Lab Exercise 1: Tools of the Trade

Exercise 1: nslookup

Use the nslookup command from the "Tools of the Trade" and answer the following questions:

1. Which is the IP address of the website www.koala.com.au? In your opinion, what is the reason for having several IP addresses as an output?

104.21.45.210

172.67.219.46

Koala has set up two web servers across Australia to reduce the pressure of a single server and give users a better experience. Therefore, it has two different IP addresses. The DNS server will resolve the domain name to the IP address of the nearest koala and provide services.

2. Find out the name of the IP address 127.0.0.1. What is special about this IP address?

It is localhost. On almost all computers, use 127.0.0.1 as their own address, but it won't be used the real IP address during the communicating between this computer and other devices.

Exercise 2: Use ping to test host reachability

Are the following hosts reachable from your machine by using ping:

www.unsw.edu.au

ping: 64 bytes from server-18-67-93-97.syd62.r.cloudfront.net (18.67.93.97): icmp_seq=1 ttl=244 time=1.61 ms

www.getfittest.com.au

ping: unknown host www.getfittest.com.au

nslookup: ** server can't find www.getfittest.com.au: NXDOMAIN "

This website does not exist or the URL has the spelling error, it cannot find the matching IP address with this website, Therefore, it cannot send any package to test ping.

www.mit.edu

64 bytes from a104-74-47-237.deploy.static.akamaitechnologies.com (104.74.47.237): icmp_seq=1 ttl=56 time=1.33 ms

www.intel.com.au

64 bytes from a104-98-21-56.deploy.static.akamaitechnologies.com (104.98.21.56): icmp_seq=1 ttl=56 time=1.34 ms

www.tpg.com.au

64 bytes from 104.18.10.61: icmp_seq=1 ttl=56 time=1.97 ms

www.hola.hp

ping: unknown host www.hola.hp

nslookup: ** server can't find www.hola.hp: NXDOMAIN "

This website does not exist or the URL has the spelling error, it cannot find the matching IP address with this website, Therefore, it cannot send any package to test ping.

www.amazon.com

64 bytes from server-18-67-91-221.syd62.r.cloudfront.net (18.67.91.221): icmp_seq=1 ttl=244 time=1.56 ms

www.tsinghua.edu.cn

64 bytes from www.tsinghua.edu.cn (166.111.4.100): icmp_seq=1 ttl=45 time=201 ms

www.kremlin.ru

13 packets transmitted, 0 received, 100% packet loss, time 12264ms

This website is existed and it can work when I use the browser to open it. It is a website to introduce Kremlin and Red Square which belongs to Moscow government. When I ping this website, the server can be found but the request timeout. The website may allow the request of visiting, but any router or firewall between I and the server try to block my pings when it found that user only want to ping their server. It may do for security to reduce the probability of server attack like DDoS Attack.

8.8.8.8

64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=1.79 ms

Exercise 3: Use traceroute to understand the network topology

Note: Include all traceroute outputs in your report.

1. Run traceroute on your machine to www.columbia.edu . How many routers are there between your workstation and www.columbia.edu ?

24 routers

How many routers along the path are part of the UNSW network?

1 cserouter1-server.cse.unsw.EDU.AU (129.94.242.251) 0.066 ms 0.305 ms 0.284 ms

2 129.94.39.17 (129.94.39.17) 1.129 ms 1.131 ms 1.425 ms

3 ombudnex1-vl-3154.gw.unsw.edu.au (149.171.253.35) 16.921 ms libudnex1-vl-3154.gw.unsw.edu.au (149.171.253.34) 2.230 ms 2.220 ms

4 libcr1-po-5.gw.unsw.edu.au (149.171.255.165) 1.287 ms ombcr1-po-5.gw.unsw.edu.au (149.171.255.197) 1.341 ms ombcr1-po-6.gw.unsw.edu.au (149.171.255.169) 1.420 ms

5 unswbr1-te-2-13.gw.unsw.edu.au (149.171.255.105) 1.379 ms unswbr1-te-1-9.gw.unsw.edu.au (149.171.255.101) 1.386 ms 1.386 ms

6 138.44.5.0 (138.44.5.0) 1.512 ms 1.344 ms 1.324 ms

7 et-0-3-0.pe1.alxd.nsw.aarnet.net.au (113.197.15.153) 1.818 ms 1.755 ms 1.805 ms

There are 5 Routers which was a part of UNSW. 7th router is not owned by UNSW because domain name is not owned by UNSW. 6th router has only an IP address, which can be found through the Network Location Tool. It belongs to central Australia, so it is not owned by UNSW. 2nd router also has only IP address, but according to the fact that the address is near Darlinghurst, and 1st router and 3rd router belong to UNSW, it can be inferred that 2nd router belongs to UNSW.

Between which two routers do packets cross the Pacific Ocean?

8 et-0_0_2.bdr1.guam.gum.aarnet.net.au (113.197.14.137) 71.684 ms 71.673 ms 71.710 ms

9 * * *

10 * * *

11 fourhundredge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.1.30) 237.811 ms * fourhundredge-0-0-0-21.4079.core1.salt.net.internet2.edu (163.253.1.28) 237.363 ms

Between 8th routers and 11th router the delay had an extremely crease. The position of the 8th router is in Australia and 9th and 10th routers had been hoidened. The 11th router's IP address is the American's domain name. Therefore, it must cross the Pacific Ocean.

2. Run traceroute from your machine to the following destinations:

(i) www.ucla.edu (ii) www.u-tokyo.ac.jp and (iii) www.lancaster.ac.uk . At which router do the paths from your machine to these three destinations diverge?

1st, 2nd: All the data packets pass the same router. 1st (129.94.242.251) 2nd (129.94.39.17)

3rd: Three packets which sent to the University of Tokyo passed (149.171.253.35) the different router which is the same place as others. (149.171.253.34)

4th: The first two packets sent to Lancaster University and the 2nd and 3rd packets which sent to the University of Tokyo passed (149.171.255.169) the different router which is the same place as others. (149.171.255.197)

5th: The first two packets sent to University of Tokyo and the 2nd packets which sent to the Columbia University passed (149.171.255.105) the different router which is the same place as others. (149.171.255.101)

6th: All the data packets pass the same router. (138.44.5.0)

After the 2nd router, some packets were diverged and pass the different router, but all of router which they passed were in the same place. At the 6th router, all the packets reunited and after that, the packets are distributed to the three destinations diversion.

3. Several servers distributed around the world provide a web interface from which you can perform a traceroute to any other host on the Internet. Here are two examples: (i) http://www.speedtest.com.sg/tr.php and (ii) https://www.telstra.net/cgi-bin/trace . Run traceroute from both these servers towards your machine and in the reverse direction. You may also try other traceroute servers from the list at www.traceroute.org . What are the IP addresses of the two servers that you have chosen?

Name: www.speedtest.com.sg IP Address: 202.150.221.170

Name: www.telstra.net IP Address: 203.50.5.178

Does the reverse path go through the same routers as the forward path?

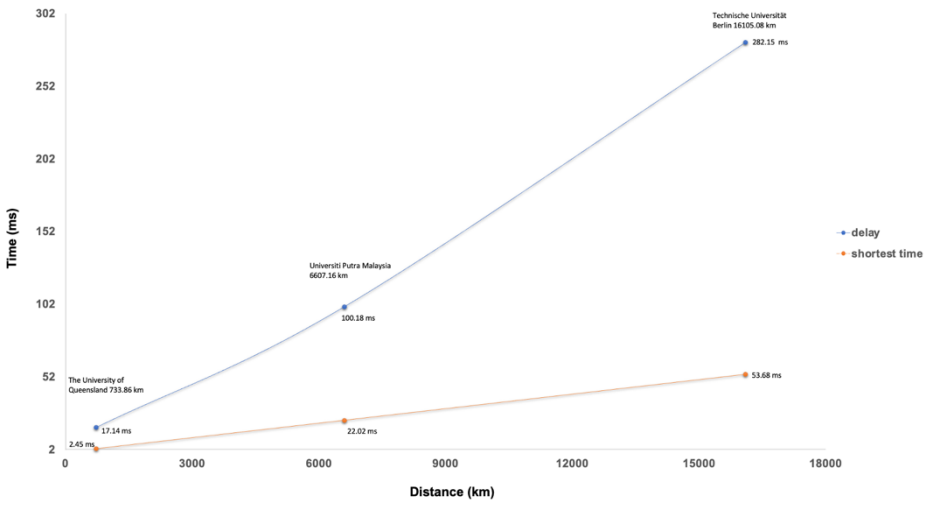
NO!

If you observe common routers between the forward and the reverse path, do you also observe the same IP addresses? Why or why not?

In my opinion, common routes between the forward and the reverse path may have the same IP address, because each router only manages the next route to be delivered according to the network status. However, according to the results, although the routers and the IP address are different, these routers are in the same area and the IP address is quite close. The router has a smaller probability of having the same IP address because routers have many choices.

Exercise 4: Use ping to gain insights into network performance

1. Plot a graph where the x-axis represents the distance to each city and the y-axis represents the ratio between the minimum delay as measured by the ping program and the shortest possible time T to reach that city from UNSW.



$$T_{UQ} = \frac{733.86\text{km}}{3 * 10^8 m/s} = \frac{733860\text{m}}{3 * 10^8 m/s} \approx 0.00245s = 2.45ms$$

$$T_{UPM} = \frac{6{,}607.16\text{km}}{3 * 10^8 m/s} = \frac{6{,}607160\text{m}}{3 * 10^8 m/s} \approx 0.02202s = 22.02ms$$

$$T_{Tu-Berlin} = \frac{16{,}105.08\text{km}}{3 * 10^8 m/s} = \frac{16{,}105080\text{m}}{3 * 10^8 m/s} \approx 0.05368s = 53.68ms$$

2. Is the delay to the destinations constant or does it vary over time? Explain why.

According to the results, it can be found that the delay to the destinations is not constant and does not vary over time. It can be seen that the different sizes of packets have little impact on the delay. The delay time of all results is very close, but they are irregular and random. Therefore, queuing delay may be the main factor leading to delay instability. When the passing router is not congested, the delay will be slightly lower than the average, otherwise it will be higher than the average.

3. The measured delay (i.e., the delay you can see in the graphs) is composed of propagation delay, transmission delay, processing delay and queuing delay. Which of these delays depend on the packet size and which do not?

Transmission delay depends on the packet size, transmission rate and bandwidth of medium.

Queuing delay depends on the congestion, server load status and the number of unprocessed packets.

Processing delay depends on the packet size and the processing speed of the switch.

Propagation delay depends on the distance between the sender and the receiver.