COMP3310/6331 – 2020 Tute/Lab #3

By this stage students will have concluded Topic 4, covering the layer model and a quick introduction to the Internet Protocol (IP) as well as UDP and TCP as transport protocols.

#	
1	**Hands-on activities:** Let's take another look at your local area network, the Ethernet/wifi in your home, library, wherever. The first set of these activities, analysing LAN traffic, you can (and should!) try at any time, and discuss/clarify during the tutes over the next couple of weeks. The second part… you get to do some **coding**. **There is a separate instruction file for the coding exercises on the wattle site, together with a zip file of starter code for you to work on. Some of the steps may require a bit more time after the tute to follow-up, e.g. working with another student, and using an external machine as a common server. Talk with the tutors where you need any help.** • Run 'traceroute' (or equivalent for your OS) from your machine towards www.anu.edu.au. It will return both the IP addresses and the Hostnames of many of the devices along the path. Try to work out which Service Providers (companies) your path goes through, and where the big hops are (especially if you're overseas from Australia). Which hops are not returning information? Do they block everything after them, or just keep their own interface a secret? • The first hop after your machine will typically be your internet router. Use 'arp' (or equivalent) to work out the MAC address of your router. • Use wireshark to monitor a connection between your machine and your router. You can set up a filter to only monitor certain traffic types (e.g. ICMP) or certain destinations (e.g. your router). You should set up a filter for ICMP and then 'ping' the router (use ctrl-C to stop it if it keeps pinging). Open up the ping packets to see the various ICMP fields, and then unpack them all the way to the Ethernet frame. • Pick another IP address on your network (your router might be 192.168.1.1, try 192.168.1.2-<some big number>, or look at your device's IP address and add/subtract 1). If you know how to log into your router it can tell you about other devices you may have on your LAN, otherwise you'll just have to go with trialling a few numbers… Check first that it is NOT in your arp cache, then run 'ping' to it and check the arp cache again. • Set up a filter to capture 'http' traffic (port 80) and connect to your favourite news-site. For the first packet connecting to the news-site, see if you can identify the Ethernet headers, the IP headers and the TCP headers (http runs as a TCP payload). • You can also record frames for a period of time. Try to record for 30 seconds or so, to get a good number of frames, and then see how many different types you see: o Do you see broadcast frames or packets? Packets with other TCP, UDP payloads? How many network device manufacturers can you identify on your LAN?
2	Revision: 1. Why is the layer model for networking a good idea? a. Layers make it clearer which functionality is and is NOT provided by a particular service. It enforces (well, up to a point) some structured thinking about what functionality you need, and what can be left to higher/lower layers, and it helps leverage existing standards.

2. What's a Protocol Data Unit, and what is a Service Data Unit?
    a. A PDU is the package of information exchanged between two end points over some network protocol (at any given layer). A SDU is the package of information exchanged between two layers on a single end-point, usually via some API. In the lecture diagrams, a PDU is a horizontal exchange, while a SDU is a vertical exchange.

3. What's the difference between a Frame and a Packet?
    a. A Frame is something transported by a LAN protocol, of arbitrary length. A Packet usually means the variable-length payload being delivered across a wide area network, e.g. an IP packet. Different to a datagram or segment, those are carried by UDP or TCP in the Internet Protocol.

4. Why do we think of IP as being 'end-to-end' between hosts, and TCP/UDP as being 'end-to-end' between applications?
    a. IP provides wide-area machine-to-machine connectivity across any variety of LAN technologies, routers just forward packets around without looking into them very deeply - though they modify their checksum and ttl every hop, and NATs rewrite the IP addresses and ports. The operating system receives packets and unpacks them…
    b. Applications use TCP/UDP (or other transport protocols) to communicate with each other, with ports providing the key for the operating system to pass packet payloads to the correct application. Routers and other devices (excluding NATs and overly zealous network security) don't look at TCP/UDP content.

5. Why does the IETF standards process look for *'rough consensus and running code'*?
    a. Standards are a community agreement, and not everything is well understood to start with. Optimising a standard takes effort, to make it both well-designed and well-documented, and is never finished – hence "RFC". Protocols need to be clearly standardised so that **other** people can write a client/server to talk with **your** server/client purely from the RFC documentation.

6. Which IP header and which ICMP packets are important for traceroute to find the path of packets? Why? (how does it use them?)
    a. Traceroute sends packets with a linearly increasing TTL of 1,2,3, … etc towards the destination. When a router decrements the TTL to zero it drops it and returns an ICMP TTL Exceeded packet with the IP address of the router.

7. Given some /25 address range, how many hosts could we potentially have on our network? What does the /25 netmask look like in dotted-quad notation?
    a. A /25 has 25bits of network address, so 7 bits of host addressing. 2^7 = 128. THEN subtract 1 address for 'the wire' and subtract another 1 address for the broadcast address. Neither of which can be used by hosts. So 126.
    b. The /25 netmask is 25 bits of 1's, so 255.255.255.128

8. What's the benefit of using the longest-prefix rule in forwarding table?
    a. You get the benefit of aggregating an entire network's worth of host addresses into a single entry (shortening tables), as the 'default' next-hop entry, AND you can have specific exclusions to target any special address ranges while only adding 1 more entry (per exclusion).

9. Why would a host send a Gratuitous ARP frame?

	a. What is Gratuitous ARP? – a query for one’s own IP address, that nobody should reply to. If a host’s IP address changes, it could let everybody else know of the change, rather than waiting for the first (and perhaps every other) device (including the switch it is hanging off) to have a failed connection and have to re-discover it. Secondly, it can turn up any duplicate IP addresses on the subnet (broadcast domain).