

# Networked Systems Laboratory Exercise 3

Ken Li (2131620)

## IP addresses

- 20 sites were used in this exercise.
  - 12 out of 20 sites had more than one IP address.
  - 3 out of 20 sites had an IPv6 address.
- Multiple addresses can indicate:
  - The usage of multiple servers:
    - This increases robustness of the site. If one server fails, the domain name can resolve to another working one until the failing server is fixed.
    - This allows for load balancing. If a particular server is receiving an overwhelming amount of traffic, connections to it can be rerouted to another server that can handle the load.
  - The usage of both IPv4 and IPv6:
    - Some sites offer IPv6 versions in addition to IPv4, such as `ipv6.google.com`.
- When running `dnslookup`, IP addresses for the some domain names differed based on both time and location.
  - The result changes over time due to the current network load. The server corresponding to a previously-returned IP address could now be overloaded, so another server's IP address is returned instead.
  - The result changes depending on location due to the position of the source in the network. This difference could mean that a different server from before is now considered the "best" choice (e.g. a decision that could involve the shortest path), so that is returned instead.

## Router-level topology maps

- The longest path is 22 hops, which appears in the IPv4 map.
- Paths from different locations to the same destination are typically not disjoint, since the path to destinations generally converge into a single sequential path.
- In most cases, there is only one route to a destination. However, cycles exist in a few spots in the IPv4 map, which means that there can be multiple paths to some specific destinations.
- All paths to final destinations go through a short sequential path before splitting into many main sub-trees. This starting sequential path is likely local to the University of Glasgow, before splitting into addresses owned by ISPs in the UK. From there, the map splits into many self-contained sub-trees. All nodes in each of the main sub-trees typically share an IPv4 prefix, indicating that all of these addresses belong to a single organisation and correspond to a part of the world (e.g. North America).

## IPv4 and IPv6

- The IPv4 and IPv6 maps share the same overall structure. The IPv6 map is significantly smaller in scale, but it shares many characteristics with the IPv4 map. The source address follows a sequential path before splitting off into one of many sub-trees. Most nodes only have one child, especially those close to the leaves of the graph, indicating many sequential paths. A few nodes have many children, and such addresses seem to act as major intersections, perhaps as the "entrance" address to another continent.

- The similarity between maps is expected, since both IPv4 and IPv6 internets are likely to share a similar topology due to the constraints of the geography of Earth. There are more likely to be many smaller connections within a continent or landmass, and few major connections over large bodies of water.

## The traceroute tool

- ICMP is a network protocol used for communicating non-data information between routers such as errors and status messages. It is commonly used for diagnostic purposes, such as in traceroute.
- traceroute sends many dummy UDP packets to the destination. The packets' TTL (Time to Live) values are gradually increased from low to high. When a packet's TTL has been exceeded, whatever intermediate router the packet has reached will discard it and send an ICMP Time Exceeded message back to the source of the packet.
- Very small TTL values are sent to intentionally trigger a Time Exceeded ICMP message before the packet reaches the destination. This message reveals the IP address of the router that sends the message. The TTL value is varied from small to high to trigger such a message from every router along the path to the destination, thus building the trace of IP addresses to the destination.
- Packets are sent until a Echo Reply ICMP message is received, indicating that the packet has reached the destination, and therefore the trace is complete.