Networks AE Report

IP Addresses

When running dnslookup on certain domains I did find that multiple sites had multiple different IP addresses. One reason is that some sites have both IPv4 and Ipv6 addresses hence they will have one for each type. The reason a site may have multiple Ipv4 addresses or multiple Ipv6 addresses is that a company may use a content distribution network (CDN), which allows the company to host content for their customers in web caches that are in multiple different locations around the world hence there is then multiple ip addresses for wherever each of these different locations are storing data. They do this as it reduces load on main servers and puts it on to the CDN so it can distribute the load across multiple channels which in turn prevents overloading for high traffic volumes, it reduces the latency of requests as the CDN will have a cache near to the person making the request and reduces the chance of a denial of service attack.

When running dnslookup several times I found that I always got the same ip addresses being returned as I am running from the same location. However if I was to run dnslookup from different locations I should expect to see different ip addresses returned as the command would go through a different route due to nature of CDN splitting load across multiple locations. Another reason ip addresses may always be returned as the same is that due to the caching undertaken by CDN then it should always look for the address that is closes to the user.

I found that when running dnslookup that there was a smaller proportion of sites that had an IPv6 address, this is because IPv6 is a newer standard and Ipv4 has been around much longer, hence more sites will have an Ipv4 address but may not have an Ipv6. Of the Ipv4 sites that I looked up using dnslookup I found that 80% had an Ipv6 address but I was also trying to keep my traceroute analysis of the domains as consistent as possible.

Router-level Topology Maps

For my router level topology map for Ipv4 addresses I found the longest path to be 14 addresses. From looking at the graph I gathered that there weren’t multiple routes to the same address and that all addresses eventually ended made there way to an end addresses although this occurred at different levels of tree structure that was produced. I noticed also that initially the addresses followed a linear path then began to split off to multiple nodes which carried out until all addresses reached a final node.

For my router level topology map for Ipv6 addresses I found the longest path to be 13 addresses. There was not multiple routes to the same address. However the main difference I noticed with the Ipv6 map was that there was a longer chain of linear addresses before they split off into other tree nodes.

IPv4 and IPv6

From analysing both my router level topology map for Ipv4 and Ipv6, I found that they did not match in terms of structure and length. As stated above, the Ipv6 map had a more liner structure before splitting into only 3 other tree nodes which then other nodes in a linear formation each of them. Where as I found that for Ipv4 there was a wider spread of nodes with larger depth for each node.

The graphs did not match which was expected as Ipv4 and Ipv6 are different networks that are not interchangeable.

The Traceroute tool

Traceroute is a command that traces the path that data packets take from their source to their destination. It maps the route the data takes from a specific sever and when data is transmitted from two points it “hops” through multiple devices. Traceroute maps each hop and provides details along with the round trip time RTT. Traceroute also uses the TTL (Time To Live) field in the packet header, the TTL is the number of hops that a packet is set to exist inside a network and is reduced by 1 each time a packet is forwarded by a router and when it reaches 0, that packet is discarded. Now traceroute uses ICMP time exceeded messages to trace a network route. During IP the TTL is used as above described to avoid routing loops. Traceroute takes advantage as say we have a address that is 3 hops away, then the source traceroute sends a packet with TTL 1. The address it reaches, makes the TTL 0 and sends back a time exceeded message to the root source and hence we identify address 1 of 3. This processes continues until we reach the destination and all other addresses along the way are identified.