COMP3310/6331 – Tute/Lab #3 – Week 7 – 16-17 April

Outline of Tute/Lab:

- Reminder: Any particular real-world network systems, technologies, challenges, etc. that you'd like to have a guest lecture on (Weeks 10-12)? Already have lined up AARNet, one on TransACT/NBN, and one on NCI. Can do 2-3 more.

- **Assignment 1** review and discussion: Outline of key points for each question has been posted with the tute outline

- **Mid-semester exam** review and discussion. Sample answers for each question has been posted with the tute outline. Students will be able to review their papers during the tute.

- **Command line intro**
  - **ping** – read the man-page for ping(1) and try to ping various well-known websites. Note that ping reports the IP address of the server being ping'ed
    - Why do some servers reply (www.google.com), and some do not (mail1.asd.gov.au)?
    - Do well-known busy sites like google.com always use the same IP address? Try a ping a few times, or compare notes with your lab neighbour.
  - **traceroute/tracert –** read the man-page for traceroute(1) (or tracert on Windows), and then run a traceroute to various well-known websites. Pick somewhere outside of Australia (e.g. *www.bbc.co.uk*)
    - Does every hop report back properly? If not, why not?
      - Also try *mail1.asd.gov.au* and compare
    - Can you identify all the hosts along the path, and where they are?
    - Note the changing round-trip-time for the (3) probes from each host, what is that telling you about the location?
    - Why do you sometimes get a hostname **or** an IP address reported back in various cases?
      - How does traceroute work that out?
  - **nslookup/dig –** these provide DNS lookups from the command line. The nslookup command is an older tool, but has an interactive mode, while dig has a few more specific query features. The most common use is to get the IP address for a specific hostname. You can ask more detailed questions of the DNS using dig for specific resource records.
    - What's the IP address of 3310exp.hopto.org?
    - Identify the main name server for the ANU using the SOA record
    - Repeat, using the NS (nameserver) record. Why are they different?
    - Which resource record identifies the mail server for the ASD.gov.au domain?
      - See section 3.3 of RFC 1035

- **Packet Sniffing:**
  - We'll use wireshark (with admin privileges, via sudo) to sniff the traffic to/from your computer. Wireshark runs a 'capture' from go to stop and provides a report – there's a lot of traffic, and it goes by quickly! You can then filter the report to identify the packets

you’re interested in and examine them at your leisure. This is also good practice for understanding filters. You can set up a filter in advance before the capture, but they have to be ‘right’ before you start.

- Identify packets/frames on the lab ethernet, and look at the different traffic types
    - Try to find ARP packets, broadcasts, and non-IP traffic – what’s happening out there?
    - Try to drill into the layers – look at a TCP segment, its IP packet, its Ethernet frame, and how they are encapsulated.
- Run a capture for a ‘ping’ command. What are the packets being sent and received?
- Run a capture for a ‘traceroute’ command.
    - What are the packets being sent and received, and how do they vary?
    - What are the DNS queries that traceroute is using, and what responses does it get?
    - What does traceroute do at the very end of tracing a route?
- If time permits, or on your machine later, run a capture of a http session, e.g. from your browser or your assignment 2 crawler code. Identify the DNS call to get the IP address, maybe an ARP call to find the gateway router, then the TCP connection to the server and finally the HTTP requests/responses.