Lab 01 - Ryan McClue (z5346008)

1. Nslookup

1. The domain `www.koala.com.au` has 2 IP addresses: `104.21.45.210` and `172.67.219.46` In my opinion, the reason for having several IP addresses as an output is for load balancing reasons. Specifically, there are several webservers for the domain to allow traffic be distributed across multiple resources.

2. The IP address `127.0.0.1` is also known as localhost or the loopback device. It's purpose is to provide an interface that allows a host to interact with its own network services. Applies to all addresses with CIDR `127.0.0.1 /8`

2. Ping

- **www.unsw.edu.au:** reachable.
- **www.getfittest.com.au:** unreachable; unreachable via web browser as domain has no registered DNS records
- **www.mit.edu:** reachable
- **www.intel.com.au:** reachable
- **www.tpg.com.au:** reachable
- **www.hola.hp:** unreachable; unreachable via web browser as not domain not registered under `.hp` name server, rather `.com`, i.e. `www.holahp.com` is accessible
- **www.amazon.com:** reachable
- **www.tsinghua.edu.cn:** reachable
- **www.kremlin.ru:** unreachable; reachable via web browser as server is configured to reject ping ICMP packets but to serve web pages
- **8.8.8.8:** reachable; not reachable via web browser as IP represents Google's Public DNS server and is therefore not configured to serve web pages.

3. Traceroute

1. There are 23 routers between my workstation and `www.columbia.edu`. There are 5 routers along the path that are part of the UNSW network. Between routers 8 and 9 do packets cross the Pacific Ocean.

2. The router at which the paths from my machine to the 3 destinations diverge is `138.44.5.0` This router is part of the *Australian Academic and Research Network*, the ISP that serves UNSW. The number of hops on each path is not proportional to distance. Routers physically close to one another and others separated by large distances are interleaved with each other in each path.

3. The IP of *www.speedtest.com.sg* is `202.150.221.170` (lab tutor mentioned only required to do 1 traceroute web service)
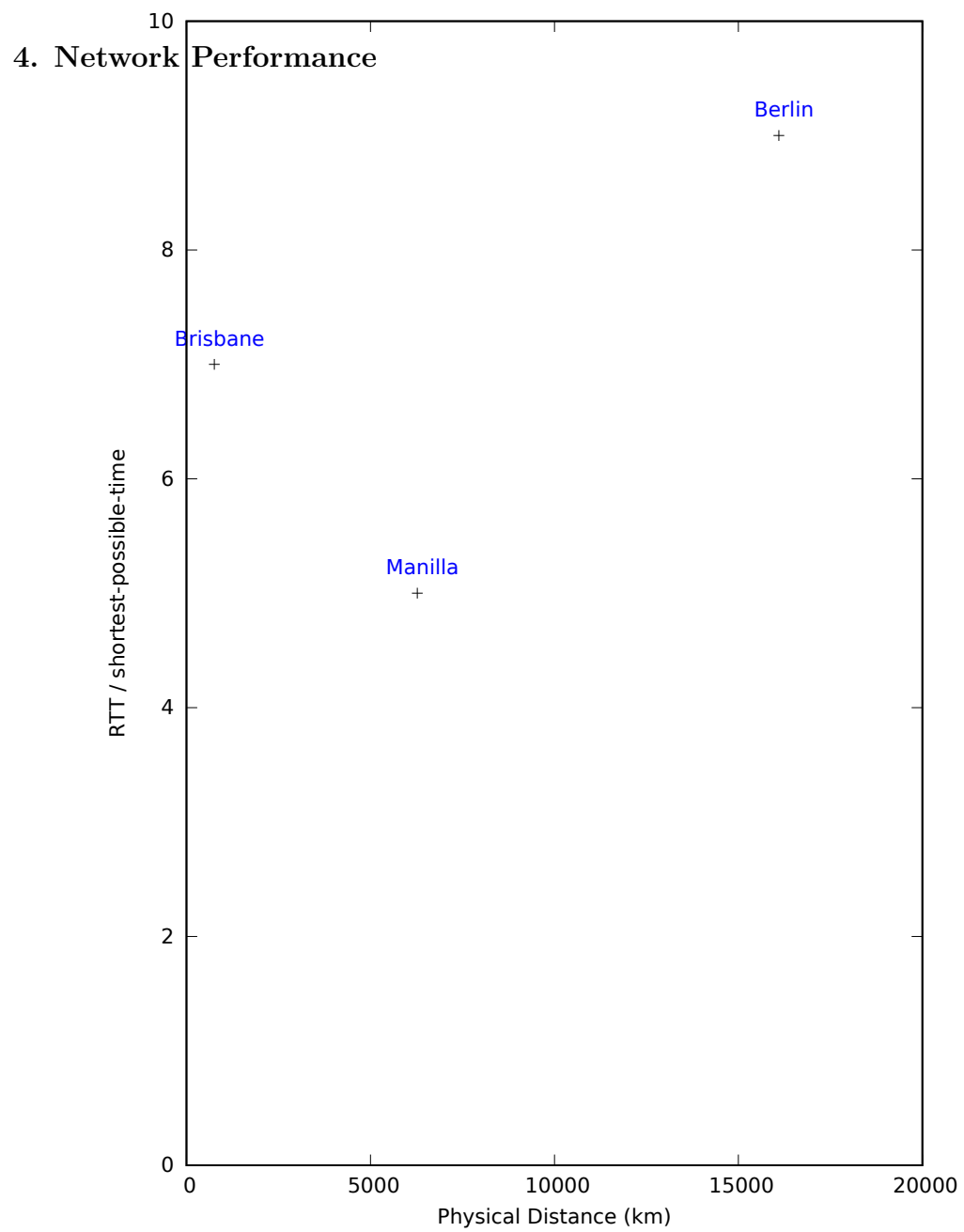
The reverse path does not go through the same routers as the forward path. This is because of different routing tables used by the access ISPs serving my machine and the web traceroute service. Furthermore, how a packet is routed through a network is dependent on network congestion. The state of the network when each traceroute is performed is different, therefore yielding a different path. Although no common routers between my particular reverse and forward paths, a single router has multiple interfaces. This is because routers route between different networks, therefore requiring different IP addresses to interface between multiple networks.

> if traceroute ' ' *out, what does this mean? just use last IP for determining location?* " and further traffic indicates it did pass router if ' ' *tail at end, routers sensititve to information leaking and cannot say where it ends how does it give a* " and then continue onwards?
>
> car keys use Zigbee. holding to head increases signal strength

3. determine public ip with: `dig +short myip.opendns.com @resolver1.opendns.com`

(observe RTT; geolocation data from IP can be deliberatley forged for security reasons) (different end result due to many end router destination server possibilities) > IANA to regional, APNIC, ARIN, etc. > interesting get 'direct IP not allowed' when using last IP given by traceroute for domain > how do geolocation tools like yougetsignal work?

4. Network Performance

The chart plots RTT / shortest-possible-time versus Physical Distance (km), with the y-axis ranging from 0 to 10 and the x-axis from 0 to 20000.

Data points:
- Brisbane (~756 km, ~7)
- Manilla (~6,273 km, ~5)
- Berlin (~16,100 km, ~9.2)

brisbane: 756km, 17.5ms / 0.00252secs (7) manilla: 6,273km, 1.5ms / 0.02091
() berlin: 16,100km, 279ms / 0.0537 (5)

1. Reasons for y-axis being larger than 2 is because ping command measures round-trip-time, while shortest possible time is end-to-end. Furthermore, there is associated nodal delay as the packet is routed, e.g. processing + queueing + transmission delays
2. Delay to destinations varies over time. Packets take different routes of different times based on network conditions, e.g. congestion. As network conditions are not constant, the delay will not be constant.
3. Transmission delay depends on packet size. Propagation delay, processing delay and queuing delay don't.

processing delay: inspecting header to determine where packet needs to go. (fixed number based on header size, e.g UDP less bytes thans TCP) queuing: depends on number of packets