
cisco Live!
Let's go

The bridge to possible

Tune your Cisco Wi-Fi Designs for the Most Demanding Clients and Applications

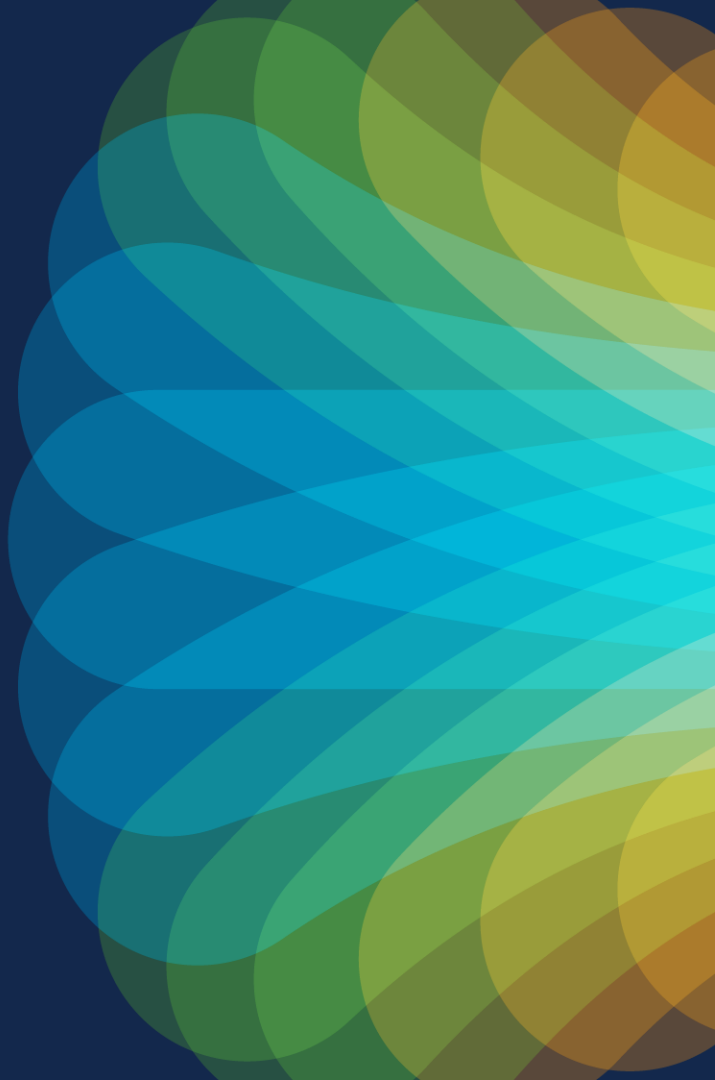
Boosted with Applied AI

Jerome Henry, Distinguished Engineer, Office of the Wireless CTO

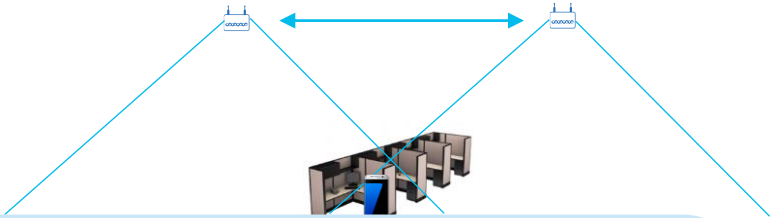
Agenda

- Introduction
- What is this Client?
  - How this information helps you
- How do your clients see the World?
  - Use it to better design your cells, their power and their overlap
- Why did the client leave?
  - Use it to better troubleshoot issues
- Conclusion

Why Are We Here Together?



Different Perspectives



AP

- AP understands its own RF environment and the success of downstream traffic
- AP sees client upstream data rate and the 'retry' bit, but can only infer why there is a difference
- AP has visibility of neighboring cells their client load

Client

- Client has limited awareness of other clients in the cell
- Client has limited awareness of neighboring cells
- Client has no awareness of cell edge location or next cell conditions

Cisco brings to your customer the client view

Cisco is the *only* company with the size and power to partner with the largest client vendors

Your clients send exclusive messages to Cisco APs that help make your network better

What is this client?

- Form factor (phone/tablet/laptop) – Helps learn behavior
- HW (what chipset), SW (what drivers, what OS)
- Spot bugs / specific behavior overrides

How does the client see the RF?

- AP RSSI, neighbor APs signal, Retries, problems

Why did it leave?

- 802.11 has ‘standard’ reasons
- what if you click another SSID in your client OS?
- User reasons, upper layer reasons, deeper 802.11 reasons

Next: let’s exchange further

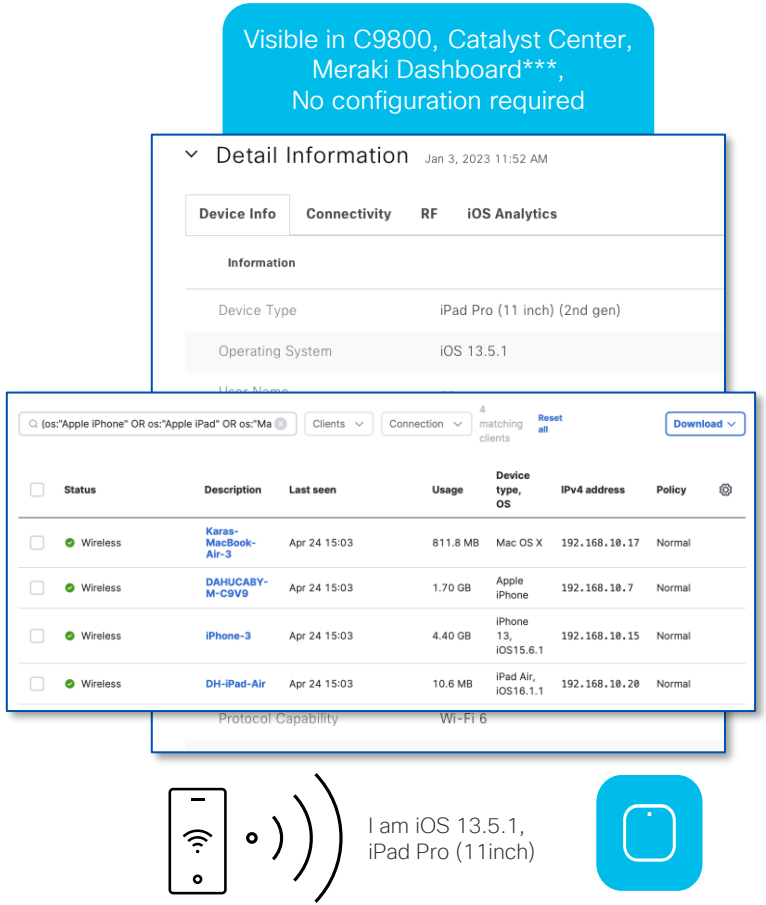
- Bring the ‘view from the ceiling’ to the client
- Clients roam faster, find the best cell, optimize its traffic

Better Knowing Your Clients

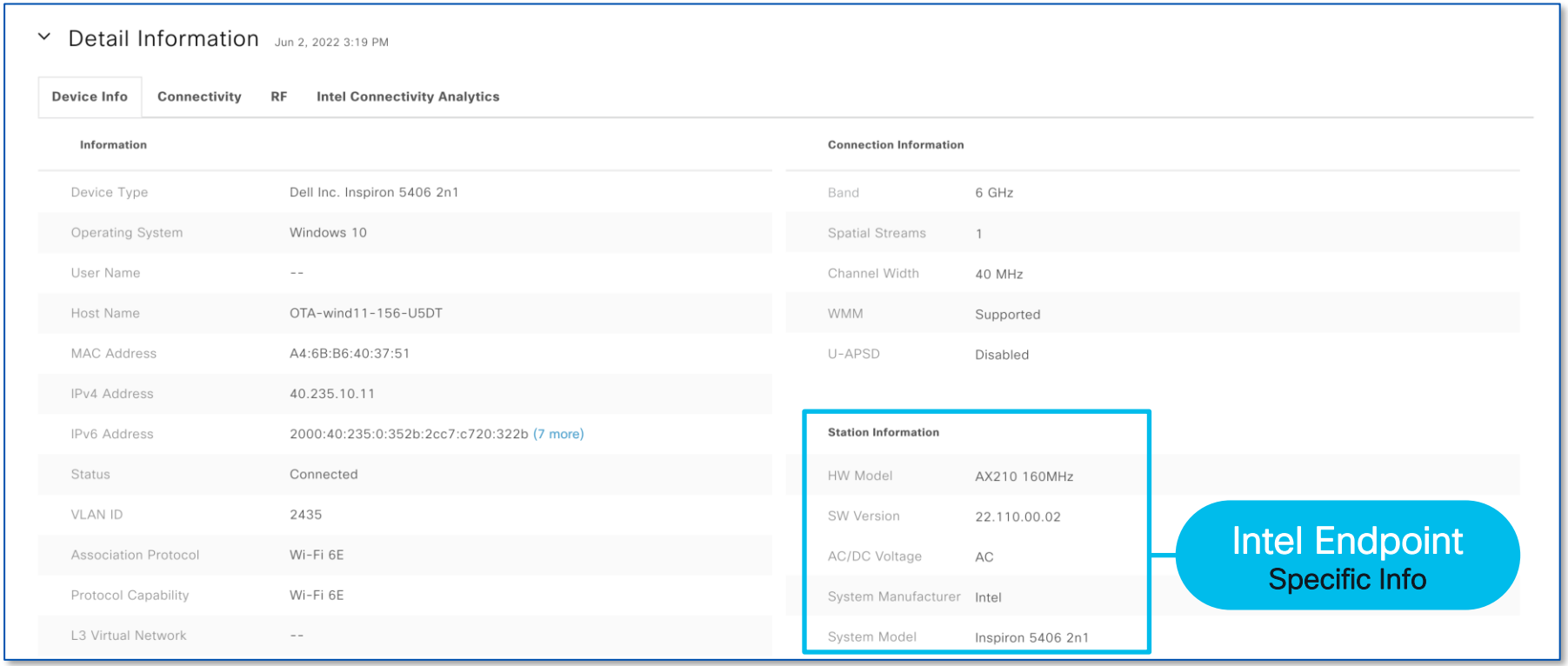
What is this client?

- **Apple**: Immediately after association, the iOS / MacOS** client sends an unsolicited (encrypted) action frame with platform (“iPhone 14”) and OS (“iOS 13.5.1”)
- **Intel**: Immediately after association, the Intel (AX200 and later) client sends an unsolicited (encrypted) action frame with HW-Model (“AX210”), driver versions (“4.5.12”), OS Version (Win 11.0.12”), AC/DC voltage (“AC” - useful for plugged/on battery)
- **Samsung**: Immediately after association, the Samsung (Galaxy S10 and later, Android 9 and later) client sends an unsolicited (encrypted) action frame with platform “(Galaxy 22 Ultra)”, OS (“Android 14.1”), Manufacturer build (Samsung v5.917”), SP build (“AT&T v4.1.17”)
- Technical points: Frame is of type “action”, “vendor-specific” subtype. Client only sends it when detecting a Cisco AP (from probe responses/beacons).

** MacOS: supported on Intel platforms since 2918, added to Mx (M1/M2) platforms in June 2023
*** Samsung details are not supported in Meraki Dashboard yet



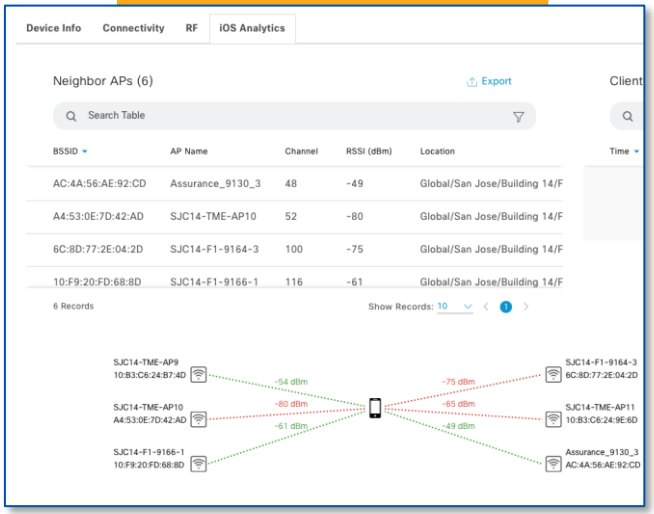
Intel Analytics on Catalyst Center Client 360

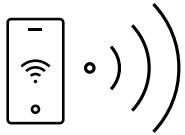


How does the client see the Network?

- **Apple:** Right after successful key-exchange during association (and after sending the model number), the iOS /MacOS device sends to its AP an 802.11k Beacon Report (Unsolicited mode) with list of BSSIDs/channels /RSSI for the current SSID
- **Intel:** After association (after sending client details), the Intel client sends to its AP an 802.11k Beacon Report (table). At any time, your can also ask for another 11k Beacon Report (table, passive, active)
- **Samsung:** After association (upon receiving STA specs), AP auto-queries the phone (802.11k beacon report request) to send an 802.11k Beacon Report (table). At any time, you can also ask for another 11k Beacon Report (table, passive, active)
- **Technical points:** There are 3 types of beacon reports: table (in the phone memory as a result of previous scan – valid for a few secs as the phone may be moving), passive/active (AP instructs phone to go scan passively (silent but longer) or actively (faster) one or many channels). On demand scan is from WLC CLI, with command 'wireless client mac-address <a.b.c> scan-report'

Visible in Catalyst Center, Meraki Dashboard*,

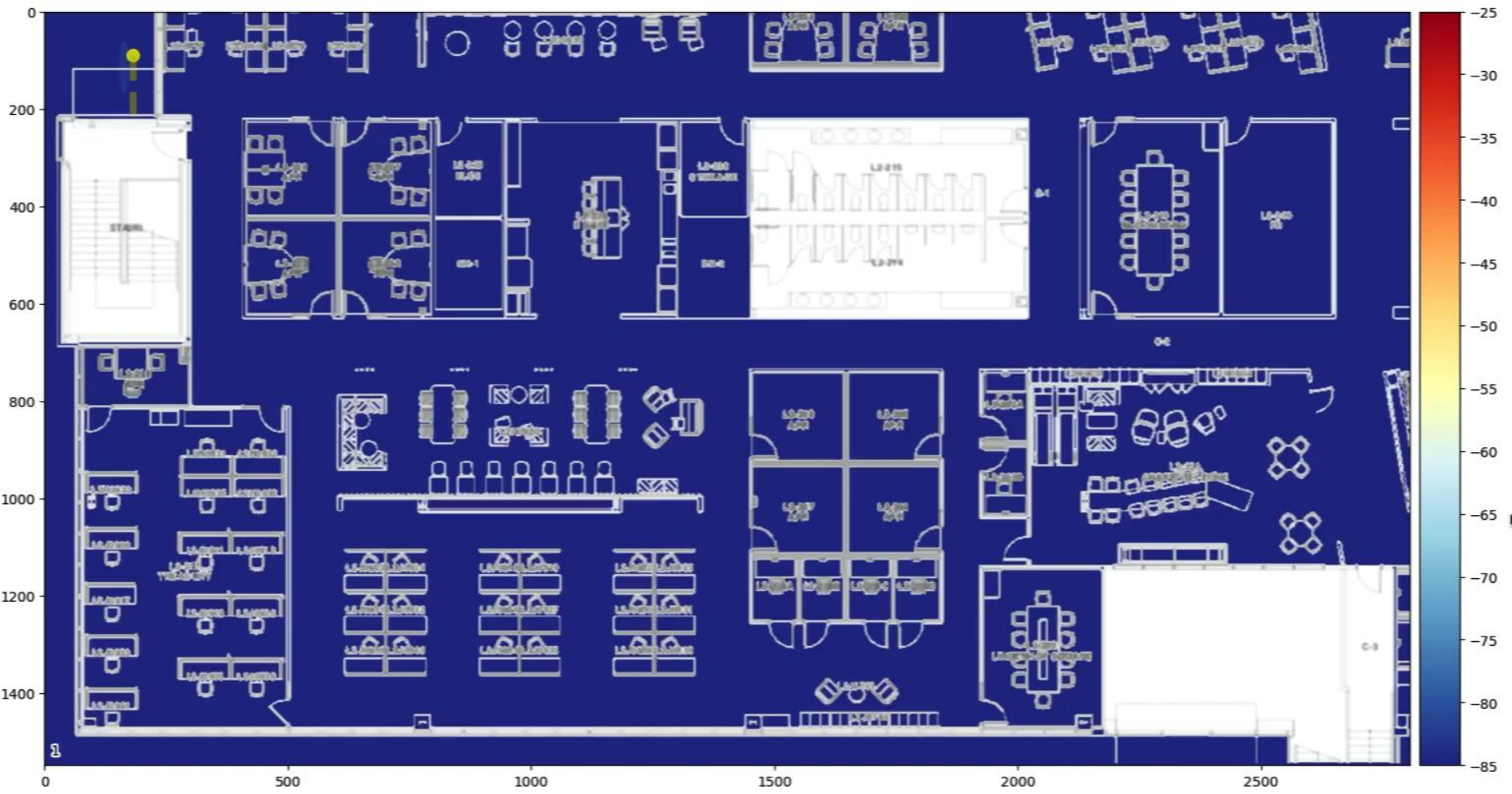




Here is the list of APs I see

* Samsung details are not supported in Meraki Dashboard yet

Use Client 11k Reports to Map your RF Floor



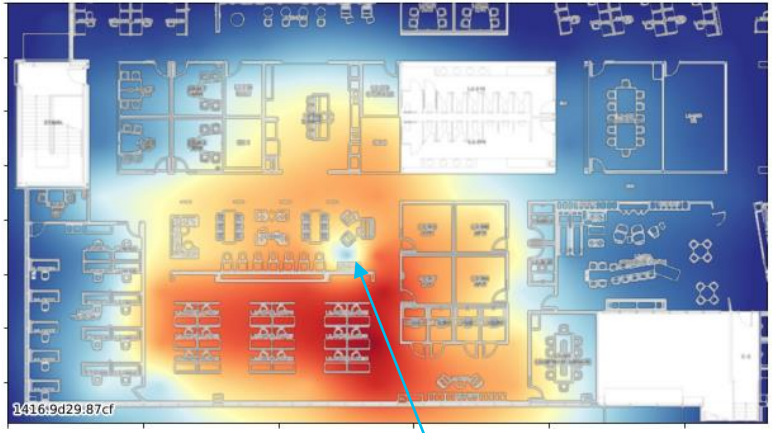
Map your RF Floor

From your client viewpoint

With a Cisco network and any recent Samsung galaxy or Intel client, you can send 802.11k (MBO) requests* to get the client view, anywhere, anytime

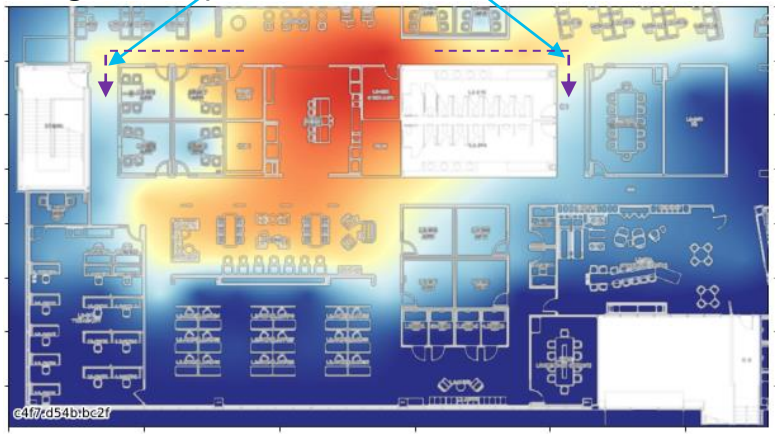
- Table report (last scan, 0 scanning cost)
- Channel report (how do you see me?)
- Channel class report (go scan channels A, B and C)

*https://github.com/jhenry-github/floor-heatmap



Fast fading coverage gap behind a pillar

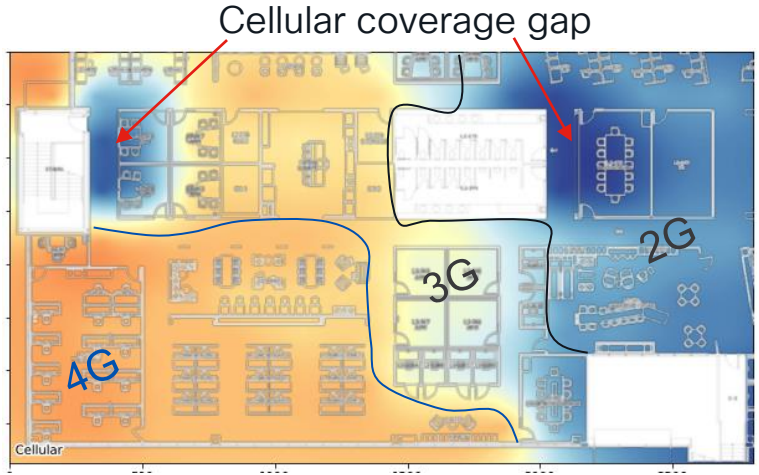
Signal drop as client turns the corner

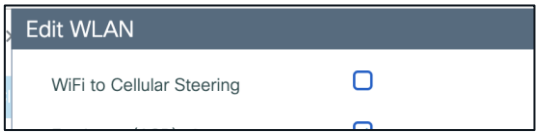


Mapping your RF Floor

Bonus

- Intel clients also send us “Bad Coverage” and Temporary disconnection” reports
  - “I hear you, but been below -75 dBm for x minutes”
  - “Moved to you, but lost contact with AP1 at -X dBm Y minutes ago”
- Samsung clients also send us their cellular signal (along with Wi-Fi)
  - For the first time, you can map your indoor cellular coverage!... and automatically push your Samsung clients to cellular at the edge of the Wi-Fi domain!



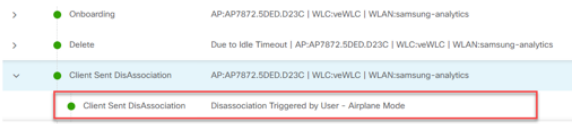


Why did the client go away?

- When a client roams or disconnects, it sends a disassociation message. The Apple, Samsung and Intel client sends a proprietary reason code telling us when the reason is not 802.11 in nature (in addition to the 802.11 reason code)
- **Apple:** Adds #9 upper Layer reasons to the 802.11 reasons (DHCP failed, EAP timed out, 802.1X failed, device is idle, captive portal security failed, decryption failed, Wi-Fi interface disabled, user triggered deassoc, AP-triggered deassoc)
- **Samsung:** Adds #34 Layer 2 or higher reasons (same family as Apple, but detailed, for example DHCP failed, Samsung says at what step)
- **Intel:** Intel sends other reports (next slide)

Used internally in WLC, Catalyst Center and Meraki Dashboard
No configuration required

Additional Reason Code [15:0]							
STEP 1 Reason [15:8]		STEP 2 Reason [7:4]		STEP 3 Reason [3:0]		AP	STA
0	Reserved	0~15	Reserved				
1	User Triggered Disconnect	0	Unspecified	0~15	Reserved		O
		1	Power Off or Wi-Fi Off				O
		2	Connecto to other AP				O
		3	Remove AP profile				O
		4	Airplane mode On				O
		5~15	Reserved				O
2	L2 Connection	0	Unspecified	0: Unspecified 1: Sent but not acked 2: Not received (Sent and acked well) 3: Received but something wrong 4~15: Reserved		O	O
		1	Association			O	O
		2~15	Reserved			O	O
3	4-Way Handshake	0	Unspecified	0~15	Reserved	O	O
		1	M1 for 4-Way Handshake			O	O
		2	M2 for 4-Way Handshake			O	
		3	M3 for 4-Way Handshake			O	O
		4	M4 for 4-Way Handshake			O	
		5	M1 for Groupkey Handshake			O	O
		6	M2 for Groupkey Handshake			O	
		7~15	Reserved			O	O
4	DHCP Fail	0	Unspecified				O
		1	Time Out				O
		2	Time out after Roaming				O
		3	Lease Expired (no response for renew)				O
		4	Nak in renew				O
		5	Renew lease wrong IP				O
		6	internal error				O
		7~15	Reserved				O
		0	Unspecified	0~15	Reserved		O



* Samsung details are not supported in Meraki Dashboard yet

Even More Feedback – Intel

Station Information

Reports: Hardware model, OS version, driver version, manufacturer, voltage, system model.

Helps troubleshoot and identify Intel devices based on their specific attributes.

Low RSSI

Reports: When RSSI is below -75 dBM for 5 mins, Last Reported Time.

Raise a sticky client issue and understand why a roam hasn't been triggered.

Neighboring AP

Reports: BSSIDs of Top 5 APs based on RSSI, Roaming Reasons based on Missed Beacons and 11v recommendations.

Provides a client-side view of the network and the reason for a roam.

Temporary Disconnects

Reports: When a client disconnection is due to a missed beacon.

Helps understand why a client has disconnected from the network.

Unknown AP

Reports: Reports a list of APs not part of Neighboring AP report.

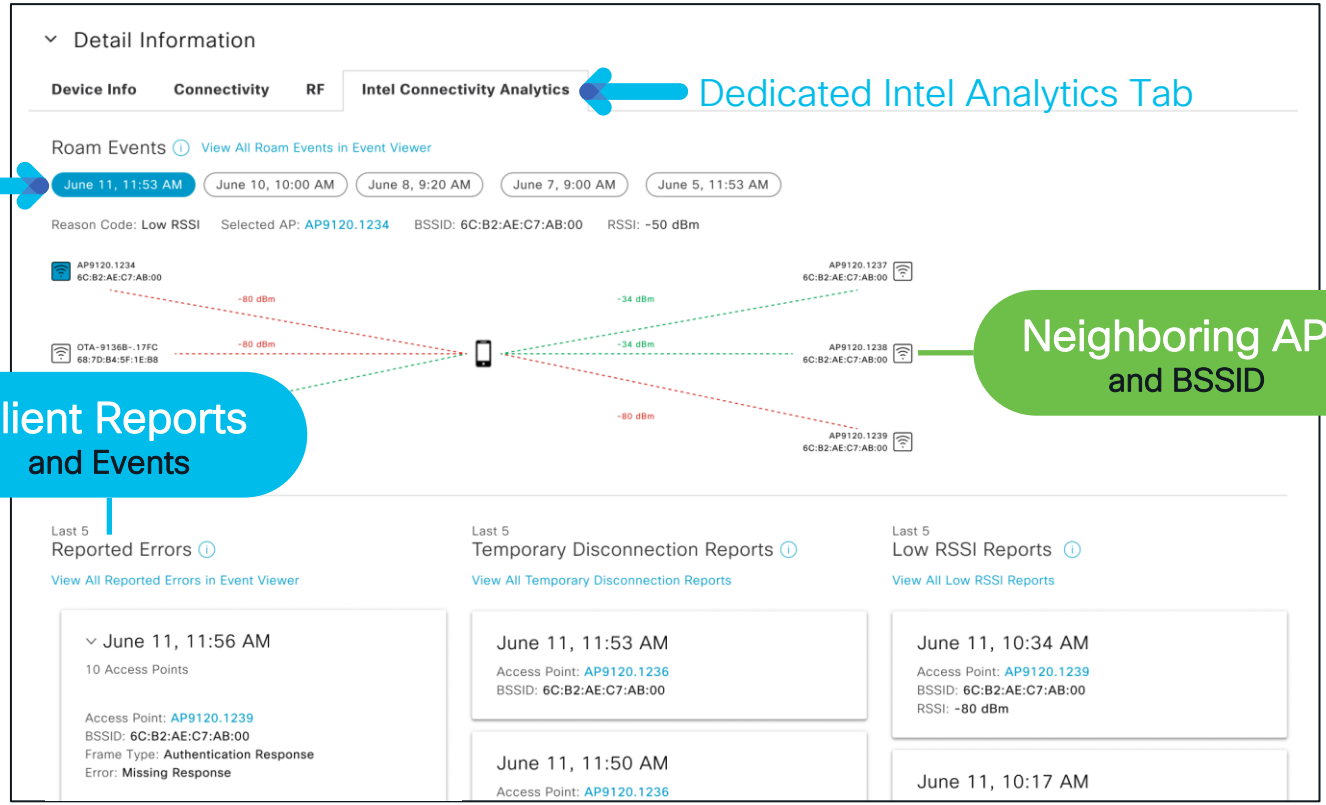
Helps troubleshoot issues with non-valid IEs and see why AP isn't responding.

Failed APs

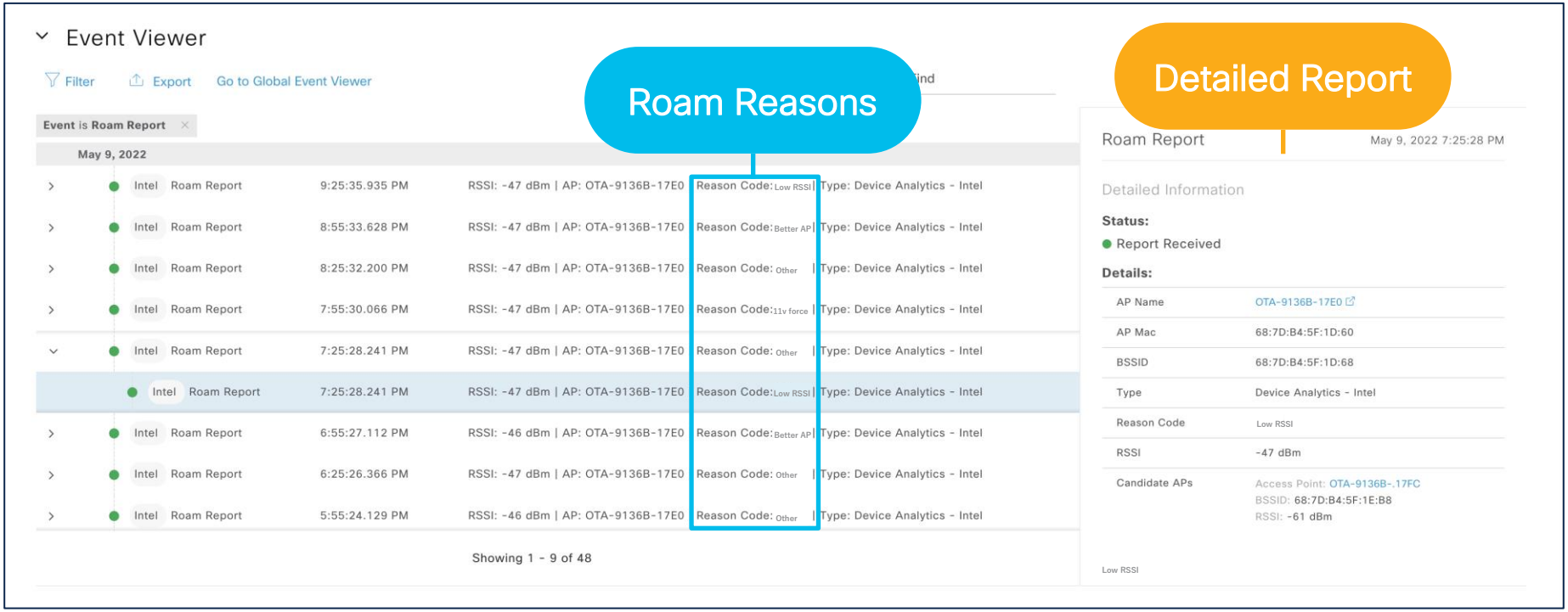
Reports: Reports invalid IEs in beacons/probe responses/association responses, BSSID.

Used to identify and flag rogue BSSIDs

Intel Connectivity Analytics on Client 360

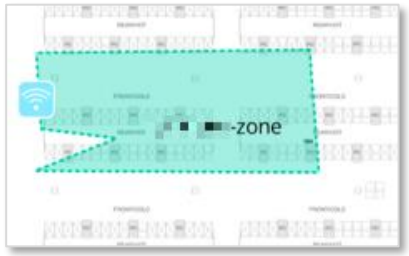


Intel Connectivity Analytics on Client 360 (cont.)



Why it Matters

- Better Troubleshooting
  - 96% of STAs disconnecting in this zone are Galaxy S23 running Android 14



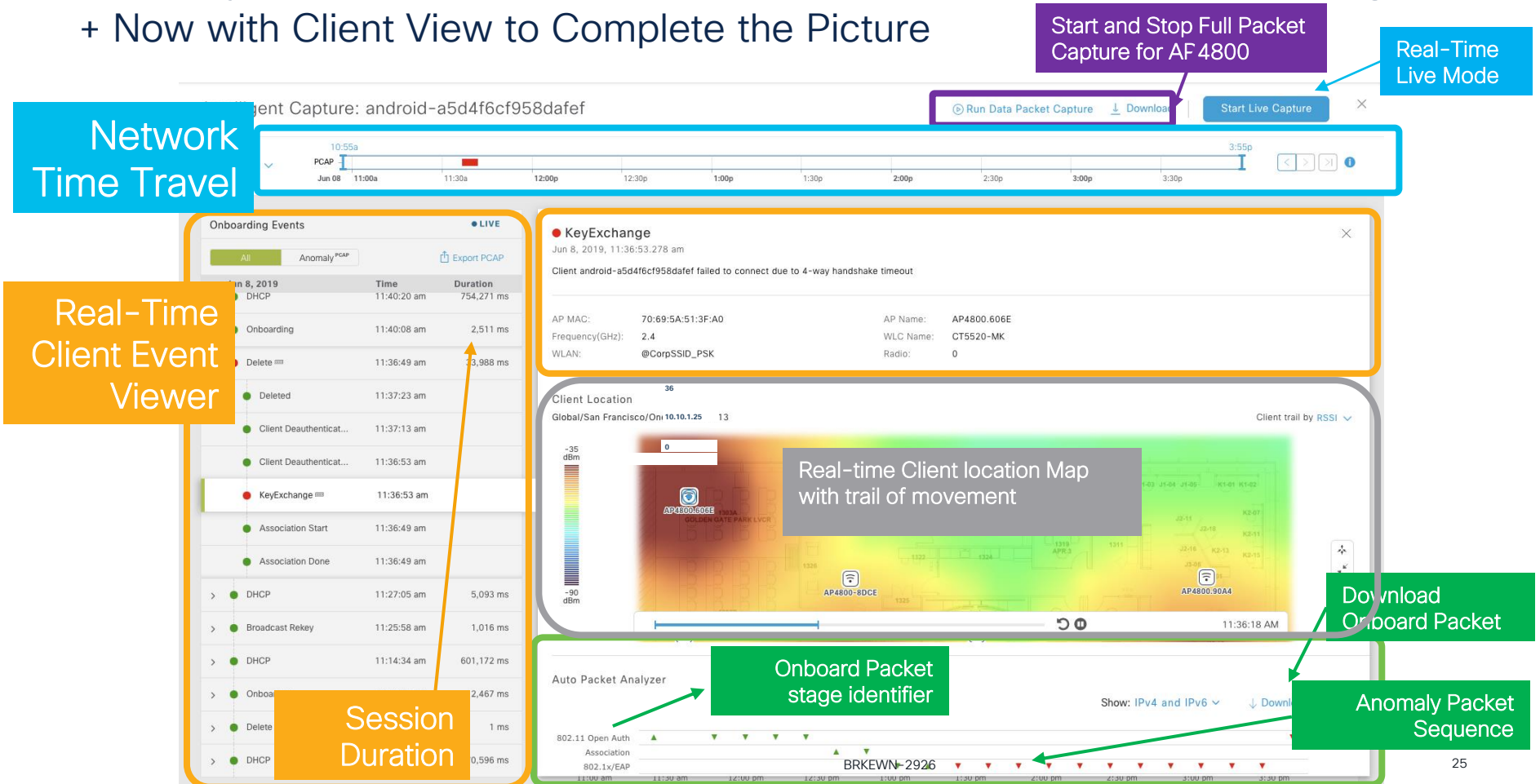
- Proactive maintenance
  - Day 0 issue affects Android 14
  - Identify which devices run this version

- Roaming Issues
  - iPhone 15 roams here
    - Short connection drops reported

  - Galaxy S23 roams here
    - No issues reported

Catalyst Center – Better Client Troubleshooting

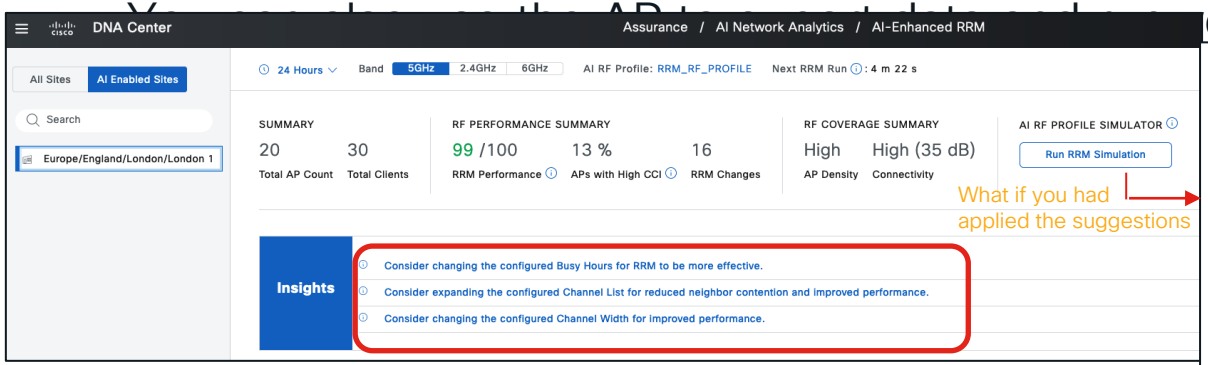
+ Now with Client View to Complete the Picture



Feeding Device Ecosystem Data Into your AIML Projects

- We already include them in our AI RRM computations (Catalyst Center)
  - Cisco Wireless AIOps – BRKEWN-2029
  - Advanced RF Tuning for Wi-Fi 6E… while getting a little help from AI – BRKEWN-3413

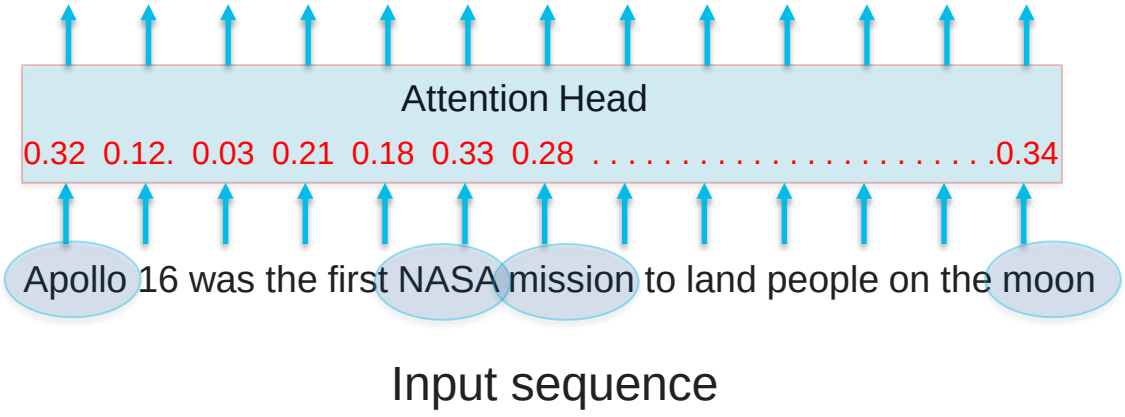
…our own AIML engines



AI-based predictions and suggestions

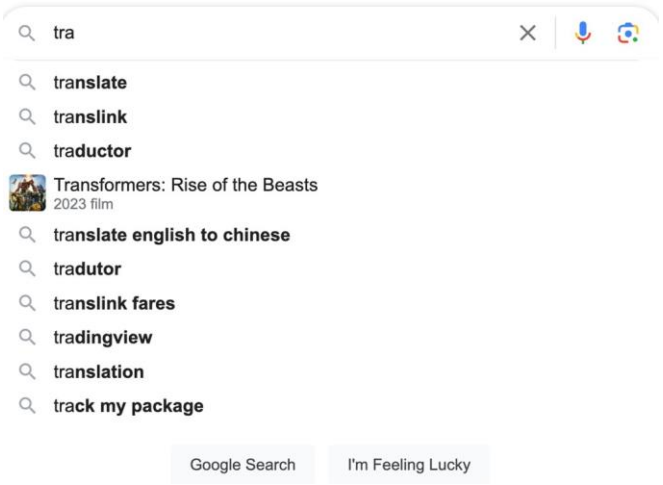
Example Customized AIML: Air Capture LLM

- How do you build a Large Language Model?
  - Language modeling (LM) is a technique that uses statistical and probabilistic models to determine the probability of a word (token) or a sequence of words (tokens) in a sentence (i.e., given previous words)
  - To build a LLM, take a (large) set of text, cut it into logical units (tokens), then compute how many times tokens follow each other



Example Customized AIML: Air Capture LLM

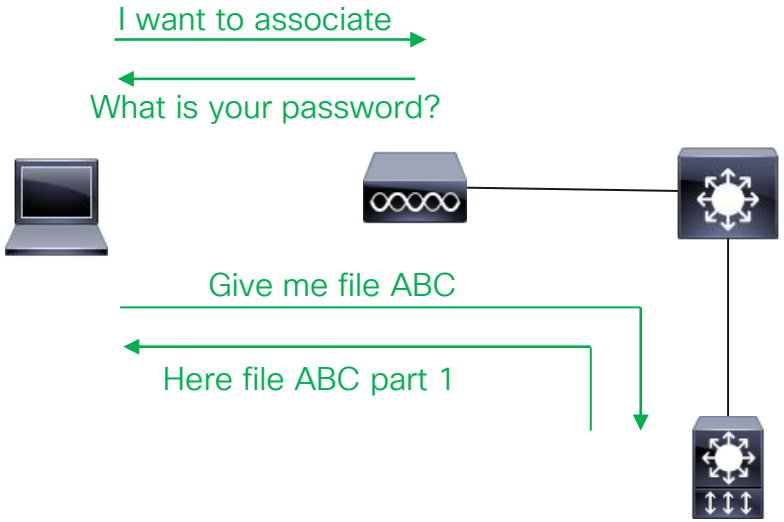
- LLM Inference
  - Then you start a word sequence, and the tool can either:
    - Predicts what comes next (and tell you)
    - Tell you if there is something strange about the sequence

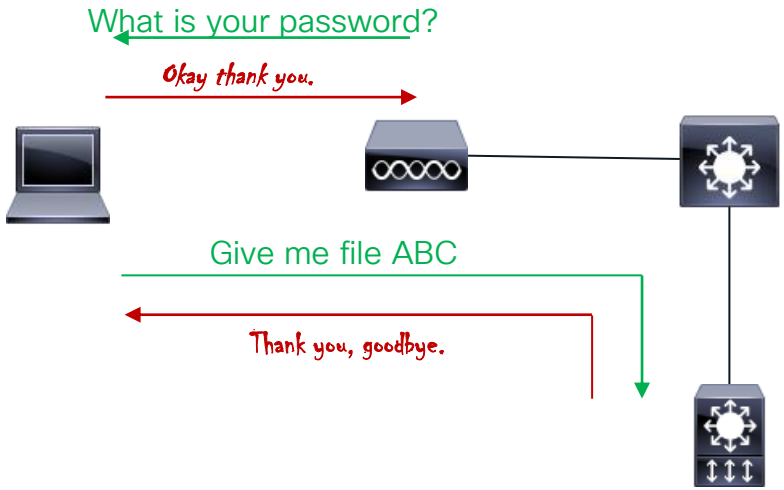


The language model assigns a prediction to all of these words, with highest probability ranked first

Example Customized AIML: Air Capture LLM

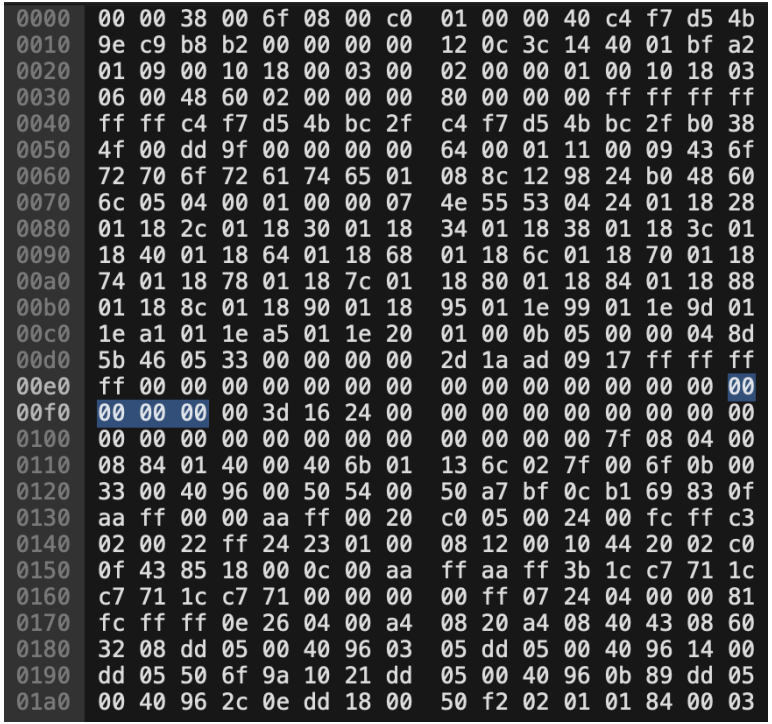
- Networking Exchanges are sentences





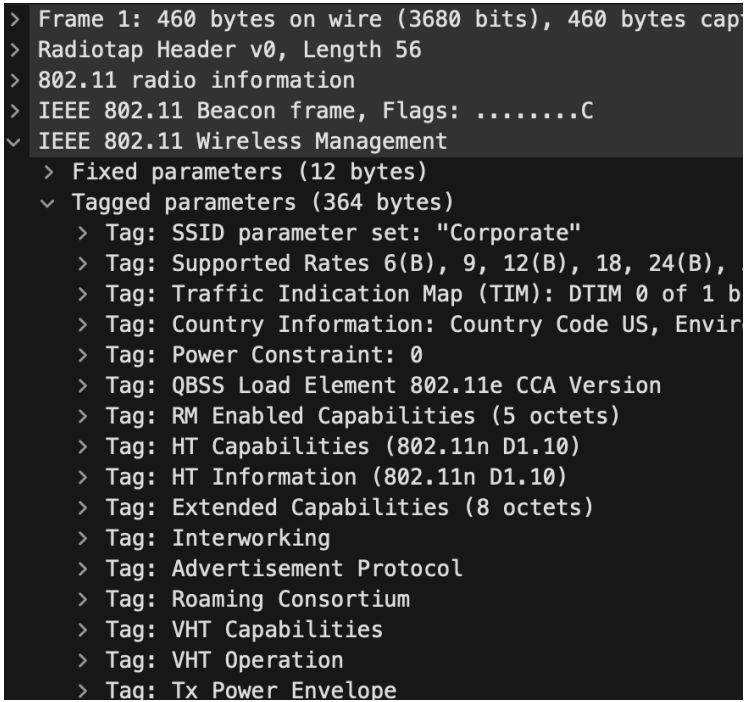
Language of Network Exchanges

- Network frames are sequences of bits
  - The order of the bits results in meaning
  - Fields have different lengths
    - The byte-based approach ignores this fundamental property
    - The meaning is ritualized – bits 64 to 98 means XYZ not because of the meaning of 64 and 98, but because the position of XYZ is described in a ritual manual (IEEE 802.11/802.3 etc.)
  - Time between frames has meaning
    - Individual frames need to be tied (in time) to one another



Language of Network Exchanges

- Wireshark has documented the ritual manual
  - A promising direction is to use the ritual words in the sentence, because this is what the field ‘means’
    - When 16th field, “SSID” says “Corporate”, the meaning is different from the 16th field in another frame (which may also be a string)



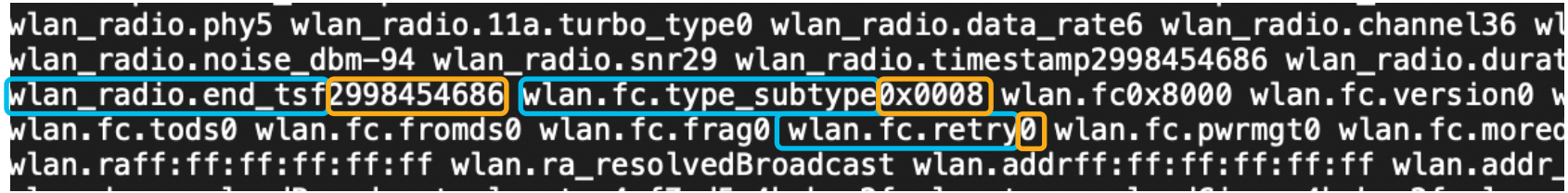
Language of Network Exchanges

- Let's convert the Wireshark captures to csv files, now each frame is a sentence, where each word is a field.

```
num1 len460 caplen460 frame.section_number1 frame.interface_id0 frame.interface_nameen0 frame.encap_type23 frame.offset_shift0.000000000
frame.time_epoch1681917506.078047000 frame.time_delta0.000000000 frame.time_delta_displayed0.000000000 frame.time_relative0.000000000 frame.number1
frame.len460 frame.cap_len460 frame.marked0 frame.ignored0 frame.protocolsradiotap:wlan_radio:wlan radiotap.version0 radiotap.pad0 radiotap.length56
radiotap.present.word0xc000086f radiotap.present.tsft1 radiotap.present.flags1 radiotap.present.rate1 radiotap.present.channel1
radiotap.present.fhss0 radiotap.present.dbm_antsignal1 radiotap.present.dbm_antnoise1 radiotap.present.lock_quality0
radiotap.present.tx_attenuation0 radiotap.present.db_tx_attenuation0 radiotap.present.dbm_tx_power0 radiotap.present.antenna1
radiotap.present.db_antsignal0 radiotap.present.db_antnoise0 radiotap.present.rxflags0 radiotap.present.txflags0 radiotap.present.data_retries0
radiotap.present.xchannel0 radiotap.present.mcs0 radiotap.present.ampdu0 radiotap.present.vht0 radiotap.present.timestamp0 radiotap.present.he0
radiotap.present.he_mu0 radiotap.present.0_length.psdu0 radiotap.present.l_sig0 radiotap.present.tlv0 radiotap.present.rtap_ns0
radiotap.present.vendor_ns1 radiotap.present.ext1 radiotap.present.word0x40000001 radiotap.present.rtap_ns0 radiotap.present.vendor_ns1
radiotap.present.ext0 radiotap.mactime2998454686 radiotap.flags0x12 radiotap.flags.cfp0 radiotap.flags.preamble1 radiotap.flags.wep0
radiotap.flags.frag0 radiotap.flags.fcs1 radiotap.flags.datapad0 radiotap.flags.badfcs0 radiotap.flags.shortgi0 radiotap.datarate6
radiotap.channel.freq5180 radiotap.channel.flags0x0140 radiotap.channel.flags.700mhz0 radiotap.channel.flags.800mhz0 radiotap.channel.flags.900mhz0
radiotap.channel.flags.turbo0 radiotap.channel.flags.cck0 radiotap.channel.flags.ofdm1 radiotap.channel.flags.2ghz0 radiotap.channel.flags.5ghz1
radiotap.channel.flags.passive0 radiotap.channel.flags.dynamic0 radiotap.channel.flags.gfsk0 radiotap.channel.flags.gsm0
radiotap.channel.flags.sturbo0 radiotap.channel.flags.half0 radiotap.channel.flags.quarter0 radiotap.dbm_antsignal-65 radiotap.dbm_antnoise-94
radiotap.antenna1 radiotap.vendor_namespace00:10:18:00:03:00:02:00:00 radiotap.vendor_oui4120 radiotap.vendor_subns0 radiotap.vendor_data_len3
radiotap.vendor_namespace00:10:18:03:06:00:48:60:02:00:00:00 radiotap.vendor_oui4120 radiotap.vendor_subns3 radiotap.vendor_data_len6
wlan_radio.phy5 wlan_radio.11a.turbo_type0 wlan_radio.data_rate6 wlan_radio.channel36 wlan_radio.frequency5180 wlan_radio.signal_dbm-65
wlan_radio.noise_dbm-94 wlan_radio.snr29 wlan_radio.timestamp2998454686 wlan_radio.duration564 wlan_radio.preamble20 wlan_radio.start_tsf2998454122
wlan_radio.end_tsf2998454686 wlan.fc.type_subtype0x0008 wlan.fc0x8000 wlan.fc.version0 wlan.fc.type0 wlan.fc.subtype8 wlan.flags0x00 wlan.fc.ds0x00
wlan.fc.tods0 wlan.fc.fromds0 wlan.fc.frag0 wlan.fc.retry0 wlan.fc.pwrmgt0 wlan.fc.moredata0 wlan.fc.protected0 wlan.fc.order0 wlan.duration0
wlan.raff:ff:ff:ff:ff:ff wlan.ra_resolvedBroadcast wlan.addrff:ff:ff:ff:ff:ff wlan.addr_resolvedBroadcast wlan.daff:ff:ff:ff:ff:ff
wlan.da_resolvedBroadcast wlan.tac4:f7:d5:4b:bc:2f wlan.ta_resolvedCisco_4b:bc:2f wlan.sac4:f7:d5:4b:bc:2f wlan.sa_resolvedCisco_4b:bc:2f
wlan.bssidc4:f7:d5:4b:bc:2f wlan.bssid_resolvedCisco_4b:bc:2f wlan.addrc4:f7:d5:4b:bc:2f wlan.addr_resolvedCisco_4b:bc:2f wlan.addrc4:f7:d5:4b:bc:2f
wlan.addr_resolvedCisco_4b:bc:2f wlan.frag0 wlan.seq907 wlan.fcs0x3e27c7df wlan.fcs.status2 wlan.fixed.timestamp2682060879 wlan.fixed.beacon100
wlan.fixed.capabilities0x1101 wlan.fixed.capabilities.ess1 wlan.fixed.capabilities.ibss0 wlan.fixed.capabilities.reserved10
wlan.fixed.capabilities.reserved20 wlan.fixed.capabilities.privacy0 wlan.fixed.capabilities.short_preamble0 wlan.fixed.capabilities.reserved30
wlan.fixed.capabilities.reserved40 wlan.fixed.capabilities.spec_man1 wlan.fixed.capabilities.qos0 wlan.fixed.capabilities.short_slot_time0
wlan.fixed.capabilities.apsd0 wlan.fixed.capabilities.radio_measurement1 wlan.fixed.capabilities.end0 wlan.fixed.capabilities.reserved50
```

Language of Network Exchanges

- The structure of the language we build has word roots, and conjugation



Language of Network Exchanges

- “ChatNetPT” tokenizes roots and terminations, and finds relationships
- For example:
  - We insert a frame (a series of fields)
    - This is a “sentence” that one side (e.g. a client) says
  - We ask ChatNetPT what is the most likely next frame
    - This is “the answer that the other side should say”
  - We can also train ChatNetPT to classify (recognize) frame types (trivial)

```
if __name__ == "__main__":
    main()
```

```
What do you want to do? ↑↓ for history
```

apabilities.40mhzintolerant0,wlan.ht.capabilities.lsig0,wlan.ht.ampduparam0x1b,wlan.ht.ampduparam.maxlength0x03,wlan.ht.ampduparam.mpdudensity0x06,wlan.ht.ampduparam.reserved0x00,wlan.ht.mcsset.rxbitmask.0to70x000000ff,wlan.ht.mcsset.rxbitmask.8to150x000000ff,wlan.ht.mcsset.rxbitmask.16to230x00000000,wlan.ht.mcsset.rxbitmask.24to310x00000000,wlan.ht.mcsset.rxbitmask.320x00000000,wlan.ht.mcsset.rxbitmask.33to380x00000000,wlan.ht.mcsset.rxbitmask.39to520x00000000,wlan.ht.mcsset.rxbitmask.53to760x00000000,wlan.ht.mcsset.highestdatarate0x0000,wlan.ht.mcsset.txsetdefined0,wlan.ht.mcsset.txrxmcsnotequal0,wlan.ht.mcsset.txmaxss0x0000,wlan.ht.mcsset.txunequalmod0,wlan.htex.capabilities0x0000,wlan.htex.capabilities.pco0,wlan.htex.capabilities.transtime0x0000,wlan.htex.capabilities.mcs0x0000,wlan.htex.capabilities.htc0,wlan.htex.capabilities.rdresponder0,wlan.txbf0x00000000,wlan.txbf.txbf0,wlan.txbf.rxss0,wlan.txbf.txss0,wlan.txbf.rxndp0,wlan.txbf.txndp0,wlan.txbf.impltxbf0,wlan.txbf.calibration0x00000000,wlan.txbf.csi0,wlan.txbf.fm.uncompressed.tbf0,wlan.txbf.fm.compressed.tbf0,wlan.txbf.rcsi0x00000000,wlan.txbf.fm.uncompressed.rbf0x00000000,wlan.txbf.fm.compressed.bf0x00000000,wlan.txbf.mingroup0x00000000,wlan.txbf.csinumant0x00000000,wlan.txbf.fm.uncompressed.maxant0x00000000,wlan.txbf.fm.compressed.maxant0x00000000,wlan.txbf.csi.maxrows0x00000000,wlan.txbf.channelest0x00000000,wlan.txbf.reserved0x00000000,wlan.asel0x00,wlan.asel.capable0,wlan.asel.txcsi0,wlan.asel.txif0,wlan.asel.csi0,wlan.asel.if0,wlan.asel.rx0,wlan.asel.sppdu0,wlan.asel.reserved0x00,wlan.tag.number127,wlan.tag.length8,wlan.extcap0x00,wlan.extcap.b00,wlan.extcap.b10x00,wlan.extcap.b20,wlan.extcap.b30x00,wlan.extcap.b40,wlan.extcap.b50x00,wlan.extcap.b60,wlan.extcap.b70,wlan.extcap0x00,wlan.extcap.b80,wlan.extcap.b90,wlan.extcap.b100,wlan.extcap.b110,wlan.extcap.b120,wlan.extcap.b130,wlan.extcap.b140,wlan.extcap.b150,wlan.extcap0x08,wlan.extcap.b160,wlan.extcap.b170,wlan.extcap.b180,wlan.extcap.b191,wlan.extcap.b200,wlan.extcap.b210,wlan.extcap.b220,wlan.extcap.b230,wlan.extcap0x04,wlan.extcap.b240,wlan.extcap.b250,wlan.extcap.b261,wlan.extcap.b270,wlan.extcap.b280,wlan.extcap.b290,wlan.extcap.b300,wlan.extcap.b310,wlan.extcap0x00,wlan.extcap.b320,wlan.extcap.b330,wlan.extcap.b340,wlan.extcap.b350x00,wlan.extcap.b360,wlan.extcap.b370,wlan.extcap.b380,wlan.extcap.b390,wlan.extcap0x00,wlan.extcap.b400,wlan.extcap.serv_int_granularity0,wlan.extcap.b440,wlan.extcap.b450,wlan.extcap.b460,wlan.extcap.b470x00,wlan.extcap0x00,wlan.extcap.b480,wlan.extcap.b490,wlan.extcap.b500,wlan.extcap.b510,wlan.extcap.b520,wlan.extcap.b530,wlan.extcap.b540,wlan.extcap.b550,wlan.extcap0x40,wlan.extcap.b560,wlan.extcap.b570,wlan.extcap.b580,wlan.extcap.b590x00,wlan.extcap.b600,wlan.extcap.b610,wlan.extcap.b621,wlan.extcap.b630,wlan.tag.number191,wlan.tag.length12,wlan.vht.capabilities0x0f817032,wlan.vht.capabilities.maxmpdulength0x00000002,wlan.vht.capabilities.supportedchanwidthset0x00000000,wlan.vht.capabilities.rxldpc1,wlan.vht.capabilities.short801,wlan.vht.capabilities.short1600,wlan.vht.capabilities.txstbc0,wlan.vht.capabilities.rxstbc0x00000000,wlan.vht.capabilities.subeamformer0,wlan.vht.capabilities.subeamformee1,wlan.vht.capabilities.beamformee_sts_cap0x00000003,wlan.vht.capabilities.soundingdimensions0x00000001,wlan.vht.capabilities.mubeamformer0,wlan.vht.capabilities.mubeamformee0,wlan.vht.capabilities.vhttxopps0,wlan.vht.capabilities.vhthtc0,wlan.vht.capabilities.maxampdu0x00000007,wlan.vht.capabilities.linkadapt0x00000003,wlan.vht.capabilities.rxpatconsist0,wlan.vht.capabilities.txpatconsist0,wlan.vht.capabilities.ext_nss_bw_support0x00000000,wlan.vht.mcsset.rxmcsmap0xfff5,wlan.vht.mcsset.rxmcsmap.ss10x0001,wlan.vht.mcsset.rxmcsmap.ss20x0001,wlan.vht.mcsset.rxmcsmap.ss30x0003,wlan.vht.mcsset.rxmcsmap.ss40x0003,wlan.vht.mcsset.rxmcsmap.ss50x0003,wlan.vht.mcsset.rxmcsmap.ss60x0003,wlan.vht.mcsset.rxmcsmap.ss70x0003,wlan.vht.mcsset.rxmcsmap.ss80x0003,wlan.vht.mcsset.rxhighestlonggirate0x0000,wlan.vht.mcsset.max_nsts_total0,wlan.vht.mcsset.txmcsmap0xfff5,wlan.vht.mcsset.txmcsmap.ss10x0001,wlan.vht.mcsset.txmcsmap.ss20x0001,wlan.vht.mcsset.txmcsmap.ss30x0003,wlan.vht.mcsset.txmcsmap.ss40x0003,wlan.vht.mcsset.txmcsmap.ss50x0003,wlan.vht.mcsset.txmcsmap.ss60x0003,wlan.vht.mcsset.txmcsmap.ss70x0003,wlan.vht.mcsset.txmcsmap.ss80x0003,wlan.vht.mcsset.txhighestlonggirate0x0000,wlan.vht.ncsset.ext_nss_bw_cap0,wlan.vht.ncsset.reserved0x0000,wlan.tag.number221,wlan.tag.length11,wlan.tag.oui6130,wlan.tag.vendor.oui.type10,wlan.tag.vendor.data0a:00:01:04:00:00:00:00,wlan.tag.number221,wlan.tag.length5,wlan.tag.oui36940,wlan.tag.vendor.oui.type4,wlan.vs.pren.type4,wlan.vs.pren.unknown_data07,wlan.tag.number221,wlan.tag.length10,wlan.tag.oui4120,wlan.tag.vendor.oui.type2,wlan.tag.vendor.data02:00:00:10:00:00:00,wlan.tag.number221,wlan.tag.length7,wlan.tag.oui20722,wlan.tag.vendor.oui.type2,wlan.wfa.ie.type0x02,wlan.wfa.ie.wme.subtype0,wlan.wfa.ie.wme.version1,wlan.wfa.ie.wme.qos_info0x00,wlan.wfa.ie.wme.qos_info.sta.max_sp_length0x00,wlan.wfa.ie.wme.qos_info.sta.ac_be0,wlan.wfa.ie.wme.qos_info.sta.ac_bk0,wlan.wfa.ie.wme.qos_info.sta.ac_vi0,wlan.wfa.ie.wme.qos_info.sta.ac_vo0,wlan.wfa.ie.wme.qos_info.sta.reserved0x00,
This frame is: an association request
What do you want to do? what is this frame?
Enter a set of values separated by a comma.
 NA,len68,caplen68,frame.section_number1,frame.interface_id0,frame.interface_nameen0,frame.encap_type23,frame.offset_shift0.000000000,frame.time_epoch1698532538.455748000,frame.time_delta0.000014000,frame.time_delta_displayed0.000014000,frame.time_relative23.127411000,frame.number4614,frame.len68,frame.cap_len68,frame.marked0,frame.ignored0,frame.protocolsradiotap:wlan_radio:wlan,radiotap.version0,radiotap.pad0,radiotap.length54,radiotap.present.word0xc000086f,radiotap.present.tsft1,radiotap.present.flags1,radiotap.present.rate1,radiotap.present.channel1,radiotap.present.fhss0,radiotap.present.dbm_antsignal1,radiotap.present.dbm_antnoise1,radiotap.present.lock_quality0,radiotap.present.tx_attenuation0,radiotap.present.db_tx_attenuation0,radiotap.present.dbm_tx_power0,radiotap.present.antenna1,radiotap.present.db_antsignal0,radiotap.present.db_antnoise0,radiotap.present.rxflags0,radiotap.present.txflags0,radiotap.present.data_retries0,radiotap.present.xchannel0,radiotap.present.mcs0,radiotap.present.ampdu0,radiotap.present.vht0,radiotap.present.timestamp0,radiotap.present.he0,radiotap.present.he_mu0,radiotap.present.0_length.psdu0,radiotap.present.l_sig0,radiotap.present.tlv0,radiotap.present.rtap_ns0,radiotap.present.vendor_ns1,radiotap.present.ext1,radiotap.present.word0x40000001,radiotap.present.rtap_ns0,radiotap.present.vendor_ns1,radiotap.present.ext0,radiotap.mactime2730419686,radiotap.flags0x12,radiotap.flags.cfp0,radiotap.flags.preamble1,radiotap.flags.wep0,radiotap.flags.frag0,radiotap.flags.fcs1,radiotap.flags.datapad0,radiotap.flags.badfcs0,radiotap.flags.shortgi0,radiotap.datarate6,radiotap.channel.freq5500,radiotap.channel.flags0x0140,radiotap.channel.flags.700mhz0,radiotap.channel.flags.800mhz0,radiotap.channel.flags.900mhz0,radiotap.channel.flags.turbo0,radiotap.channel.flags.cck0,radiotap.channel.flags.ofdm1,radiotap.channel.flags.2ghz0,radiotap.channel.flags.5ghz1,radiotap.channel.flags.passive0,radiotap.channel.flags.dynamic0,radiotap.channel.flags.gfsk0,radiotap.channel.flags.gsm0,radiotap.channel.flags.sturbo0,radiotap.channel.flags.half0,radiotap.channel.flags.quarter0,radiotap.dbm_antsignal-40,radiotap.dbm_antnoise-79,radiotap.antenna1,radiotap.vendor_namespace00:10:18:00:03:00:02:00:00,radiotap.vendor_oui4120,radiotap.vendor_subns0,radiotap.vendor_data_len3,radiotap.vendor_namespace00:10:18:03:04:00:03:01:00:00,radiotap.vendor_oui4120,radiotap.vendor_subns3,radiotap.vendor_data_len4,wlan_radio.phy5,wlan_radio.11a.turbo_type0,wlan_radio.data_rate6,wlan_radio.channel100,wlan_radio.frequency5500,wlan_radio.signal_dbm-40,wlan_radio.noise_dbm-79,wlan_radio.snr39,wlan_radio.timestamp2730419686,wlan_radio.duration44,wlan_radio.preamble20,wlan_radio.ifs255,wlan_radio.start_tsf2730419642,wlan_radio.end_tsf2730419686,wlan.fc.type_subtype0x001d,wlan.fc0xd400,wlan.fc.version0,wlan.fc.type1,wlan.fc.subtype13,wlan.flags0x00,wlan.fc.ds0x00,wlan.fc.tods0,wlan.fc.fromds0,wlan.fc.frag0,wlan.fc.retry0,wlan.fc.pwrmgt0,wlan.fc.moredata0,wlan.fc.protected0,wlan.fc.order0,wlan.duration0,wlan.ra4e:b3:48:6a:f5:ce,wlan.ra_resolved4e:b3:48:6a:f5:ce,wlan.addr4e:b3:48:6a:f5:ce,wlan.addr_resolved4e:b3:48:6a:f5:ce,wlan.fcs0xd9b29af6,wlan.fcs.status2,
This frame is: an association response
What do you want to do?

]:

]:

Using Client Knowledge for better Design

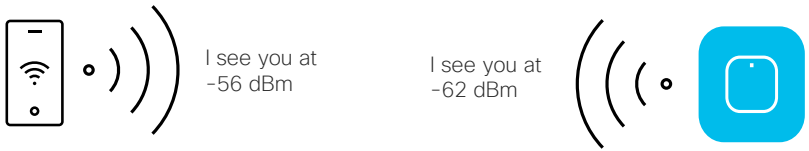
cisco Live!

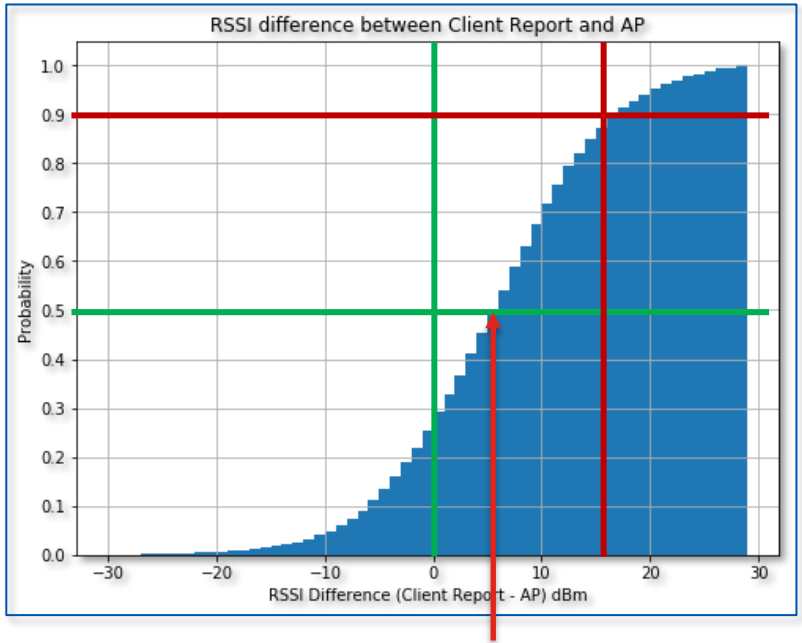
The “View from my Hand” is Different from the “View from the Ceiling”

- Six months report from network “designed from the ceiling”:

  AP power set with “AP to AP” in mind (max ‘level 1’)

- RSSI seen by the AP is lower than that seen by Client (likely due to lower transmit power of Client)
  - 50% of time difference is up to 6 dB.
  - 90% of time difference is up to 15 dB

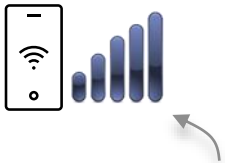




If half the clients’ power was the same as half the APs’ power, this point would be at the center of the green cross… but it is 6 dB below

If AP Signal is Strong, Client Uses High Data Rate

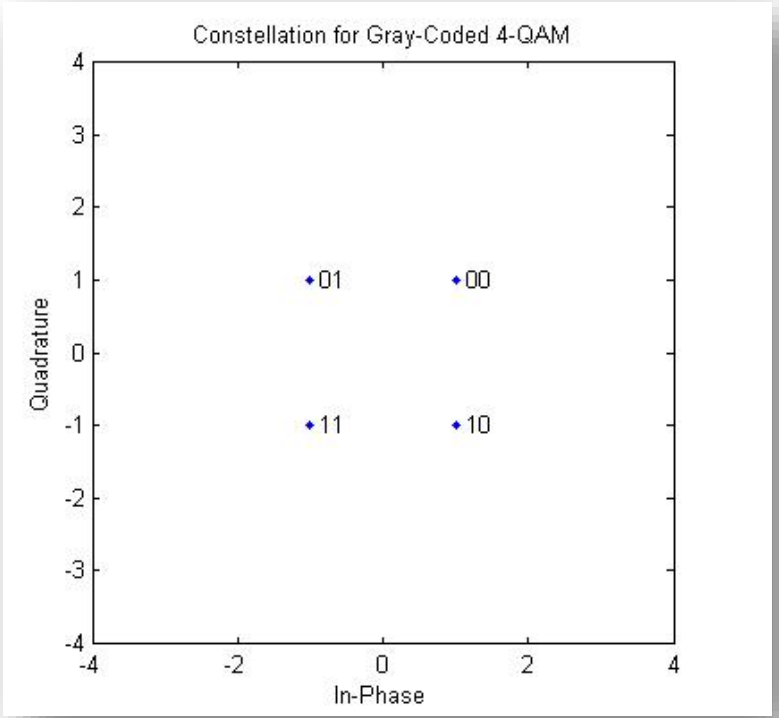
- Client power can be low, noise at the AP high, HW specs may be different…



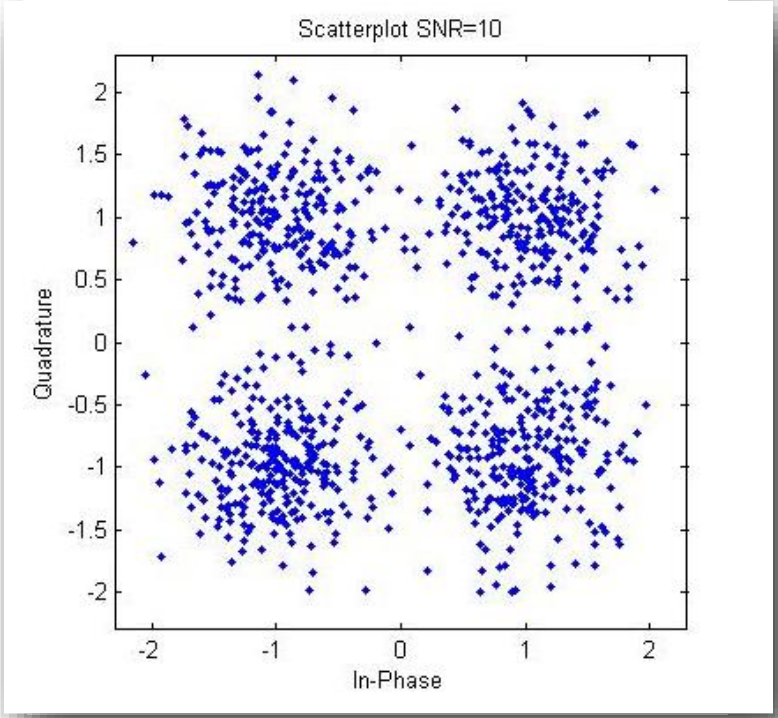
This is the AP 'signal' (at phone level)

This is the phone 'signal' (at AP level)

Modulation, SNR and Data Rates



4-QAM



SNR=10

Relationship Between Modulation and SNR

Protocol and Channel Width	MCS Value Achieved by Clients at Various Signal to Noise Ratio (SNR) Levels													
	0	1	2	3	4	5	6	7	8	9	10	11	12	
IEEE_802.11b 20 MHz	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MC
IEEE_802.11ag 20 MHz	None	None	MCS 0	MCS 0	MCS 1	MCS 2	MCS 2	MCS 2	MCS 2	MCS 3	MCS 3	MCS 4	MCS 4	MC
IEEE_802.11n 20 MHz	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MC
IEEE_802.11n 40 MHz	None	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MC
IEEE_802.11ac 20 MHz	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MC
IEEE_802.11ac 40 MHz	None	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MC
IEEE_802.11ac 80 MHz	None	None	None	None	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MC
IEEE_802.11ac 160 MHz	None	None	None	None	None	None	None	None	None	None	None	MCS 0	MCS 0	MC

Can Power Really Damage Cell Conditions?

- Bad design example: Client @ 12 dBm, AP @20 dBm

17	0.039879000	172.31.255.101	172.31.255.103	UDP	1420	34	-35 55 dB	54.0	Source port: 50857	Destination port: search-agent
18	0.040266000	172.31.255.101	172.31.255.103	UDP	1420	34	-35 55 dB	54.0	Source port: 50857	Destination port: search-agent
19	0.040648000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857	Destination port: search-agent
20	0.041938000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857	Destination port: search-agent
21	0.042217000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	36.0	Source port: 50857	Destination port: search-agent
22	0.043444000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	12.0	Source port: 50857	Destination port: search-agent
23	0.043445000		Cisco_0a:04:2e (RA)	802.11	40		-45 45 dB	12.0	Acknowledgement, Flags=........C	
24	0.043850000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857	Destination port: search-agent
25	0.044245000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857	Destination port: search-agent
26	0.044641000	172.31.255.101	172.31.255.103	UDP	1420	34	-34 56 dB	54.0	Source port: 50857	Destination port: search-agent
27	0.045023000	172.31.255.101	172.31.255.103	UDP	1420	34	-35 55 dB	54.0	Source port: 50857	Destination port: search-agent
28	0.045750000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	36.0	Source port: 50857	Destination port: search-agent
29	0.046223000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	36.0	Source port: 50857	Destination port: search-agent
30	0.047450000	172.31.255.101	172.31.255.103	UDP	1420	34	-29 61 dB	12.0	Source port: 50857	Destination port: search-agent
31	0.047450000		Cisco_0a:04:2e (RA)	802.11	40		-47 43 dB	12.0	Acknowledgement, Flags=........C	

```
Frame 29: 1420 bytes on wire (11360 bits), 1420 bytes captured (11360 bits) on interface 0
Radiotap Header v0, Length 26
IEEE 802.11 QoS Data, Flags: ....R.F.C
  Type/Subtype: QoS Data (0x28)
⊟ Frame Control: 0x0A88 (Normal)
    Version: 0
    Type: Data frame (2)
    Subtype: 8
  ⊟ Flags: 0xA
      .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)
      .... .0.. = More Fragments: This is the last fragment
      .... 1... = Retry: Frame is being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = Protected flag: Data is not protected
      0... .... = Order flag: Not strictly ordered
```

Based on Rx AP signal, client thinks 54 Mbps rate is okay…
But client message is too weak, and AP does not ACK until rate falls to 12 mbps

Each message takes 8 times more to be transmitted (including EIFS and retries)

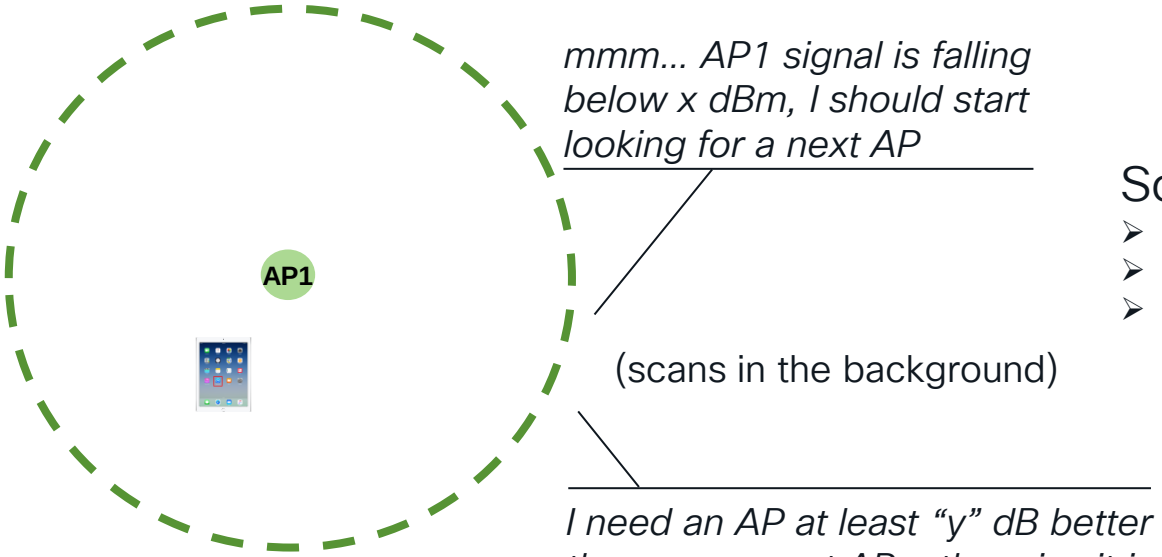
So... You need your cell edge where signal is still strong, and MCS high

There can be a 20 dB difference between these photos

It is not Because You Decide that The Cell Should Stop There, That It Will

Clients will stay connected until they decide to roam…

Client Cell Edge Logic



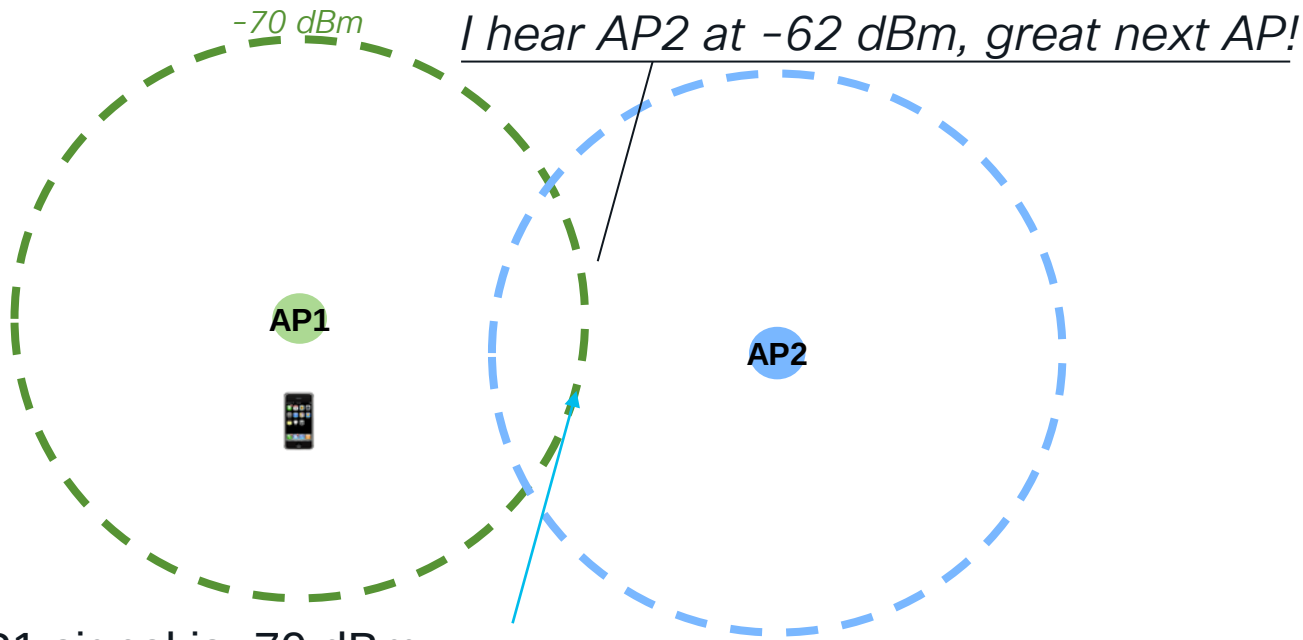
Some clients add conditions:

- Active traffic? -> less picky* than if idle
- Fast MCS drop? -> less picky*
- Lots of retries -> less picky*

*accepts next AP ‘less than *y* better’

Cell Edge Math – iPhone Example

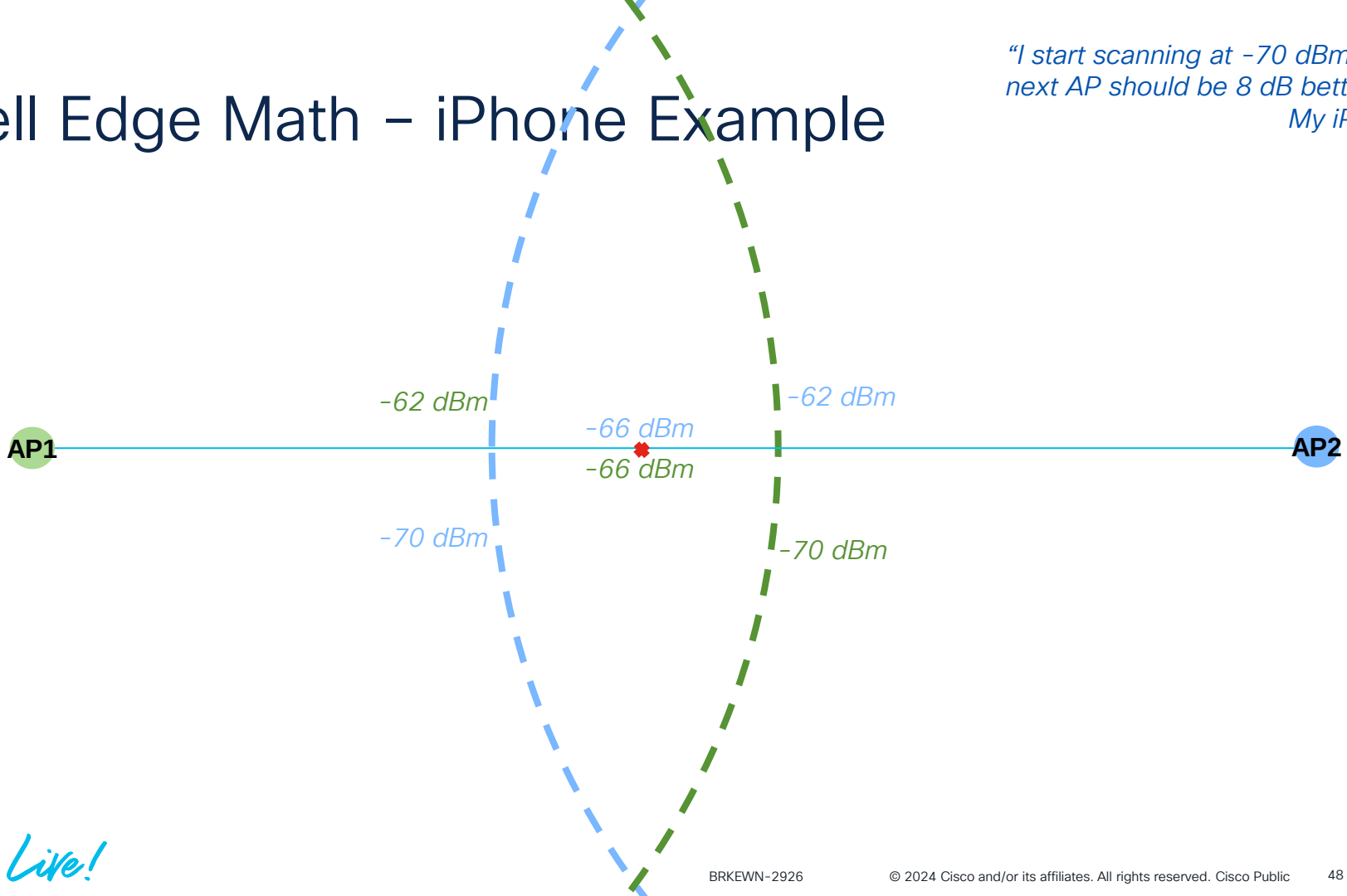
"I start scanning at -70 dBm, next AP should be 8 dB better"…
My iPhone



AP1 signal is -70 dBm…
So AP2 signal should be? -62 dBm!

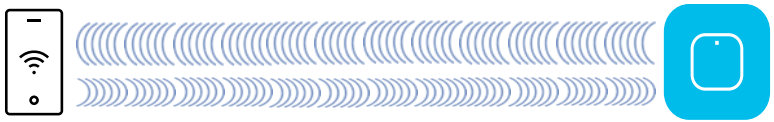
Cell Edge Math – iPhone Example

"I start scanning at -70 dBm, next AP should be 8 dB better"…
My iPhone

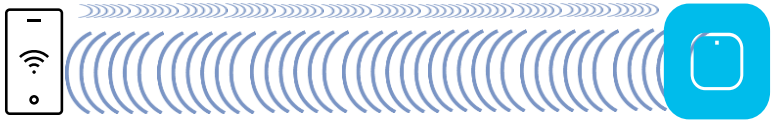


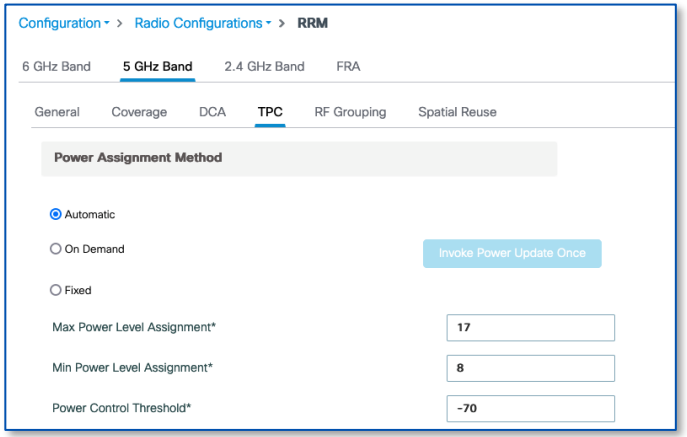
-66 dBm, but What is the AP Power?

- In short: right AP max power value is at your worst client max power
  - Experience shows you can allow a 3 dB margin
  - For 5 GHz, most worst clients are at 14 dBm, set your AP power to 17 dBm max



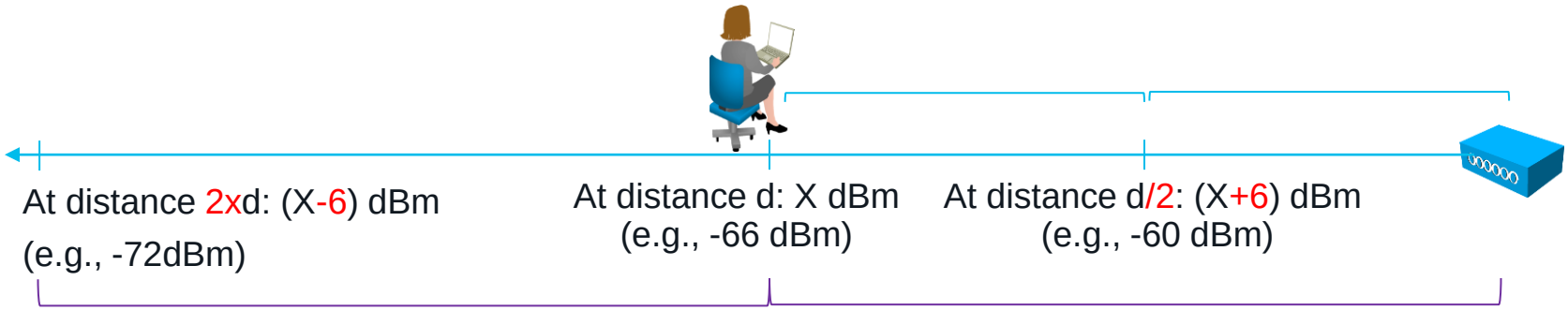
- Otherwise, you get this:





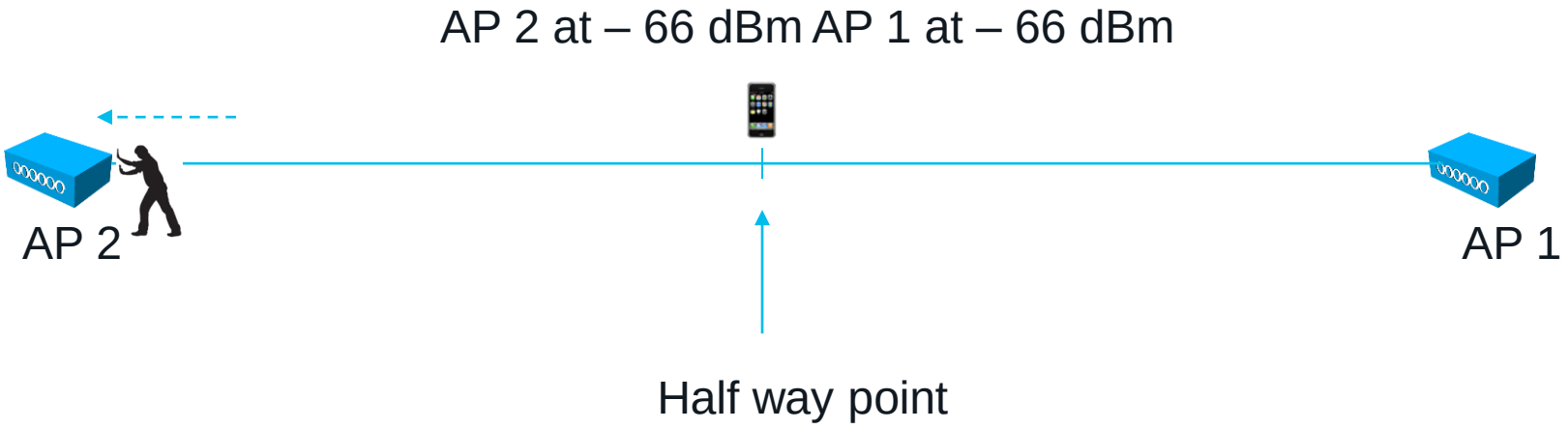
How To Design Your Overlap

- First trick to know:
  - Twice the distance = -6 dB
  - Half the distance = + 6dB



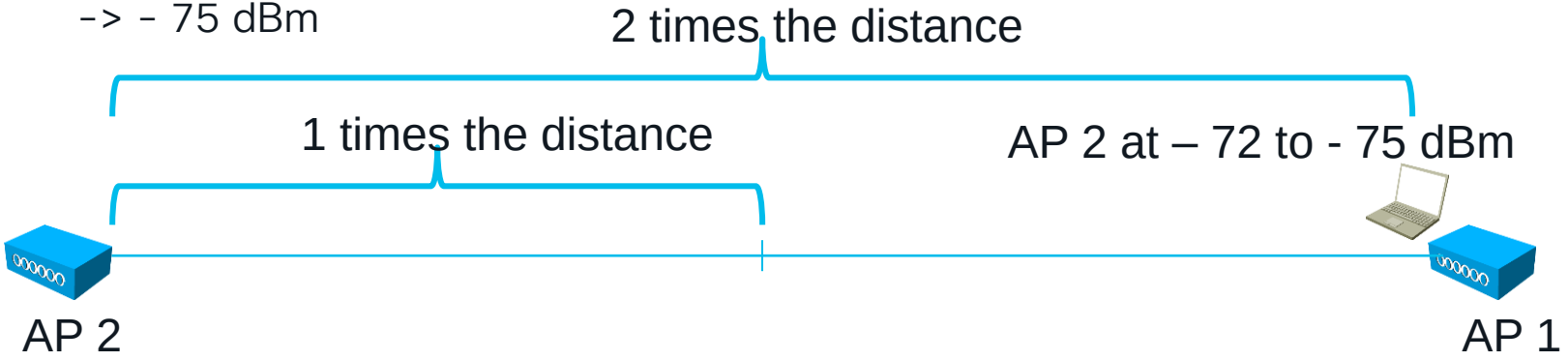
The – 6 dBm Rule

- So if you stand at the "-66 dBm border"…
  - Move away from AP 1 until you get – 66 dBm
  - Then pull AP 2 in the other direction until you also hear it at – 66 dBm



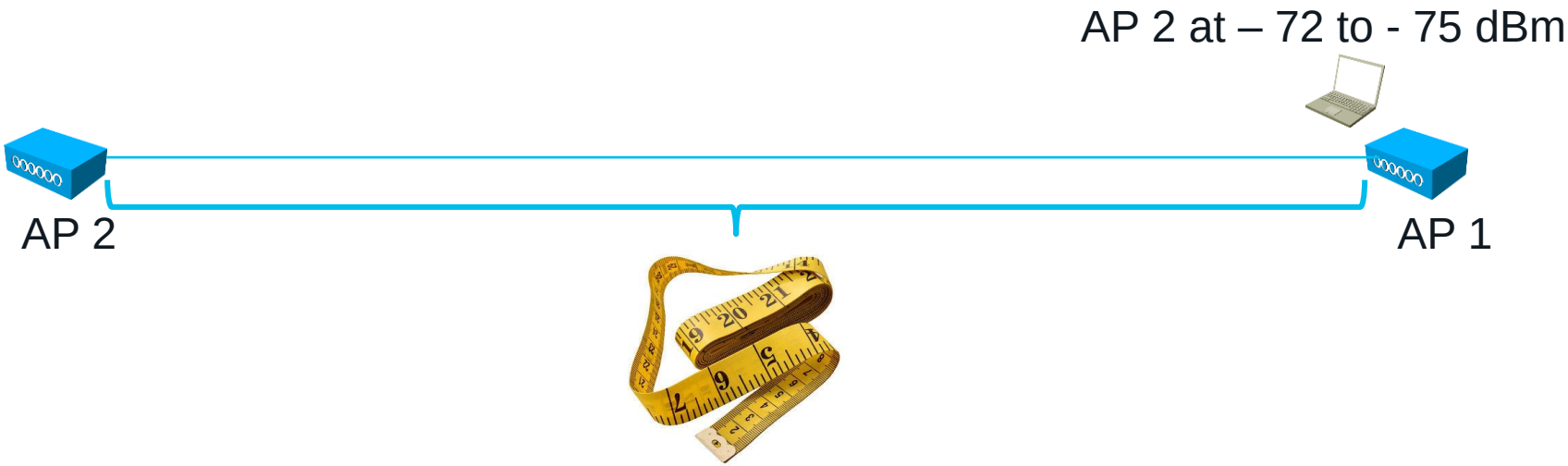
The – 6 dBm Rule

- Go back to AP 1
  - AP2 should be at “– 66 – 6” = –72 dBm. Add 2–3dB loss if there is a plaster wall –> – 75 dBm



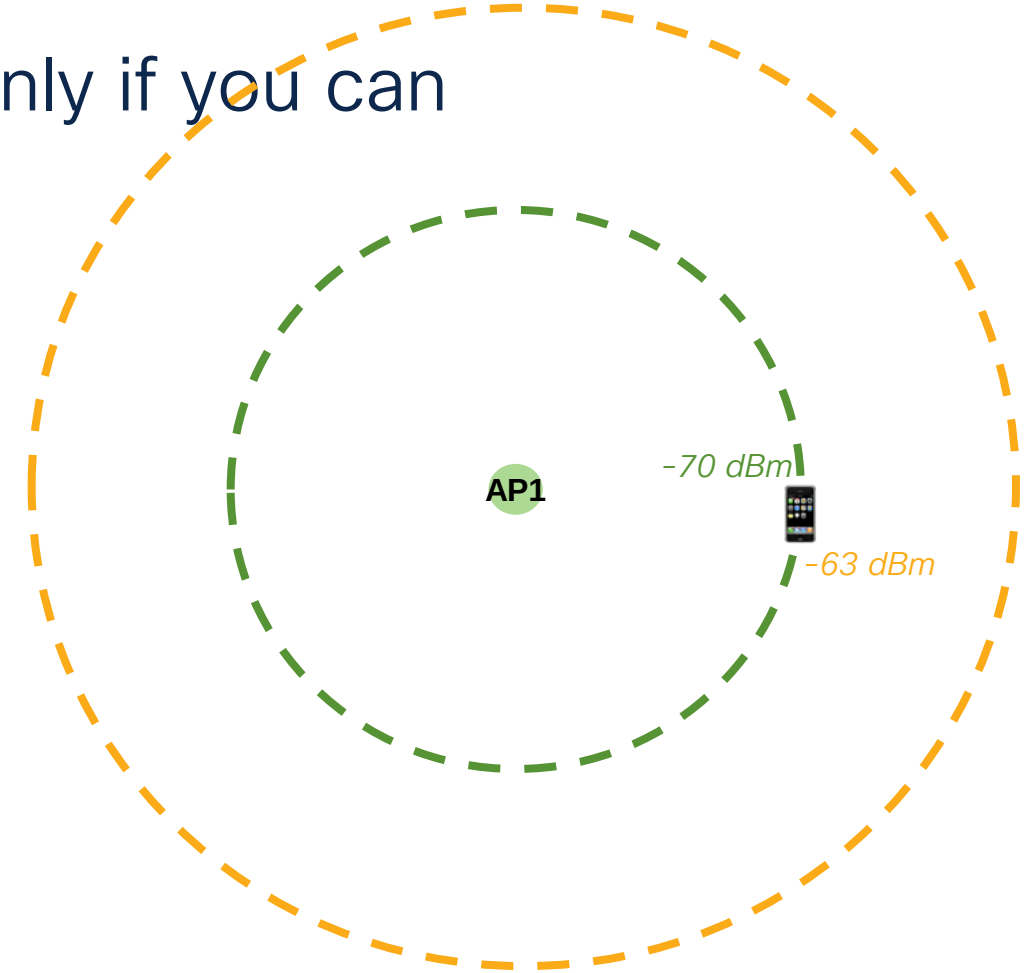
The – 6 dBm Rule

- Measure
  - This is your average AP to AP distance for this environment

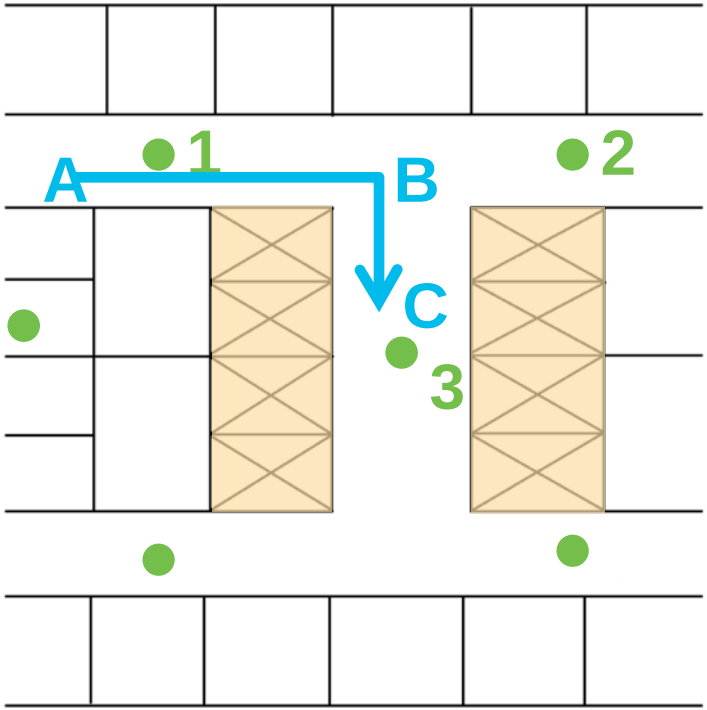


Design for 5/6 GHz-only if you can

- 2.4 GHz signal, at same distance from the AP, is commonly 7 dB better than 5 GHz signal
- Your client may roam to the same AP 2.4Ghz radio

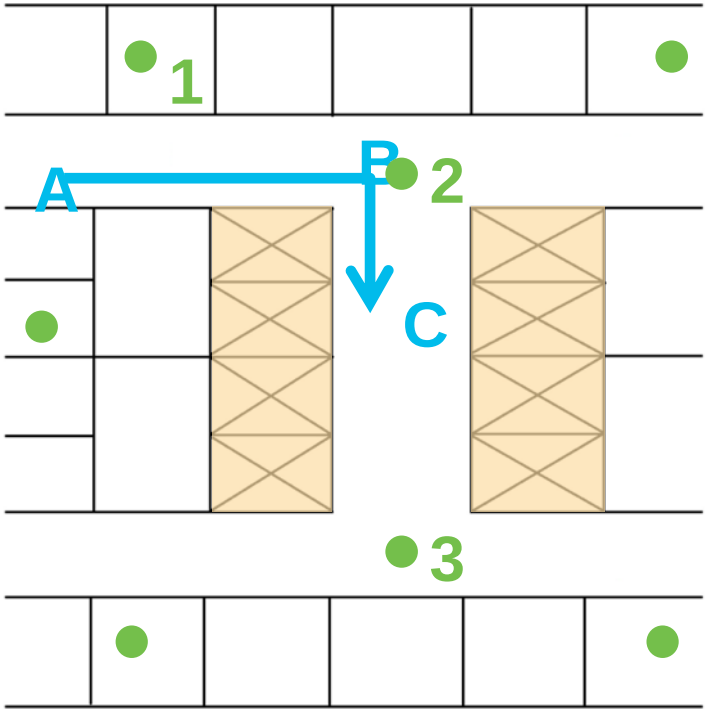


Use the Reports to Strategically Position Your Transition APs



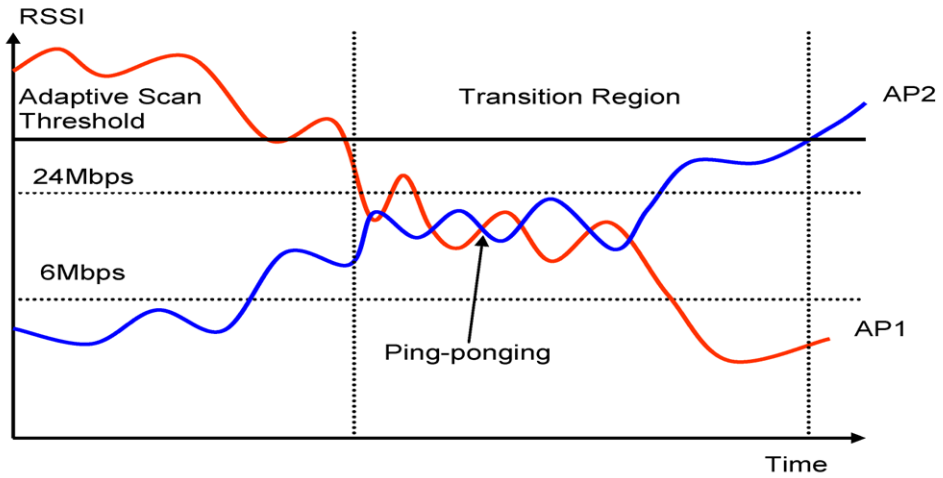
- At “A” the phone is connected to AP 1
- At “B” the phone has AP 2 in the neighbor list, AP 3 has not yet been scanned due to the RF shadow caused by the elevator bank
- At “C” the phone needs to roam, but AP 2 is the only AP in the neighbor list
- The phone then needs to rescan and connect to AP 3
  - 200 B frame @ 54 Mbps is sent in 3.7 µs
  - 200 B frame @ 24 Mbps is sent in 8.3 µs
  - Rate shifting from 54 Mbps to 24 Mbps can waste 1100 µs

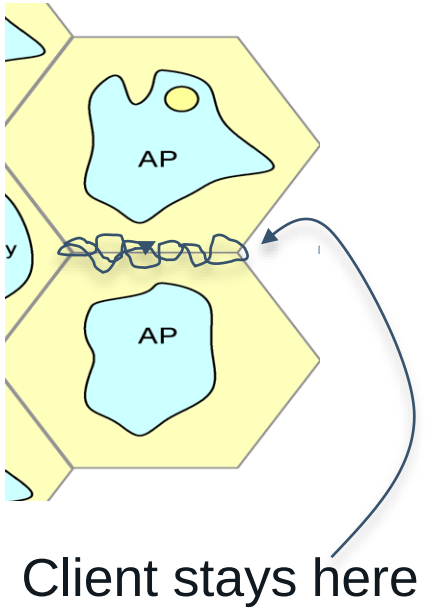
Use the Reports to Strategically Position Your Transition APs



- At point A the phone is connected to AP 1
- At point B the phone has AP 2 in the neighbor list as it was able to scan it while moving down the hall
- At point C the phone needs to roam and successfully selects AP 2
- The phone has sufficient time to scan for AP 3 ahead of time

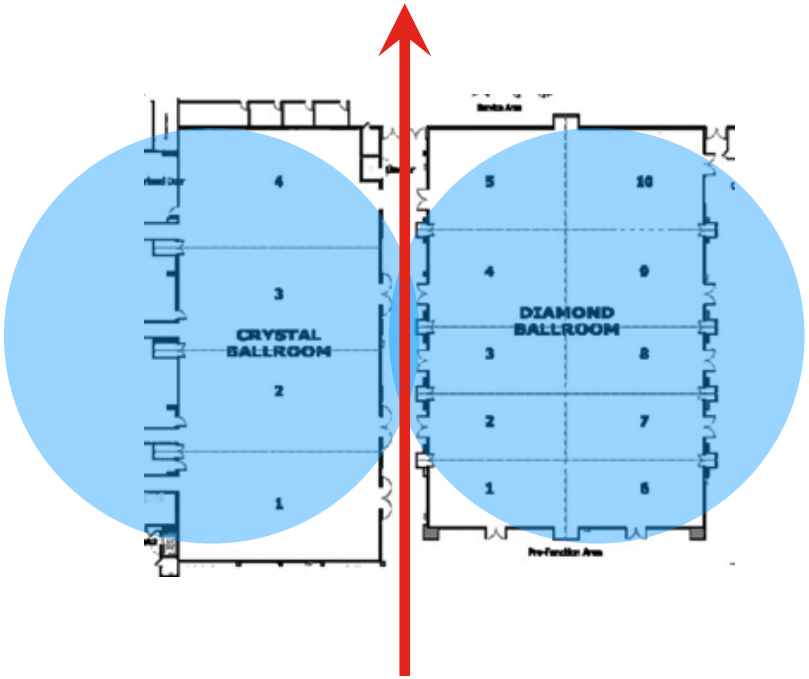
Avoid Ping Pong Zones

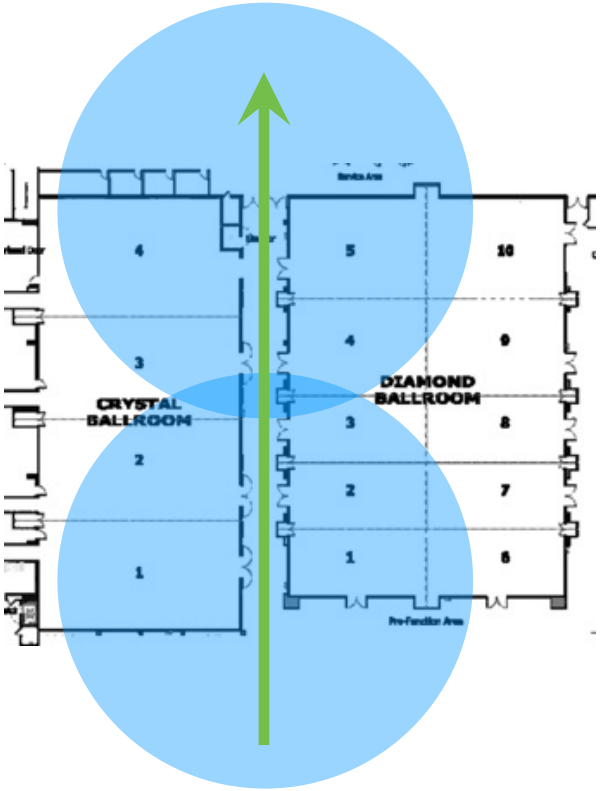




Ping-pong effect occurs when a wireless client is at the edge of two cells and hops between them.

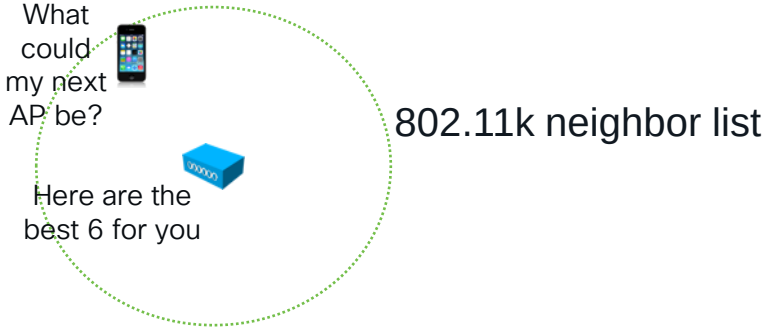
Avoiding Ping Pong Zones



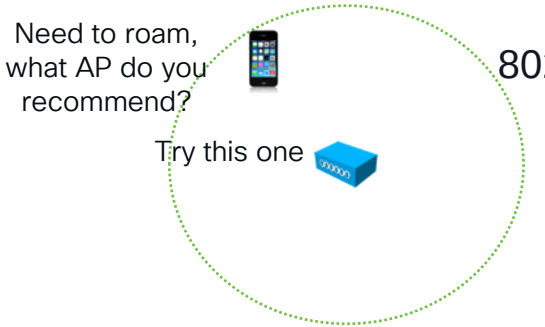


Tell your Clients About the Next (Best) Cell

- 802.11k and 802.11v BSS Transition Management



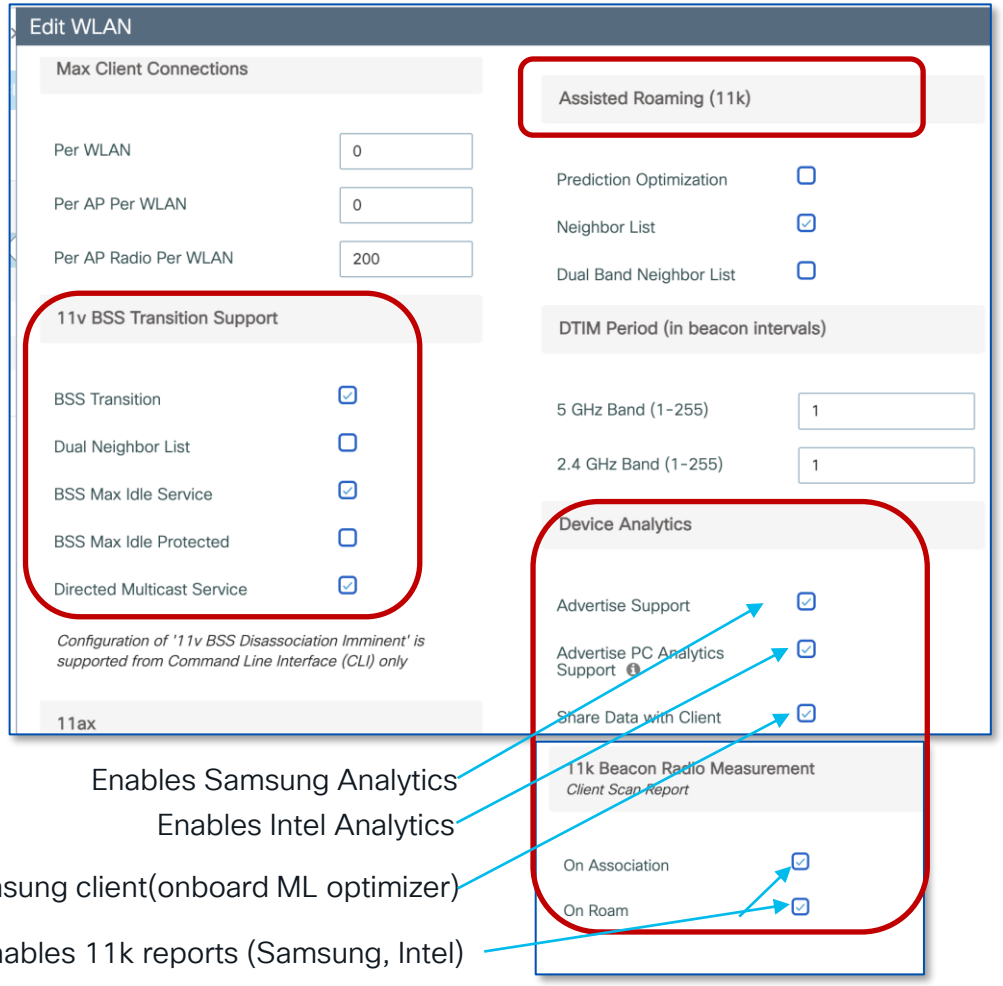
802.11k neighbor list



802.11v Solicited request

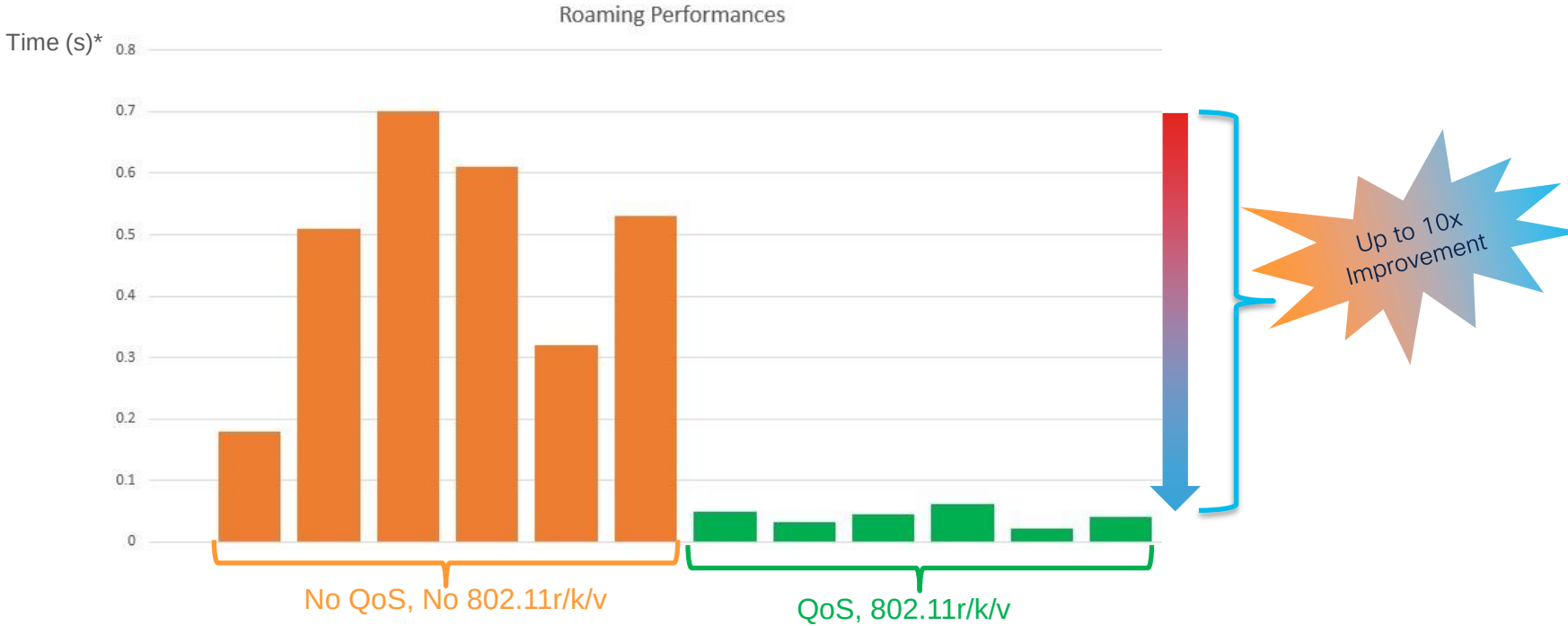
Where this Happens

- Enable individually 802.11k,v
- There is no downsides to 802.11k/v
- Enable Device Analytics to get information from client
- Share data with client to help upstream reports



Roaming Performance :

10x Better end-user Browsing and App Experience

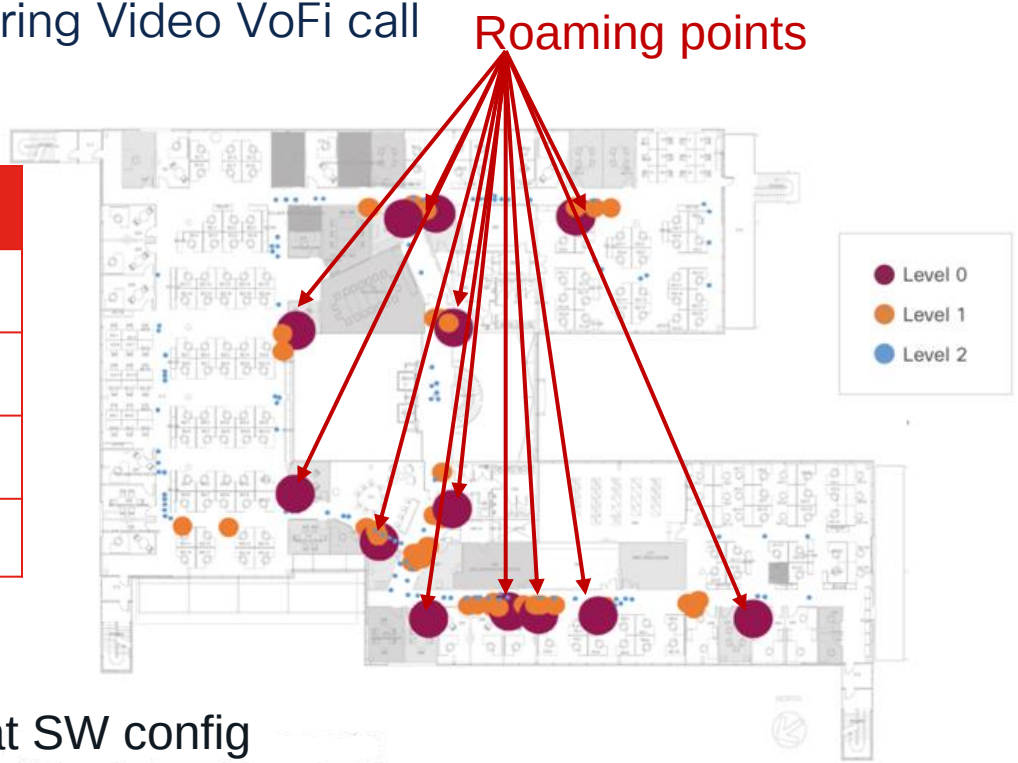


*Time Interval between last packet on previous AP, and first packet on next AP

An Example – Cisco Bedfont Lakes

Support requests – Wi-Fi issues during Video VoFi call

Incident level	(Before upgrade) Count over 1 week
Level 0 (productivity Crusher) - Call disconnected -	13
Level 1 (Productivity Inhibitor) - Audio & video gaps -	36
Level 2 (Minor Annoyance) - Audi glitch or light pixelization-	131
Total	180



1. Determine coverage gaps
2. If coverage is satisfactory, look at SW config

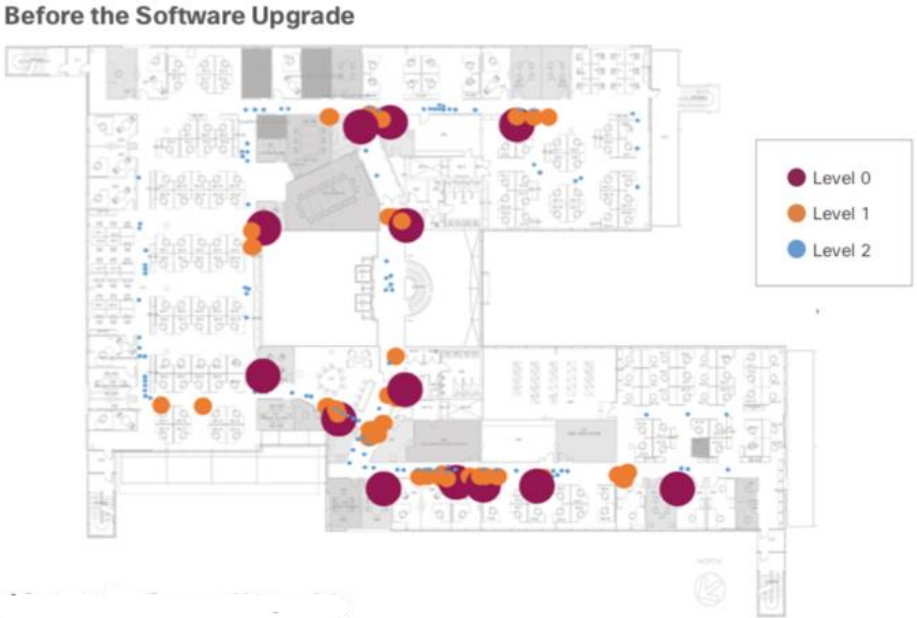
An Example – Cisco Bedfont Lakes

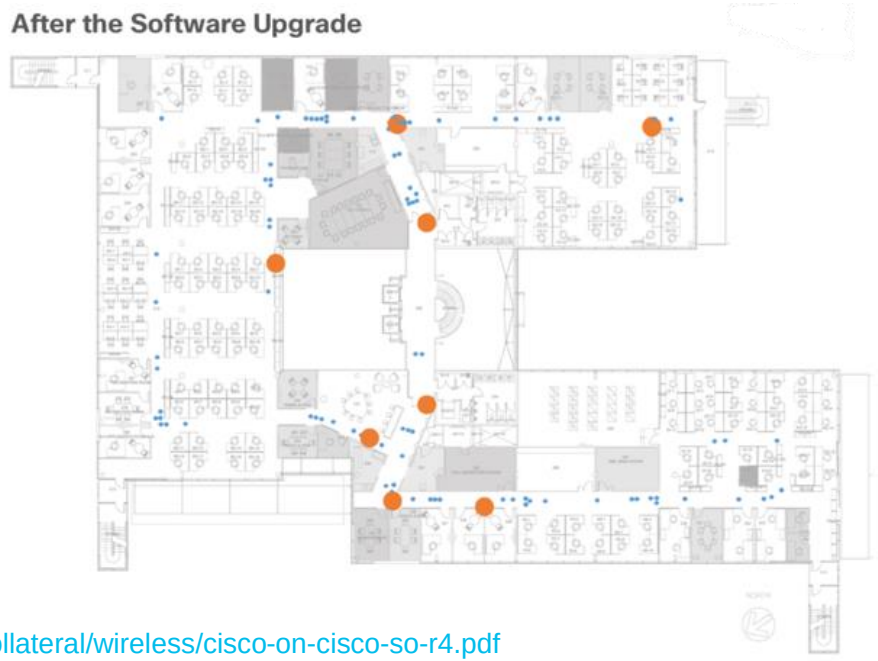
Support requests – Wi-Fi issues during Video VoFi call

Incident level	(Before upgrade) Count over 1 week	(After upgrade) Count over 1 week	Change (%)
Level 0 (productivity Crusher) - Call disconnected -	13	0	- 100%
Level 1 (Productivity Inhibitor) - Audio & video gaps -	36	8	- 78%
Level 2 (Minor Annoyance) - Audi glitch or light pixelization-	131	96	- 27%
Total	**180**	**104**	-42 %

An Example – Cisco Bedfont Lakes

Support requests – Wi-Fi issues during Video VoFi call





https://www.cisco.com/c/dam/en/us/products/collateral/wireless/cisco-on-cisco-so-r4.pdf

Takeaways

Conclusion

- Leverage the knowledge of your Wi-Fi clients in Cisco networks
  - Who is the client, how the client sees the world, why did the client leave
  - Use the pre-built tools in WLC/Catalyst Center/Meraki Dashboard, or build your own scrips if you have custom needs – we give you the raw data to empower you further
  - Set your AP power to match your client power
    - Remember, -70 dBm roaming edge is common, 14 dBm is common
- Think “roaming path”, position your APs so that view from the ceiling = view from the ground
- Enable 11k/r/v, QoS, 5 GHz-only SSIDs if you can

Meet The Engineer

- If you have specific questions, ChatGPT suggest an MTE:

  “ChatGPT, write an ode to getting an MTE with Jerome”

Meet the Engineer with wisdom, Jerome by name,
Optimizing WiFi networks, his claim to fame.
For real-time apps demanding high connectivity,
He fine-tunes signals with profound efficacy.

In crowded halls and bustling spaces,
Jerome's expertise embraces,
Video streams and urgent commands,
He eradicates WiFi's limiting strands.

With keen proficiency, he seeks channels free,
From interference, ensuring seamless glee.
In milliseconds, success is defined,
Jerome's guidance, a network's lifeline.

Raise your voice, celebrate this wondrous seer,
Meet the Engineer, Jerome, connectivity's pioneer.
With his expertise, fear not a flawed connection,
WiFi optimized with Jerome's perfection.


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go