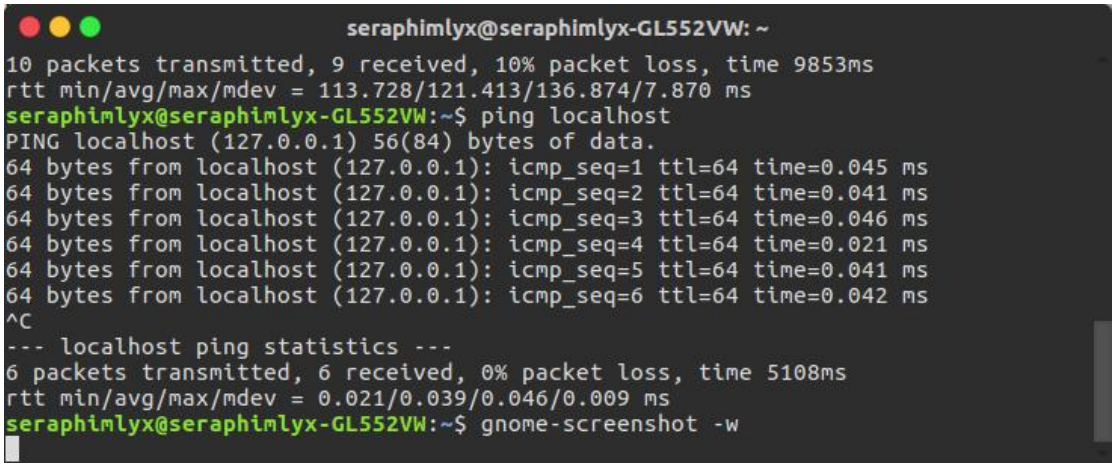
a) Use ping on your workstations to familiarize yourself with these commands. List a few of the flags that are used with these two commands.

-s determine the size of the packets

-c determine how many packets to send

-M (do/want/dont) Select path MTU Discovery strategy

i) Ping your workstation's loopback interface (localhost). What command did you use? Was the ping successful? If the ping is successful, then TCP/IP is properly ECE 9303 — Assignment # 1 2 installed and functioning on this workstation.



Answer: Yes. Ping 0.0.0.0 (or127.0.0.1)

ii) Ping your default gateway and your DNS server. What command did you use?

Answer:

In Linux:

>>nmcli device show | grep GATEWAY

>>IP4.GATEWAY 172.30.72.1

>>ping 172.30.72.1

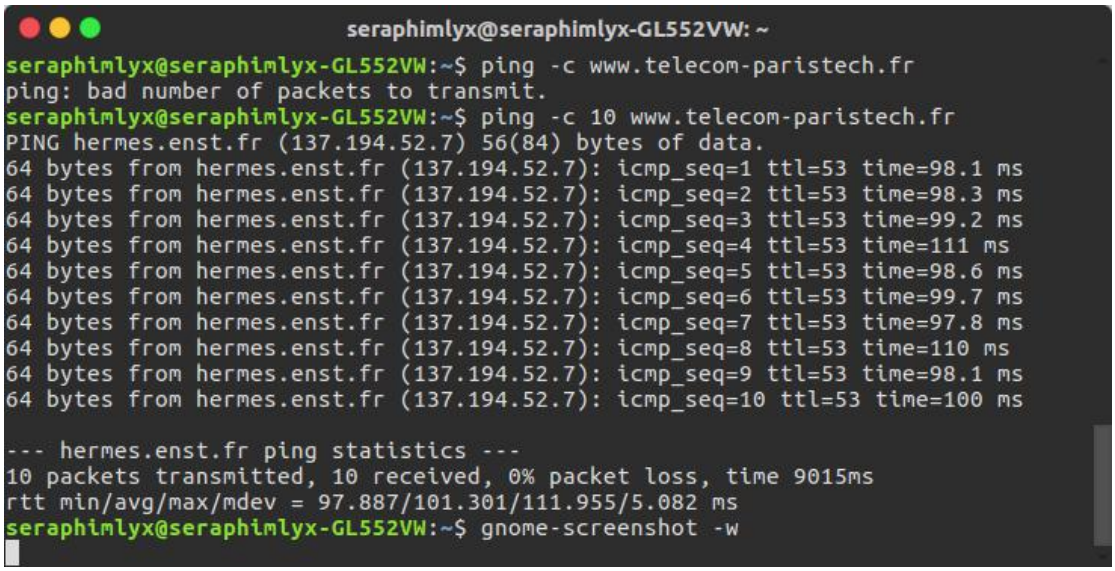
>>nmcli device show| grep DNS

>>IP4.DNS[1]: 129.100.74.79

>>ping 129.100.74.79

b) Ping www.telecom-paristech.fr . What is the IP address of the computer you pinged (2 Points)? What are the minimum (2 Points), average (2 Points) and maximum (2 Points) round trip times?

Answer:



IP Address-137.194.52.7

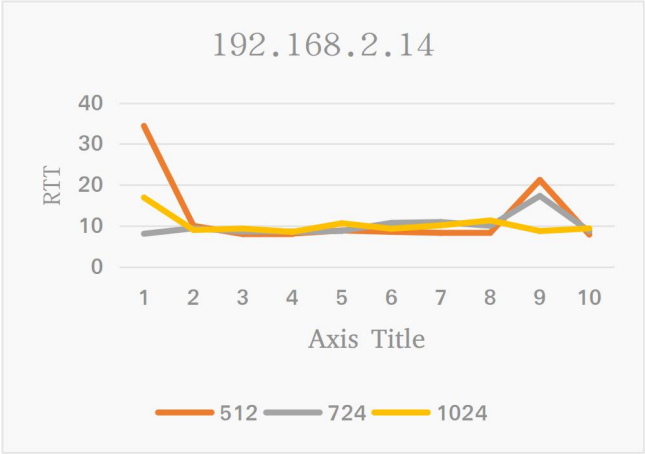
Min-97.887ms

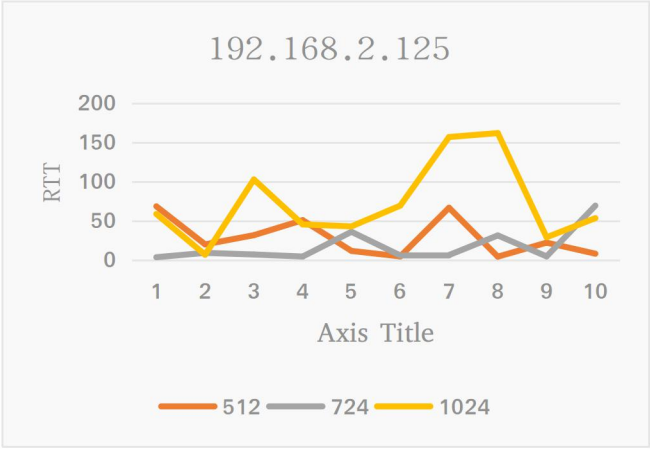
Avg-101.301ms

Max-111.955ms

c) Use ping to measure Round Trip Time (RTT) for 10 messages of size 512, 724,1024, and 4072 bytes. Use the "-f" configuration switch to make sure that the message is not fragmented. Graph the message size versus RTT for:

i) Two hosts on a LAN (two workstations in the lab or in your house)

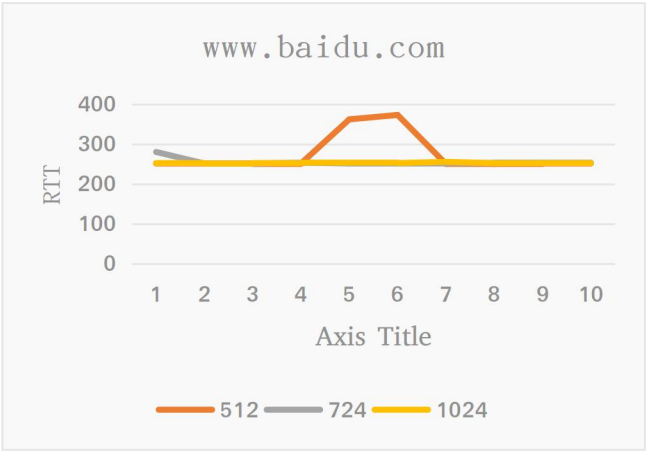


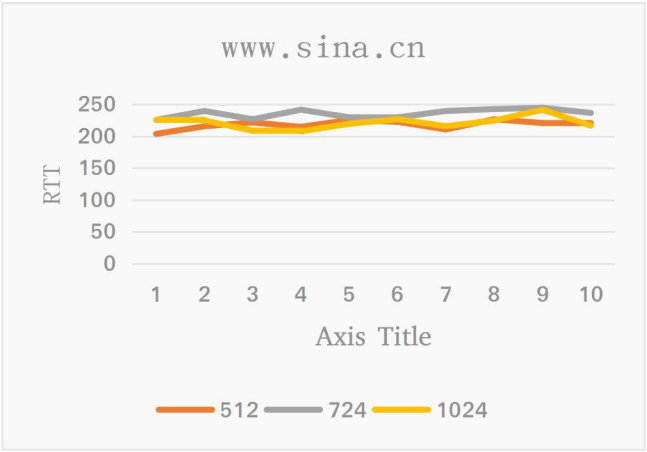


Answer:

	192.168.2.125		192.168.2.14	
	Average	Standard Deviation	Average	Standard Deviation
512	29.31	23.49	12.340	8.297
724	18.25	20.44	10.101	2.602
1024	73.24	49.51	10.314	2.357
4012	N/A	N/A	N/A	N/A

ii) Two nodes on a WAN (for instance, your workstation and a host in China)





	www.baidu.com		www.sina.cn	
	Average	Standard Deviation	Average	Standard Deviation
512	275.50	46.62	219.02	6.81
724	256.05	8.418	236.23	6.68
1024	253.79	1.275	221.99	9.482
4012	N/A	N/A	N/A	N/A

Analyze your results. Calculate the average and standard deviation for every destination.(4 Points) Discuss the effects of distance, message size, and their relationship with bandwidth and latency. (3 Points)

Answer:

Because of MTU = 1500, sending unfragmented data with 4072 bytes is restricted.

The distance will significantly affect the latency of the data transmission, which is called propagation delay. The equation of the propagation delay is d prop = d(distance)/s(speed). According to the data above, the delay to the Chinese hosts are much larger than that of the LAN hosts because of the distance.

The transmission delay can be described by d trans = L(packet length)/R(rate). We could see that the larger the packets or the smaller the bandwidth is, the bigger the transmission delay will be.

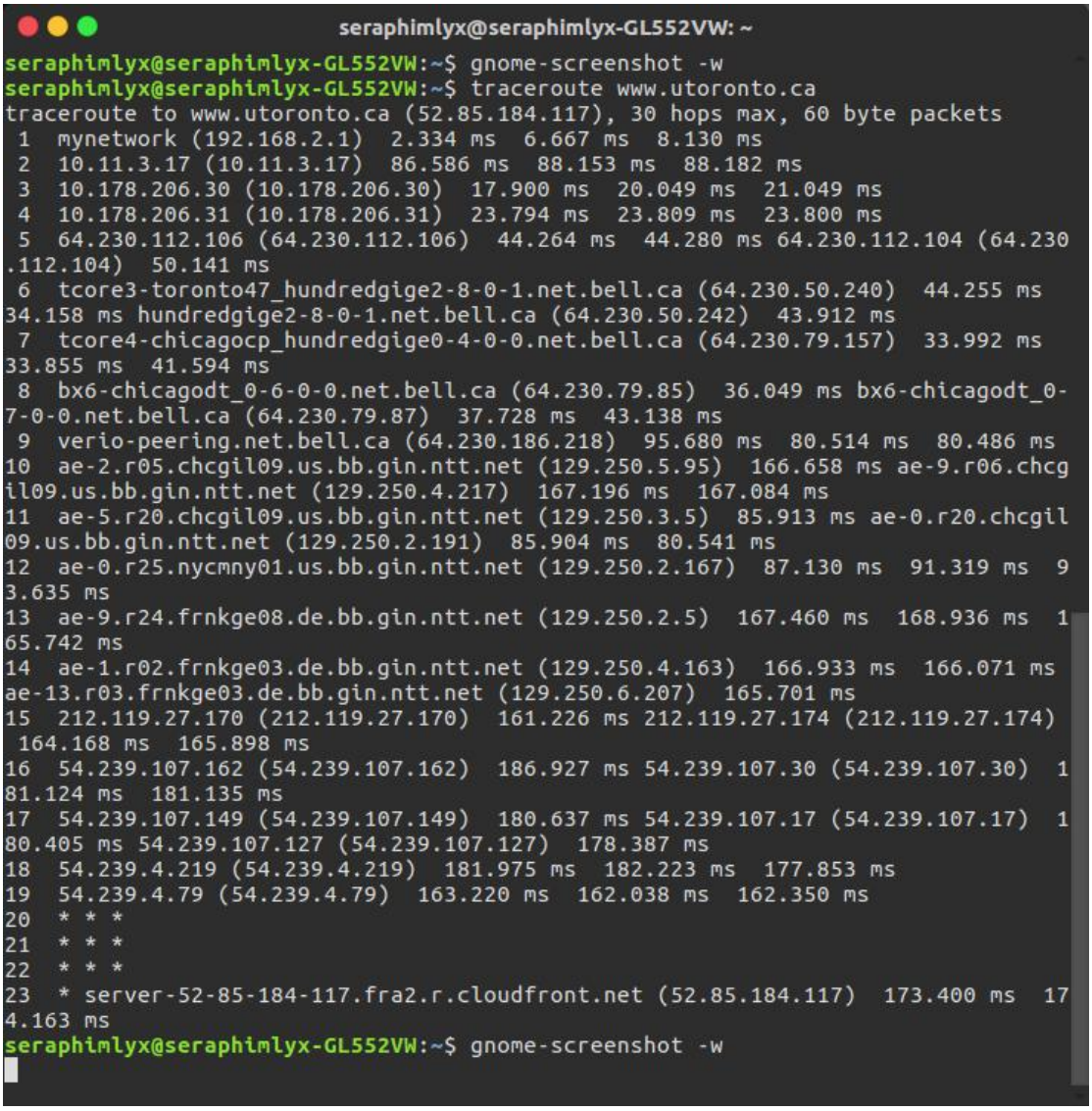
d) Use the tracert utility on your workstation to find the route to a host:

i) In Toronto: How many hops did it take to reach the destination host? (3 Points) How many ISPs did you traverse? (3 Points)

Answer:

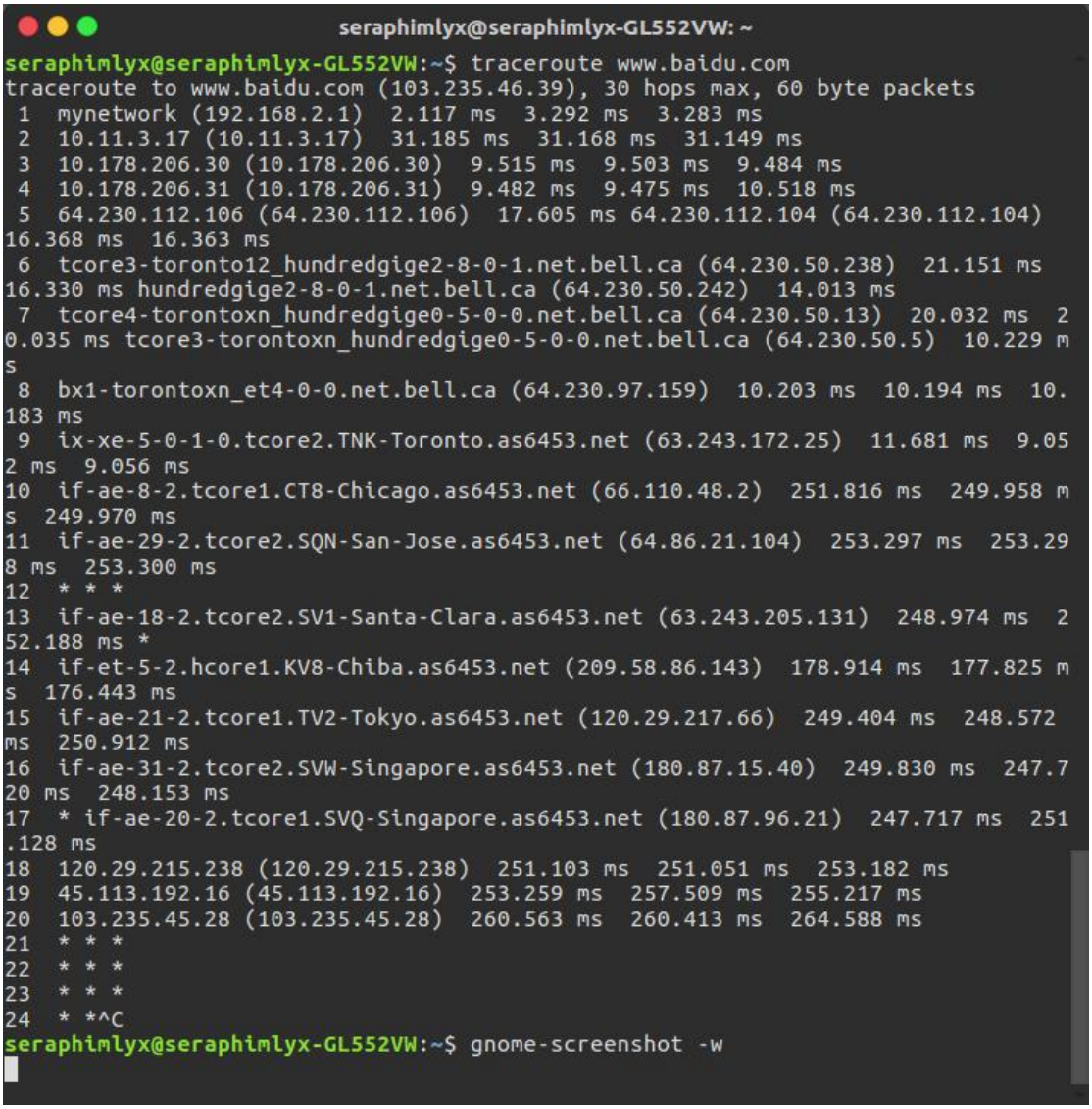
Typing traceroute https://www.utoronto.ca/ in the Terminal

The result is the picture below



We could see in the way to the https://www.utoronto.ca/, there are **23** hops for our request to go through as well as **4** ISPs are shown in the picture.

ii) In China: How many hops did it take to reach the destination host? (3 Points) How many ISPs did you traverse? (3 Points)



Answer: As we see, by using the command traceroute www.baidu.com to trace the request to the Chinese server, the terminal shows that **20** hops with **3** ISPs are needed to go by before the packets get to the destination.

The output of the command “traceroute” contains 6 columns.

The first one means the number of the hops.

The second and third one mean the ISP and its IP address respectively. If it is a LAN, the second column will show a IP address the same as the third column.

The forth to sixth column means the delay from one router to another.

When the ‘*’ comes out, it means that the router does not response to the probes. This is led by the lost of the probes or the not replying of the router.

e) Use the trace route utilities at the site

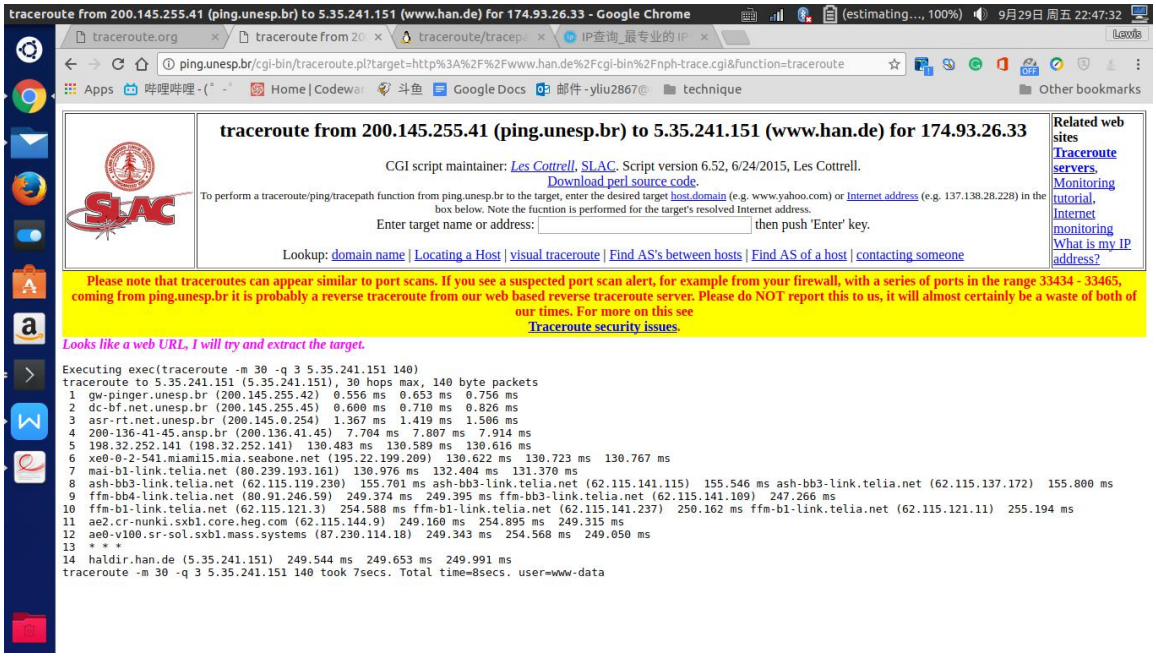
www.traceroute.org to find the routes between a host in Europe and a host in South America.

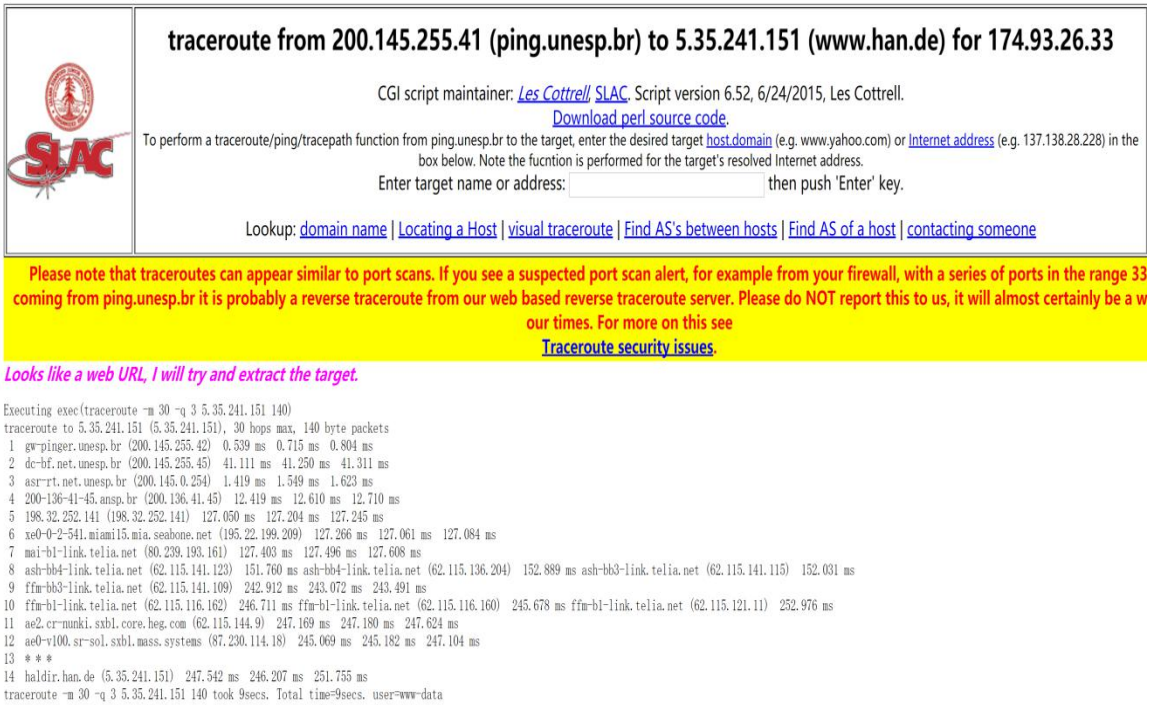
i) In 50 words, explain how tracert discovers a path to a remote host. (2 Points)

The traceroute uses TTL values. Starting from 1 for the first packet, the TTL values increase from packet to packet.When the packets reach the router, the TTL values decrease by 1 and send an ICMP error message to source when there is TTL value reach 0. Hence, the traceroute uses the error message to build a path until the destination is reached.

ii)Trace the route again between these two hosts after at least an hour.
Provide reasons why the two routes could differ. (3 Points)

Answer: The result of the trace is as picture below. These are the routes traced from Brazil to German. The hops 5 and 6 is in America between Brazil and German.





traceroute from 200.145.255.41 (ping.unesp.br) to 5.35.241.151 (www.han.de) for 174.93.26.33

CGI script maintainer: *Les Cottrell*, SLAC. Script version 6.52, 6/24/2015, Les Cottrell.
Download perl source code.
To perform a traceroute/ping/tracepath function from ping.unesp.br to the target, enter the desired target host.domain (e.g. www.yahoo.com) or Internet address (e.g. 137.138.28.228) in the box below. Note the fucntion is performed for the target's resolved Internet address.
Enter target name or address: then push 'Enter' key.

Lookup: domain name | Locating a Host | visual traceroute | Find AS's between hosts | Find AS of a host | contacting someone

Please note that traceroutes can appear similar to port scans. If you see a suspected port scan alert, for example from your firewall, with a series of ports in the range 33 coming from ping.unesp.br it is probably a reverse traceroute from our web based reverse traceroute server. Please do NOT report this to us, it will almost certainly be a w our times. For more on this see
Traceroute security issues.

Looks like a web URL, I will try and extract the target.

```
Executing exec(traceroute -m 30 -q 3 5.35.241.151 140)
traceroute to 5.35.241.151 (5.35.241.151), 30 hops max, 140 byte packets
 1  gw-pinger.unesp.br (200.145.255.42)  0.539 ms  0.715 ms  0.804 ms
 2  dc-bf.net.unesp.br (200.145.255.45)  41.111 ms  41.250 ms  41.311 ms
 3  asr-rt.net.unesp.br (200.145.0.254)  1.419 ms  1.549 ms  1.623 ms
 4  200-136-41-45.ansp.br (200.136.41.45)  12.419 ms  12.610 ms  12.710 ms
 5  198.32.252.141 (198.32.252.141)  127.050 ms  127.204 ms  127.245 ms
 6  xe0-0-2-541.miami15.mia.seabone.net (195.22.199.209)  127.266 ms  127.061 ms  127.084 ms
 7  mai-b1-link.telia.net (80.239.193.161)  127.403 ms  127.496 ms  127.608 ms
 8  ash-bb4-link.telia.net (62.115.141.123)  151.760 ms ash-bb4-link.telia.net (62.115.136.204)  152.889 ms ash-bb3-link.telia.net (62.115.141.115)  152.031 ms
 9  ffm-bb3-link.telia.net (62.115.141.109)  242.912 ms  243.072 ms  243.491 ms
10  ffm-b1-link.telia.net (62.115.116.162)  246.711 ms ffm-b1-link.telia.net (62.115.116.160)  245.678 ms ffm-b1-link.telia.net (62.115.121.11)  252.976 ms
11  ae2.cr-nunki.sxb1.core.heg.com (62.115.144.9)  247.169 ms  247.180 ms  247.624 ms
12  ae0-v100.sr-sol.sxb1.mass.systems (87.230.114.18)  245.069 ms  245.182 ms  247.104 ms
13  * * *
14  haldir.han.de (5.35.241.151)  247.542 ms  246.207 ms  251.755 ms
traceroute -m 30 -q 3 5.35.241.151 140 took 9secs. Total time=9secs. user=www-data
```

The difference of the routes may be caused by the stuck or the no response of the routers on the path. From one router to another, if there is a heavy congestion or no response on the path, then the router will calculate another better way to transmit the data, which is so-called “load-balance”.

f) Briefly discuss why ping would not necessarily provide an accurate estimate of the round trip time for packets exchanged by two hosts on the Internet?

Answer: Ping relies on the ICMP protocol to test the reachability.

However, because of the “load-balance” of the router, the destination you ping will not necessary go on the same path, which affect the accuracy of the RTT. Besides, QoS(Quality of Service) will also affect the consistency of the the ICMP replies.

g) List at least three other such utilities and briefly describe their use. (9 Points; 3 Points for each utility)

In Linux:

1. ifconfig: ‘Ifconfig’ is used to set the network interface and get their information.
2. nslookup: ‘nslookup’ command is used to check the IP address and its domain name it associates.
3. namp: ‘namp’ can allow user to scan the IP address of all the hosts connected in a specific range of IP area.