Networked Systems (H) 2020-2021 – Exercise 2 Report

2359451d

11 March 2021

IP addresses

Obviously, some sites have several IP addresses to access. A typical example is "www.netflix.com" with more than two of IPv4 and Ipv6 address. There could be several purposes involved why a server has multiple IP addresses. When it comes to a server need to process large scale access and traffic, it is important to achieve load balancing where the balancer forwards user requests to a available server IP address. So the service proceeds when one IP is down as users is forwarded to other IP. It is more maintainable with a server using multiple addresses rather a shared one. When an attack exists on the shared IP, it is hard to troubleshoot the source if several websites hosted on it. It is same for a blocked shared IP as all the services running on it would be affected.

Run dnslookup program several times, sometimes IP address for the same host-name would differ. The output depends on DNS server chosen and its corresponding load balancing algorithm used. DNS server also provide the hostname resolution in terms of geographical locations where chooses the nearest server address. So if run the look up in different locations it would change (DNS server chosen is a factor as well).

Conduct the DNS look up of 16 websites in total and only 6 of them supports IPv6 address, that is about 6/16=0.375=37.5%.

Router-level Topology Maps

The longest path of IPv4 topology map is trace-route to 114.31.62.190("www.koreaherald.com"). And that of IPv6 topology map is 2a01:578:0:4006:8000:0:6442:8a7 with trace-route to "www.netflix.com".

It can be seen from the leftmost bottom part of IPv4 topology that from different locations to the same destination sometimes overlaps. When trace to 104.193.88.5, the path is divided into two with 63.218.178.58 and 63.223.60.58 somehow then they are join together again to the IP 63.219.23.98 later.

There are multiple routes to the same destination. For example, if tracing the route to 148.153.34.38, which is at the bottom center of the IPv4 router topology, along the trace path, when the packet arrives at 212.187.174.237 and next hop could be either 154.54.57.153 or 154.54.58.173.

When the IP prefix largely changed, the node might be network boundary. For example, trace route to IP 104.193.88.5 along the path, the first notable change exists between 130.209.2.114 and 146.97.154.1 which means they are the border routers in their own network. Then change again happens between IP addresses 195.66.236.167(where belongs to 146.97.xx.xxx network) and 63.218.178.58/63.223.60.58. And so forth for 63.219.23.98 and 104.193.88.5.

IPv4 and IPv6

IPv4 and IPv6 topology map match and has similar structure where both exist multiple paths to the same destination and some paths are disjoint but sometimes would join together again at some points. This is true may because there still is a requirements of transit rom IPv4 to IPv6 addresses gradually. And the most direct way to implement it requires the nodes support dual-stack protocol technique where user can benefit from IPv6 but also able to communicate with those using IPv4. So a similar topology structure would be more flexible to satisfy the need. Obviously, it is hard to deploy IPv6 if a completely different structure used.

The traceroute Tool

Traceroute is a tool to find out all the routers from host to the destination. It relies on sending the packet where has set the TTL(Time to Live) header to the router. Each time the packet reaches to a router, the TTL counter decrement by 1, when it decreases to 0, router discards the packet and send a time exceeded response to the source along with its IP address. Thus set different TTL in the packet, and repeat increment the TTL number till the packet arrives the destination, all the routers could be found.

ICMP packet is used to send the control message between host and routers, including the error message and etc. Core fields of ICMP is Type and Code where indicates packet type and its subtype. It is a part of IP, since IP is not reliable where cannot guarantee whether IP datagram can reach the destination so if choose to send ICMP packet, when it runs into error, the router sends a ICMP packet to the source, reporting errors.

Traceroute can be based on the UDP and ICMP pakcets, when Traceroute sends UDP packet with a large destination port and the packet arrives at the destination with TTL 0, router discards the packet then send a ICMP packet of Type=3, Code=3 to the source, indicating the destination port is unreachable. Thus, the source knows the packet already reaches the destination and records the destination IP address, finishing the tracing. However, sometimes the destination may not support UDP service or packet blocked by the firewall, so there exist situations where packets actually arrives at the destination but won't stop increasing the TTL since unable getting any response from server. In this case, could consider using ICMP echo request where the server sends ICMP echo reply as the response. Also, could consider TCP traceroute where sends the SYN packet to probe and cross the firewall as it seems like a normal TCP connection.