0.253
                                                       11.142ms
3.471ms
  192.168.203.229
                                             2.179ms
                                   3.345ms
3 wl127.cc.ntu.edu.tw
                                             9.130ms
                                   4.723ms
  140.112.0.210
                                   2.640ms
                                             3.306ms
                                                        2.324ms
  140.112.0.206
140.112.0.34
                                   4.772ms
                                             4.733ms
                                                       6.232ms
                                   7.308ms
                                             2.825ms
                                                        4.048ms
  202.169.174.50
                                   5.794ms
                                             4.005ms
                                                        3.205ms
  202.169.174.75
jucc2-lacp-10g.hkix.net
203.188.117.6
                                   32.576ms
                                             34.207ms
                                   62.600ms
                                             63.683ms
                                                       62.754ms
                                   244.331ms
                                             175.643ms 176.246ms
10
  147.8.239.15
                                   176.522ms
                                              185.578ms
                                                          178.326ms
                                   Timeout.
                                             Timeout.
                                                       Timeout.
```

Local responses are often faster and with shorter path. On the other hands, foreign responses are often slower and with more hop. Additionally, tracerouting to foreign is easier to delay, dropped, or timeout. Basically, the reason is the physical distance.

# Difference by using TCP, UDP, and ICMP

Because our group didn't finish this part of code, we use Linux's traceroute to take its place.

#### TCP:

**Principle:** Probing the routing path by sending TCP SYN packets, seems just like trying to establish a TCP connection.

**Observation:** It's faster than UDP and little slower than ICMP. Doesn't find unresponsive condition.

```
(root)-$ traceroute -T www.google.com traceroute to www.google.com (172.217.160.100), 30 hops max, 60 byte packets
1 10.118.0.253 (10.118.0.253) 18.681 ms 19.641 ms 19.622 ms
2 192.168.203.229 (192.168.203.229) 19.596 ms 20.477 ms 20.463 ms
3 w127.cc.ntu.edu.tw (140.112.4.254) 20.452 ms * 20.433 ms
4 * 140.112.6.210 (140.112.0.210) 21.472 ms *
5 140.112.0.210 (140.112.0.206) 21.464 ms 22.405 ms 22.293 ms
6 140.112.0.34 (140.112.0.34) 22.292 ms 6.446 ms 6.331 ms
7 72.14.196.229 (72.14.196.229) 7.320 ms 8.504 ms 8.414 ms
8 108.170.244.129 (108.170.244.129) 8.367 ms 108.170.244.97 (108.170.244.97) 6.599 ms 108.170.244.129 (108.170.244.129) 7.207 ms
9 108.170.225.177 (108.170.225.177) 13.468 ms 13.467 ms 216.239.48.135 (216.239.48.135) 10.943 ms
10 tsa03.806.in.fd 12100 net (172.217.160.100) 9.860 ms 9.927 ms 14.164 ms
```

#### UDP:

**Principle**: Probing the routing path by sending UDP packets, final reply is "ICMP Destination Unreachable".

**Observation**: It has the slowest RTT and usually fail in the end. (Not receive the response)

#### ICMP:

**Principle:** Probing the routing path by sending ICMP Echo Reply, final reply is "ICMP Echo Reply". **Observation:** Sometimes may not receive response but it is the fastest one of three.

```
(root)~$ traceroute -I www.google.com
traceroute to www.google.com (172.217.160.100), 30 hops max, 60 byte packets
1 10.118.0.253 (10.118.0.253) 14.507 ms 14.414 ms 14.398 ms
2 192.168.203.229 (192.168.203.229) 26.570 ms 27.458 ms 27.748 ms
3 wl127.cc.ntu.edu.tw (140.112.4.254) 27.763 ms 28.034 ms 28.025 ms
4 140.112.0.170 (140.112.0.170) 28.356 ms 28.652 ms 140.112.0.210 (140.112.0.210) 28.657 ms
5 140.112.0.206 (140.112.0.206) 28.914 ms 29.183 ms 29.474 ms
6 140.112.0.34 (140.112.0.34) 36.926 ms 4.489 ms 4.103 ms
7 72.14.196.229 (72.14.196.229) 6.814 ms 4.695 ms 4.614 ms
8 108.170.244.129 (108.170.244.129) 7.459 ms 108.170.244.97 (108.170.244.97) 6.097 ms *
9 * * *
10 tsa03s06-in-f4.1e100.net (172.217.160.100) 7.967 ms 10.108 ms 9.434 ms
```

#### Conclusion:

**TCP traceroute** is imitating establishing a real connection, which makes it more likely pass the firewall, so it has the highest success rate. However, this mechanism also makes some overhead.

**UDP traceroute** is simple but often fail if some of the routers on the path choose to ignore responding final reply. Its unreliability also makes it easier to be block by firewall for security issue, and the instability causes it has higher RTT.

**ICMP traceroute** is also simple but fast. Similarly, ICMP often be blocked by firewall.

## Reference

## [1] DNS Look-up:

https://github.com/CyberChimeraUSA/C-Networking/blob/master/C-DNS%20lookup%20using%20getaddrinfo/dnsUpdatedvid.c)

### [2] Traceroute implementation:

https://stackoverflow.com/questions/15458438/implementing-traceroute-using-icmp-in-c

## [3]Traceroute implementation:

https://stackoverflow.com/questions/29344543/simple-icmp-traceroute-implementation-in-c

### [4] Traceroute in UDP:

https://learningnetwork.cisco.com/s/question/0D53i00000Kt6Ms/how-does-traceroute-work-with-udp-on-packet-level

### [5] TCP/UDP/ICMP Traceroute:

https://zhuanlan.zhihu.com/p/101810847