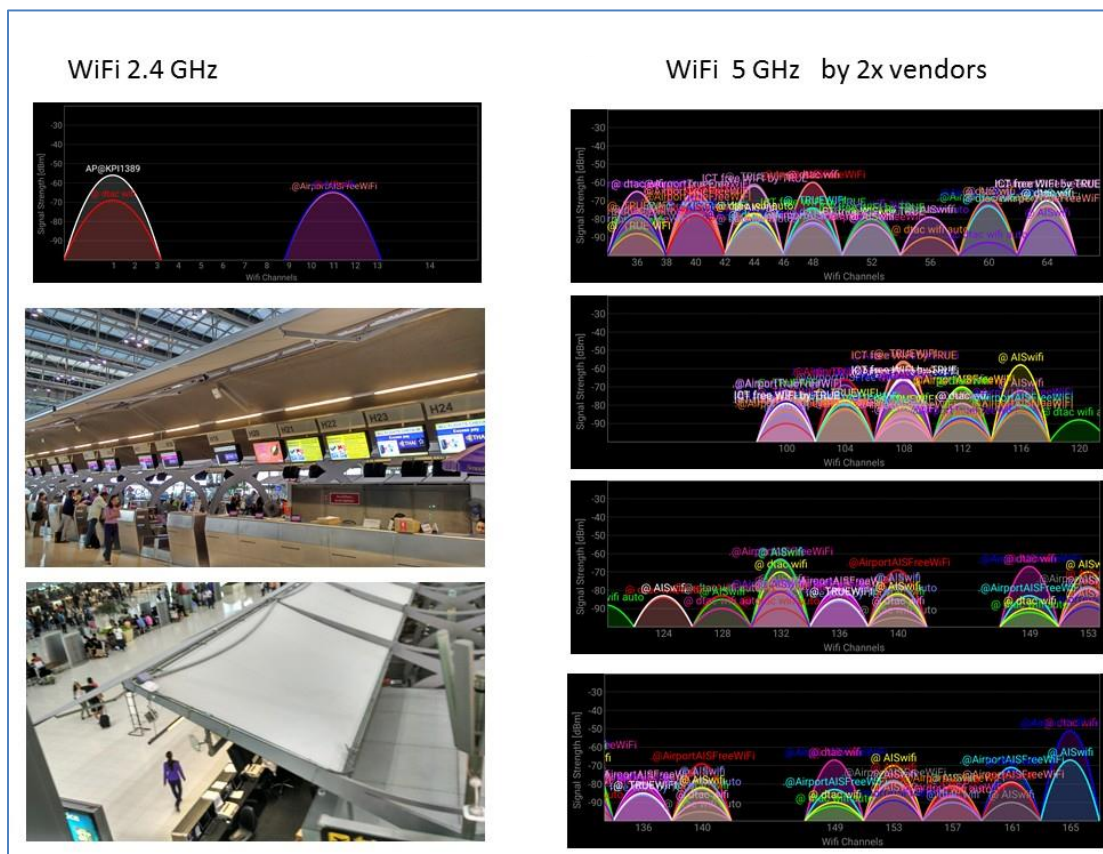


Wi-Fly or We-Cry?

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

HD-MCII – High Density Moving Clients Induced Interference

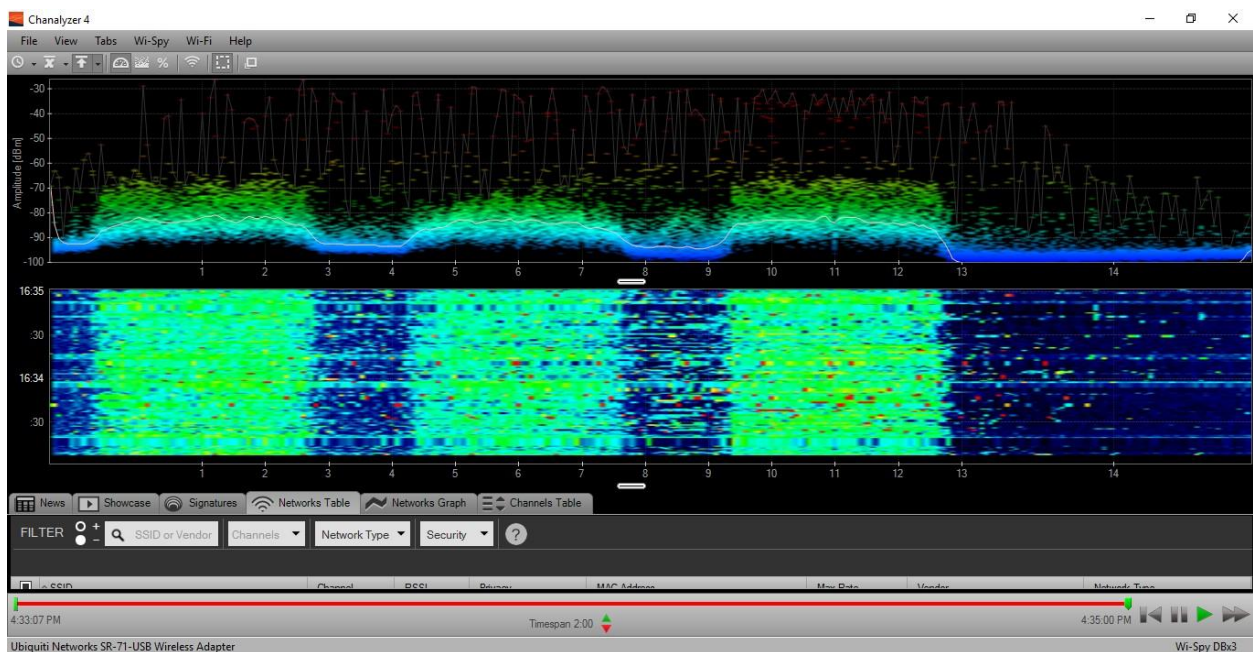
While travelling it almost becomes a standard habit to understand how system integrators and/or vendors implement their Wi-Fi solutions at airports and airplanes. This is the first write-up with the focus on an airport. This “Wi-Fi design” is a typical sales approach; sell as many APs plus antenna’s 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.



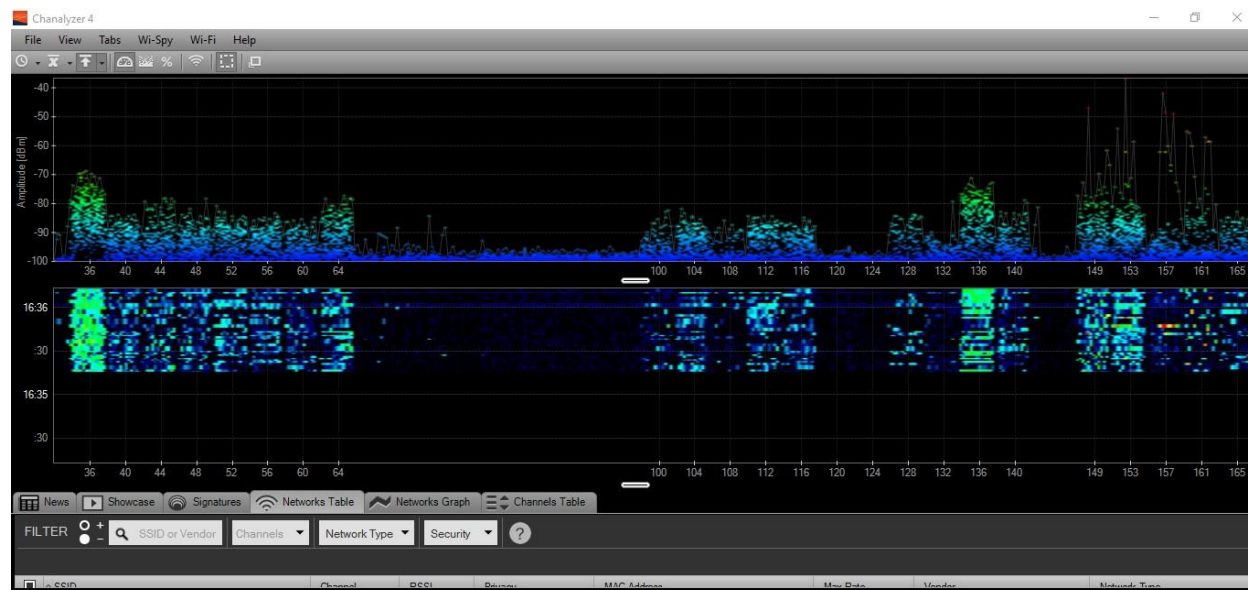
However having all APs and multiple SSIDs on these channels does not mean that clients are connected to it and therefore a deeper Wi-Fi analysis is required. This Wi-Fi analysis is done at a single physical location (no walking or roaming has been done). It was also done during peak hour (Sunday afternoon) 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	Last
9B:4A:0C	-76	64	a, n	54 Mbps Open							16:36:59	now
D3:C6:58	-71	1	g, n	144.4 Mbps			MGT-CCMP	MGT-CCMP			16:36:59	now
B7:03:BE	-70	36+40+44+48	n, ac	1300.05 Mbps Open							16:36:59	00:00:5
1B:4A:0D	-74	64	a, n	54 Mbps				MGT-CCMP			16:36:59	00:00:0
95:AA:2C	-84	40	a, n	54 Mbps Open							16:36:59	00:00:0
55:AA:2C	-86	40	a, n	54 Mbps Open							16:36:59	00:00:0
13:C6:59	-70	1	g, n	54 Mbps				MGT-CCMP			16:36:59	now
B7:03:7B	-66	36+40+44+48	n, ac	1300.05 Mbps				PSK-CCMP			16:36:59	00:00:0
99:5D:09	-77	36+40+44+48	n, ac	1300.05 Mbps				MGT-CCMP			16:36:59	00:00:0
99:6F:89	-71	36+40+44+48	n, ac	1300.05 Mbps				MGT-CCMP			16:36:59	00:00:3
15:AA:2C	-84	40	a, n	54 Mbps Open							16:36:59	00:00:0
99:6F:8C	-95	36+40+44+48	n, ac	1300.05 Mbps Open							16:36:59	00:00:3
F2:E6:A9	-69	36+40+44+48	n, ac	1300.05 Mbps							16:36:59	00:00:0
35:80:3C	-83	64	a, n	216.7 Mbps Open				MGT-CCMP			16:36:59	now
F2:E6:A8	-67	36+40+44+48	n, ac	1300.05 Mbps Open							16:36:59	now
F6:22:DC	-72	36+40+44+48	n, ac	1300.05 Mbps Open							16:36:59	00:00:0
16:F9:9B	-75	36+40+44+48	n, ac	1300.05 Mbps				PSK-CCMP			16:36:59	00:00:0
CF:8E:6C	-78	60	a, n	216.7 Mbps			MGT-CCMP	MGT-CCMP			16:36:59	00:00:1
D0:7C:2C	-76	40	a, n	216.7 Mbps			MGT-CCMP	MGT-CCMP			16:36:59	00:00:1
CD:F4:BA	-73	44	n, ac	1300.05 Mbps Open							16:36:59	now
DC:82:79	-88	36+40+44+48	n, ac	1300.05 Mbps				MGT-CCMP			16:36:59	00:03:1

Acrylic Wi-Fi Home GO Pro f g+ t in												
SSID	MAC Address	RSSI	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Vendor	First	La
	99:5D: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:D8:AA	-72	36+40+44+48	n, ac	1300.05 Mbps Open						16:37:16	00:00:
	B3:C1:EE	-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:82:EC	-88	64	a, n	216.7 Mbps Open						16:37:16	00:00:
	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	00:00:
	57:85:49	-87	36+40+44+48	n, ac	1300.05 Mbps			MGT-CCMP			16:37:16	00:02:
	68:36:ED	-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:8B: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 Open						16:37:13	00:01:
	0D:9D:8D	-80	44	a, n	216.7 Mbps			MGT-CCMP			16:37:13	00:00:
	AD:01:00	-83	56	a, n	216.7 Mbps Open						16:37:13	00:00:

Acrylic Wi-Fi Home GO Pro f g+ t in												
SSID	MAC Address	RSSI	Chan	802.11	Max Speed	WEP	WPA	WPA2	WPS	Vendor	First	Las
	DC:8D: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:CB: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:D9:89	-79	149+153+157+161	n, ac	1300.05 Mbps			MGT-CCMP			16:37:30	00:03:4
	1A:D9:8B	-79	149+153+157+161	n, ac	1300.05 Mbps			PSK-CCMP			16:37:30	00:03:3
	1A:D9:8E	-81	149+153+157+161	n, ac	1300.05 Mbps Open						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
	BD: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 Open						16:37:30	00:00:3
	AD:01:00	-83	56	a, n	216.7 Mbps Open			PSK-CCMP			16:37:30	00:03:4

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

Node	Type	Channel	Band	Encryption	Trust	Cur. Signal	Cur. Noise	Total Bytes	Packets Sent	Packets Received	Total F
ArubaNetwork:13:59:4A	AP	165	802.11a		Unknown	42	7	1,836	11	5	
Mango	ESSID	60						0	0	0	
24:DE:C6:5A:FF:DC	AP	60	802.11a	COMP	Unknown	2	0	370	2	0	
LSB8	ESSID	60						0	0	0	
Cisco-LinkBE:07:55	AP	60	802.11a		Unknown	18	0	21,055	203	10	
PG-Guest	ESSID	60, 149, 157...						0	0	0	
24:DE:C6:5A:FF:D8	AP	60	802.11a		Unknown	0	0	166	1	0	
ArubaNetwork:49:AA:D4	AP	149	802.11a		Unknown	57	10	3,558	22	4	
24:DE:C6:5A:FF:FD	AP	157	802.11a		Unknown	55	7	4,445	27	7	
24:DE:C6:5A:FF:7C	AP	161	802.11a		Unknown	60	7	6,094	40	2	
24:DE:C6:5A:FF:5C	AP	161	802.11a		Unknown	50	7	6,083	40	2	
Customs_WiFi1	ESSID	149						0	0	0	
04BD:88:9A:81:12	AP	149	802.11a	COMP	Unknown	20	2	241	1	0	
GOA	ESSID	149, 157, 16...						0	0	0	
ArubaNetwork:49:AA:D0	AP	149	802.11a		Unknown	57	24	4,948	43	8	
20D3:90:2E:D1:17	STA	149	802.11a		Unknown	26	10	878	4	26	
24:DE:C6:5A:FF:FB	AP	157	802.11a		Unknown	55	7	4,896	31	5	
24:DE:C6:5A:FF:7A	AP	161	802.11a		Unknown	57	5	4,701	31	4	
24:DE:C6:5A:FF:5A	AP	161	802.11a		Unknown	52	2	5,917	38	6	
ArubaNetwork:13:59:48	AP	165	802.11a		Unknown	39	5	1,817	12	2	
BB850Hz	ESSID	161						0	0	0	
CC:E1D5:30:75:66	AP	161	802.11a	COMP	Unknown	100	5	6,195	21	0	
PG-Rowf	ESSID	165						0	0	0	
ArubaNetwork:13:59:4D	AP	165	802.11a		Unknown	37	2	2,127	13	3	

After 04.07 minutes, the following was observed:

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

Node	Type	Channel	Band	Encryption	Trust	Cur. Signal	Cur. Noise	Total Bytes	Packets Sent	Packets Received	Total F
THAI AIRWAYS	ESSID	1						0	0	0	
Cisco-A1:A5:61	AP	1	802.11b		Unknown	63	31	1,517	7	0	
@ dtac wifi	ESSID	1, 11, 36, 4...						0	0	0	
2C:5D:93:9B:3F:48	AP	1	802.11bg		Unknown	68	37	7,241	37	1	
2C:5D:93:9B:4A:78	AP	1	802.11bg		Unknown	60	31	2,398	12	2	
24:C9:A1:93:C6:58	AP	1	802.11bg		Unknown	70	31	21,140	109	6	
24:C9:A1:8D:25:C8	AP	11	802.11bg		Unknown	73	37	3,360	17	1	
24:C9:A1:8D:2C:08	AP	11	802.11bg		Unknown	76	34	50,018	261	23	
24:C9:A1:85:7E:4C	AP	36	802.11a		Unknown	23	7	7,793	49	7	
34:31:11:8E:46:CF	STA	36	802.11a		Unknown	2	0	394	1	12	
2C:5D:93:8F:6B:1C	AP	40	802.11a		Unknown	7	0	8,370	43	5	
2C:5D:93:8C:AC:2C	AP	40	802.11a		Unknown	13	0	2,100	11	3	
2C:5D:93:90:7C:2C	AP	40	802.11a		Unknown	10	0	6,173	33	1	
24:C9:A1:8F:19:DC	AP	40	802.11a		Unknown	13	0	1,168	6	5	
2C:5D:93:8D:5A:8C	AP	44	802.11a		Unknown	15	0	7,774	40	7	
2C:5D:93:8D:90:8C	AP	44	802.11a		Unknown	2	0	2,031	10	8	
24:C9:A1:8F:18:9C	AP	44	802.11a		Unknown	13	0	3,422	17	5	
8C:0C:90:8D:33:CC	AP	44	802.11a		Unknown	2	0	415	2	0	
2C:5D:93:8C:AE:2C	AP	44	802.11a		Unknown	15	2	7,157	36	4	
2C:5D:93:9B:49:7C	AP	44	802.11a		Unknown	15	5	7,210	39	16	
2C:5D:93:8C:AB:5C	AP	48	802.11a		Unknown	13	0	15,047	82	13	
24:C9:A1:94:55:5C	AP	48	802.11a		Unknown	2	0	421	2	2	
2C:5D:93:8C:B0:5C	AP	48	802.11a		Unknown	7	0	426	2	4	
2C:5D:93:8D:05:4C	AP	48	802.11a		Unknown	2	0	449	2	4	

After 14.23 minutes, the following was observed:

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

Omnipeek interface showing network statistics and a list of wireless networks. The top bar indicates 485,743 packets received and 100% buffer usage. The left sidebar shows various filters and views. The main table lists wireless networks with columns for Node, Type, Channel, Band, Encryption, Trust, Cur. Signal, Cur. Noise, Total Bytes, Packets Sent, Packets Received, and Total F.

Node	Type	Channel	Band	Encryption	Trust	Cur. Signal	Cur. Noise	Total Bytes	Packets Sent	Packets Received	Total F
THAIAIRWAYS	ESSID	1						0	0	0	
00:C1:64:B3:C1:51	AP	1	802.11b		Unknown	44	15	12,899	59	2	
00:C1:64:F2:E6:A2	AP	1	802.11b		Unknown	47	15	504	2	0	
74:A2:E6:BF:00:F1	AP	6	802.11b		Unknown	50	23	1,512	6	0	
80:AA:77:BA:2B:D1	AP	11	802.11b		Unknown	47	15	1,546	7	1	
00:C1:64:99:74:51	AP	11	802.11b		Unknown	39	7	252	1	0	
74:A2:E6:CE:D7:31	AP	11	802.11b		Unknown	52	23	504	2	0	
00:C1:64:99:72:CE	AP	36	802.11a		Unknown	60	20	2,520	10	0	
00:C8:8B:F6:26:ED	AP	36	802.11a		Unknown	5	0	2,037	7	0	
00:C8:8B:AB:7E:FE	AP	36	802.11a		Unknown	0	0	3,201	11	0	
74:A2:E6:CA:88:FE	AP	36	802.11a		Unknown	5	0	3,201	11	0	
74:A2:E6:CD:F7:6E	AP	36	802.11a		Unknown	2	0	1,455	5	0	
00:C1:64:99:67:4E	AP	36	802.11a		Unknown	2	0	1,746	6	0	
00:C8:8B:1B:9D:2D	AP	36	802.11a		Unknown	2	0	3,201	11	0	
00:C1:64:FF:F7:6D	AP	36	802.11a		Unknown	0	0	291	1	0	
00:C1:64:99:6F:8E	AP	36	802.11a		Unknown	0	0	582	2	0	
74:A2:E6:CA:88:DE	AP	36	802.11a		Unknown	15	0	12,513	43	0	
00:C1:64:99:6F:8E	AP	36	802.11a		Unknown	23	10	9,603	33	0	
00:C1:64:DC:83:BE	AP	36	802.11a		Unknown	34	13	11,349	39	0	
00:C1:64:99:69:5E	AP	36	802.11a		Unknown	0	0	291	1	0	
00:C1:64:99:71:3E	AP	36	802.11a		Unknown	15	0	582	2	0	
74:A2:E6:BF:00:F0	AP	36	802.11a		Unknown	47	10	58,782	202	0	
74:A2:E6:BF:03:BE	AP	36	802.11a		Unknown	18	2	11,640	40	0	

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).

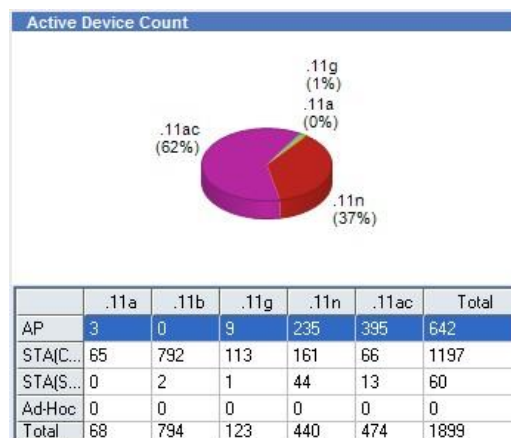
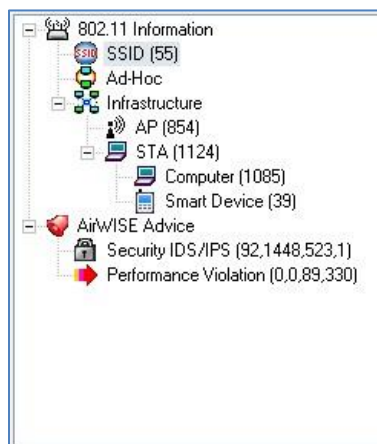
Omnipeek interface showing a list of wireless networks. The top bar indicates 485,743 packets received and 100% buffer usage. The left sidebar shows various filters and views. The main table lists wireless networks with columns for Node, Type, Channel, Band, Encryption, Trust, Cur. Signal, Cur. Noise, Total Bytes, Packets Sent, Packets Received, and Total F.

Node	Type	Channel	Band	Encryption	Trust	Cur. Signal	Cur. Noise	Total Bytes	Packets Sent	Packets Received	Total F
FE:28:45:F1:1A:60	STA	44	802.11a		Unknown			2,332	0	11	
FE:28:45:F1:1A:60	STA	128	802.11a		Unknown	18	2	1,157	1	5	
FE:28:45:F1:1A:60	STA	112	802.11a		Unknown	26	0	935	1	4	
FE:2E:97:F3:81:E0	STA	108	802.11a		Unknown			196	0	1	
FE:30:6B:BD:30:ED	STA	136	802.11a		Unknown			187	0	1	
FE:3A:FB:4B:06:88	STA	161	802.11a		Unknown			302	0	2	
FE:3F:02:11:B8:90	STA	149	802.11a		Unknown			448	0	3	
FE:3F:02:11:B8:90	STA	56	802.11a		Unknown			234	0	1	
FE:3F:02:11:B8:90	STA	132	802.11a		Unknown			436	0	2	
FE:45:8D:56:CE:07	STA	149	802.11a		Unknown			194	0	1	
FE:45:8D:56:CE:07	STA	153	802.11a		Unknown	26	7	122	1	0	
FE:45:8D:56:CE:07	STA	149	802.11a		Unknown	31	7	122	1	0	
FE:51:0F:4B:14:6F:B	STA	112	802.11a		Unknown			383	0	2	
FE:51:0F:4B:14:6F:B	STA	140	802.11a		Unknown			2,342	0	11	
FE:5F:E4:19:AE:B6	STA	64	802.11a		Unknown			236	0	1	
FE:5F:E4:19:AE:B6	STA	100	802.11a		Unknown			598	0	3	
FE:60:82:85:12:98	STA	60	802.11a		Unknown			146	0	1	
FE:60:82:85:12:98	STA	44	802.11a		Unknown			602	0	3	
FE:70:88:6C:9D:28	STA	132	802.11a		Unknown			802	0	4	
FE:71:1B:C1:59:A3	STA	136	802.11a		Unknown	29	2	1,723	1	8	
FE:71:1B:C1:59:A3	STA	128	802.11a		Unknown			236	0	1	
FE:71:1B:C1:59:A3	STA	100	802.11a		Unknown	26	0	1,409	1	6	
FE:79:14:E1:AC:DE	STA	104	802.11a		Unknown			623	0	3	
FE:7D:99:AC:3C:84	STA	36	802.11a		Unknown			1,444	0	5	
FE:8E:23:4F:31:A9	STA	104	802.11a		Unknown			1,574	0	8	
FE:9C:D0:BD:31:6A	STA	108	802.11a		Unknown			2,062	0	10	

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
 - STA : 1124
- AP: 642
- STA: 1197 + 60 = 1257



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

