Traceroute

Motivation

Traceroute is an excellent tool to diagnose the internet. Many researchers use the tool in their research for different purposes. I felt excited when I first learned on the first day of the class that using the tool, we can find out the route from sender to receiver. I felt that I would also be able to use this tool in the future for various purposes, and it would give me a very clear view of the traversing of a packet.

The tool is already available, but I need the program to use it extensively. As an example, in this project, I used 3700 times ping responses for the RTT vs Congested network experiment. I was able to make the experiment automated by modifying the code. As a result, doing the experiment was comparatively easy for me.

Besides this, many researchers also use ICMP socket for their various purpose experiments. The ICMP socket is different from the other standard sockets.

So, I got it as an opportunity to be very familiar with both of the things.

System design

The basic architecture of the Traceroute is based on the TTL value of a packet. When a packet passes from one hop to another hop, then the intermediate each router decrements the TTL value by one. When the TTL value gets zero, then the router sends an ICMP time exceeded response to the source. The router includes its own IP information.

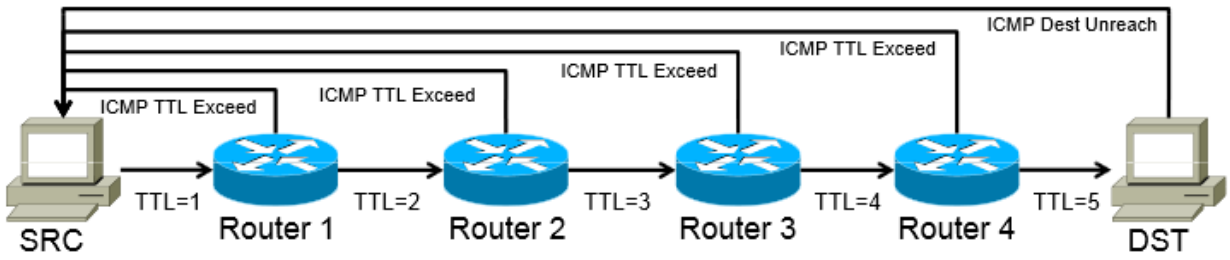


Fig: Basic architecture of the Traceroute. (1)

Then I had an experiment on RTT to observe the behavior of RTT on a different level of a congested network. For this experiment, at first, I find out the IP addresses of a link using the Traceroute. Then I selected an IP address to create the congestion by sending the traffic to the next IP address.

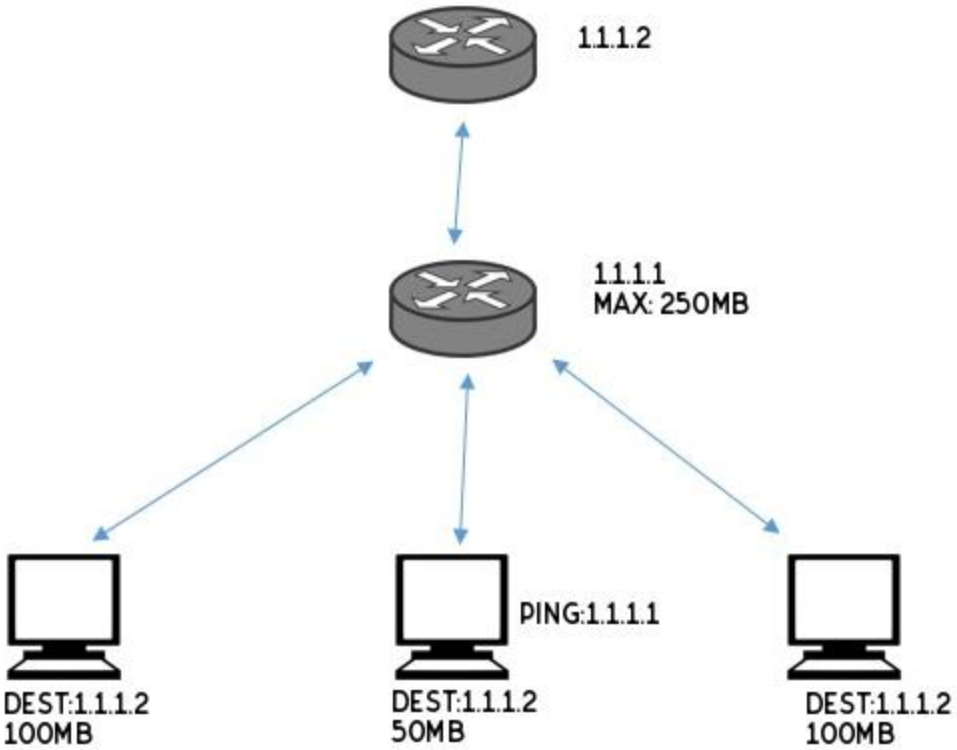


Fig: The architecture to create congestion in the selected router.

In this figure, we are sending 250Mb traffic from three different computers to 1.1.1.2. All of those data are going through 1.1.1.1 and creating the desired congestion.

Evaluation

We observed several information by doing several experiments.

Route Information: We had an experiment to find out the intermediary hop's IP addresses and other related information including hostname, geo-location, and organization names from source to destination. Here is an example,

root@salahuddin-PC:/media/salahuddin/traceroute# python traceroute.py www.uh.edu
Traceroute to www.uh.edu (129.7.97.54) 30 hops max 16 bytes packets
1 192.168.0.1 (192.168.0.1) 1.092 ms 1.694 ms 0.913 ms
2 96.120.16.33 (96.120.16.33) 8.862 ms 18.862 ms 0.386 ms
3 ae-103-rur01.airport.tx.houston.comcast.net (69.139.209.177) 0.049 ms 11.376 ms 0.033 ms
4 ae-68-ar01.bearcreek.tx.houston.comcast.net (68.85.247.229) 0.019 ms 11.087 ms 13.718 ms
5 be-33662-cr02.dallas.tx.ibone.comcast.net (68.86.92.61) 0.017 ms 16.215 ms 17.537 ms
6 be-12441-pe01.1950stemmons.tx.ibone.comcast.net (68.86.89.206) 0.022 ms 18.160 ms 3.444 ms

7 xe-11-0-3.0.rtsw.dall.net.internet2.edu (64.57.20.93) 0.017 ms 20.256 ms 1.379 ms
8 xe-11-0-3.0.rtsw.dall.net.internet2.edu (64.57.20.93) 13.950 ms * *
9 et-0-3-0.3707.rtsw.houh.net.internet2.edu (198.71.47.93) 497.969 ms 132.558 ms 183.197 ms
10 198.71.47.94 (198.71.47.94) 198.452 ms 101.134 ms 125.821 ms
11 74.200.190.42 (74.200.190.42) * 147.761 ms 20.862 ms
12 uh-trcps-1.setg.net (198.32.230.130) 8.933 ms 108.685 ms 0.832 ms
13 uh-trcps-1.setg.net (198.32.230.130) 0.017 ms * *
14 coogscity.com (129.7.97.54) 87.232 ms 43.807 ms 70.903 ms

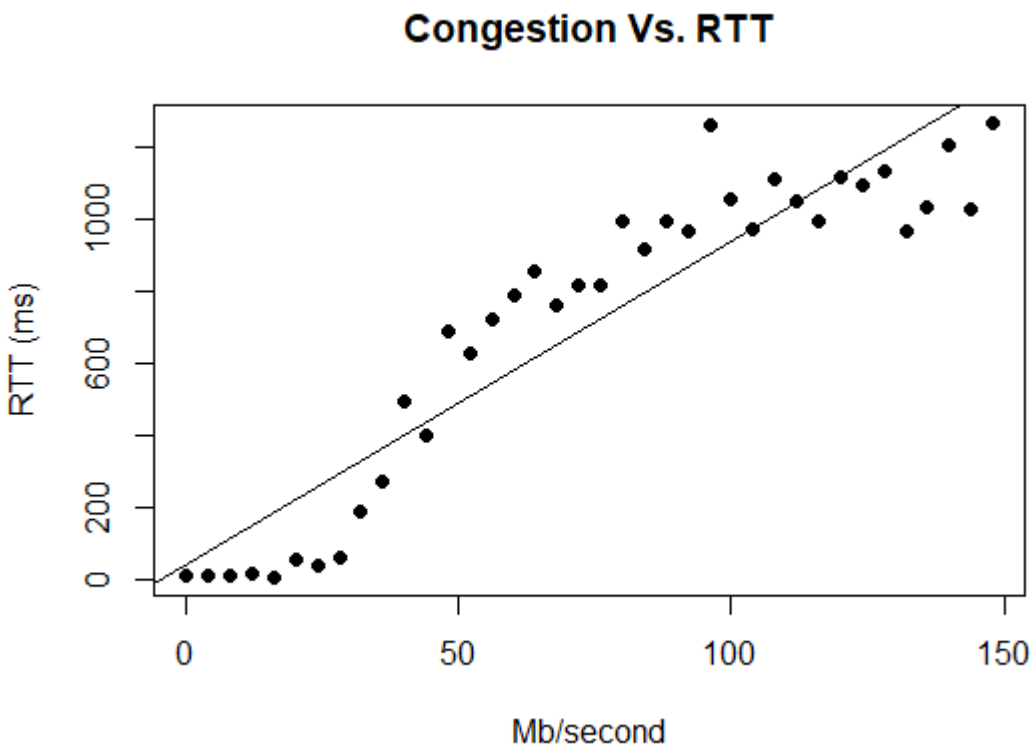
Geolocation of the route:
==========

1 192.168.0.1 not resolved!
2 IP: 96.120.16.33; Org: Comcast Cable Communications, LLC; Location: Reno County, Kansas, USA (37.751, -97.822)
3 IP: 69.139.209.177; Org: Comcast Cable Communications, LLC; Location: Reno County, Kansas, USA (37.751, -97.822)
4 IP: 68.85.247.229; Org: Comcast Cable Communications, LLC; Location: Reno County, Kansas, USA (37.751, -97.822)
5 IP: 68.86.92.61; Org: Comcast Cable Communications, LLC; Location: Reno County, Kansas, USA (37.751, -97.822)
6 IP: 68.86.89.206; Org: Comcast Cable Communications, LLC; Location: Reno County, Kansas, USA (37.751, -97.822)
7 IP: 64.57.20.93; Org: Internet2; Location: Reno County, Kansas, USA (37.751, -97.822)
8 IP: 64.57.20.93; Org: Internet2; Location: Reno County, Kansas, USA (37.751, -97.822)
9 IP: 198.71.47.93; Org: Internet2; Location: Fairfield Court, Pittsfield Township, Washtenaw County, Michigan, 48108, USA (42.2167, -83.7406)
10 IP: 198.71.47.94; Org: Internet2; Location: Fairfield Court, Pittsfield Township, Washtenaw County, Michigan, 48108, USA (42.2167, -83.7406)
11 IP: 74.200.190.42; Org: LEARN; Location: Reno County, Kansas, USA (37.751, -97.822)
12 IP: 198.32.230.130; Org: Rice University; Location: 5507, Belmont Street, West University Place, Harris County, Texas, 77005, USA (29.7228, -95.4251)
13 IP: 198.32.230.130; Org: Rice University; Location: 5507, Belmont Street, West University Place, Harris County, Texas, 77005, USA (29.7228, -95.4251)
14 IP: 129.7.97.54; Org: University of Houston; Location: 4959, Oak Forest Drive, Candlelight Estates, Houston, Harris County, Texas, 77018, USA (29.8365, -95.4363)

In this example, I sent the request from Harris County, Houston to the University of Houston. The physical distance from the client to the server is about two kilometers. But, from the response, we can see that the packet has traveled from source to destination via Reno County, Kansas which is hundreds of kilometers away. So we can say that packets can be traveled hundreds of miles, even though the receiver stays within a mile.

Broken Link Identification: We can identify the broken link using the Traceroute. If we have several known information then we can decide it. Suppose, we know the server of the UH is running that my friend can access it from a different location, but I cannot access it then we can have a fair assumption that there may have a broken link from me to the server.

Congestion vs RTT: We had another experiment to see the RTT changing behavior on different congestion level in the network. I prepared a multi-threaded dynamic client to generate the desired multilevel network traffic. I tested the RTT for 0, 4, 8, 12, 16… 144, 148 Mb/second congestion level. I took the average time from 100 RTT for each congestion level. Here is the plot to show the relationship between different congestion level and RTT.



From the plot, we can observe that the RTT was linearly increasing by the increasing network traffic on the internet.

Sources:

1. https://bit.ly/2PDTKxd