By: Ronald van Kleunen (CWNE #108) – Twitter @Globeron  – E-mail:  ronald@globeron.com

Date: 7 August 2016  - Version 1.0

## Wi-Fly or We-Cry?

## Wi-Fi AA:  Wi-Fi at Airports and in Airplanes

## HD-MCII – High Density Moving Clients Induced Interference

While travelling it almost becomes a standard habit to understand how system integrators and/or vendors implement their Wi-Fi solutions at airports and airplanes. This is the first write-up with the focus on an airport. This "Wi-Fi design" is a typical sales approach; sell as many APs plus antenna's as possible. Sometimes I call this the "1 AP per traveler" approach. The installation is a problem as APs are mounted too close to each other (e.g. 1x AP per two check-in rows and 4x APs per area). Having seen many airports, this is the only one I have seen so far where all 5 GHz channels have been used by the service providers.
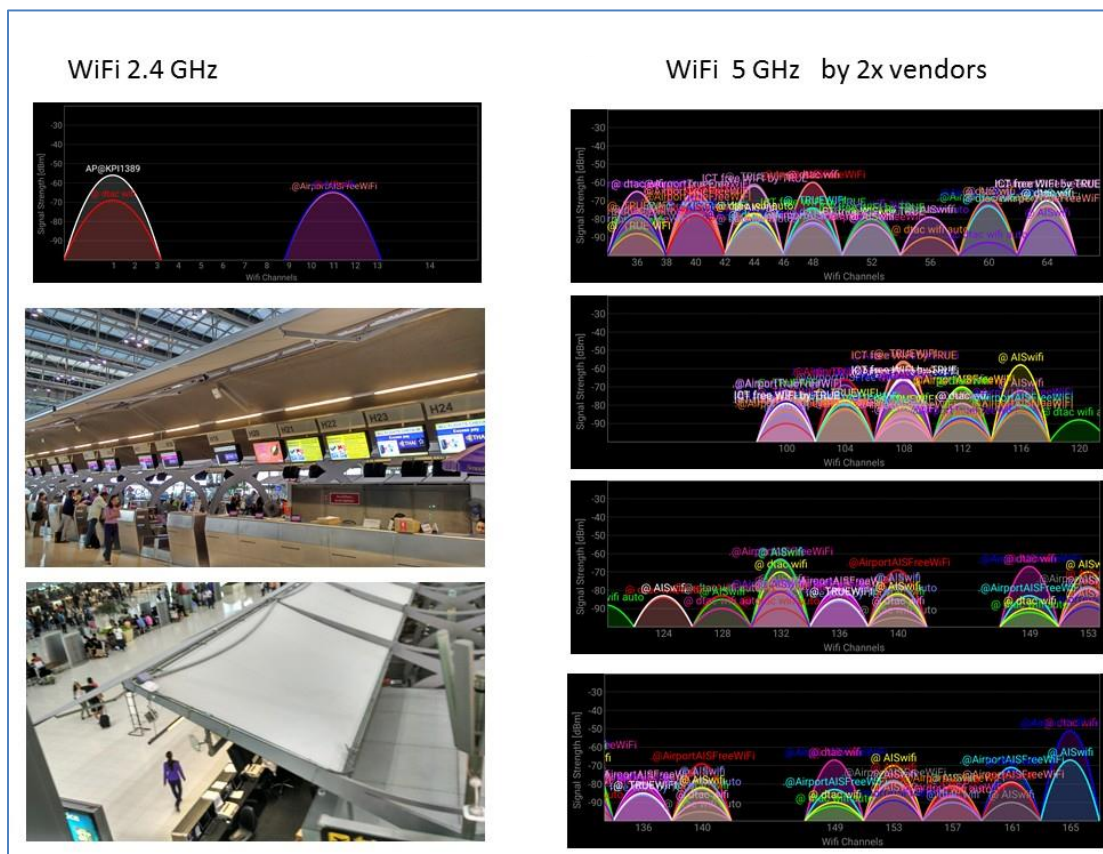
However having all APs and multiple SSIDs on these channels does not mean that clients are connected to it and therefore a deeper Wi-Fi analysis is required. This Wi-Fi analysis is done at a single physical location (no walking or roaming has been done). It was also done during peak hour (Sunday afternoon) to understand what can be observed.



Similar as at many locations globally the 2.4 GHz Spectrum is full, with the main transmissions on Channel 1, 6 and 11 and Bluetooth (FHSS) activity over the band.
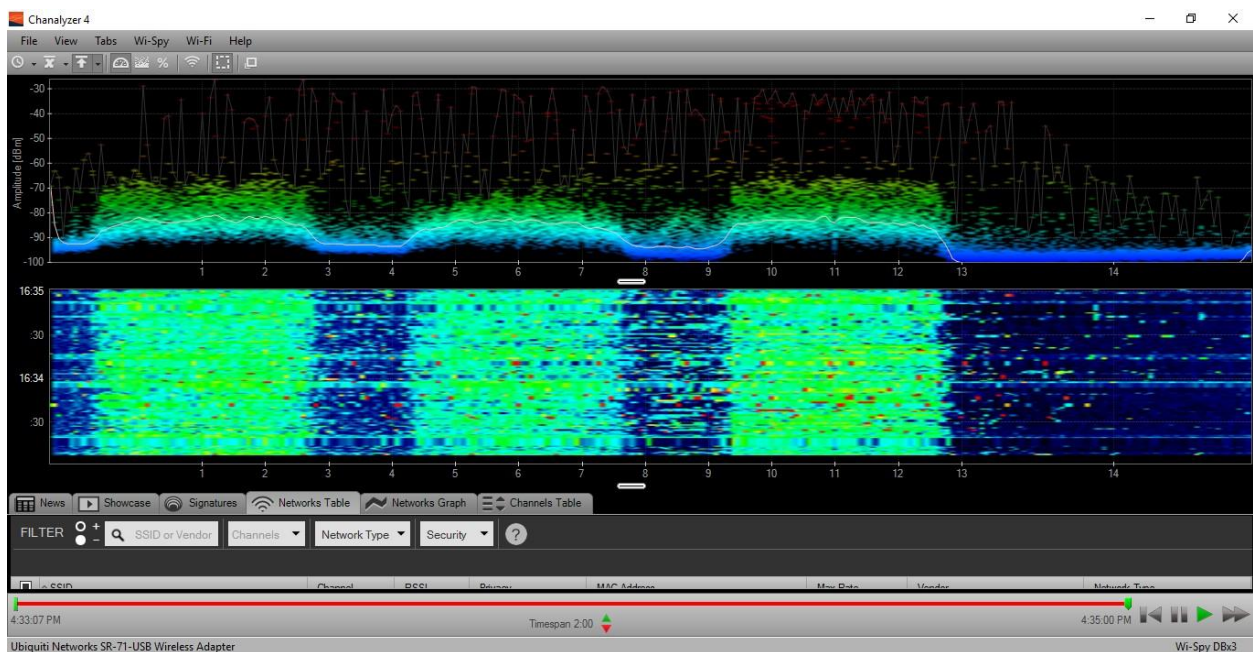
Looking into the 5 GHz spectrum, the transmissions are equally spread over the UNII-bands. Channel 36 looks higher in utilization, because this is the Primary channel used to send the Beacons (20 MHz bandwidth) by the APs. Note most APs are configured for 80 MHz channels (36+40+44+48), or in correct IEEE 802.11ac standard terminology channel "42". Similar for channel 149 is used as the Beacon channel (802.11ac 80 MHz channel "155"). Clients connected to these 80 MHz APs are in most cases only using 20 MHz bandwidth.
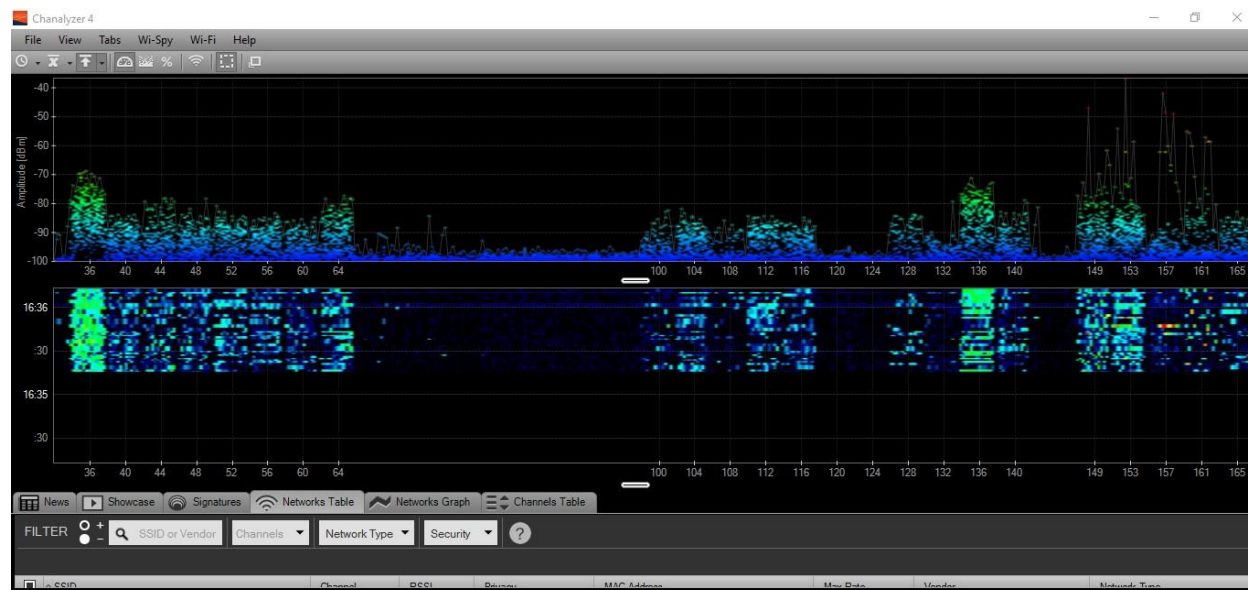


Most APs and SSIDs are configured for 80 MHz channels (36+40+44+48) and (149+153+157+161) and the rest of the channels on single 20 MHz channels. The screenshots below are subsets of the reconnaissance done.

| SSID | MAC Address | RSSI | Chan | 802.11 | Max Speed | WEP | WPA | WPA2 | WPS | Vendor | First | La |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 99:6D:0E | -80 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:16 | now |
| | F0:19:FA | -66 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:13 | 00:00: |
| | AC:10:ED | -82 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:13 | 00:03: |
| | F4:DB:AA | -72 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:16 | 00:00: |
| | B3:C1:5E | -64 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:13 | now |
| | CC:52:EC | -88 | 64 | a, n | 216.7 Mbps | | MGT-CCMP | MGT-CCMP | | | 16:37:16 | 00:01: |
| | F6:23:9A | -70 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:13 | 00:00: |
| | F6:23:9C | -72 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:13 | 00:00: |
| | 8C:52:EC | -88 | 64 | a, n | 216.7 Mbps | Open | | | | | 16:37:16 | 00:02: |
| | 8A:26:9B | -72 | 36+40+44+48 | n, ac | 1300.05 Mbps | | | PSK-CCMP | | | 16:37:13 | 00:00: |
| | 8A:26:9F | -72 | 36+40+44+48 | n, ac | 1300.05 Mbps | | | PSK-CCMP | | | 16:37:13 | 00:00: |
| | 4C:52:EC | -88 | 64 | a, n | 216.7 Mbps | Open | | | | | 16:37:16 | 00:01: |
| | 0C:52:ED | -89 | 64 | a, n | 216.7 Mbps | | | MGT-CCMP | | | 16:37:16 | 00:01: |
| | 0C:52:EC | -87 | 64 | a, n | 216.7 Mbps | Open | | | | | 16:37:16 | 00:02: |
| | 57:85:49 | -87 | 36+40+44+48 | n, ac | 1300.05 Mbps | | | MGT-CCMP | | | 16:37:16 | 00:02: |
| | 68:36:5D | -79 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:13 | 00:00: |
| | AB:7E:FA | -76 | 36+40+44+48 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:13 | 00:00: |
| | AB:7E:FB | -76 | 36+40+44+48 | n, ac | 1300.05 Mbps | | | PSK-CCMP | | | 16:37:13 | 00:00: |
| | CA:88:A9 | -77 | 36+40+44+48 | n, ac | 1300.05 Mbps | | | MGT-CCMP | | | 16:37:13 | 00:00: |
| | 54:11:CC | -84 | 40 | a, n | 144.4 Mbps | | | | | | 16:37:13 | 00:01: |
| | 0D:9D:8D | -80 | 44 | a, n | 216.7 Mbps | | | MGT-CCMP | | | 16:37:13 | 00:00: |



| SSID | MAC Address | RSSI | Chan | 802.11 | Max Speed | WEP | WPA | WPA2 | WPS | Vendor | First | Las |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | DC:80:8A | -76 | 149+153+157+161 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:30 | 00:00:2 |
| | F2:ED:9F | -75 | 40 | n, ac | 1300.05 Mbps | | | PSK-CCMP | | | 16:37:30 | 00:00:2 |
| | E9:04:7A | -80 | 149+153+157+161 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:30 | 00:03:2 |
| | E9:04:7C | -81 | 149+153+157+161 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:30 | 00:00:2 |
| | E9:04:7E | -81 | 149+153+157+161 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:30 | 00:03:4 |
| | F2:ED:49 | -77 | 149+153+157+161 | n, ac | 1300.05 Mbps | | | MGT-CCMP | | | 16:37:30 | 00:03:3 |
| | F2:ED:4C | -76 | 149+153+157+161 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:30 | 00:03:2 |
| | B3:C8:0E | -72 | 149+153+157+161 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:30 | 00:03:4 |
| | 35:80:3D | -85 | 64 | a, n | 216.7 Mbps | | | MGT-CCMP | | | 16:37:30 | 00:00:1 |
| | F0:19:F9 | -67 | 36+40+44+48 | n, ac | 1300.05 Mbps | | | MGT-CCMP | | | 16:37:30 | 00:00:2 |
| | 1A:D3:89 | -79 | 149+153+157+161 | n, ac | 1300.05 Mbps | | | MGT-CCMP | | | 16:37:30 | 00:03:4 |
| | 1A:D3:8B | -79 | 149+153+157+161 | n, ac | 1300.05 Mbps | | | PSK-CCMP | | | 16:37:30 | 00:03:3 |
| | 1A:D3:8E | -81 | 149+153+157+161 | n, ac | 1300.05 Mbps | | | | | | 16:37:30 | 00:03:4 |
| | CD:01:5C | -80 | 157 | a, n | 216.7 Mbps | | MGT-CCMP | MGT-CCMP | | | 16:37:30 | 00:00:2 |
| | 8D:01:5C | -80 | 157 | a, n | 216.7 Mbps | Open | | | | | 16:37:30 | 00:00:2 |
| | F2:E7:0C | -78 | 149+153+157+161 | n, ac | 1300.05 Mbps | Open | | | | | 16:37:30 | 00:03:1 |
| | 4D:01:5C | -81 | 157 | a, n | 216.7 Mbps | Open | | | | | 16:37:30 | 00:00:2 |
| | 0D:01:5D | -79 | 157 | a, n | 216.7 Mbps | | | MGT-CCMP | | | 16:37:30 | 00:03:2 |
| | FA:A4:6C | -81 | 157 | a, n | 216.7 Mbps | | MGT-CCMP | MGT-CCMP | | | 16:37:30 | 00:03:4 |
| | BA:A4:6C | -81 | 157 | a, n | 54 Mbps | Open | | | | | 16:37:30 | 00:03:4 |
| | CA:86:CA | -70 | 36+40+44+48 | n, ac | 1300.05 Mbps | | | | | | 16:37:30 | 00:00:3 |

These 80 MHz channels occupy most of the UNII-1 and UNII-3 bands, which means less spectrum available for other APs on these channels (in that specific area as the scan is done at one location only).

It is also good to understand how many STA (Stations) client actually connect to these APs on 5 GHz. The following reconnaissance is done with a packet / protocol analyzer to see the trend at different time intervals.

After 01.50 minutes, the following was observed:

- Wireless Networks:  26
- Access Points: 954
- Clients: 1,317



After 04.07 minutes, the following was observed:

- Wireless Networks:  29
- Access Points: 1,071
- Clients: 2,944

After 14.23 minutes, the following was observed:

- Wireless Networks:  56
- Access Points: 1894
- Clients: 10,557



But one of the issues is that the protocol/packet analyser is not aggregating the Wi-Fi devices properly (on both 2.4 GHz and 5 GHz, like dual-band clients probing for the network or clients moving channels). An example of redundant clients (STA's) is shown in the screenshot below (indicated with red rectangles).
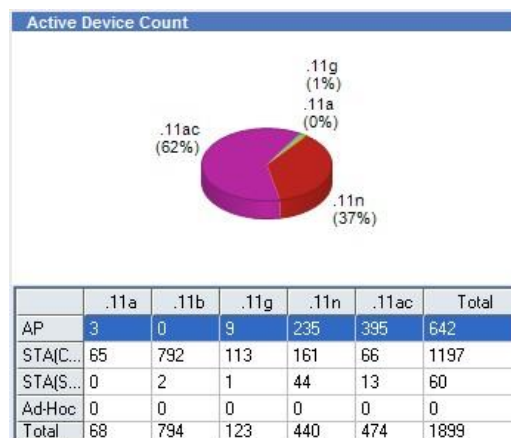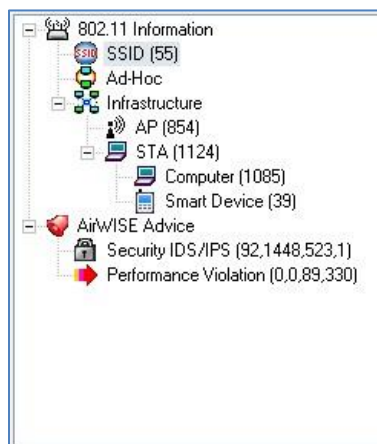
Therefore the packet/protocol capture has been exported and imported into another Wi-Fi tool to see if the Wi-Fi devices could be aggregated. One packet/protocol analyser visualized it better, but still different aggregations are observed.

After 14.23 minutes, the following could be seen:

- SSIDs:  55
- AP    : 854                        AP: 642
- STA  : 1124                      STA:  1197 + 60 = 1257





| | .11a | .11b | .11g | .11n | .11ac | Total |
|---|---|---|---|---|---|---|
| AP | 3 | 0 | 9 | 235 | 395 | 642 |
| STA(C... | 65 | 792 | 113 | 161 | 66 | 1197 |
| STA(S... | 0 | 2 | 1 | 44 | 13 | 60 |
| Ad-Hoc | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 68 | 794 | 123 | 440 | 474 | 1899 |

Furthermore note the distribution of Active Device counts per IEEE standard:

- IEEE 802.11ac :  62%
- IEEE 802.11n   : 37%
- IEEE 802.11a   :  0%
- IEEE 802.11g   :  1%

Another issue are the Wi-Fi clients RF transmissions, which have been explained in-depth by:

- Keith Parsons (CWNE #3):  see the ("**Don't Want**") part
  Reference: http://wirelesslanprofessionals.com/wp-content/uploads/2010/01/Want-Dont-Want-Dont-Care.pdf
- Devin Akin (CWNE #1): See minute 25:27  **("Client Induced Interference")**
  Reference: https://www.brighttalk.com/webcast/5522/178095/designing-for-one-ap-per-classroom
- Gregor Vucajnk (CWNE # 96):  WLPC Dallas 2015 conference, see minute 39:00 onwards
  (**visualizing Client RF coverage area in Ekahau**). Reference:  https://vimeo.com/120208422

Because of the exponential growth of Wi-Fi clients and especially when they are moving (roaming), there is another issue at airports. These moving clients in public Wi-Fi environments can be categorized as:  **"HD-MCII:  High Density – Moving Client Induced Interference".**

You will see other scenarios of HD-MCII at high density train stations, especially at train interchanges when people move in and out the train. Sometimes these type of train stations are located and integrated with the airports, sometimes they are located underground, sometimes above the ground ("sky trains") and some are far enough of the main airport terminals' Wi-Fi networks.

MRT – Mass Rapid Train