# Lab 7: Wireless Networks

50.012 Networks

Hand-out: Nov 17
eDimension hand-in: Nov 24

## 1 Objectives

- Understand 802.11 infrastructure mode in detail, e.g., using wireshark in monitor mode
- Observe and experiment with ad-hoc mode and access points
- Note: You can try to run this exercise on a non-lab machine, but it will not work with all wireless adapters. It will certainly not work in a VM guest.
- Note: configuration of the wireless settings can be tricky. If you get stuck, try to reboot
- Note: the *eth0* and *wlan0* interfaces are recently renamed to *eno1* and *wlp3s0* on the lab machines - check which one is correct

## 2 Experiments

### 2.1 Set up your machine

- Install the script from eDimension folder: `bash install.sh`
  - During installation, kismet might ask you to say "yes" and your username, i.e. "student". Use `Tab` to switch between buttons/fields.
- Disconnect from the wired network, if you are connected, using the applet in the top right

### 2.2 Traffic sniffing with wireshark

1. Simple sniffing in promiscious mode
   - Connect to the `SUTD_Student` network with your normal account
   - Use `ifconfig` to find your IP and note it down
   - Use `iwconfig` to find out more about your 802.11 configuration. In particular, find which 802.11 standard is supported, and which frequency you are using.
   - Start `sudo wireshark` and make sure to set your card to `promiscious mode`
   - Observe the ongoing traffic, what can you see? What can't you see?
2. Sniffing of SUTD_Guest

- Connect to `SUTD_Guest`. You don't need to use the portal to authenticate yourself. The portal will simply configure the network to allow your traffic to be forwarded through the AP. Associating to the AP is enough.
- Monitor the traffic in promiscious mode in wireshark again. Can you observe interesting traffic? What did you see? This might only work during lab hours.

### 2.3 Monitor mode

- Note: please use `sudo service network-manager stop` to stop the network manager from interfering. You will lose Internet access.

1. Monitor mode I: Wireshark
   - Take down your wlan0/wlp3s0 interface manually: `sudo ifconfig wlan0 down` (or: `sudo ifconfig wlp3s0 down`)
   - Activate *monitor* mode: `sudo airmon-ng start wlan0` (or: `sudo airmon-ng start wlp3s0`)
     - In monitor mode, the interface will accept frames *without being associated to the corresponding access point*
     - This command will create the `mon0` interface. Use that interface in wireshark to listen on.
   - Now start a new capturing session in wireshark:
     - What kind of messages are you capturing, and why?
       - Hint: you can filter out the most common type of message with `!(wlan.fc.type_subtype==8)` as filter in wireshark.
     - Can you see other machines' traffic?
       - In particular, do you see `Probe request` packets? For which ESSID are they asking?
     - Do you see ACKs? Do they have a source address? Reason will be explained in the lecture on Friday
2. Monitor mode II: Kismet
   - kismet is a tool to analyze wireless network traffic
   - It is actually two applications: a server part, and a gui
   - start `sudo kismet_server` from the command line, with `mon0` set up as described previously
   - start the gui by typing `kismon`.
   - You should be on the main menu now, seeing the wireless traffic being analyzed
   - Wait a couple of minutes, how many networks/BSSIDs are encountered? What do you think how these are related? Which channels are used by the APs?
   - In view->network type, select only "probe network". What networks do you see, why?
3. Restoring normal networking
   - After you are done with monitor mode, you need to restore normal networking:

- stop the running kismet_server by pressing CTRL-C
- `sudo airmon-ng stop mon0`
- `sudo ifconfig wlan0 up` (or: `sudo ifconfig wlp3s0 up`)
- `sudo service network-manager start`

## 2.4 Ad-hoc Mode

- Team up with another person or pair. One of you will set up an *ad-hoc* network (TeamA), and the other one will connect to it (TeamB).
- Both teams need to restart their desktops, and make sure that they DO NOT automatically connect to any wireless network. TeamB should also disconnect from wired network.
- TeamA uses the network applet in the top right to "Create a new wifi network". Wired network should also be connected.
  - Choose an appropriate network name and **no security/access key**
  - Team B should now see and be able to connect to your new network. Both sides can check their IP configuration with `ifconfig` and `route`. Can you `ping` each other?
  - Team B should still have its wired adapter disconnected. Can Team B ping the server, i.e. 10.0.1.10? Why? How did we define ad-hoc mode?

## 2.5 Set up your own infrastructure network

- It is actually fairly *simple* to set up your PC to act similar to an home "router"
- You can now turn on network-manager again `sudo service network-manager start`
- If do not use the lab machines, use "iw list" to find out if your wlan card support `AP` mode. This part requires a card that does support it (look for "Supported interface modes: AP")
- Enable your wired network with the applet on the top right again. Disconnect from `SUTD_Student`
- Run `sudo ./ap-hotspot configure`
  - Use the `eth0/eno1` interface as first interface, and `wlan0/wlp3s0` as second. Provide an SSID and password (8+ characters) for your access point.
- Start the AP with `sudo ./ap-hotspot start`
- Ask a friend to connect to your access point
  - Which IP address is he getting?
  - If he disconnects from the wired network, can he ping the server in the lab, i.e. 10.0.1 .10? Why?
  - Hint: use `wireshark` and `route` on your machine to figure out what is going on
  - Hint2: this configuration is actually more like a router, and less like the layer 2 access point discussed in class

# 3 What to Hand in

## 3.1 eDimension submission:

Please provide a writeup (in PDF format with your name) that includes the following information:

- While using wireshark on SUTD_Students, what did you see/not see? In particular, did you see other people's traffic, and what kind?
- While connected to SUTD_Guest, do you see different kind of traffic? Why?
- 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?
- How many networks/BSSIDs did you see with kismet? Which channels were used?
- Did ad-hoc mode work for you? Was TeamB able to ping the server through TeamA?
- Did the "router" mode work? How is the setup different from a layer 2 access point?

## 3.2 Checkoff:

- No checkoff required if you submitted your reply sheet