Vishal Gauba
1410110501
vg396

Computer Networks (Homework 1)

1 Ch 1 – Question 36

The Unix utility ping can be used to find the RTT to various Internet hosts. Read the man page for ping, and use it to find the RTT to www.cs.princeton.edu in New Jersey and cisco.com in California. Measure the RTT values at different times of day, and compare the results. What do you think accounts for the differences?

Ans: The server at *www.**cs**.princeton.edu* was not accessible at any time of the day and the request would get timed out. Possible reasons for this could be:

- Response from ICMP Echo (ping) is disabled on their server (by closing port 7) [1]
- Ping is disabled in Firewall [2]

To maintain the same geographical location, I have used the results of Princeton.edu instead, which is also located in New Jersey.

Time	Ping	Location	Average RTT (ms)
10 am	www.princeton.edu cisco.com	New Jersey (East) California (West)	266 290
1 pm	www.princeton.edu cisco.com	New Jersey (East) California (West)	262 282
4 pm	www.princeton.edu cisco.com	New Jersey (East) California (West)	265 293

The below factors account for the differences in the RTTs to the given servers:

- At each time of pinging, the IP may have used a different route to the server. Which could cause varying latency.
- Each of the routes would have different number of hops based on the routers in that path for the packet to reach the destination and back. Each hop would take finite amount of processing time.
- The size of the queue/buffer at every device would be different depending on the traffic based on the time of the day.
- The geographical location (distance between host & client) also matters a lot. The ping to New Jersey than to California is almost ~20 milliseconds (9-10%) faster in all case

1. http://security.stackexchange.com/questions/22711/is-it-a-bad-idea-for-a-firewall-to-block-icmp
   http://www.techexams.net/forums/network/8777-icmp-port-number.html
2. https://kb.iu.edu/d/aopy
   https://csguide.cs.princeton.edu/access/firewall

2 Ch 1 – Question 37

The Unix utility traceroute, or its Windows equivalent tracert, can be used to find the sequence of routers through which a message is routed. Use this to find the path from your site to some others. How well does the number of hops correlate with the RTT times from ping? How well does the number of hops correlate with geographical distance?

Ans: The findings are in correlation to the RTTs (ping). It took 13 hops to reach the server at www.princeton.edu and 15 hops to reach the server at cisco.com. Also, the time taken for hop at the endhost and back is given in the 13th hop & the 15th hop, which matches the RTT from ping.

Note: -d switch is to turn off DNS resolution which slows down the process.

```
C:\Users\vishg>tracert -d www.princeton.edu

Tracing route to www.princeton.edu [140.180.223.42]
over a maximum of 30 hops:

  1     2 ms     3 ms     2 ms  192.168.2.1
  2    41 ms    36 ms    42 ms  122.160.130.157
  3     *        *        *     Request timed out.
  4    47 ms    38 ms    38 ms  125.18.20.101
  5   191 ms   178 ms   188 ms  182.79.255.110
  6   190 ms   182 ms   181 ms  182.79.224.66
  7    70 ms    73 ms    74 ms  182.79.235.249
  8   189 ms   263 ms   220 ms  182.79.222.78
  9   189 ms   185 ms   194 ms  195.66.224.21
 10   272 ms   267 ms   274 ms  72.52.92.166
 11   267 ms   268 ms   268 ms  216.66.49.74
 12   277 ms   292 ms   268 ms  128.112.12.130
 13   268 ms   261 ms   263 ms  140.180.223.42

Trace complete.
```

```
C:\Users\vishg>tracert -d cisco.com

Tracing route to cisco.com [72.163.4.161]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.2.1
  2    40 ms    37 ms    43 ms  122.160.130.157
  3     *        *        *     Request timed out.
  4    41 ms    40 ms    40 ms  59.144.176.121
  5   166 ms   173 ms   160 ms  182.79.203.130
  6   178 ms   159 ms   158 ms  182.79.208.62
  7    73 ms    71 ms   146 ms  182.79.255.225
  8   159 ms   163 ms   162 ms  182.79.245.134
  9   162 ms   159 ms   163 ms  213.242.116.161
 10     *        *        *     Request timed out.
 11   300 ms   312 ms   325 ms  4.30.74.46
 12     *        *        *     Request timed out.
 13   308 ms   323 ms   290 ms  72.163.0.178
 14   307 ms   310 ms   325 ms  72.163.2.98
 15   298 ms   387 ms   318 ms  72.163.4.161

Trace complete.
```

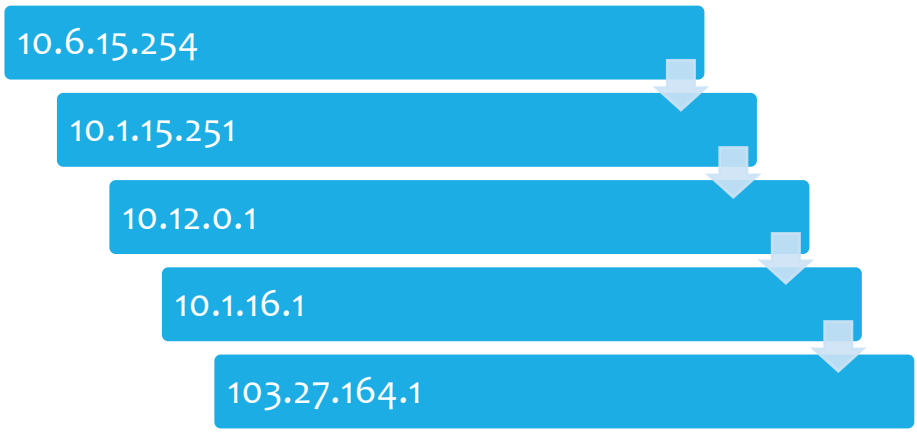
3 Chapter 1 – Question 38

Use traceroute, above, to map out some of the routers within your organization (or to verify none is used).

```
Tracing route to www.google.com [216.58.203.68]
over a maximum of 30 hops:

  1     5 ms     3 ms     2 ms  10.6.15.254
  2     1 ms     1 ms     1 ms  10.1.15.251
  3     1 ms     6 ms     1 ms  10.12.0.1
  4     5 ms     5 ms     3 ms  10.1.16.1
  5     2 ms     2 ms     2 ms  103.27.164.1
  6   296 ms   702 ms   491 ms  115.249.6.102
  7     4 ms    11 ms     5 ms  72.14.204.158
  8    14 ms    11 ms    10 ms  66.249.95.122
  9     5 ms     5 ms     3 ms  209.85.240.17
 10    13 ms     8 ms     7 ms  del01s07-in-f4.1e100.net [216.58.203.68]

Trace complete.
```



Based on the *very low RTTs* and also on my *own device's IP address*, it can be safely assumed that the first four **10.*.*.*** routers are within SNU.

It would appear to be that 103.27.164.1 is the public IP of the router that connects SNU network to the outside Internet.