# CN-Lab Experiment 1 report Group 15

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
 1 10.118.0.253                    2.786ms   2.581ms   3.270ms
 2 192.168.203.229                 2.652ms   4.295ms   2.005ms
 3 wl127.cc.ntu.edu.tw             3.180ms   2.723ms   4.373ms
 4 www.ntu.edu.tw                  8.453ms   6.702ms   2.731ms
```

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

```
(root)~/CNLab-Ass01$ ./traceroute www.hku.hk
traceroute to www.hku.hk (147.8.2.58), 64 hops max
 1 10.118.0.253                   7.922ms   2.831ms   3.296ms
 2 192.168.203.229                3.345ms   2.179ms   11.142ms
 3 wl127.cc.ntu.edu.tw            4.723ms   9.130ms   3.471ms
 4 140.112.0.210                  2.640ms   3.306ms   2.324ms
 5 140.112.0.206                  4.772ms   4.733ms   6.232ms
 6 140.112.0.34                   7.308ms   2.825ms   4.048ms
 7 202.169.174.50                 5.794ms   4.005ms   3.205ms
 8 202.169.174.75                 32.576ms  34.207ms  32.501ms
 9 jucc2-lacp-10g.hkix.net        62.600ms  63.683ms  62.754ms
10 203.188.117.6                  244.331ms  175.643ms  176.246ms
11 147.8.239.15                   176.522ms  185.578ms  178.326ms
12 *                              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.

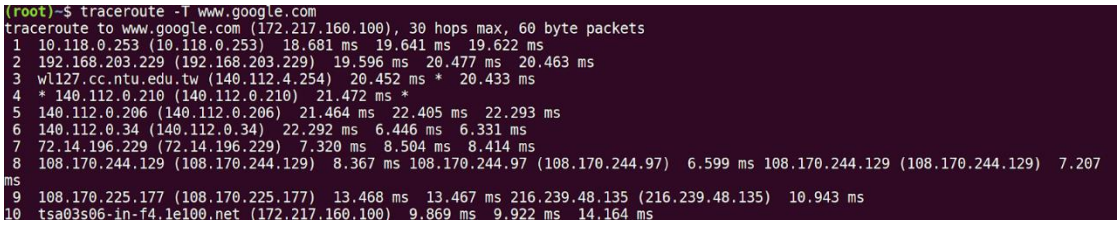
# Difference by using TCP, UDP, and ICMP

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.

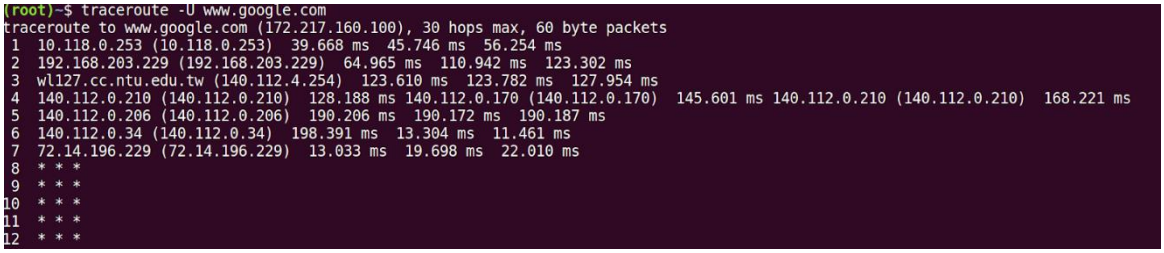
**Observation:** It's faster than UDP and little slower than ICMP. Doesn't find unresponsive condition.




**UDP:**

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

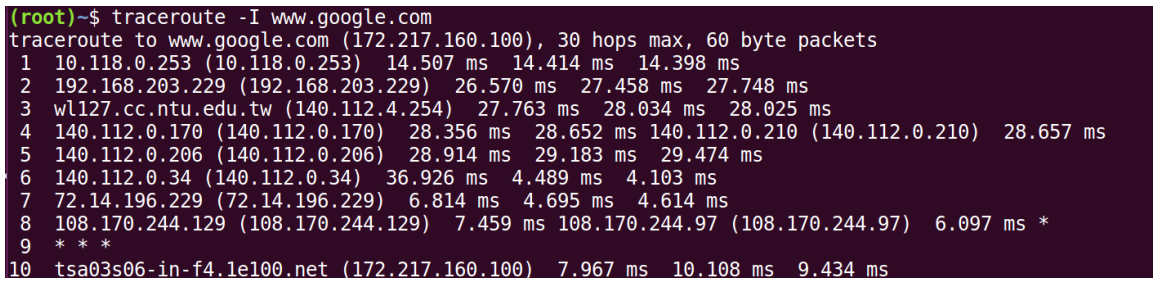
**Observation**: It has the slowest RTT and usually fail in the end. (Not receive the response)




**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.




**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