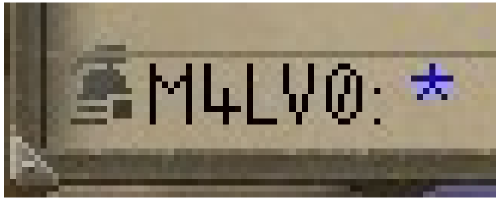
Lightbulb Moment

Robbie Mckennie

Who am I?

Robbie
Code, networks, electronics


M4LV0: *

Total level:
2053

The Scene

UBIQUITI NETWORKS

- Mikrotik router
- Unifi UAP-AC-LR
- Good performance, well made
- In my case, not the best mounting situation
- Floor

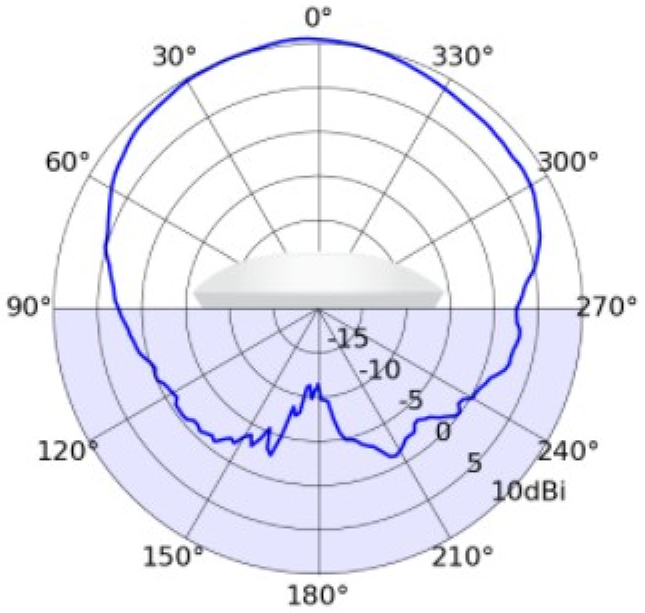
The Case

- Victim complains of slow wifi
- Victim was close to the access point
- No one else had any problems
- I think it’s nothing
- However

It keeps happening

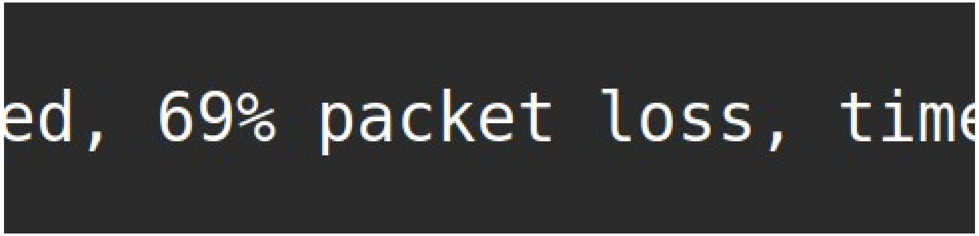
(and I keep hearing about it)

- Now I’m taking it seriously
- These APs aren’t optimized for “downwards”
- Shall we flip it over?



Now it’s personal

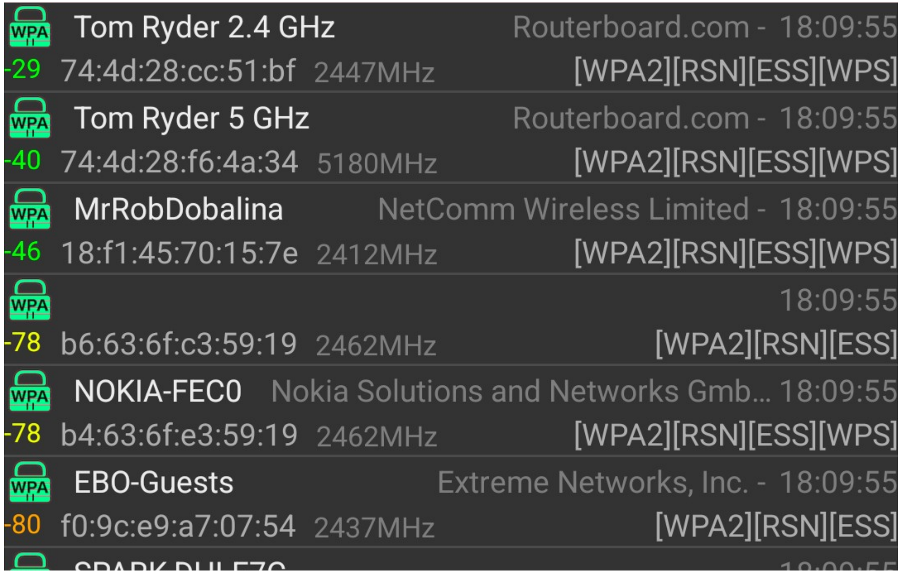
- Now I’m being directly affected
- High pings, packet loss
- So what gives?
- Extenders? IOT devices?



```
ed, 69% packet loss, time
```

Signal Strength II: The Channeling

- Let’s actually measure signal strength
- How’s our channel usage looking?



Tom Ryder 2.4 GHz — Routerboard.com - 18:09:55
-29 74:4d:28:cc:51:bf 2447MHz [WPA2][RSN][ESS][WPS]

Tom Ryder 5 GHz — Routerboard.com - 18:09:55
-40 74:4d:28:f6:4a:34 5180MHz [WPA2][RSN][ESS][WPS]

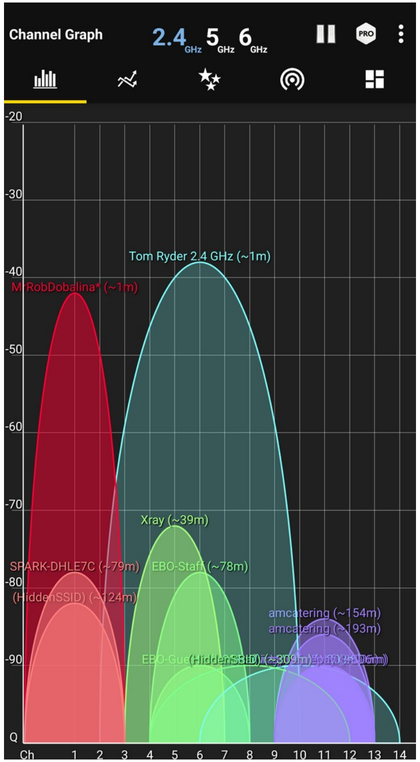
MrRobDobalina — NetComm Wireless Limited - 18:09:55
-46 18:f1:45:70:15:7e 2412MHz [WPA2][RSN][ESS][WPS]

18:09:55
-78 b6:63:6f:c3:59:19 2462MHz [WPA2][RSN][ESS]

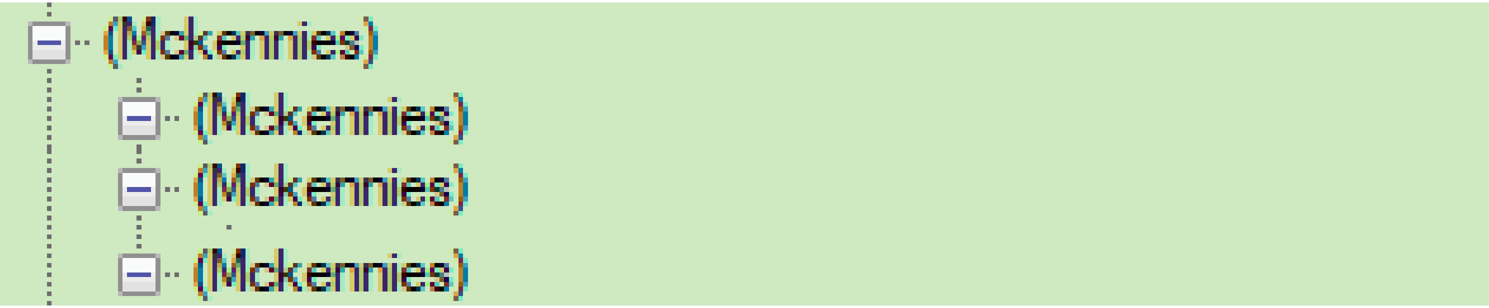
NOKIA-FEC0 — Nokia Solutions and Networks Gmb... 18:09:55
-78 b4:63:6f:e3:59:19 2462MHz [WPA2][RSN][ESS][WPS]

EBO-Guests — Extreme Networks, Inc. - 18:09:55
-80 f0:9c:e9:a7:07:54 2437MHz [WPA2][RSN][ESS]

SPARK-DHLE7C 18:09:55



The Shocking Realization



(Mckennies)

(Mckennies)

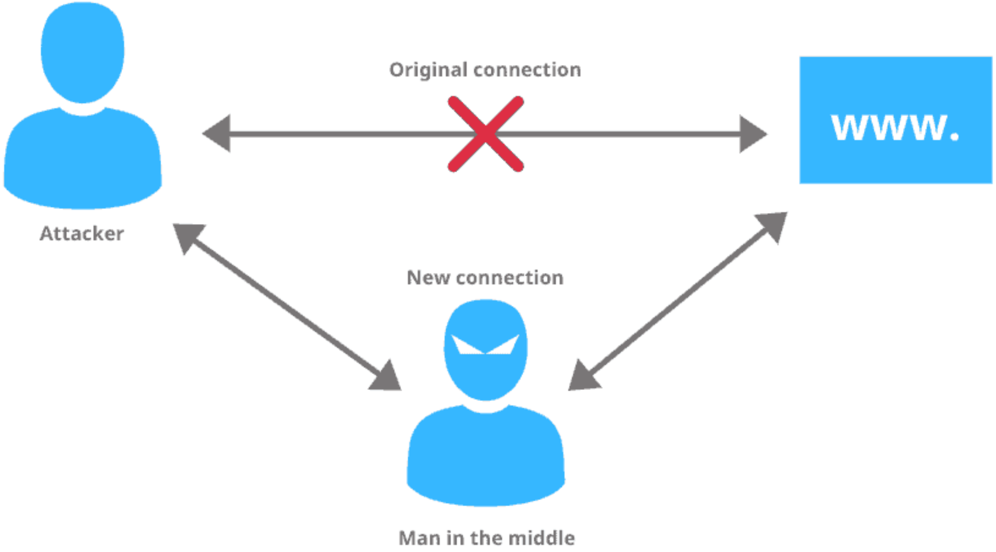
(Mckennies)

(Mckennies)

Changing the main SSID causes the extras to disappear
(And yes these are all 2.4GHz)

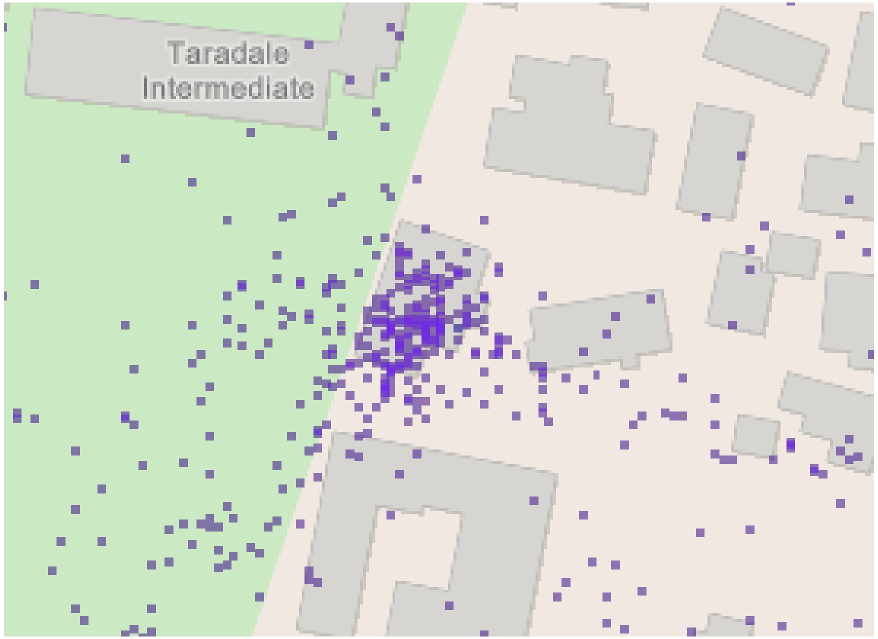
The Evil Twin Attack

A Man in the Middle



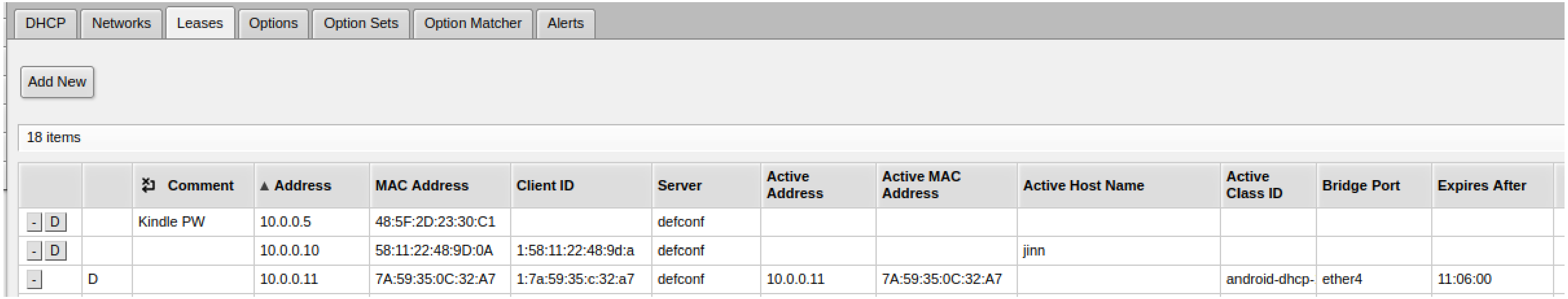
Time for a Fox Hunt

- Using signal strength, I can triangulate the position of the rogue AP



The WiFi is coming from inside the house!

It needs an IP address, right?



18 items

		Comment	▲ Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host Name	Active Class ID	Bridge Port	Expires After
- D		Kindle PW	10.0.0.5	48:5F:2D:23:30:C1		defconf						
- D			10.0.0.10	58:11:22:48:9D:0A	1:58:11:22:48:9d:a	defconf			jinn			
-	D		10.0.0.11	7A:59:35:0C:32:A7	1:7a:59:35:c:32:a7	defconf	10.0.0.11	7A:59:35:0C:32:A7		android-dhcp-	ether4	11:06:00

Migrated devices one by one to a new access point

And then there were two

- 2 devices left, 2 rogue access points
- Strange cryptic hostnames
- Maybe I can google it?
- And I learn

I was pwned by a god damn lightbulb

Postmortem

- So like what the hell?

Thanks