Tan Shun Yu | 1001171 | Networks Lab 7

• While using wireshark on SUTD_Students, what did you see/not see? In particular, did you see other people's traffic, and what kind?

I did not see other people's traffic. In fact, I can only see my own traffic, in particular the DHCP, ARP and NTP packets. There are ARP broadcasts from other hosts.

• While connected to SUTD_Guest, do you see different kind of traffic? Why?

Yes, it is different. As the SUTD_Guest network is insecured as compared to the SUTD_Student network, I should have been able to capture the traffic of those connected to the SUTD_Guest network as it is unencrypted. However, at the lab, I did not see the expected traffic from other people. This could be that we are connected to different APs unde the same SUTD_Guest ESSID.

• Using monitor mode, what kind of traffic do you see, and why? – Can you see queries for non-SUTD ESSIDs? – Why do you see these? – Why is the source address of ACKs the way it is?

I captured wireless traffic in the vicinity. By turning on monitor mode, it allowed packets to be captured without having to associate with an access point or ad-hoc network.

Yes, I see queries for non-SUTD ESSIDs, specifically the probe request packets asking for ESSIDs that are automatically saved in the machine's wireless configuration. These devices are specifying that they are looking for a particular ESSID to connect to. If that ESSID is supported on an AP, that AP will reply to it. Some examples include AIRPORT-FREE-WIFI and TAIPEI 101 Free WiFi.

I see ACKs but they do not have a source address. This is because as the sender already knows which receiver it is getting the ACK from, for efficiency purposes, it omits the header with the source address in the ACK packet to save a few bytes per ACK.

• How many networks/BSSIDs did you see with kismet? Which channels were used?

It was one BSSID per SSID and there are 430 BSSIDs that I saw with kismet. Channels 1, 6 and 11 were used for the 2.4GHz band and channels 36, 40, 44, and 48 were used for the 5GHz band.

• Did ad-hoc mode work for you? Was TeamB able to ping the server through TeamA?

Yes, ad-hoc mode worked for me. Team B was able to ping the server through Team A, and this is because Team A, as a neighbour of Team B, helped to forward the packets to the server and back for Team B. This is what we learnt earlier in class on how neighbours work.

• Did the "router" mode work? How is the setup different from a layer 2 access point?

Yes, setting up our own infrastructure network worked. A friend who connected to my access point managed to ping the server (10.0.1.10) in the lab while being disconnected from the wired network.

This setup is different from a layer 2 access point because NAT was used (that requires IP address which is layer 3) instead of forwarding frames from a MAC address table.