Network Systems (H) Assessed Exercise 2 Report

IP Addresses:

While running the DNS lookups on different websites, I noticed that some of the websites (the larger scaled ones, for example Google) have more than one IP. This is due to the fact that the website is a giant, meaning that it has many servers in order to be able to function with all its users without the need for them to wait, and without crashing with overflowing requests. Another observation that I noticed was that when I ran DNS lookup more than once I did not get the same IP for the given website each time (not on all websites). Again I will give an example with Google. I believe that happens, because it puts me to a different server each time depending on the load on all servers, and a different server means a different IP. When running the DNS lookup for the same website, but from a different location, again depending on the website, sometimes I would get different IP's. This is due to the fact that some websites (usually the ones that are being hosted by larger companies) have multiple servers in different locations, and you get connected to the closest most suitable one. Although this is not the case for all websites. Some smaller websites, for example somebody running a blogging website from his home, will have only his IP. From the number of websites that I ran my test, only one third of them had IPv6. I have ran my DNS lookup on total of 9 websites.

Router-level Topology Maps:

I will be discussing the IPv4 topology map in this section, because it is easier to give examples and answer most of the questions.

The longest path that I have from source to destination is 10. It is the path from my home IP to one of Moodle's IP's. Although when I ran traceroute on moodle's IP's I got a consecutive sequence of * in the end meaning that a firewall was blocking my traceroute to finish. Since I ran all the DNS lookups/traceroutes from home I did not have different locations to compare, but I assume that the path will be disjoint to some level if I have ran DNS lookup/traceroute to the same website but from a different location, because of the reasons mentioned in the above paragraph. From close inspection we can observe that there are multiple routes to some of the destinations. They can be observed on the left-hand side of the graph. When taking a look at the graph, it is easy to see which IP's are from the same ISP, and then it can be observed that on different levels the IP's change drastically.

IPv4 and IPv6:

The topology maps of the different protocols do not match. While the addresses between IPv4 and IPv6 are different, their structures differ as well. I did not expect them to have the similar structure. Since not all website support IPv6, there will be different routes to them. If we compare for example one of the routes from my home address to one of the Google' destination addresses in the IPv4 topology map to the route in the IPv6 map, we see that the path in IPv6 is shorter. Another thing to take note for is that while websites have different and many IPv4 IP's, they only have one IPv6.

The traceroute Tool:

The traceroute tool generally can use two types of packets to send, either UDP or ICMP Echo request. In this case I will discuss the ICMP Echo request packets. The traceroute tool uses TTL (time to live) value to determine the routers in between the source and destination addresses. How it operates is that each router in the path decrements the given TTL value. For example I have address A and want to reach address D (let's assume B and C are the routers in the path between source A and destination D). Traceroute initially sets the TTL value to 1, when that packet is received by router B, it decrements the TTL value, and if that value is 0 return an ICMP (internet control message protocol) Error: ICMP Time Exceeded. Now traceroute knows that router B is 1st, and now again traceroute sends a packet but this time with an incremented TTL value, in this case TTL = 2. The packet passes through address B because after it decrements the TTL value is greater than 0 so it continues onwards. After it reaches the next router (C) the TTL value is 0 and again an ICMP Time Exceeded error is return. Finally the TTL value sent from the source is 3, it reaches the destination address D, and an ICMP Echo Reply message is returned meaning that traceroute has reached the final destination.