Unit 3 Reflection

This unit introduced the basics of networking that includes understanding of Open Systems Interconnect (OSI) and the TCP/IP networking model. A network facilitates communication between multiple connected devices which transmit data via *packets* using a specified *protocol.* Two vendor-independent network protocols are the OSI seven-layer model (developed by the ISO organisation) and TCP/IP (developed by the US Department of Defence). TCP/IP is the most well-known model today mainly because by around 1983 TCP/IP was baked into the UNIX operating system which was leveraged by universities and research institutes and because ARPANET switched from NCP to TCP/IP around this time too (Maathuis & Smit, 2003). To communicate with devices across different networks, routers (operate at OSI layer 3and connect to Service Providers' Wide Area Network) route data packets based on logical addresses; bridges are used to link two LAN networks and route data packets based on physical addresses; gateways connect two networks that have different transmission protocols and are usually found at the edges of networks.

IPv4 (which uses 32-bit addressing) and IPv6 (which uses 128-bit addressing) are both OSI internet layer protocols for packet switched internetworking. Since IPv4 addressing have a limit of 4.2 billion addresses, IPv6 will provide 3.4×10^38 addresses. Understanding the address limitations for IPv4 elucidated the role of Network Address Translation (NAT). I found interesting that IPv4 has a range of reserved addresses according to RFC5735 (https://www.hjp.at/doc/rfc/rfc5735.html). Also, learning that IPv6 is designed for IPSEC, supports larger network packets, and has built-in Quality of Service (QoS) was illuminating too. IPv6 address formats are more complex (8 groups of 2 bytes separated by ":", for example "FFED:2E44:6006:9FBC:10BB:BA98:3210:4562") than IPv4 address which consist of 4 groups of 1 byte (expressed in decimal form) for example "172.16.210.198". Due to the complex address format of IPv6, I think there may need to be a simpler addressing technique for novice network users such as bitly (https://bitly.com/) which shortens long URLs for example https://bit.ly/2Kz43O which could represent https://www.organisation.com/subresource/resource1/item1/sub-item.html.

In this unit I worked with the team to perform basic network scanning against out team's assigned website, using basic tools such as traceroute, ping, dnslookup and whois. The scan activity led to a deeper understanding that public websites have a lot of useful information such as the mail email server, the registered owners and the servers that exist between a consumer's PC and the host website. I learned that the traceroute tool uses Time To Live (TTL) in IP packets to prevent routing loops and endless network traversal if a destination is not found. The TTL is decremented as each device transmits the packet and when the TTL

reaches zero, the device processing the IP packet will drop it and return an Internet Control Message Protocol (ICMP) packet to the sender.

I provided a summary post for the collaborative discussion started in unit 1.

References

Maathuis, I. & Smit, W.A. (2003). The battle between standards: TCP/IP Vs OSI victory through path dependency or by quality? *Proceedings of the 33rd European Solid-State Device Research-ESSDERC'03:* 161-176.