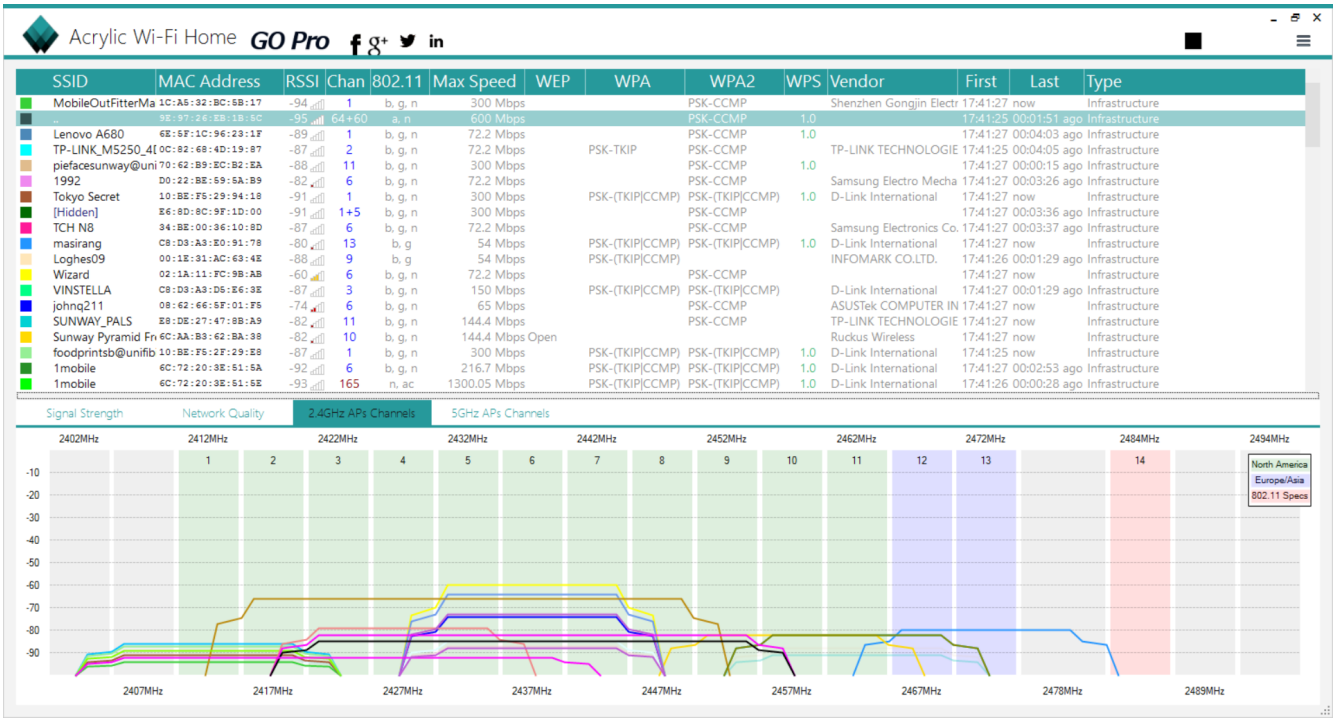
Assignment 2 - FIT 1047

Group Members :
1. IRTAZA NASIR (28112199)
2. WONG ZHIWEI (28190068)
3. BRYAN CHAN CHUING SEANG (28463536)
4. NIZNI ASHARD MOHAMMAD NIZAR (28313623)
5. MD NIAZ UDDIN KHAN (28252306)

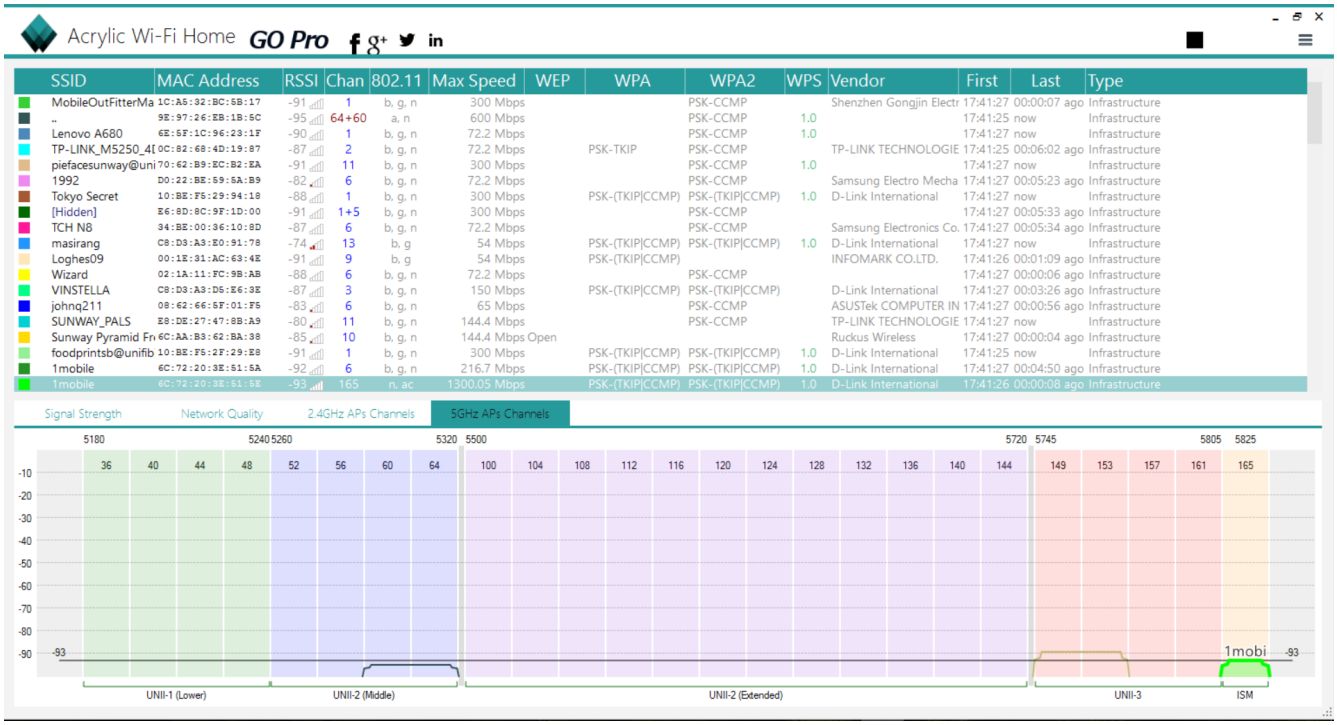
Task 1.1
Shopping Centre : **Sunway Pyramid**

Locations :

1. **Pizza Hut (LG2)**



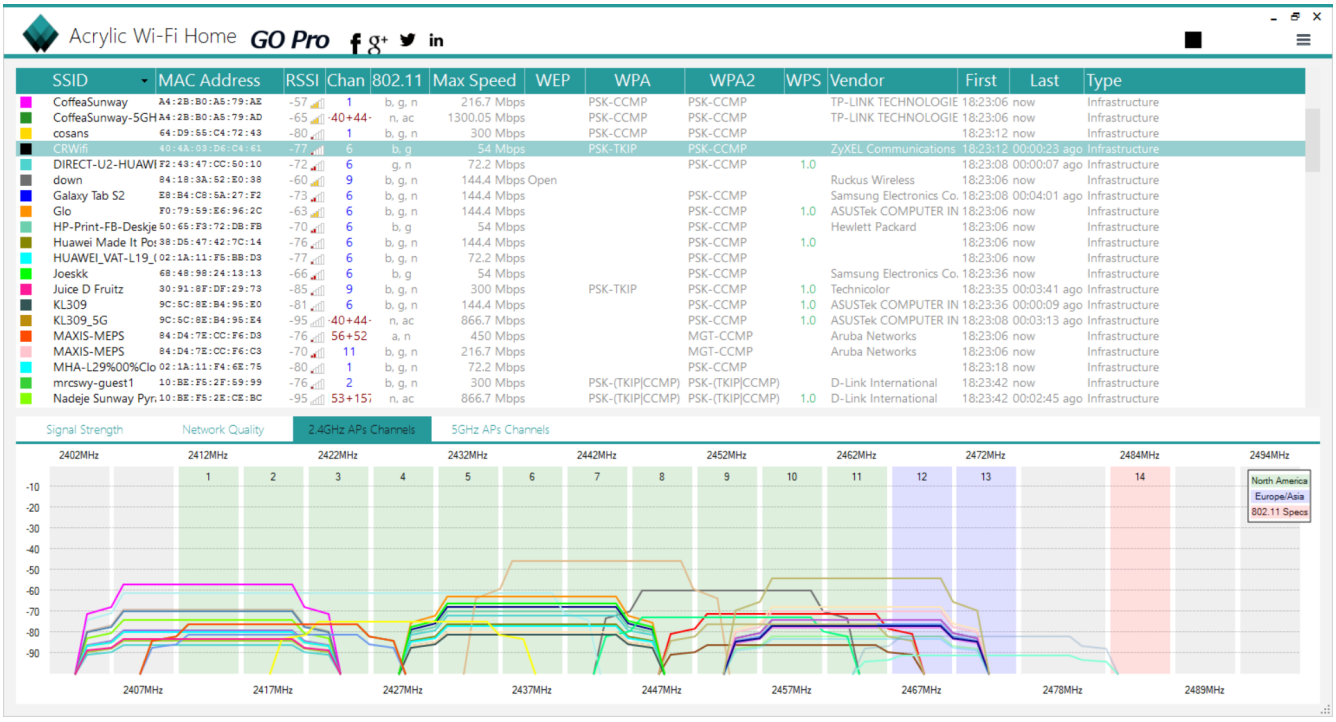
2.4 GHz Graph



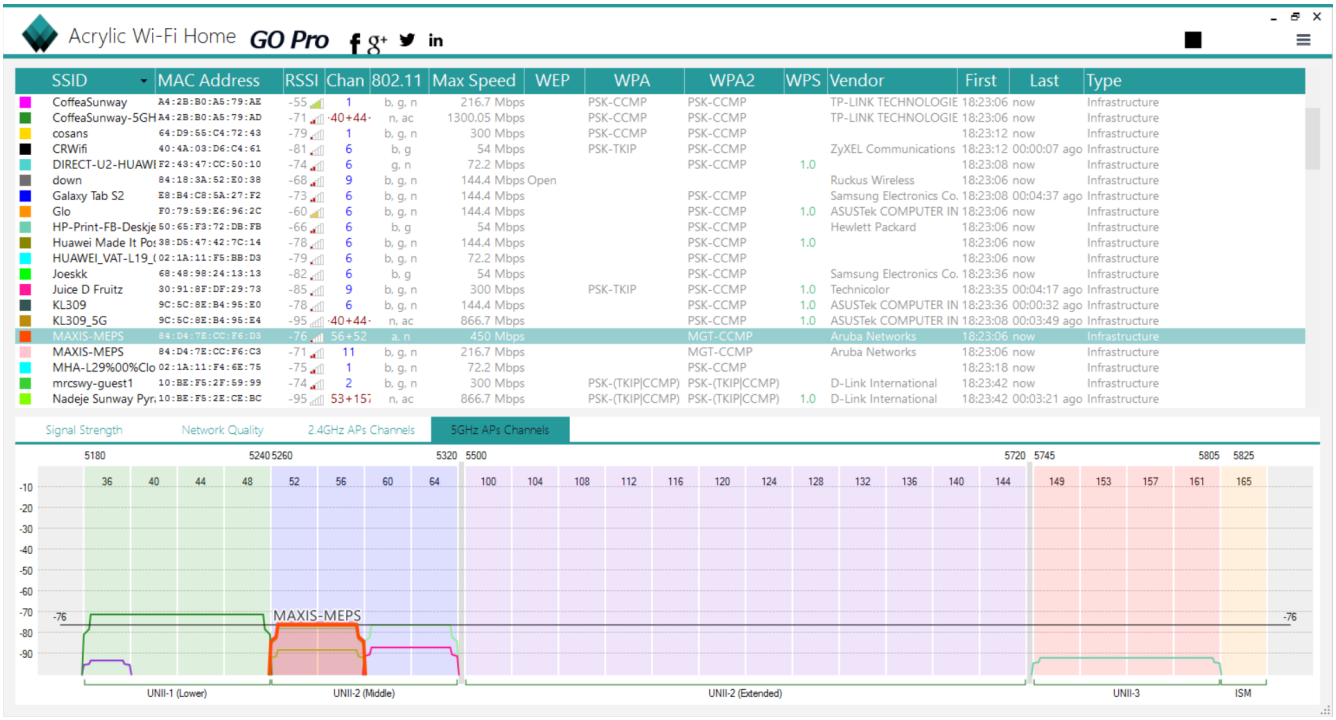
5 GHz graph

SSID	CHANNEL	RSSI	802.11 STANDARD	SECURITY	SUPPORTED DATA RATE	MAC ADDRESS
MobileOutFitterMa	1	-94	b, g, n	WPA2	300 Mbps	1C:A5:32:BC:5B:17
..	64+60	-95	a, n	WPA2	600 Mbps	9E:97:26:EB:1B:5C
Lenovo A680	1	-89	b, g, n	WPA2	72.2 Mbps	6E:5F:1C:96:23:1F
TP-LINK-M520_4	2	-87	b, g, n	WPA/WPA2	72.2 Mbps	0C:82:68:4D:19:87
piefacesunway@unifibiz	11	-88	b, g, n	WPA2	300 Mbps	70:62:B9:EC:B2:EA
1992	6	-82	b, g, n	WPA2	72.2 Mbps	D0:22:BE:59:5A:B9
Tokyo Secret	1	-91	b, g, n	WPA/WPA2	300 Mbps	10:BE:F5:29:94:18
[Hidden]	1+5	-91	b, g, n	WPA2	300 Mbps	E6:8D:8C:9F:1D:00
TCH N8	6	-87	b, g, n	WPA2	72.2 Mbps	34:BE:00:36:10:8D
masirang	13	-80	b, g	WPA/WPA2	54 Mbps	C8:D3:A3:E0:91:78
Loghes09	9	-88	b, g	WPA	54 Mbps	00:1E:31:AC:63:4E
Wizard	6	-60	b, g, n	WPA2	72.2 Mbps	02:1A:11:FC:9B:AB
VINSTELLA	3	-87	b, g, n	WPA/WPA2	150 Mbps	C8:D3:A3:D5:E6:3E
johnq211	6	-74	b, g, n	WPA2	65 Mbps	08:62:66:5F:01:F5
SUNWAY_PALS	11	-82	b, g, n	WPA2	144.4 Mbps	E8:DE:27:47:8B:A9
Sunway Pyramid Free Wifi	10	-82	b, g, n	WEP (Open)	144.4 Mbps	6C:AA:B3:62:BA:38
foodprintsb@unifibiz	1	-87	b, g, n	WPA/WPA2	300 Mbps	10:BE:F5:2F:29:E8
1mobile	6	-92	b, g, n	WPA/WPA2	216.7 Mbps	6C:72:20:3E:51:5A
1mobile	165	-93	n, ac	WPA/WPA2	1300.05 Mbps	6C:72:20:3E:51:5E

2. **Blue Atrium (LG1)**



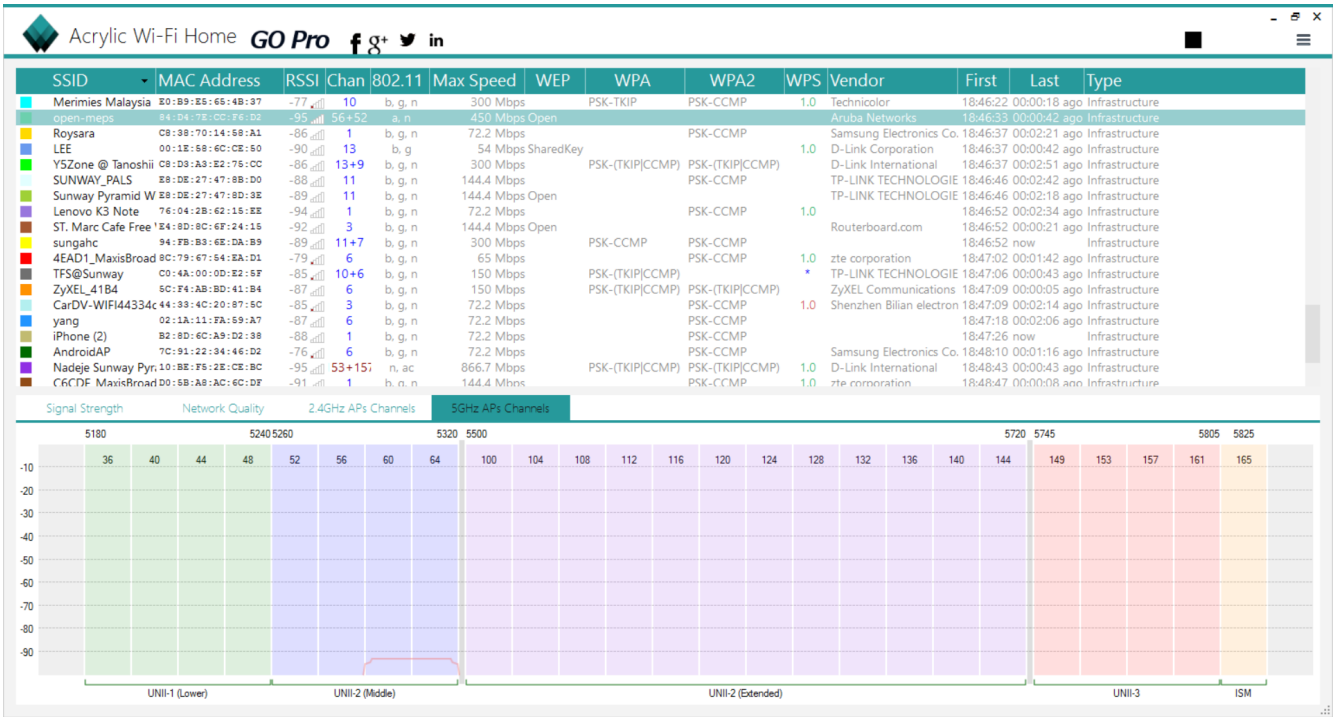
2.4 GHz Graph



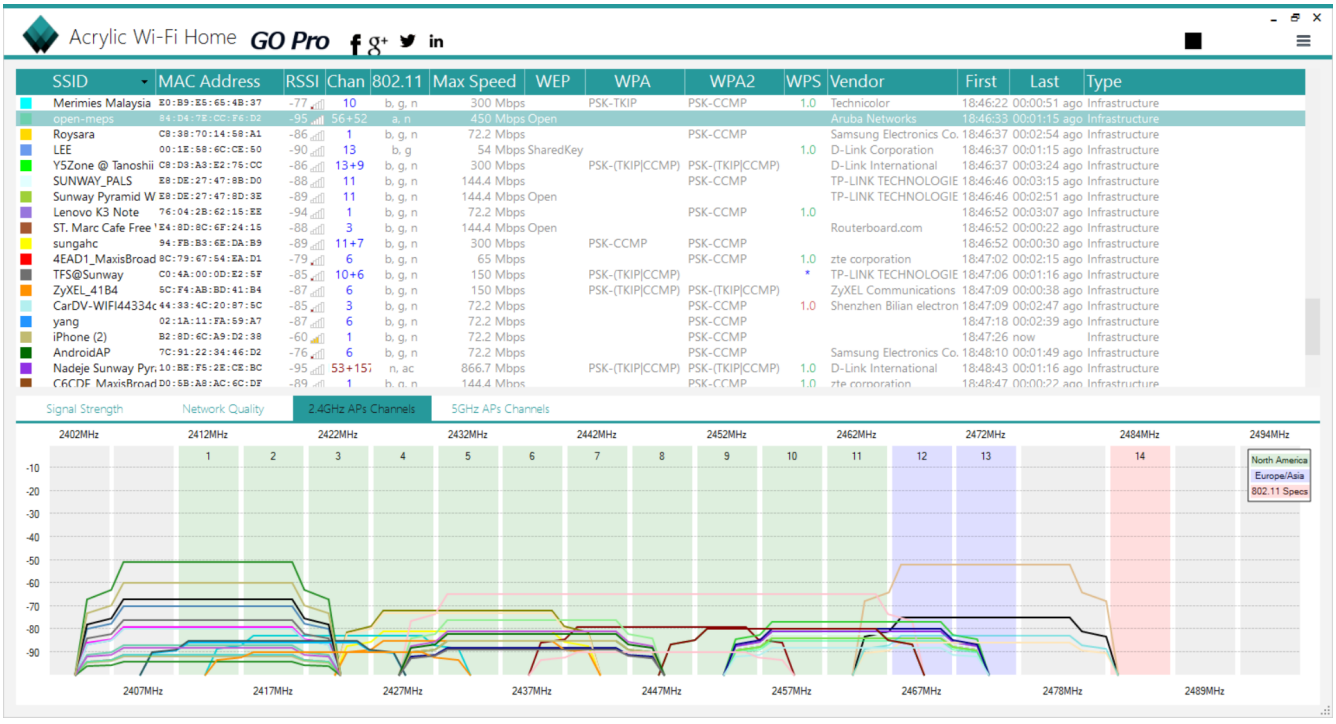
5GHz Graph

SSID	CHANNEL	RSSI	802.11 STANDARD	SECURITY	SUPPORTED DATA RATE	MAC ADDRESS
CoffeaSunway	1	-57	b, g, n	WPA/WPA2	216.7 Mbps	A4:2B:B0:A5:79:AE
CoffeaSunway-5GHz	40+44	-65	n, ac	WPA/WPA2	1300.05 Mbps	A4:2B:B0:A5:79:AD
cosans	1	-80	b, g, n	WPA/WPA2	300 Mbps	64:D9:55:C4:72:43
CRWifi	6	-77	b, g	WPA/WPA2	54 Mbps	40:4A:03:D6:C4:61
DIRECT-U2-HUAWEI	6	-72	g, n	WPA2	72.2 Mbps	F2:43:47:CC:50:10
down	9	-60	b, g, n	WEP (Open)	144.4 Mbps	84:18:3A:52:E0:38
Galaxy Tab S2	6	-73	b, g, n	WPA2	144.4 Mbps	E8:B4:C8:5A:27:F2
Glo	6	-63	b, g, n	WPA2	144.4 Mbps	F0:79:59:E6:96:2C
HP-Print-FB-Deskjet	6	-70	b, g	WPA2	54 Mbps	50:65:F3:72:DB:FB
Huawei Made It Possible	6	-76	b, g, n	WPA2	144.4 Mbps	38:D5:47:42:7C:14
HUAWEI_VAT-L19_	6	-77	b, g, n	WPA2	72.2 Mbps	02:1A:11:F5:BB:D3
Joeskk	6	-66	b, g	WPA2	54 Mbps	68:48:98:24:13:13
Juice D Fruitz	9	-85	b, g, n	WPA/WPA2	300 Mbps	30:91:8F:DF:29:73
KL309	6	-81	b, g, n	WPA2	144.4 Mbps	9C:5C:8E:B4:95:E0
KL309_5G	40+44	-95	n, ac	WPA2	866.7 Mbps	9C:5C:8E:B4:95:E4
MAXIS-MEPS	56+52	-76	a, n	WPA2	450 Mbps	84:D4:7E:CC:F6:D3
MAXIS-MEPS	11	-70	b, g, n	WPA2	216.7 Mbps	84:D4:7E:CC:F6:C3
MHA-L29%00%Clo	1	-80	b, g, n	WPA2	72.2 Mbps	02:1A:11:F4:6E:75
mrcswy-guest1	2	-76	b, g, n	WPA/WPA2	300 Mbps	10:BE:F5:2F:59:99
Nadeje Sunway Pyramid	53+157	-95	n, ac	WPA/WPA2	866.7 Mbps	10:BE:F5:2E:CE:BC

3. **Converse (1st Floor)**



2.4 GHz Graph



5GHz Graph

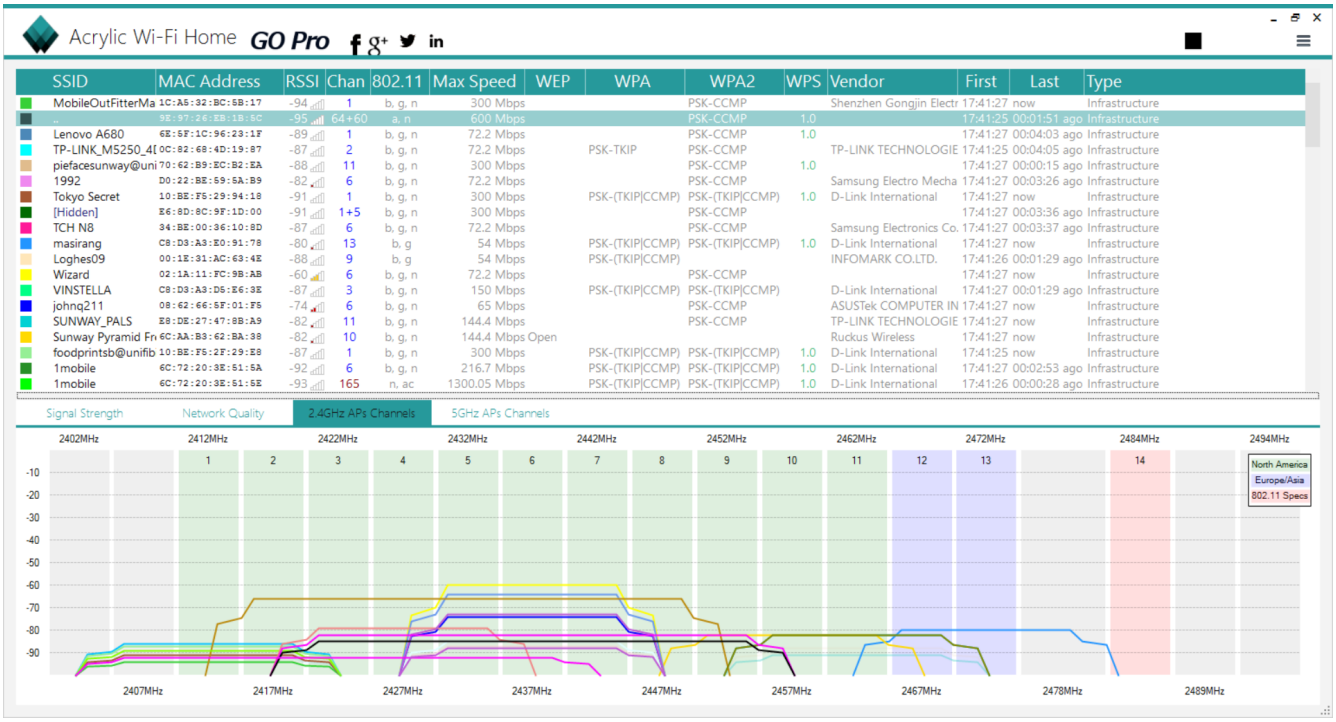
SSID	CHANNEL	RSSI	802.11 STANDARD	SECURITY	SUPPORTED DATA RATE	MAC ADDRESS
Merimies Malaysia	10	-77	b, g, n	WPA/WPA2	300 Mbps	E0:B9:E5:65:4B:37
open-meps	56 + 52	-95	a, n	WEP (Open)	450 Mbps	84:D4:7E:CC:F6:D2
Roysara	1	-86	b, g, n	WPA2	72.2 Mbps	C8:38:70:14:58:A1
LEE	13	-90	b, g	WEP	54 Mbps	00:1E:58:6C:CE:50
Y5Zone @ Tanoshii	13+9	-86	b, g, n	WPA/WPA2	300 Mbps	C8:D3:A3:E2:75:CC
SUNWAY_PALS	11	-88	b, g, n	WPA2	144.4 Mbps	E8:DE:27:47:8B:D0
Sunway Pyramid W	11	-89	b, g, n	WEP (Open)	144.4 Mbps	E8:DE:27:47:8D:3E
Lenovo K3 Note	1	-94	b, g, n	WPA2	72.2 Mbps	76:04:2B:62:15:EE
ST. Marc Cafe Free	3	-92	b, g, n	WPA(Open)	144.4 Mbps	E4:8D:8C:6F:24:15
sungahc	11+7	-89	b, g, n	WPA/WPA2	300 Mbps	94:FB:B3:6E:DA:B9
4EAD1_MaxisBroadband	6	-79	b, g, n	WPA2	65 Mbps	8C:79:67:54:EA:D1
TFS@Sunway	10+6	-85	b, g, n	WPA	150 Mbps	C0:4A:00:0D:E2:5F
ZyXEL_41B4	6	-87	b, g, n	WPA/WPA2	150 Mbps	5C:F4:AB:BD:41:B4
CarDV-WIFI44334	3	-85	b, g, n	WPA2	72.2 Mbps	44:33:4C:20:87:5C
yang	6	-87	b, g, n	WPA2	72.2 Mbps	02:1A:11:FA:59:A7
iPhone (2)	1	-88	b, g, n	WPA2	72.2 Mbps	B2:8D:6C:A9:D2:38
AndroidAP	6	-76	b, g, n	WPA2	72.2 Mbps	7C:91:22:34:46:D2
Nadeje Sunway Pyramid	53+157	-95	n, ac	WPA/WPA2	866.7 Mbps	10:BE:F5:2E:CE:BC
C6CDF MaxisBroadband	1	-91	b, g, n	WPA2	144.4 Mbps	D0:5B:A8:AC:6C:DF

Task 1.2

Usage of Different WLAN Channels

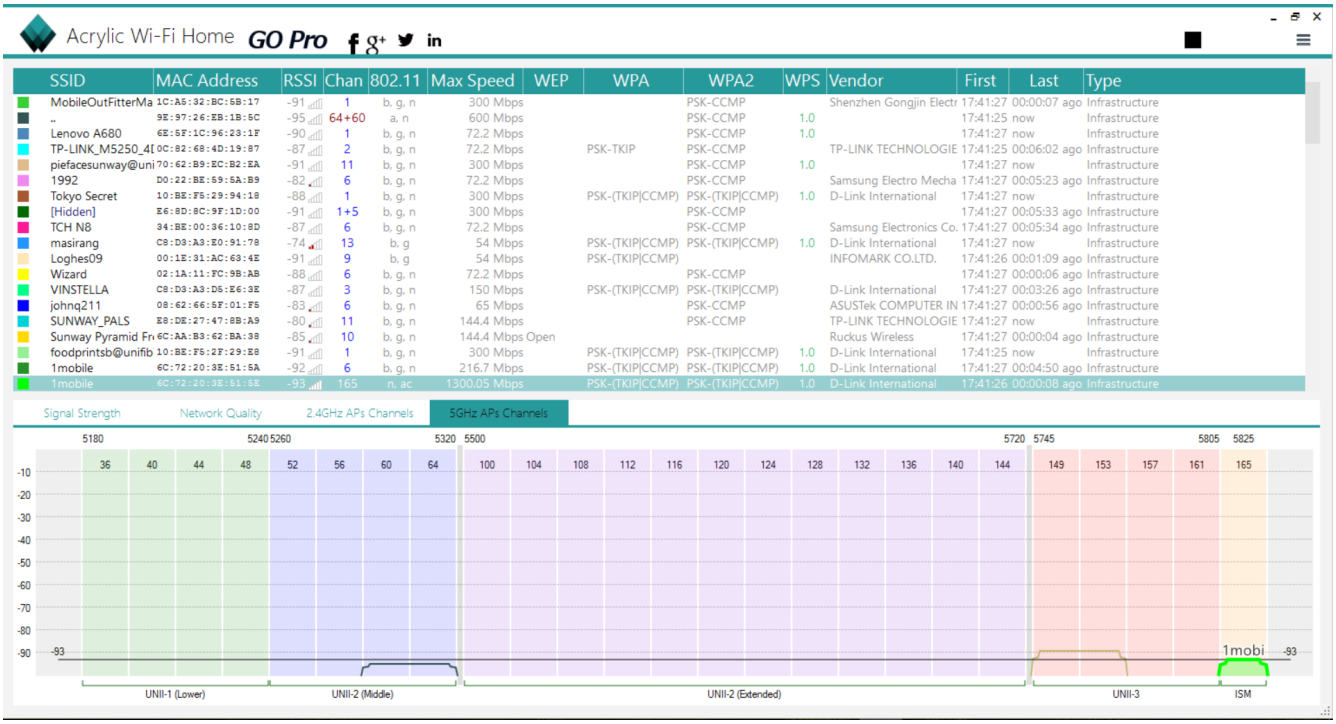
Optimally, WLAN channels should be allocated in a a way that prevents interference.

For a 2.4Ghz band WLAN, although there are 13 channels, only 3 of them can be used in an area without causing interference. Transmitters using the same channel in the same area can also be attenuated by -50 dBr to prevent interference. Normally, channels 1,6 and 11 are used as these 3 channels don’t overlap with each other. Similar channels can be used only if their frequencies do not overlap.



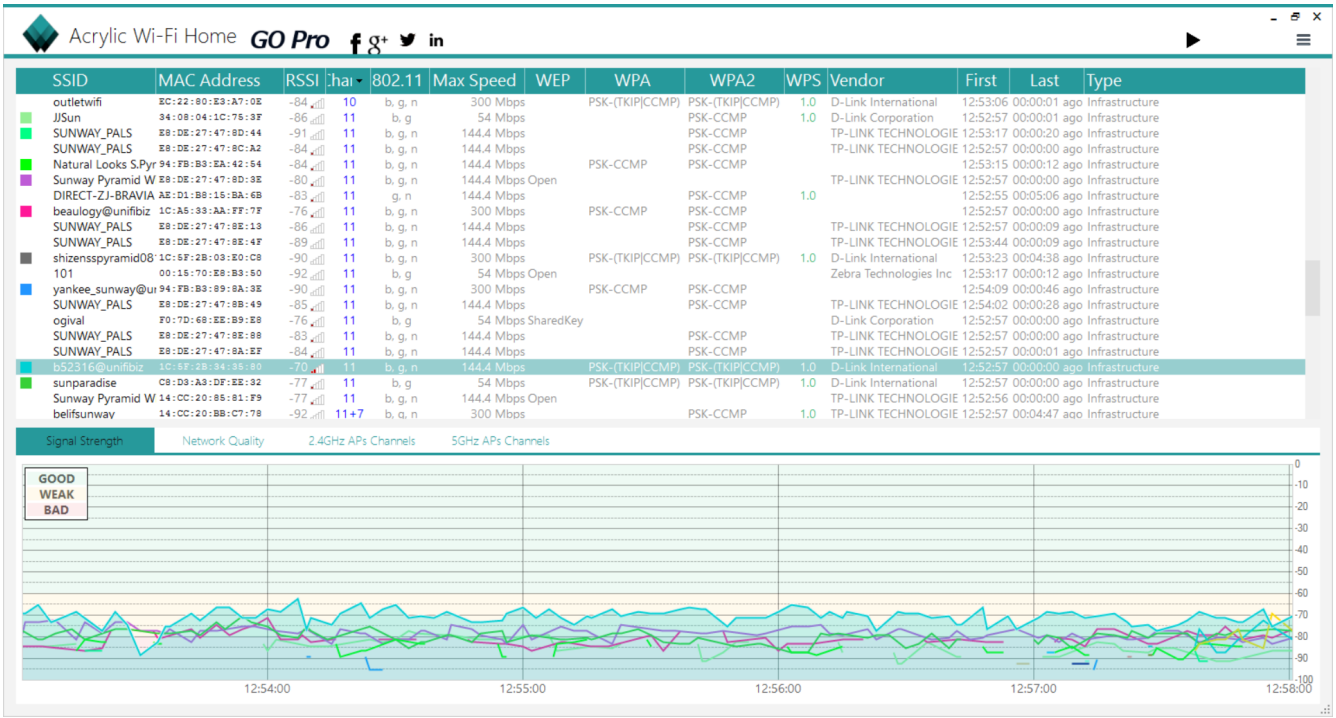
(2.4 Ghz Graph. Taken at Pizza Hut)

From the graph above, channel 1 and 6 are relatively crowded. However, channel 11 is free, with only 1 signal using it.



(5Ghz Graph. Taken at Pizza Hut)

In the 5Ghz band, interference is less of a problem as there are many channels available. As we can see, each access point has its own non-overlapping channel.



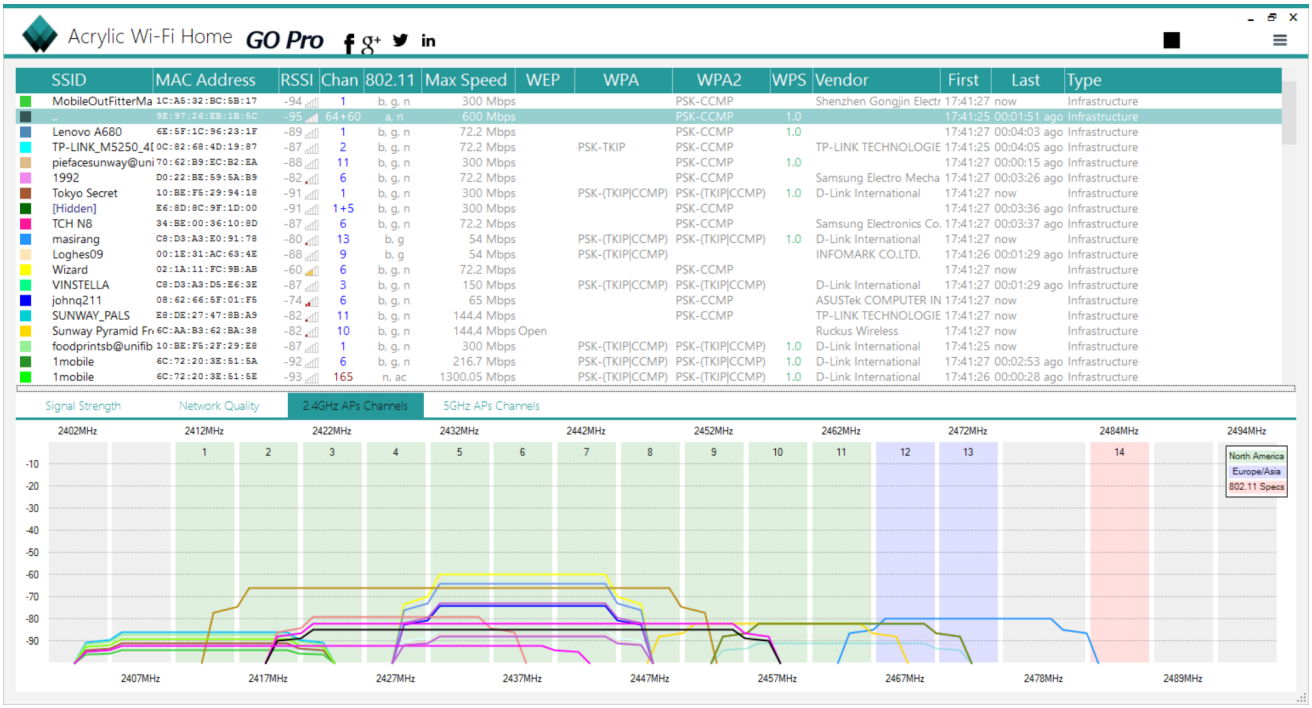
(Signal Strength Graph. Taken at Blue Atrium)

We can also look at the signal strength graph. Lines that are choppy, such as for 'sunparadise', and those with high fluctuations in signal strength, such as for 'b52316@unifibiz', are probably using crowded channels.

Interference from Neighbouring Access Points and Its Effects

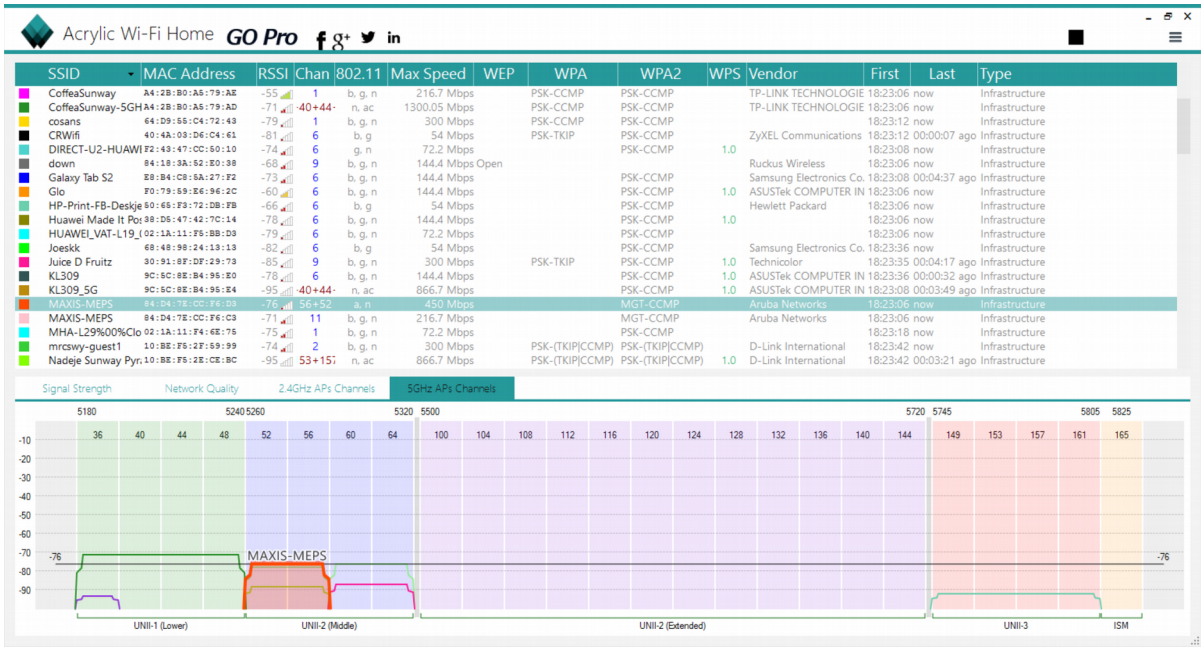
Choosing channels with a small or no separation between them, such as channel 1 and 2, will cause interference as their frequency overlaps. Also, when an 802.11 client hears another signal of similar frequency, either from a WiFi signal or another device like a microwave, it defers transmission until the signal stops (David Callisch, 2010). Interference during transmission leads to packet loss that forces retransmissions. These retransmissions slow throughput, resulting in fluctuating performance for users sharing an access point (AP).

In my data gathered for the 2.4Ghz band, there are many possibilities for interference. As we can see in the graph below, every access point has another access point with overlapping frequencies. For example, between the access point 'Lenovo A680' and 'Tokyo Secret'.



(2.4 GHz Graph. Taken at Pizza Hut)

For the 5Ghz band, there are less chances for interference as there are more channels. However, there is still that possibility, such as at channels 52-56, where 2 APs use the same channels.

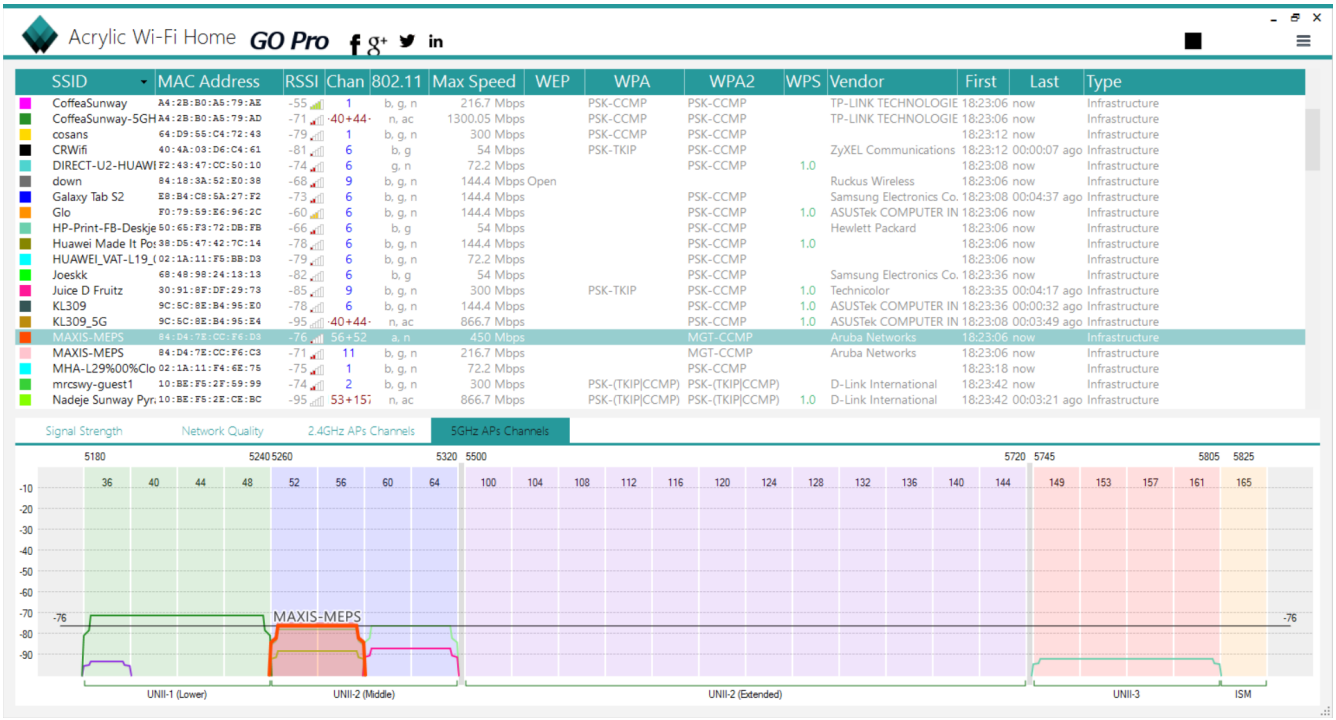


(5GHz Graph. Taken at Blue Atrium)

Dual band WiFi

One of the advantages of using dual-band wifi is it alleviates the problem of signal interference. Since the 2.4Ghz band is facing oversaturation due to the lack of non-conflicting channels, dual-band WiFi allows the user to use the less congested 5Ghz frequency.

However, using dual-band WiFi has its technical consequences. To get the benefits of the 5Ghz range, user devices should have adapters that are compatible with it. There are many devices that do not support this band yet due to cost issues. The range of a 5GHz wireless signal is also shorter compared to the 2.4Ghz as higher frequency waves experience higher attenuation.

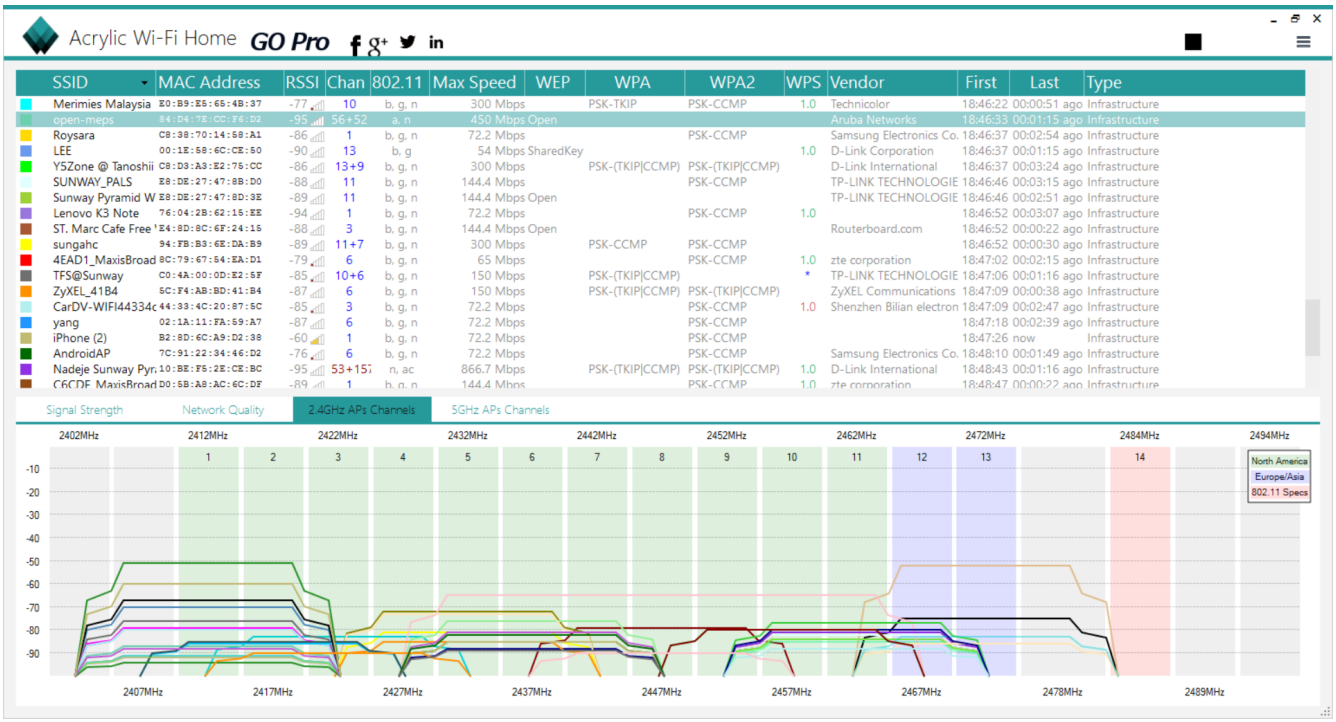


(5Ghz Graph. Taken at Blue Atrium)

From the table above, we can see that the 2 access points with the same SSIDs, "MAXIS-MEPS", are probably using dual-band WiFi as they have very similar MAC addresses and identical signal strengths.

Security Situation

The different options for providing secure WLAN access are :
1. WEP (Wired Equivalent Privacy)
2. WPA (Wi-Fi Protected Access)
3. WPA2 (Wi-Fi Protected Access II)



(Taken at Converse)

In the picture above, there are networks that use WEP, WPA and WPA2. Only one access point, named "LEE", uses WEP. However, WEP has multiple security flaws, and the increase in computing power made it easier to exploit them. Hence, the Wi-Fi alliance officially retired WEP in 2004 (Jason Fitzpatrick, 2013). Users who connect to these networks should be careful as they are easily hijacked.

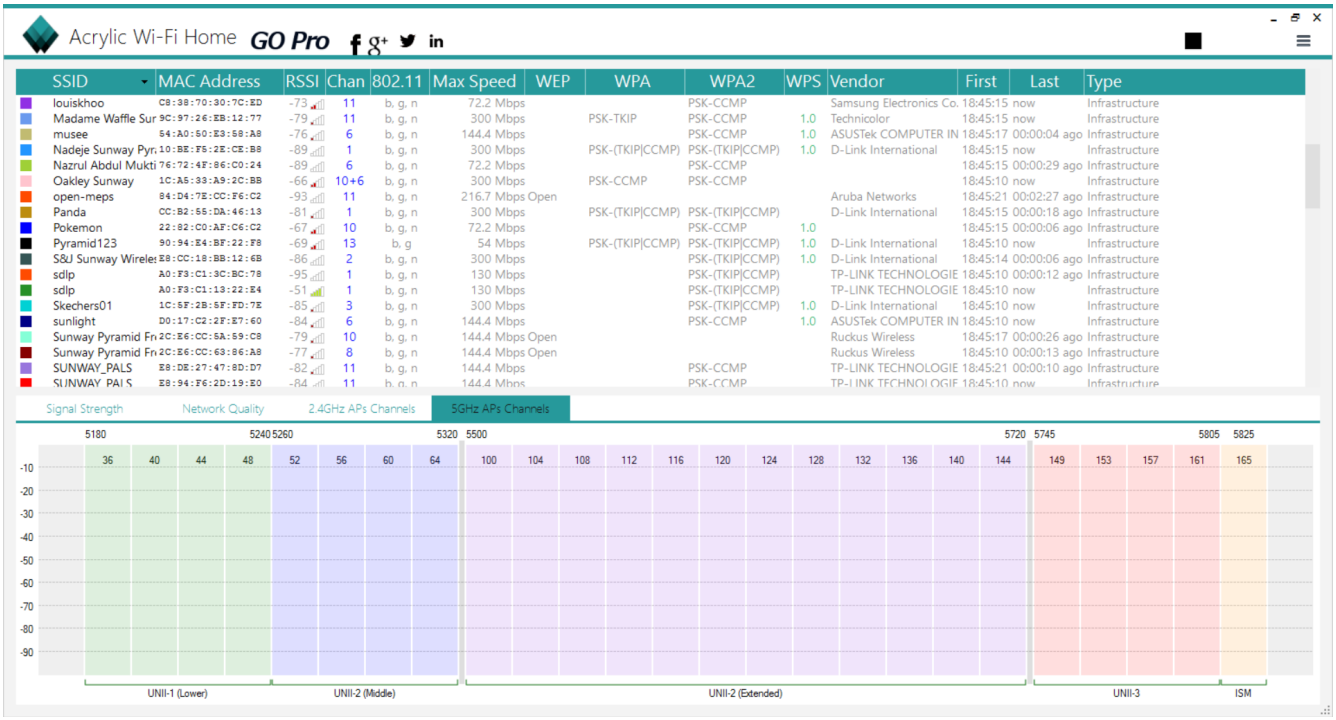
Although WPA is an improvement over WEP, it is also a vulnerable security standard. WPA2 superseded WPA in 2006, one of the biggest changes being the compulsory use of AES algorithms as well as the introduction of CCMP to replace TKIP. TKIP stands for "Temporal Key Integrity Protocol". TKIP is quite similar to WEP encryption, and is no longer considered secure. CCMP, which stands for Counter Mode Cipher Block Chaining Message Authentication Code Protocol, uses the AES (Advanced Encryption Standard) block cipher, and is considered to be quite secure (Chris Hoffman, 2014).

Although WPA2 is generally more secure than WPA, WPA2 networks that use TKIP instead of CCMP to be backward-compatible are as vulnerable as WPA. Hence, users should be careful when connecting to these APs. The safest option, therefore, is to use WPA2 networks with only CCMP.

Support For Roaming Between Access Points

Roaming is a method of providing a seamless wireless connection to users within an Extended Service Set (ESS). Essentially, users can move between different access points without losing connection ("What is WiFi roaming", 2016). When they leave the proximity of one access point, another access point nearer to the client device takes over. To maximize coverage, different APs have very little coverage overlaps, with just enough to allow for smooth transitioning. They are also arranged in a way that prevents overlapping channels to reduce interference.

In the table below, it is difficult to ascertain whether the access points are set up for roaming. I suspect that the access point "Sunway Pyramid Free WiFi" has roaming support, as the 2 APs have similar SSIDs and non-overlapping channels.



(Taken from Converse)

Tracking customers using WiFi

When users leave their phone's Wi-Fi switched on, shopping centers can use the footprint left behind to track shoppers' movements around the mall (Subramanian Gopalaratnam, 2015). By using access points or sensors as well as location-tracking algorithms, a device's MAC address can be used to identify and follow the device's movement. By mapping customer movement, shopping mall managers can maximize rent for certain spaces by setting appropriate price zones. Exposing the routes that shoppers use also helps potential leasing customers to make profit-related decisions. From my data, I have identified access points with their SSIDs named after Sunway Pyramid, which could imply that these are the tools used to track their customers.

Task 2

Short Summary

On the morning of October 21 2016, a global DdoS (Distributed Denial of Service) attack was carried out on Dyn's DNS infrastructure. Dyn is a company that provides core Internet services for Twitter, Spotify and other websites (Lorenzo Franceschi-Bicchierai, 2016). The attack caused outages and slowness for many of Dyn's customers.

Which Software/Hardware/System is Affected

The attack mainly targeted Dyn's Domain Name System (DNS) management services infrastructure on the East Coast of the United States (Brian Krebs, 2016).

How the Problem was Discovered and How It Was Initially Published

The problem was discovered by the Dyn itself. On the day of attack at approximately 7:00 am ET, Dyn realized it was experiencing a DDoS attack and worked to monitor and mitigate it (Dyn, Inc. Status, 2016). The incident was first reported on Dyn's own website when the attack started, with a detailed statement released the day after the attack (Kyle York, 2016).

How Serious the Issue is, The Consequences and Necessary Reactions

The characteristic that separates this DDoS attack from regular attacks is the massive botnet army of hacked Internet of Things (IoT) devices that was used to carry it out. The botnet, powered by the malware Mirai, is identified to be at least in part responsible for the outages (Lorenzo Franceschi-Bicchierai, 2016). However, Dale Drew, chief security officer at Level 3 Communications, said that the attack was using "about 10 percent" of the nodes that make up the Mirai botnet. As of now, Mirai consists of about half a million nodes and is constantly increasing. The Mirai malware is self-propogating, and it constantly scans the Internet for vulnerable IoT devices, using a short list of 62 common default usernames and passwords to infect new devices (Lily Hay Newman, 2016).

This is concerning as the Mirai botnet consists of unsecured Internet of Things devices which cannot be easily updated, and is thus close to impossible to secure. On September 20 2016, a security blog was targeted by a DdoS attack powered by Mirai, resulting in one of the largest attacks on record, exceeding 620 gigabits per second. Later on in the same month, another Mirai attack broke the record for the largest DdoS attack, which was at least 1.1 terabits per second, spanning up to 1.5 Tbps. At the end of September 2016, the malware source code was published

online, opening up the possibility of widespread DdoS attacks and more botnets being created (Lorenzo Franceschi-Bicchierai, 2016).

Steps are necessary from both the general public and cybersecurity professionals. Cybersecurity professionals should strengthen networks against the chance of a DdoS attack. Users should reboot their IoT devices to clear the malware, then change the password to a secure one, so that devices become harder to infect and the size of botnets decrease. ("Heightened DDoS Threat Posed by Mirai and Other Botnets", 2016) The government could even take it further to make it compulsory to change the default passwords of IoT devices.

References

Callisch, D. (2010). Coping with Wi-Fi's biggest problem: interference. Network World. Retrieved 19 January 2017, from http://www.networkworld.com/article/2215287/tech-primers/coping-with-wi-fi-s-biggest-problem--interference.html

Dyn, Inc. Status - DDoS Attack Against Dyn Managed DNS. (2016). *Dynstatus.com*. Retrieved 19 January 2017, from https://www.dynstatus.com/incidents/nlr4yrr162t8

Fitzpatrick, J. (2013). *The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords*. *Howtogeek.com*. Retrieved 19 January 2017, from http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

Franceschi-Bicchierai, L. (2016). *Twitter, Reddit, Spotify Were Collateral Damage In Major Internet Attack*. *Motherboard*. Retrieved 19 January 2017, from https://motherboard.vice.com/read/twitter-reddit-spotify-were-collateral-damage-in-major-internet-attack

Franceschi-Bicchierai, L. (2016). *The Internet of Things Sucks So Bad Even 'Amateurish' Malware Is Enough*. *Motherboard*. Retrieved 19 January 2017, from https://motherboard.vice.com/read/internet-of-things-malware-mirai-ddos

Franceschi-Bicchierai, L. (2016). *Blame the Internet of Things for Destroying the Internet Today*. *Motherboard*. Retrieved 19 January 2017, from https://motherboard.vice.com/read/blame-the-internet-of-things-for-destroying-the-internet-today

Gopalaratnam, S. (2015). In-store analytics: tracking real-world customers just like online shoppers. TechRadar. Retrieved 20 January 2017, from http://www.techradar.com/news/world-of-tech/future-tech/in-store-analytics-tracking-real-world-customers-just-like-online-shoppers-1286293

Heightened DDoS Threat Posed by Mirai and Other Botnets. (2016). *Us-cert.gov*. Retrieved 19 January 2017, from https://www.us-cert.gov/ncas/alerts/TA16-288A

Hoffman, C. (2014). *Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both?*. *Howtogeek.com*. Retrieved 19 January 2017, from http://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/

Krebs, B. (2016). *DDoS on Dyn Impacts Twitter, Spotify, Reddit — Krebs on Security*. *Krebsonsecurity.com*. Retrieved 19 January 2017, from https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

Newman, L. (2016). *The Botnet That Broke the Internet Isn't Going Away*. *WIRED*. Retrieved 19 January 2017, from https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

What is WiFi roaming - How Wifi roaming works - WiFi roaming. (2016). *WiFi Notes*. Retrieved 19 January 2017, from http://wifinotes.com/how-wifi-roaming-works.html

York, K. (2016). *Dyn Statement on 10/21/2016 DDoS Attack | Dyn Blog*. *Dyn.com*. Retrieved 19 January 2017, from http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/