



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
BRKEWN-2926

CISCO *Live!*

#CiscoLive

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

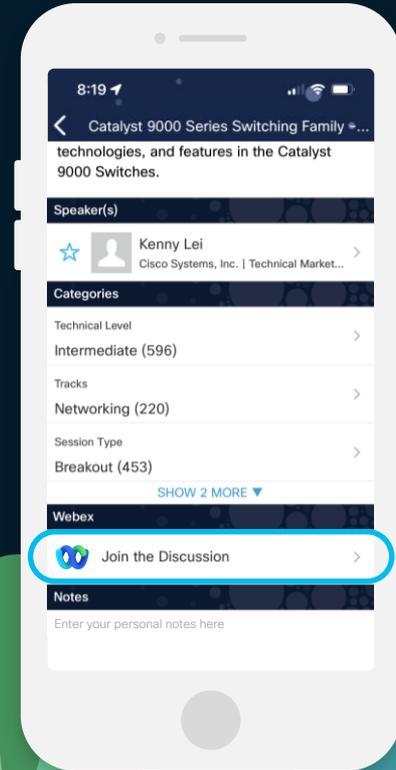
How

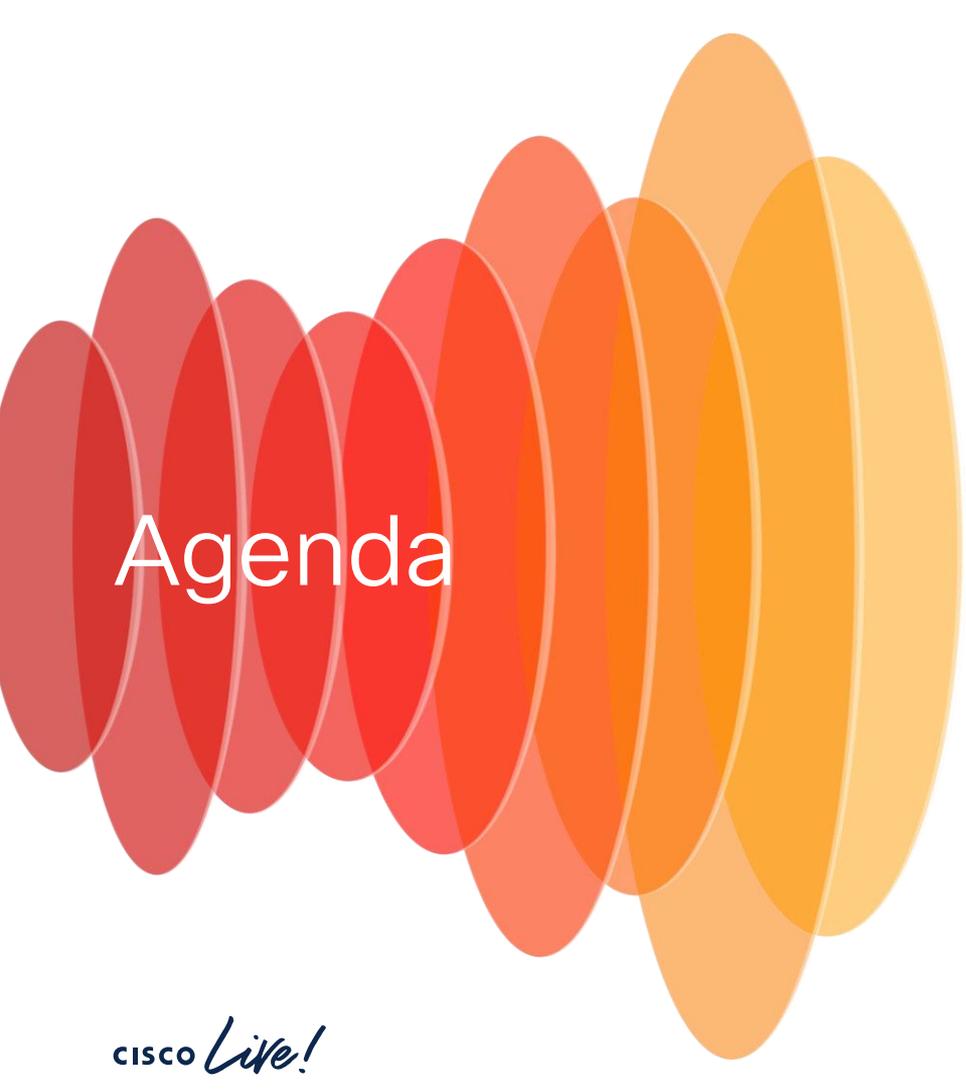
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 7, 2024.

CISCO *Live!*

<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2926>

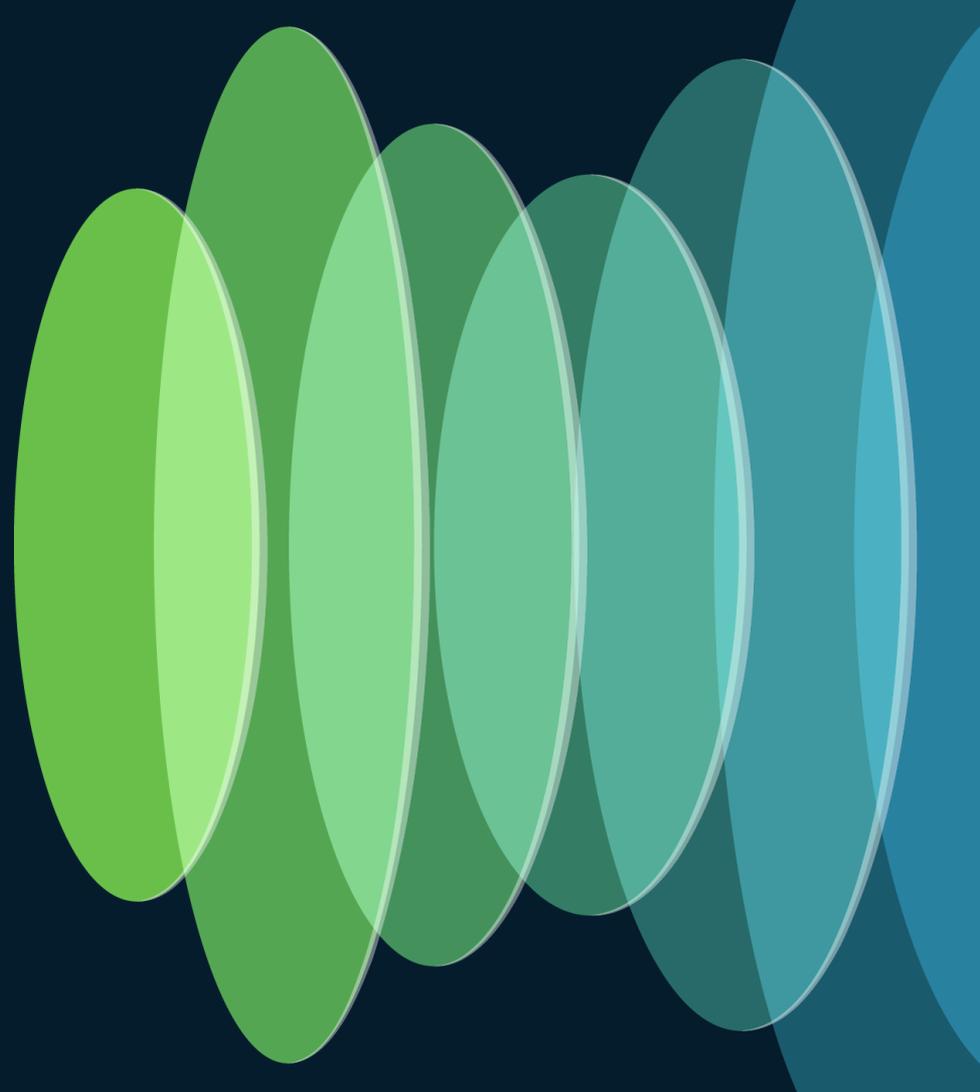




Agenda

- 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

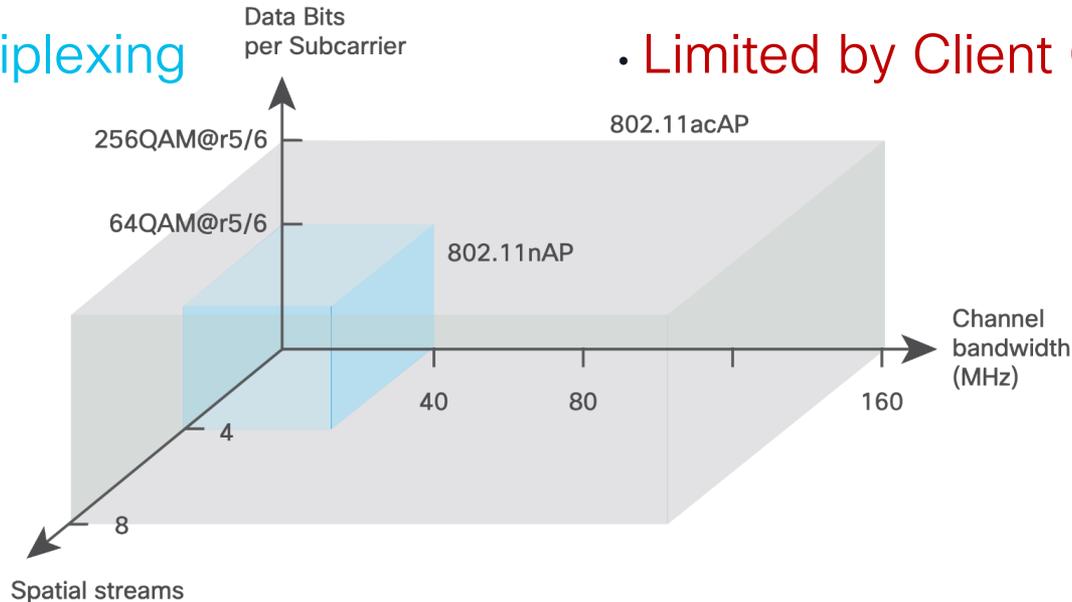
Why Are We
Here Together?



Three Dimensions to Wi-Fi Performance

- Digital Modulation
- Channel Aggregation
- Spatial Multiplexing

- Limited by SNR
- Limited by Spectrum Availability
- Limited by Client Capability



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

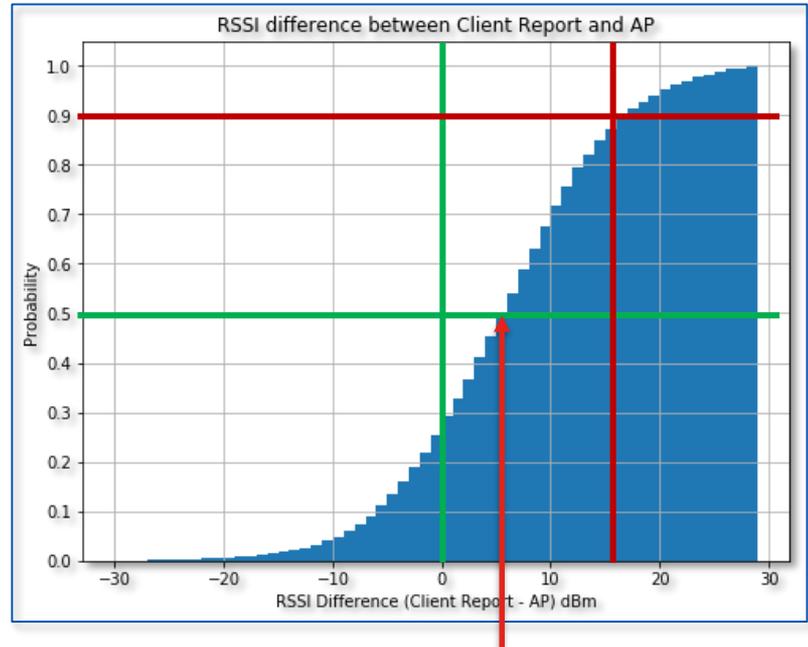
Client has limited awareness of other clients in the cell

Client has limited awareness of neighboring cells

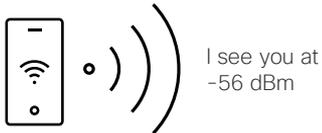
Client has no awareness of cell edge location or next cell conditions

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



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

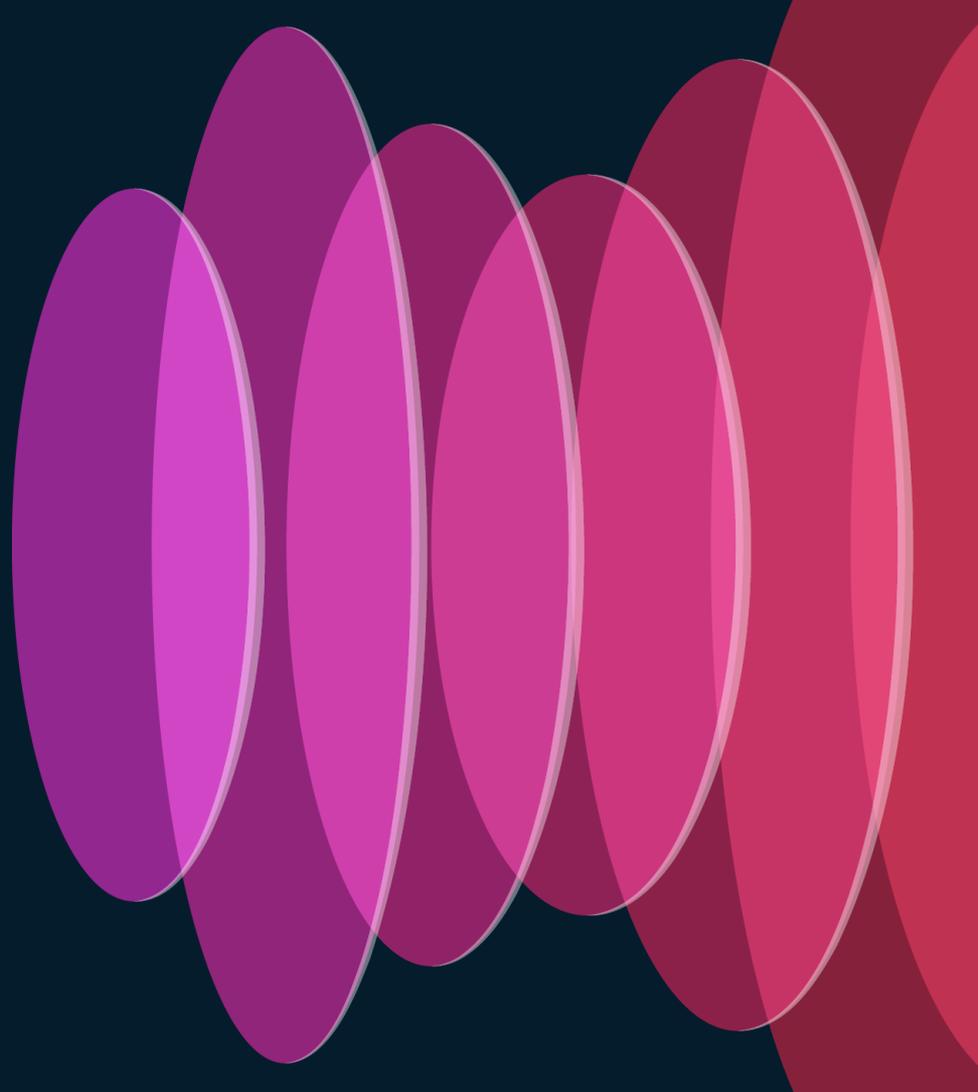
Why did it leave?

- 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?

Visible in C9800, Catalyst Center,
Meraki Dashboard***,
No configuration required

- **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

Detail Information Jan 3, 2023 11:52 AM

Device Info Connectivity RF iOS Analytics

Information

Device Type iPad Pro (11 inch) (2nd gen)

Operating System iOS 13.5.1

4 matching clients

Status	Description	Last seen	Usage	Device type, OS	IPv4 address	Policy
Wireless	Karas-MacBook-Air-3	Apr 24 15:03	811.8 MB	Mac OS X	192.168.10.17	Normal
Wireless	DAHUCABY-M-C9V9	Apr 24 15:03	1.70 GB	Apple iPhone	192.168.10.7	Normal
Wireless	iPhone-3	Apr 24 15:03	4.40 GB	iPhone 13, iOS15.6.1	192.168.10.15	Normal
Wireless	DH-iPad-Air	Apr 24 15:03	10.6 MB	iPad Air, iOS16.1.1	192.168.10.20	Normal

Protocol Capability Wi-Fi 6



I am iOS 13.5.1,
iPad Pro (11inch)

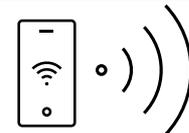
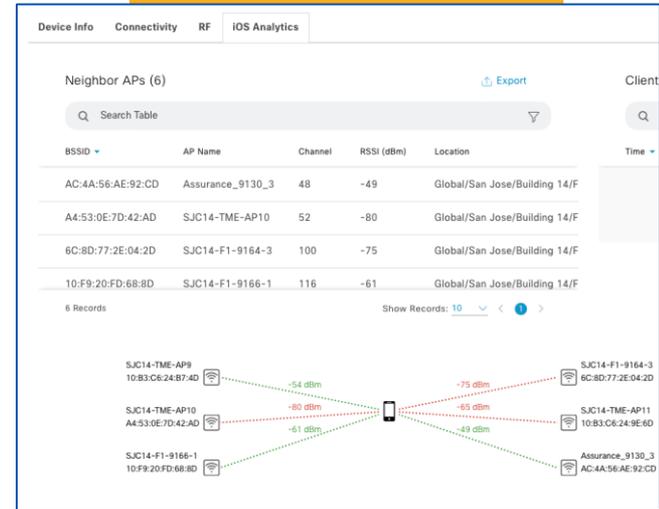


How does the client see the Network?

- **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, you 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’

* Samsung details are not supported in Meraki Dashboard yet

Visible in Catalyst Center,
Meraki Dashboard*,



Here is the list of
APs I see



Intel Analytics on Catalyst Center Client 360

Detail Information Jun 2, 2024 3:19 PM

Device Info Connectivity RF Intel Connectivity Analytics

Information

Device Type Dell Inc. Inspiron 5406 2n1

Operating System Windows 10

User Name --

Host Name OTA-wind11-156-U5DT

MAC Address A4:6B:B6:40:37:51

IPv4 Address 40.235.10.11

IPv6 Address 2000:40:235:0:352b:2cc7:c720:322b [\(7 more\)](#)

Status Connected

VLAN ID 2435

Association Protocol Wi-Fi 6E

Protocol Capability Wi-Fi 6E

L3 Virtual Network --

Connection Information

Band 6 GHz

Spatial Streams 1

Channel Width 40 MHz

WMM Supported

U-APSD Disabled

Station Information

HW Model AX210 160MHz

SW Version 22.110.00.02

AC/DC Voltage AC

System Manufacturer Intel

System Model Inspiron 5406 2n1

Intel Connectivity Analytics on Client 360

The screenshot displays the Intel Connectivity Analytics interface. At the top, there are tabs for 'Device Info', 'Connectivity', 'RF', and 'Intel Connectivity Analytics'. A blue arrow points to the 'Intel Connectivity Analytics' tab with the text 'Dedicated Intel Analytics Tab'. Below the tabs, there is a 'Roam Events' section with a dropdown menu showing dates: 'June 11, 11:53 AM', 'June 10, 10:00 AM', 'June 8, 9:20 AM', 'June 7, 9:00 AM', and 'June 5, 11:53 AM'. A blue arrow points to the 'June 11, 11:53 AM' event with the text 'Roam Event Details'. Below the date selection, the 'Reason Code' is 'Low RSSI', 'Selected AP' is 'AP9120.1234', 'BSSID' is '6C:B2:AE:C7:AB:00', and 'RSSI' is '-50 dBm'. A central diagram shows a smartphone icon connected to several access points (APs) and their BSSIDs. Red dashed lines indicate low RSSI connections to AP9120.1234 (6C:B2:AE:C7:AB:00) and OTA-9136B-17FC (68:7D:B4:5F:1E:88), both at -80 dBm. Green dashed lines indicate connections to AP9120.1237 (6C:B2:AE:C7:AB:00) and AP9120.1238 (6C:B2:AE:C7:AB:00), both at -34 dBm. A green callout bubble points to these connections with the text 'Neighboring APs and BSSID'. Below the diagram, there are three sections: 'Last 5 Reported Errors', 'Last 5 Temporary Disconnection Reports', and 'Last 5 Low RSSI Reports'. A blue callout bubble points to the 'Last 5 Reported Errors' section with the text 'Client Reports and Events'. The 'Last 5 Reported Errors' section shows an error for 'June 11, 11:56 AM' with details: '10 Access Points', 'Access Point: AP9120.1239', 'BSSID: 6C:B2:AE:C7:AB:00', 'Frame Type: Authentication Response', and 'Error: Missing Response'. The 'Last 5 Temporary Disconnection Reports' section shows reports for 'June 11, 11:53 AM' (Access Point: AP9120.1236, BSSID: 6C:B2:AE:C7:AB:00) and 'June 11, 11:50 AM' (Access Point: AP9120.1236). The 'Last 5 Low RSSI Reports' section shows reports for 'June 11, 10:34 AM' (Access Point: AP9120.1239, BSSID: 6C:B2:AE:C7:AB:00, RSSI: -80 dBm) and 'June 11, 10:17 AM'.

Intel Connectivity Analytics on Client 360 (cont.)

Event Viewer

Filter Export Go to Global Event Viewer

Event is Roam Report

May 9, 2022

Time	Device	Event	Time	RSSI	AP	Reason Code	Type
9:25:35.935 PM	Intel	Roam Report	9:25:35.935 PM	-47 dBm	OTA-9136B-17E0	Reason Code: Low RSSI	Device Analytics - Intel
8:55:33.628 PM	Intel	Roam Report	8:55:33.628 PM	-47 dBm	OTA-9136B-17E0	Reason Code: Better AP	Device Analytics - Intel
8:25:32.200 PM	Intel	Roam Report	8:25:32.200 PM	-47 dBm	OTA-9136B-17E0	Reason Code: Other	Device Analytics - Intel
7:55:30.066 PM	Intel	Roam Report	7:55:30.066 PM	-47 dBm	OTA-9136B-17E0	Reason Code: 11v force	Device Analytics - Intel
7:25:28.241 PM	Intel	Roam Report	7:25:28.241 PM	-47 dBm	OTA-9136B-17E0	Reason Code: Other	Device Analytics - Intel
7:25:28.241 PM	Intel	Roam Report	7:25:28.241 PM	-47 dBm	OTA-9136B-17E0	Reason Code: Low RSSI	Device Analytics - Intel
6:55:27.112 PM	Intel	Roam Report	6:55:27.112 PM	-46 dBm	OTA-9136B-17E0	Reason Code: Better AP	Device Analytics - Intel
6:25:26.366 PM	Intel	Roam Report	6:25:26.366 PM	-47 dBm	OTA-9136B-17E0	Reason Code: Other	Device Analytics - Intel
5:55:24.129 PM	Intel	Roam Report	5:55:24.129 PM	-46 dBm	OTA-9136B-17E0	Reason Code: Other	Device Analytics - Intel

Showing 1 - 9 of 48

Roam Reasons

Detailed Report

Roam Report May 9, 2022 7:25:28 PM

Detailed Information

Status:
● Report Received

Details:

AP Name	OTA-9136B-17E0
AP Mac	68:7D:B4:5F:1D:60
BSSID	68:7D:B4:5F:1D:68
Type	Device Analytics - Intel
Reason Code	Low RSSI
RSSI	-47 dBm
Candidate APs	Access Point: OTA-9136B-17FC BSSID: 68:7D:B4:5F:1E:B8 RSSI: -61 dBm

Low RSSI

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.

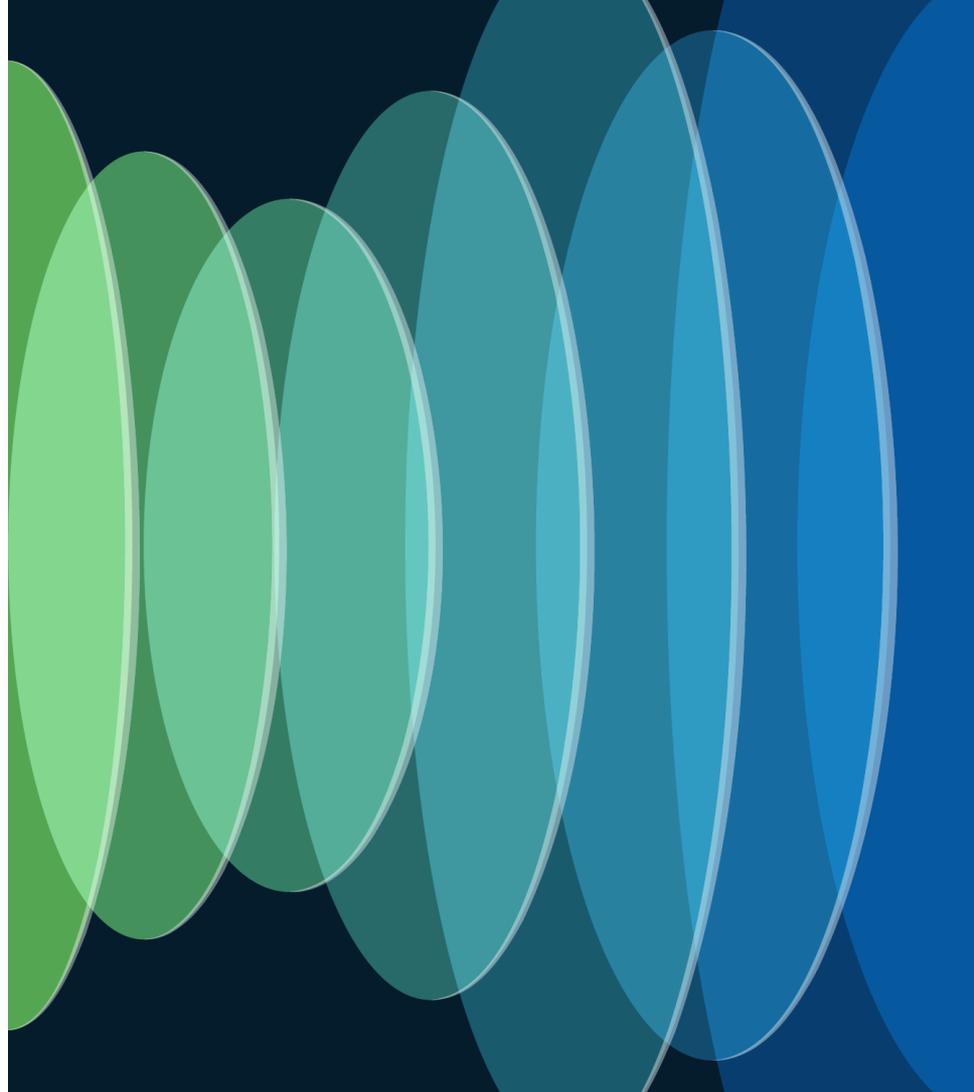
Helps troubleshoot issues with non-valid IEs and see why AP isn't responding.

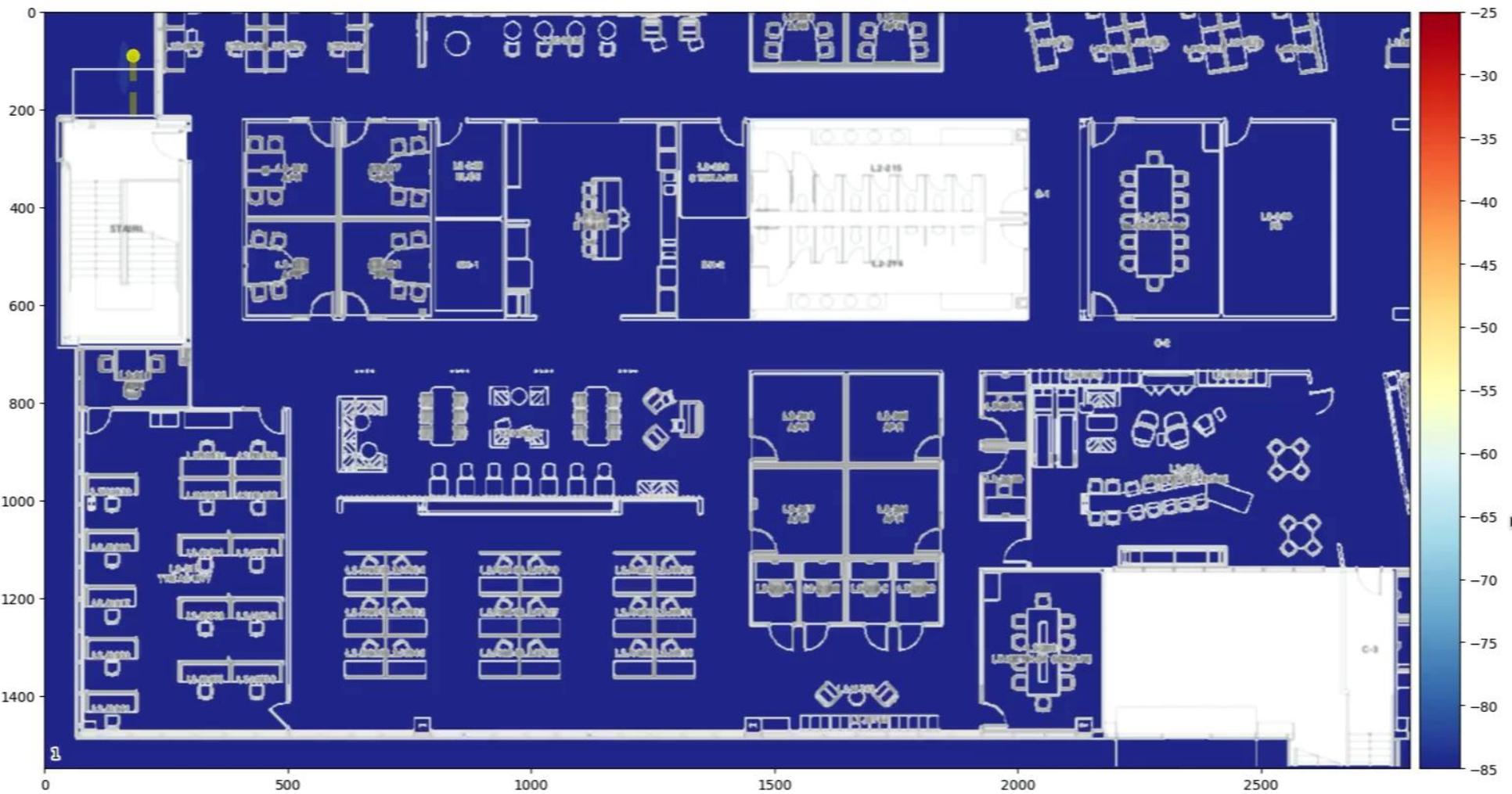
Failed APs

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

Used to identify and flag rogue BSSIDs

Use Client 11k Reports to Map your RF Floor





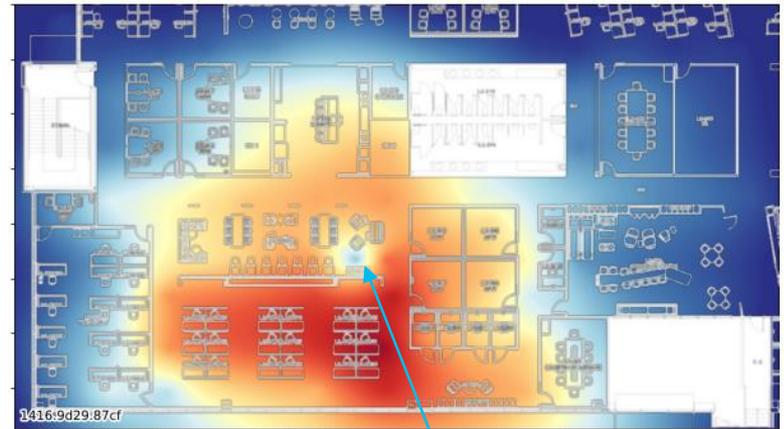
Map your RF Floor

From your client viewpoint

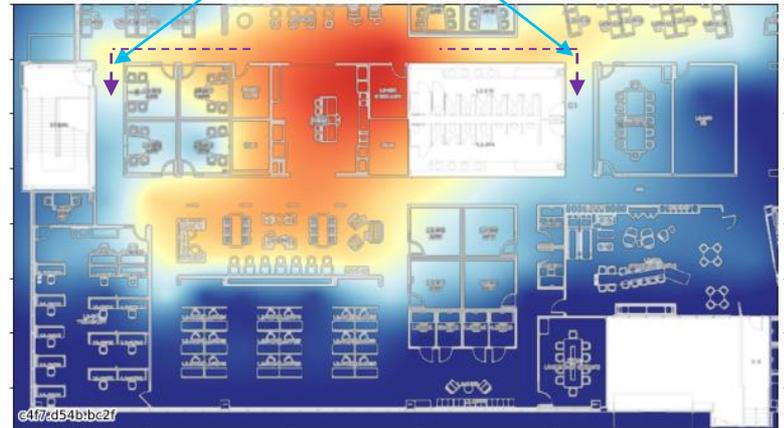
With a Cisco network and any recent Samsung galaxy or Intel client, you can send 802.11k (MBO) requests* to get the client view, anywhere, anytime

- 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

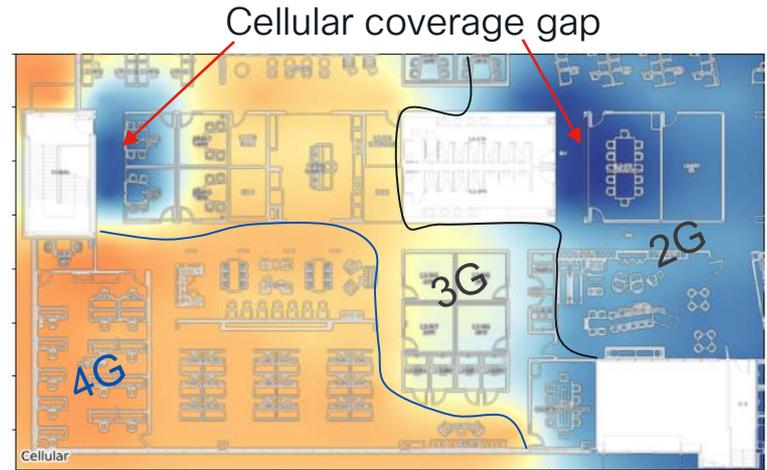


Signal drop as client turns the corner

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!



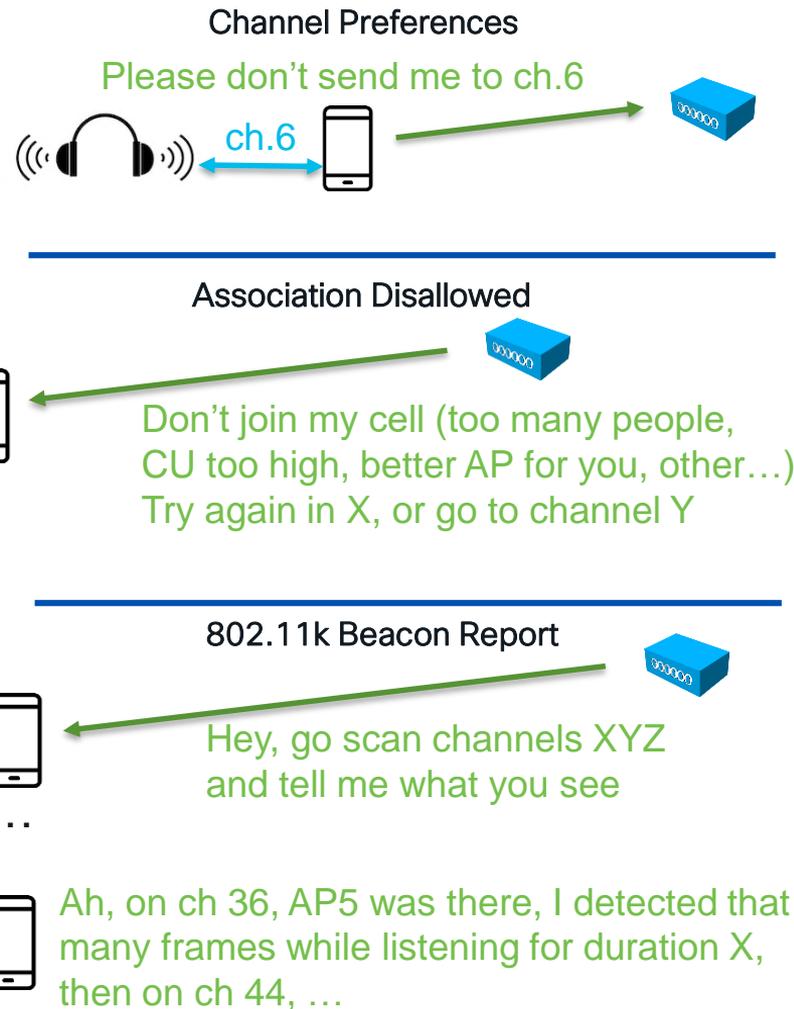
Note: Wi-Fi Aware (aka MBO)

Optimized Multiband Operations (Wi-Fi Alliance)

- At association: channel preferences (STA), association disallowed (AP)
- During the session: 802.11v (BTM), including 'go to LTE' variant, 802.11k reports
- Supported by all recent Samsung / Intel (and more) clients

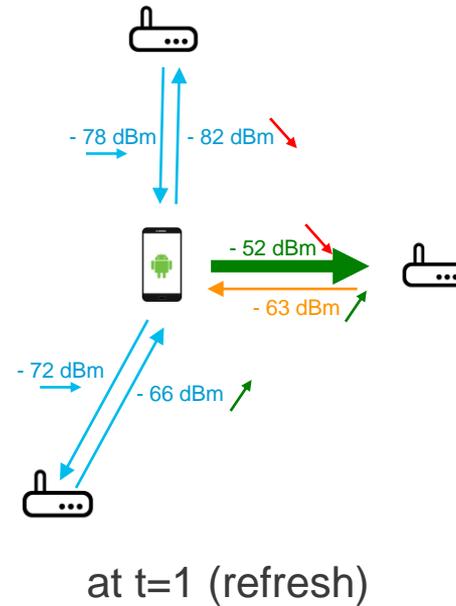
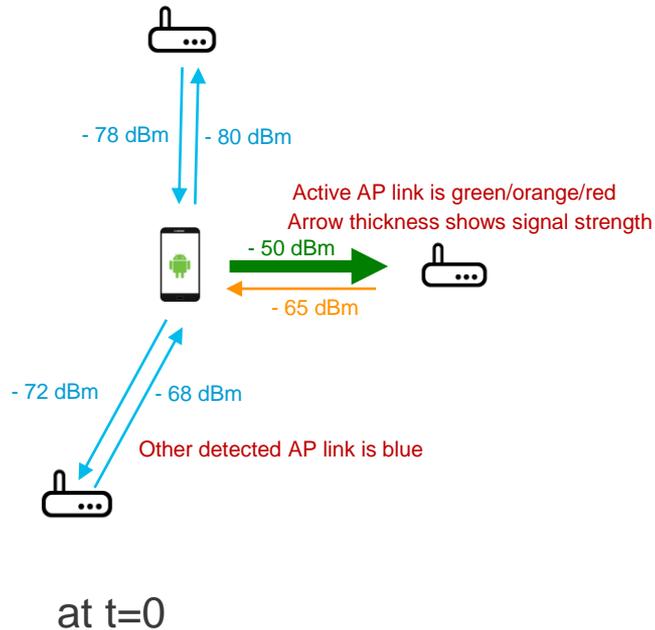
CISCO Live!

(after scan completes)



Getting the Client View Helps With Troubleshooting

Daphne complains that wi-fi is choppy on live call. You start link MBO and monitor real time UL/DL RSSI as Daphne walks about



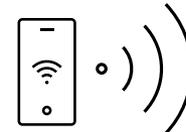
Why did the client go away?

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

- 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)

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		0
		1	Power Off or Wi-Fi Off				0
		2	Connects to other AP				0
		3	Remove AP profile				0
		4	Airplane mode On				0
		5-15	Reserved				0
2	L2 Connection	0	Unspecified	0-15	Reserved		0
		1	Association				0
		2-15	Reserved				0
3	4-Way Handshake	0	Unspecified	0-15	Reserved		0
		1	M1 for 4-Way Handshake				0
		2	M2 for 4-Way Handshake				0
		3	M3 for 4-Way Handshake				0
		4	M4 for 4-Way Handshake				0
		5	M1 for Groupkey Handshake				0
		6	M2 for Groupkey Handshake				0
		7-15	Reserved				0
							0
4	DHCP Fail	0	Unspecified	0-15	Reserved		0
		1	Time Out				0
		2	Time out after Roaming				0
		3	Lease Expired (no response for renew)				0
		4	Nak in renew				0
		5	Renew lease wrong IP				0
		6	internal error				0
		7-15	Reserved				0
							0

Cisco DNA Center



I am leaving as user turned on airplane mode



>	Onboarding	AP-AP7872.5DED.D23C WLC:veWLC WLAN:samsung-analytics
>	Delete	Due to Idle Timeout AP-AP7872.5DED.D23C WLC:veWLC WLAN:samsung-analytics
∨	Client Sent DisAssociation	AP-AP7872.5DED.D23C WLC:veWLC WLAN:samsung-analytics
	Client Sent DisAssociation	Disassociation Triggered by User - Airplane Mode

* Samsung details are not supported in Meraki Dashboard yet

Supported Software and Hardware Matrix

Cisco and Intel Chipset Devices

Cisco Access Point Hardware		Intel Chipset	
All Wave 2, Catalyst Wi-Fi 6/6E APs		AX200, AX201, AX210, AX211, AX411	
Cisco IOS XE WLC Software	Cisco AireOS WLC Software	Cisco Catalyst Center	Intel Driver Software
17.6.1	N/A	2.3.3	22.50.1
Cisco IOS XE WLC Hardware			
Embedded Wireless Controller on the AP and Switch			
C9800-CL			
C9800-L			
C9800-40			
C9800-80			

Intel Connectivity, Apple, Samsung Analytics Minimum Software Support Matrix

	Meraki	WLC Type	Catalyst Center	WLC SW Version
Intel Connectivity Analytics	MR29	IOS XE	2.3.3	17.6.1
		AireOS	N/A	N/A
Apple Analytics	MR27	IOS XE	2.2.1	16.12.1s
		AireOS	2.2.1	8.5
Samsung Analytics	MR29 Not launched yet	IOS-XE	2.2.1	17.1.1
		AireOS	N/A	N/A

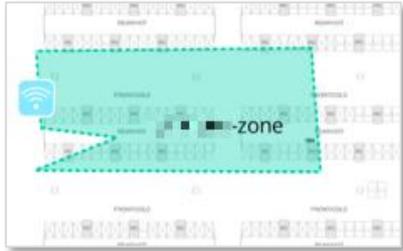
What do you need to configure?

		Intel	Apple	Samsung
What is the client type?	Catalyst (9800)	Device analytics > Advertise PC analytics support	Automatically on (CCXv5 IE has a bit set on by default)	Need Device Analytics > Advertise support
	Meraki	Automatically on, cannot be turned off	Automatically on, cannot be turned off	n.a.
How does the client see the network?	Catalyst (9800)	Automatically at association / reassociation if PC analytics is ON. Also sent dynamically	Automatically on (but only at association/reassociation time)	Automatically at association / reassociation if device analytics is ON. Also sent dynamically
	Meraki	Automatically on, cannot be turned off	Automatically on, cannot be turned off	n.a.
Why did the client leave?	Catalyst (9800)	Automatically if Advertise PC analytics support	Automatically on	Automatically if device Analytics is ON
	Meraki	Automatically on, cannot be turned off	Automatically on, cannot be turned off	n.a.
For better client experience	Catalyst (9800)	It's a good to enable 802.11k/v and Device Analytics > share data with client. Cisco sends the STA info about AP to tune its algorithms to understand what is a good AP		
	Meraki	n.a.		

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

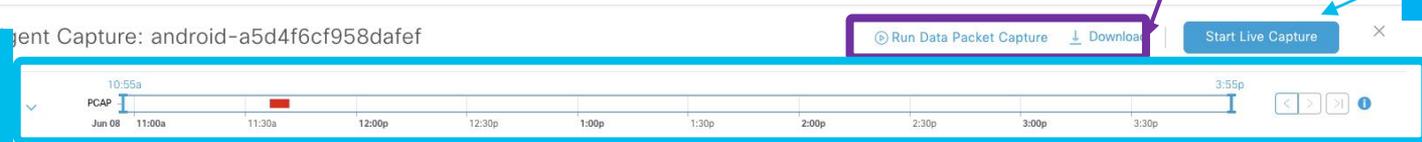
Catalyst Center – Better Client Troubleshooting

+ Now with Client View to Complete the Picture

Start and Stop Full Packet Capture for AF 4800

Real-Time Live Mode

Network Time Travel



Real-Time Client Event Viewer

Onboarding Events

Export PCAP

Time	Duration
11:40:20 am	754,271 ms
11:40:08 am	2,511 ms
11:36:49 am	3,988 ms
11:37:23 am	
11:37:13 am	
11:36:53 am	
11:36:53 am	
11:36:53 am	
11:36:49 am	
11:36:49 am	
11:27:05 am	5,093 ms
11:25:58 am	1,016 ms
11:14:34 am	601,172 ms
2,467 ms	
1 ms	
0,596 ms	

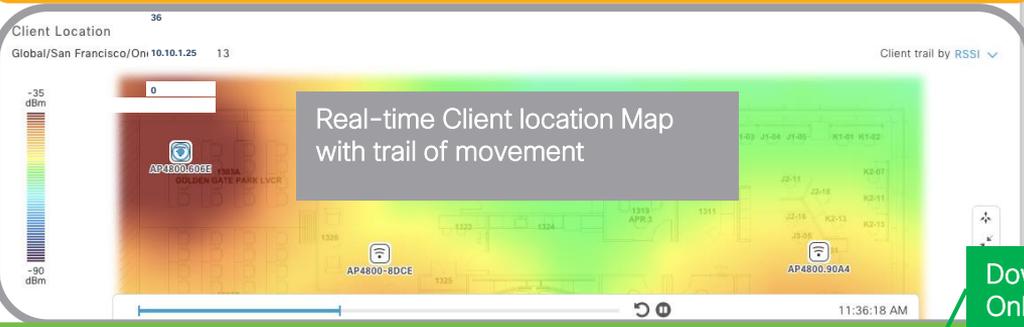
Session Duration

KeyExchange

Jun 8, 2019, 11:36:53.278 am

Client android-a5d4f6cf958dafef failed to connect due to 4-way handshake timeout

AP MAC:	70:69:5A:51:3F:A0	AP Name:	AP4800.606E
Frequency(GHz):	2.4	WLC Name:	CT5520-MK
WLAN:	@CorpSSID_PSK	Radio:	0



Real-time Client location Map with trail of movement



Onboard Packet stage identifier

Download Onboard Packet

Anomaly Packet Sequence

Feeding Device Ecosystem Data Into your AIML Projects

- We already include them in our AI RRM computations (Catalyst Center)
 - AI Wireless AIOps – BRKEWN-2039
 - Advanced RF Tuning for Wi-Fi 6E... – BRKEWN-3413
- You can also use the AP to export data and run your own AIML engines

The screenshot shows the Cisco DNA Center interface for AI Network Analytics. The top navigation bar includes 'Assurance / AI Network Analytics / AI-Enhanced RRM'. The main content area displays several summary cards: 'SUMMARY' (20 Total AP Count, 30 Total Clients), 'RF PERFORMANCE SUMMARY' (99/100 RRM Performance, 13% APs with High CCI, 16 RRM Changes), and 'RF COVERAGE SUMMARY' (High AP Density, High (35 dB) Connectivity). A 'Run RRM Simulation' button is visible. Below these cards, an 'Insights' section is highlighted with a red box, containing three suggestions: 'Consider changing the configured Busy Hours for RRM to be more effective.', 'Consider expanding the configured Channel List for reduced neighbor contention and improved performance.', and 'Consider changing the configured Channel Width for improved performance.'

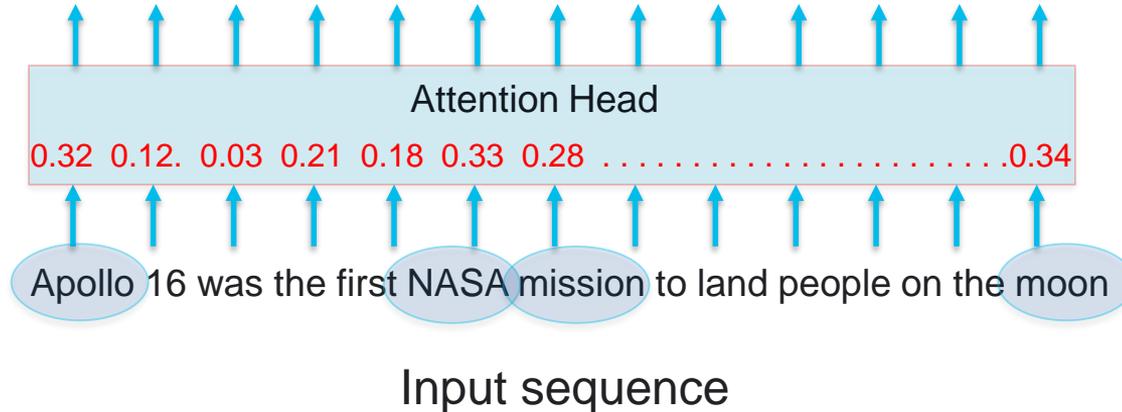
What if you had applied the suggestions

The screenshot shows the 'Create Simulation' configuration page. It includes a 'Simulation Name*' field with the value 'RRM_RF_PROFILE'. Under 'Basic Settings', there are sections for 'Radio Frequency Settings' (with 2.4 GHz, 5 GHz, and 6 GHz selected), 'Busy Hours' (with start time 8:00 and end time 17:00, and 'Medium' sensitivity selected), and 'Enable RF Settings' (with 'Flexible Radio Assignment', 'Dynamic Channel Assignment', 'Dynamic Bandwidth Selection', and 'Transmit Power Control' all enabled).

AI-based predictions and suggestions

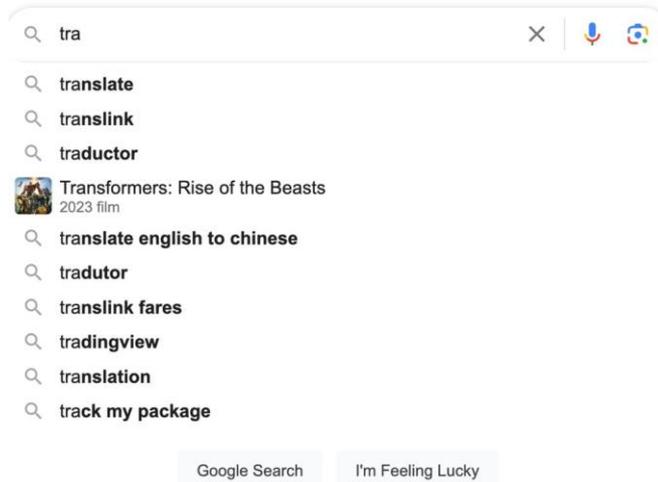
Example Customized AIML: Air Capture LLM

- 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 an 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

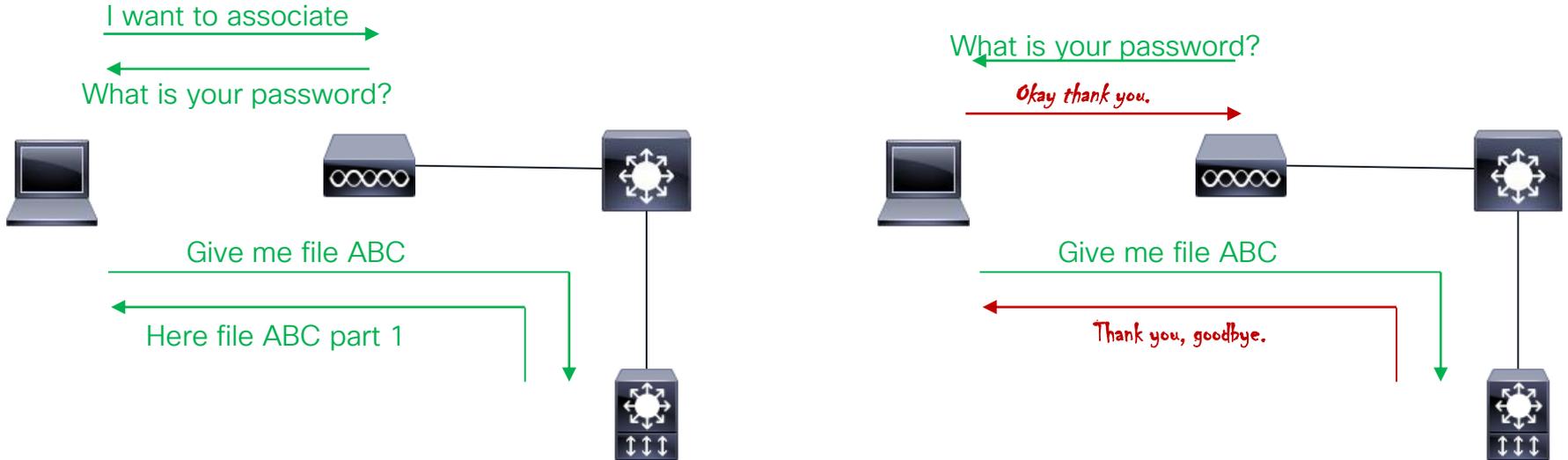
- LLM Inference
 - Then you start a word sequence, and the tool can either:
 - Predicts what comes next (and tell you)
 - Tell you if there is something strange about the sequence



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

0000	00	00	38	00	6f	08	00	c0	01	00	00	40	c4	f7	d5	4b
0010	9e	c9	b8	b2	00	00	00	00	12	0c	3c	14	40	01	bf	a2
0020	01	09	00	10	18	00	03	00	02	00	00	01	00	10	18	03
0030	06	00	48	60	02	00	00	00	80	00	00	00	ff	ff	ff	ff
0040	ff	ff	c4	f7	d5	4b	bc	2f	c4	f7	d5	4b	bc	2f	b0	38
0050	4f	00	dd	9f	00	00	00	00	64	00	01	11	00	09	43	6f
0060	72	70	6f	72	61	74	65	01	08	8c	12	98	24	b0	48	60
0070	6c	05	04	00	01	00	00	07	4e	55	53	04	24	01	18	28
0080	01	18	2c	01	18	30	01	18	34	01	18	38	01	18	3c	01
0090	18	40	01	18	64	01	18	68	01	18	6c	01	18	70	01	18
00a0	74	01	18	78	01	18	7c	01	18	80	01	18	84	01	18	88
00b0	01	18	8c	01	18	90	01	18	95	01	1e	99	01	1e	9d	01
00c0	1e	a1	01	1e	a5	01	1e	20	01	00	0b	05	00	00	04	8d
00d0	5b	46	05	33	00	00	00	00	2d	1a	ad	09	17	ff	ff	ff
00e0	ff	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00f0	00	00	00	00	3d	16	24	00	00	00	00	00	00	00	00	00
0100	00	00	00	00	00	00	00	00	00	00	00	00	00	7f	08	04
0110	08	84	01	40	00	40	6b	01	13	6c	02	7f	00	6f	0b	00
0120	33	00	40	96	00	50	54	00	50	a7	bf	0c	b1	69	83	0f
0130	aa	ff	00	00	aa	ff	00	20	c0	05	00	24	00	fc	ff	c3
0140	02	00	22	ff	24	23	01	00	08	12	00	10	44	20	02	c0
0150	0f	43	85	18	00	0c	00	aa	ff	aa	ff	3b	1c	c7	71	1c
0160	c7	71	1c	c7	71	00	00	00	00	ff	07	24	04	00	00	81
0170	fc	ff	ff	0e	26	04	00	a4	08	20	a4	08	40	43	08	60
0180	32	08	dd	05	00	40	96	03	05	dd	05	00	40	96	14	00
0190	dd	05	50	6f	9a	10	21	dd	05	00	40	96	0b	89	dd	05
01a0	00	40	96	2c	0e	dd	18	00	50	f2	02	01	01	84	00	03

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)

```
> Frame 1: 460 bytes on wire (3680 bits), 460 bytes captured on interface 0, capture length 460 bytes on interface 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
✓ IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  ✓ Tagged parameters (364 bytes)
    > Tag: SSID parameter set: "Corporate"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36(B), 48(B)
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1
    > Tag: Country Information: Country Code US, Environment Code 0
    > Tag: Power Constraint: 0
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: Interworking
    > Tag: Advertisement Protocol
    > Tag: Roaming Consortium
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: Tx Power Envelope
```

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_shift0.00000000
frame.time_epoch1681917506.078047000 frame.time_delta0.00000000 frame.time_delta_displayed0.00000000 frame.time_relative0.00000000 frame.number1
frame.len460 frame.cap_len460 frame.marked0 frame.ignored0 frame.protocolsradiotap:wlan_radio:wlan radiotap.version0 radiotap.padd0 radiotap.length556
radiotap.present.word0xc000086f radiotap.present.tsft1 radiotap.present.flags1 radiotap.present.rate1 radiotap.present.channell
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.am pdu0 radiotap.present.vht0 radiotap.present.timestamp0 radiotap.present.he0
radiotap.present.he_mu0 radiotap.present._0_length.psd0 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_namespace00:10:18:03:06:00:48:60:02:00:00:00 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.pwrmtg0 wlan.fc.moredata0 wlan.fc.protected0 wlan.fc.order0 wlan.duration0
wlan.raff:ff: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.ansd0 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

```
wlan_radio.phy5 wlan_radio.11a.turbo_type0 wlan_radio.data_rate6 wlan_radio.channel36 wlan_radio.noise_dbm-94 wlan_radio.snr29 wlan_radio.timestamp2998454686 wlan_radio.duration0 wlan_radio.end_tsf2998454686 wlan.fc.type_subtype0x0008 wlan.fc0x8000 wlan.fc.version0 wlan.fc.tods0 wlan.fc.fromds0 wlan.fc.frag0 wlan.fc.retry0 wlan.fc.pwrmt0 wlan.fc.more0 wlan.raff:ff:ff:ff:ff:ff wlan.ra_resolvedBroadcast wlan.addrff:ff:ff:ff:ff:ff wlan.addr
```

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)

Predicting the Next Frame

```
2024 --zsh--174x52
jerhenry@JERHENRY-M-61AM 2024 % python3 ChatNetPTParse.py Tshoot_assoc01.pcapng
processing
found an association with a Samsung S24
predicted authentication request:<RadioTap version=0 pad=0 len=56 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+dBm_AntNoise+Antenna+VendorNS+Ext Ext=[<RadioTapExtendedPresenceMask present=b0+b30 |>] mac_timestamp=256360316 Flags=ShortPreamble+FCS Rate=6.0 Mbps ChannelFrequency=5180 ChannelFlags=OFDM+5GHz dBm_AntSignal=-39 dBm dBm_AntNoise=-78 dBm Antenna=1 notdecoded=',/x00/x10/x18/x00/x03/x00/x02/x00/x00/x00/x00/x10/x18/x03/x06/x00//xac/x1d/x02/x00/x00/x00' |<Dot11FCS subtype=Authentication type=Management proto=0 FCfield= ID=15360 addr1=14:16:9d:29:87:cf (RA=DA) addr2=ce:ba:c0:39:e6:51 (TA=SA) addr3=14:16:9d:29:87:cf (BSSID/STA) SC=60208 fcs=0xe773fcfe |<Dot11Auth algo=open seqnum=1 status=success |>
observed authentication request:<RadioTap version=0 pad=0 len=56 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+dBm_AntNoise+Antenna+VendorNS+Ext Ext=[<RadioTapExtendedPresenceMask present=b0+b30 |>] mac_timestamp=256360316 Flags=ShortPreamble+FCS Rate=6.0 Mbps ChannelFrequency=5180 ChannelFlags=OFDM+5GHz dBm_AntSignal=-39 dBm dBm_AntNoise=-78 dBm Antenna=1 notdecoded=',/x00/x10/x18/x00/x03/x00/x02/x00/x00/x00/x00/x10/x18/x03/x06/x00//xac/x1d/x02/x00/x00/x00' |<Dot11FCS subtype=Authentication type=Management proto=0 FCfield= ID=15360 addr1=14:16:9d:29:87:cf (RA=DA) addr2=ce:ba:c0:39:e6:51 (TA=SA) addr3=14:16:9d:29:87:cf (BSSID/STA) SC=60208 fcs=0xe773fcfe |<Dot11Auth algo=open seqnum=1 status=success |>
predicted authentication response:<RadioTap version=0 pad=0 len=56 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+dBm_AntNoise+Antenna+VendorNS+Ext Ext=[<RadioTapExtendedPresenceMask present=b0+b30 |>] mac_timestamp=256362039 Flags=ShortPreamble+FCS Rate=6.0 Mbps ChannelFrequency=5180 ChannelFlags=OFDM+5GHz dBm_AntSignal=-50 dBm dBm_AntNoise=-78 dBm Antenna=1 notdecoded=',/x00/x10/x18/x00/x03/x00/x02/x00/x00/x00/x00/x10/x18/x03/x06/x00//xac/x1d/x02/x00/x00/x00' |<Dot11FCS subtype=Authentication type=Management proto=0 FCfield= ID=15360 addr1=ce:ba:c0:39:e6:51 (RA=DA) addr2=14:16:9d:29:87:cf (TA=SA) addr3=14:16:9d:29:87:cf (BSSID/STA) SC=2240 fcs=0xa61e193e |<Dot11Auth algo=open seqnum=2 status=success |>
observed authentication response:<RadioTap version=0 pad=0 len=56 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+dBm_AntNoise+Antenna+VendorNS+Ext Ext=[<RadioTapExtendedPresenceMask present=b0+b30 |>] mac_timestamp=256362039 Flags=ShortPreamble+FCS Rate=6.0 Mbps ChannelFrequency=5180 ChannelFlags=OFDM+5GHz dBm_AntSignal=-50 dBm dBm_AntNoise=-78 dBm Antenna=1 notdecoded=',/x00/x10/x18/x00/x03/x00/x02/x00/x00/x00/x00/x10/x18/x03/x06/x00//xac/x1d/x02/x00/x00/x00' |<Dot11FCS subtype=Authentication type=Management proto=0 FCfield= ID=15360 addr1=ce:ba:c0:39:e6:51 (RA=DA) addr2=14:16:9d:29:87:cf (TA=SA) addr3=14:16:9d:29:87:cf (BSSID/STA) SC=2240 fcs=0xa61e193e |<Dot11Auth algo=open seqnum=2 status=success |>
Authentication 100% match
```

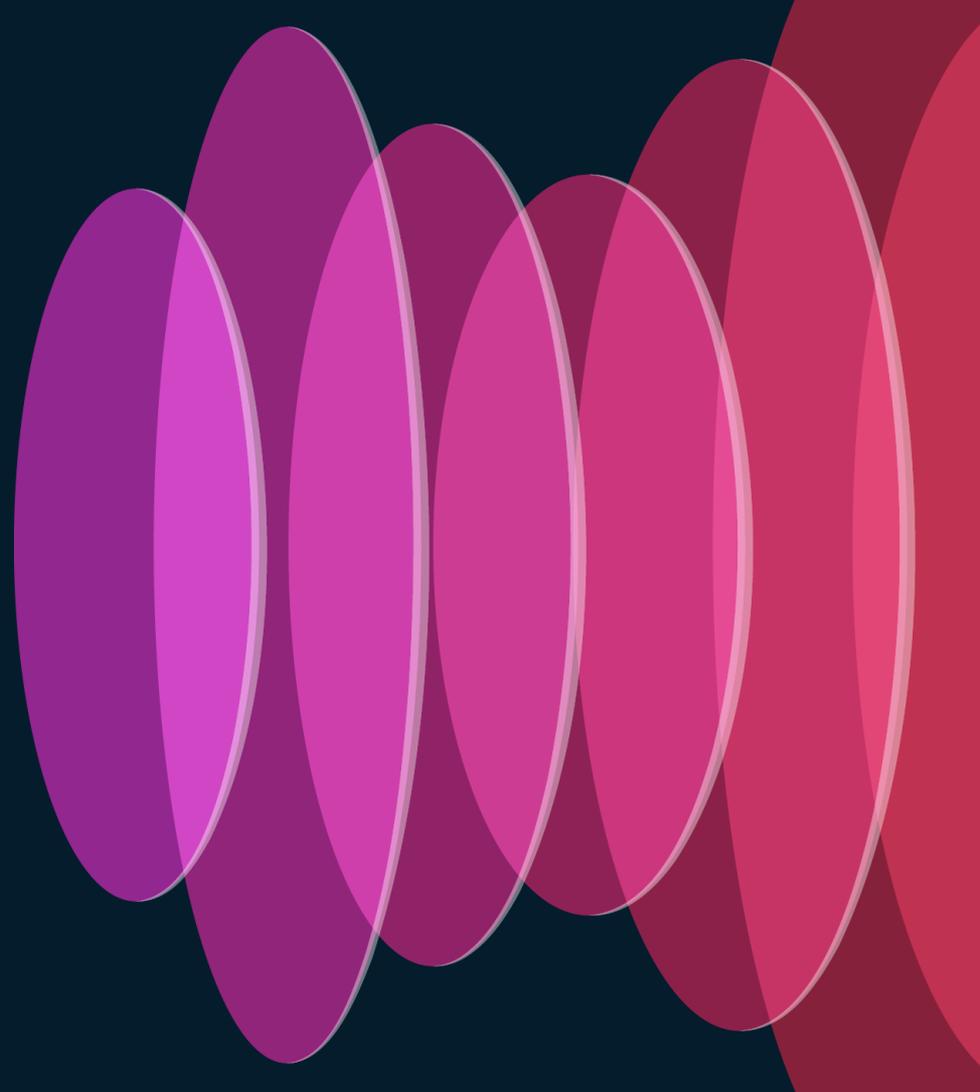
predicted association request: <RadioTap version=0 pad=0 len=56 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+dBm_AntNoise+Antenna+VendorNS+Ext Ext=[<RadioTapExtendedPresenceMask present=b0+b30 >] mac_timestamp=256363899 Flags=ShortPreamble+FCS Rate=6.0 Mbps ChannelFrequency=5180 ChannelFlags=OFDM+5GHz dBm_AntSignal=-39 dBm dBm_AntNoise=-78 dBm Antenna=1 notdecoded='D/x00/x10/x18/x00/x03/x00/x02/x00/x001/x00/x10/x18/x03/x06/x00\$/x04/x00/x00/x00/x00' |<Dot11FCS subtype=Association Request type=Management proto=0 FCfield= ID=15360 addr1=14:16:9d:29:87:cf (RA=DA) addr2=ce:ba:c0:39:e6:51 (TA=SA) addr3=14:16:9d:29:87:cf (BSSID/STA) SC=60224 fcs=0x60bc659d |<Dot11AssoReq cap=res8+res12+ESS listen_interval=1 |<Dot11Elt ID=SSID len=8 info='FlexSSID' |<Dot11EltRates ID=Supported Rates len=8 rates=[6.0(B) Mbps, 9.0 Mbps, 12.0(B) Mbps, 18.0 Mbps, 24.0(B) Mbps, 36.0 Mbps, 48.0 Mbps, 54.0 Mbps] |<Dot11Elt ID=Power Capability len=2 info='/x08/x14' |<Dot11Elt ID=Supported Channels len=10 info='\$/x044/x04d/x0c//x95/x05//xa9/x03' |<Dot11Elt ID=70 len=5 info='s/x1a//x91/x00/x04' |<Dot11Elt ID=59 len=23 info='tQSTstuvvxyz{|}~/x7f//x80//x81//x83//x84//x88//x82' |<Dot11EltHTCapabilities ID=HT Capabilities len=26 L_SIG_TXOP_Protection=0 Forty_Mhz_Intolerant=0 PSMP=0 DSSS_CCK=0 Max_A_MSDU=7935 o Delayed_BlockAck=0 Rx_STBC=1 Tx_STBC=1 Short_GI_40Mhz=1 Short_GI_20Mhz=1 Green_Field=0 SM_Power_Save=disabled Supported_Channel_Width=20Mhz+40Mhz LDPC_Coding_Capability=1 res1=0 Min_MPDCU_Start_Spacing=5 Max_A_MPDU_Length_Exponent=3 res2=0 TX_Unequal_Modulation=0 TX_Max_Spatial_Streams=0 TX_RX_MCS_Set_Not_Equal=0 TX_MCS_Set_Defined=0 res3=0 RX_Highest_Supported_Data_Rate=0 res4=0 RX_MSC_Bitmask=65535 res5=0 RD_Responder=0 HTC_HT_Support=0 MCS_Feedback=0 res6=0 PCO_Transition_Time=0 PCO=0 res7=0 Channel_Estimation_Capability=0 CSI_max_n_Rows_Beamformer_Supported=0 Compressed_Steering_n_Beamformer_Antennas_Supported=2 Noncompressed_Steering_n_Beamformer_Antennas_Supported=0 CSI_n_Beamformer_Antennas_Supported=0 Minimal_Grouping=0 Explicit_Compressed_Beamforming_Feedback=0 Explicit_Noncompressed_Beamforming_Feedback=0 Explicit_Transmit_Beamforming_CSI_Feedback=0 Explicit_Compressed_Steering=0 Explicit_Noncompressed_Steering=0 Explicit_CSI_Transmit_Beamforming=0 Calibration=0 Implicit_Transmit_Beamforming=0 Transmit_NDP=0 Receive_NDP=0 Transmit_Staggered_Sounding=0 Receive_Staggered_Sounding=0 Implicit_Transmit_Beamforming_Receive=0 ASEL= |<Dot11Elt ID=Extendend Capabilities len=10 info='/x04/x00/x08/x00/x00/x00/x00/x00' |<Dot11Elt ID=VHT Capabilities len=12 info='//xb2//xf1//x903//xfa//xff/x0c/x03//xfa//xff/x0c#' |<Dot11Elt ID=255 len=29 info='#/x03/x01/x10//xda0/x08/x040/x00//x89/x1d/x01//x80/x08/x02/x0c/x00//xfa//xff//xfa//xffy/x1c//xc7q/x1c//xc7q' |<Dot11EltVendorSpecific ID=Vendor Specific len=7 oui=00:50:f2 info='/x02/x00/x01/x00' |<Dot11EltVendorSpecific ID=Vendor Specific len=11 oui=8c:fd:f0 info='/x01/x01/x02/x01/x00/x02/x01/x01' |<Dot11EltVendorSpecific ID=Vendor Specific len=11 oui=00:00:f0 info='/x00/x01/x04/x00/x00/x00//xed' |<Dot11EltVendorSpecific ID=Vendor Specific len=40 oui=00:00:f0 info='/x02/x01/x0bvn\$/x13//xfd//xe0//xd01//x89I//xca/x05U/x17/r//xe9//xf6#//x93//xa1//x9a//xb2''/xa7//xa3//xc5M/x03//x96//xa8//xcf' |>

captured association request: <RadioTap version=0 pad=0 len=56 present=TSFT+Flags+Rate+Channel+dBm_AntSignal+dBm_AntNoise+Antenna+VendorNS+Ext Ext=[<RadioTapExtendedPresenceMask present=b0+b30 >] mac_timestamp=256363899 Flags=ShortPreamble+FCS Rate=6.0 Mbps ChannelFrequency=5180 ChannelFlags=OFDM+5GHz dBm_AntSignal=-39 dBm dBm_AntNoise=-78 dBm Antenna=1 notdecoded='D/x00/x10/x18/x00/x03/x00/x02/x00/x001/x00/x10/x18/x03/x06/x00\$/x04/x00/x00/x00/x00' |<Dot11FCS subtype=Association Request type=Management proto=0 FCfield= ID=15360 addr1=14:16:9d:29:87:cf (RA=DA) addr2=ce:ba:c0:39:e6:51 (TA=SA) addr3=14:16:9d:29:87:cf (BSSID/STA) SC=60224 fcs=0x60bc659d |<Dot11AssoReq cap=res8+res12+ESS listen_interval=1 |<Dot11Elt ID=SSID len=8 info='FlexSSID' |<Dot11EltRates ID=Supported Rates len=8 rates=[6.0(B) Mbps, 9.0 Mbps, 12.0(B) Mbps, 18.0 Mbps, 24.0(B) Mbps, 36.0 Mbps, 48.0 Mbps, 54.0 Mbps] |<Dot11Elt ID=Power Capability len=2 info='/x08/x14' |<Dot11Elt ID=Supported Channels len=10 info='\$/x044/x04d/x0c//x95/x05//xa9/x03' |<Dot11Elt ID=70 len=5 info='s/x1a//x91/x00/x04' |<Dot11Elt ID=59 len=23 info='tQSTstuvvxyz{|}~/x7f//x80//x81//x83//x84//x88//x82' |<Dot11EltHTCapabilities ID=HT Capabilities len=26 L_SIG_TXOP_Protection=0 Forty_Mhz_Intolerant=0 PSMP=0 DSSS_CCK=0 Max_A_MSDU=7935 o Delayed_BlockAck=0 Rx_STBC=1 Tx_STBC=1 Short_GI_40Mhz=1 Short_GI_20Mhz=1 Green_Field=0 SM_Power_Save=disabled Supported_Channel_Width=20Mhz+40Mhz LDPC_Coding_Capability=1 res1=0 Min_MPDCU_Start_Spacing=5 Max_A_MPDU_Length_Exponent=3 res2=0 TX_Unequal_Modulation=0 TX_Max_Spatial_Streams=0 TX_RX_MCS_Set_Not_Equal=0 TX_MCS_Set_Defined=0 res3=0 RX_Highest_Supported_Data_Rate=0 res4=0 RX_MSC_Bitmask=65535 res5=0 RD_Responder=0 HTC_HT_Support=0 MCS_Feedback=0 res6=0 PCO_Transition_Time=0 PCO=0 res7=0 Channel_Estimation_Capability=0 CSI_max_n_Rows_Beamformer_Supported=0 Compressed_Steering_n_Beamformer_Antennas_Supported=2 Noncompressed_Steering_n_Beamformer_Antennas_Supported=0 CSI_n_Beamformer_Antennas_Supported=0 Minimal_Grouping=0 Explicit_Compressed_Beamforming_Feedback=0 Explicit_Noncompressed_Beamforming_Feedback=0 Explicit_Transmit_Beamforming_CSI_Feedback=0 Explicit_Compressed_Steering=0 Explicit_Noncompressed_Steering=0 Explicit_CSI_Transmit_Beamforming=0 Calibration=0 Implicit_Transmit_Beamforming=0 Transmit_NDP=0 Receive_NDP=0 Transmit_Staggered_Sounding=0 Receive_Staggered_Sounding=0 Implicit_Transmit_Beamforming_Receive=0 ASEL= |<Dot11Elt ID=Extendend Capabilities len=10 info='/x04/x00/x08/x00/x00/x00/x00/x00' |<Dot11Elt ID=VHT Capabilities len=12 info='//xb2//xf1//x903//xfa//xff/x0c/x03//xfa//xff/x0c#' |<Dot11Elt ID=255 len=29 info='#/x03/x01/x10//xda0/x08/x040/x00//x89/x1d/x01//x80/x08/x02/x0c/x00//xfa//xff//xfa//xffy/x1c//xc7q/x1c//xc7q' |<Dot11EltVendorSpecific ID=Vendor Specific len=7 oui=00:50:f2 info='/x02/x00/x01/x00' |<Dot11EltVendorSpecific ID=Vendor Specific len=11 oui=8c:fd:f0 info='/x01/x01/x02/x01/x00/x02/x01/x01' |<Dot11EltVendorSpecific ID=Vendor Specific len=11 oui=00:00:f0 info='/x00/x01/x04/x00/x00/x00//xed' |<Dot11EltVendorSpecific ID=Vendor Specific len=40 oui=00:00:f0 info='/x02/x01/x0bvn\$/x13//xfd//xe0//xd01//x89I//xca/x05U/x17/r//xe9//xf6#//x93//xa1//x9a//xb2''/xa7//xa3//xc5M/x03//x96//xa8//xcf' |>

mismatch: predicted <Dot11Elt ID=Extendend Capabilities len=10 info='/x04/x00/x08/x00/x00/x00/x00/x00', captured field <Dot11Elt ID=Extendend Capabilities len=10 info='/x04/x00/x00/x00/x00/x00/x00' in association request

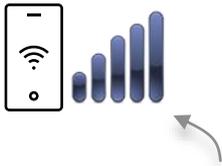
Extendend Capabilities //x08///// is BSS Transition Supported. STA predicted to say BSS Transition Supported=1 but said BSS Transition Supported=0

Using Client Knowledge for better Design



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...

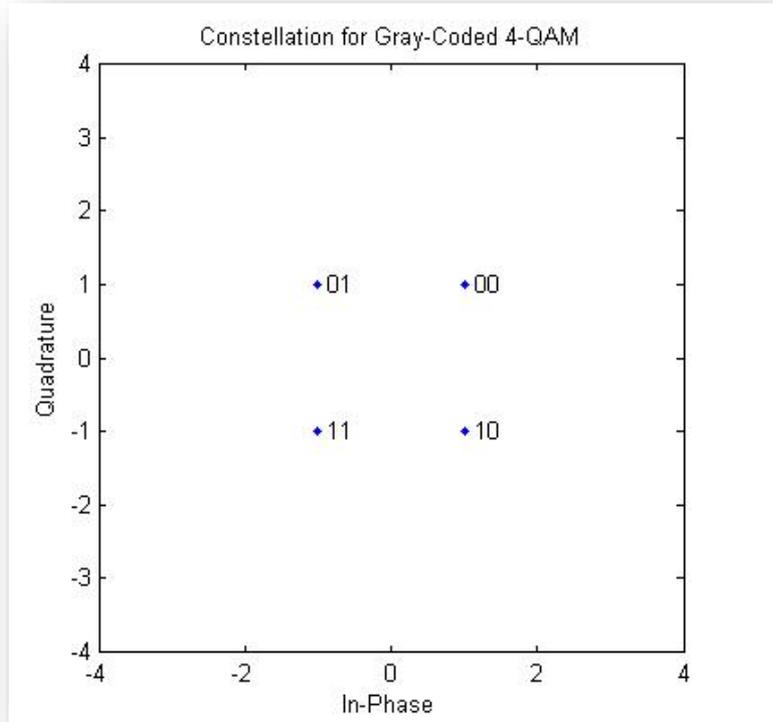


This is the AP 'signal' (at phone level)

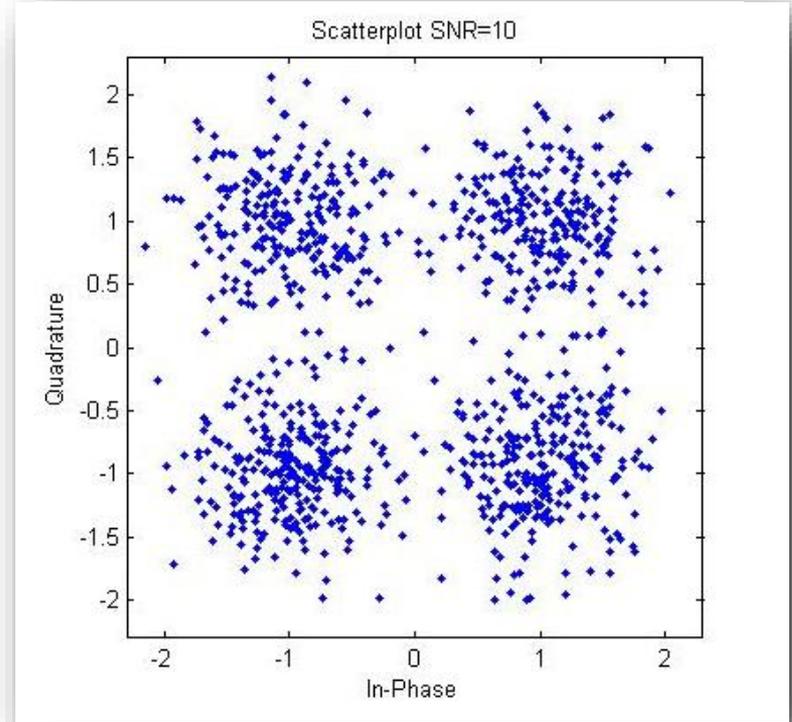


This is the phone 'signal' (at AP level)

Modulation, SNR and Data Rates



4-QAM



SNR=10

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_Oa: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_Oa:04:2e (RA)	802.11	40		-47	43	dB	12.0	Acknowledgement, Flags=.....C	
32	0.047863000	172.31.255.101	172.31.255.103	UDP	1420	34	-34	56	dB	54.0	Source port: 50857	Destination port: search-agent

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

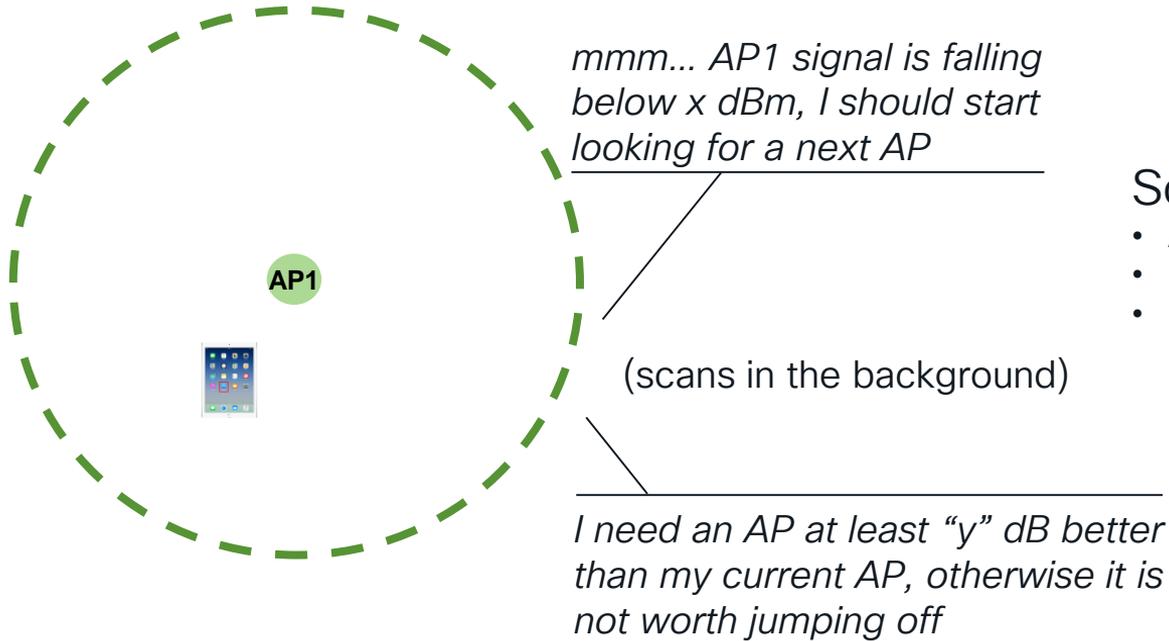


It is not Because You Decide that The Cell Should Stop There, That It Will

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’

Each Client Has Its AP Selection Logic

iPhone, iPad: **-70 dBm** -> start scanning
(device Tx/Rx data): jump if other cell is 8 dB better
(device idle): jump if other cell 12 dB better

MacOS: **-75 dBm** -> starts scanning
Jump if other cell is 12 dB better

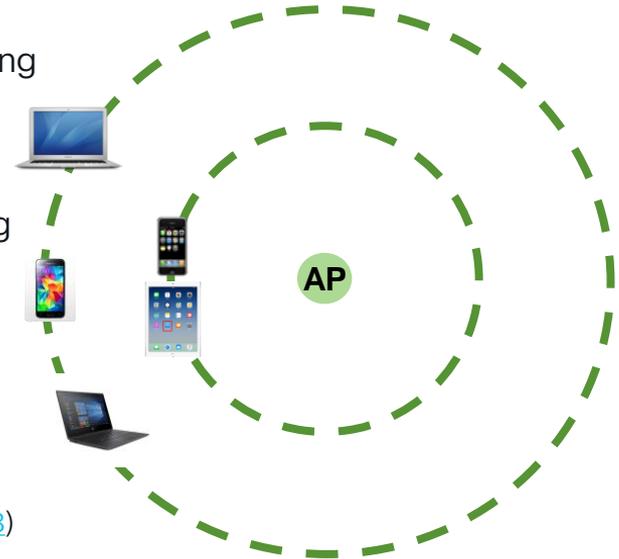
Samsung: **-75 dBm** (or {-65,75 dBm} AND CU.70%) -> starts scanning
Jump if other cell is 10 dB better

Intel: depends on the OEM (antenna type), often {-65, -75 dBm}
Depends on Roaming aggressiveness, often {5, 20 dB}

Apple IOS, iPadOS Roaming Logic (<https://support.apple.com/en-us/HT203068>)

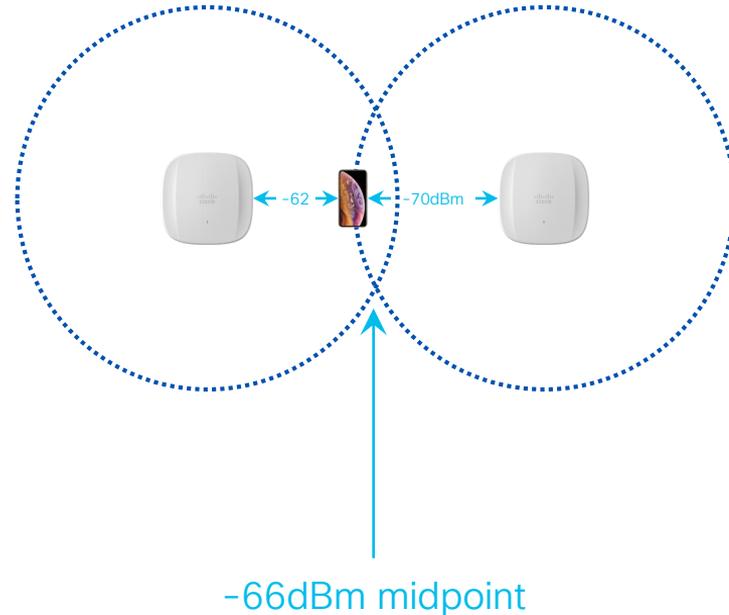
Mac OS Roaming Logic (<https://support.apple.com/en-us/HT206207>)

Samsung roaming logic (<https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-115013403768.htm>)



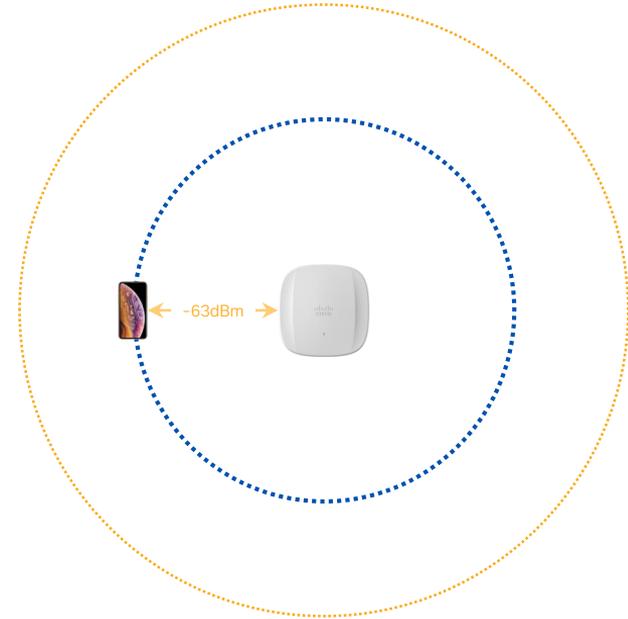
Cell Edge is Defined from the Client Perspective

- If the average client starts to look for a new AP at -70dBm , it better find one at -62dBm



Cell Edge is Defined from the Client Perspective

- If the average client starts to look for a new AP at -70dBm , it better find one at -62dBm
- Beware of 5GHz to 2.4GHz roams
 - At similar power, a 2.4GHz signal will be heard at 7dBm better than 5GHz
 - Reduce 2.4GHz transmit power to maintain similar coverage



Designing for Cell Overlap

- The 6dB Rule
 - Half the distance = +6dB
 - Twice the distance = -6dB

← Distance $d/2$ →
-60dBm



Distance $2d$
-72dBm

Radio Resource Management

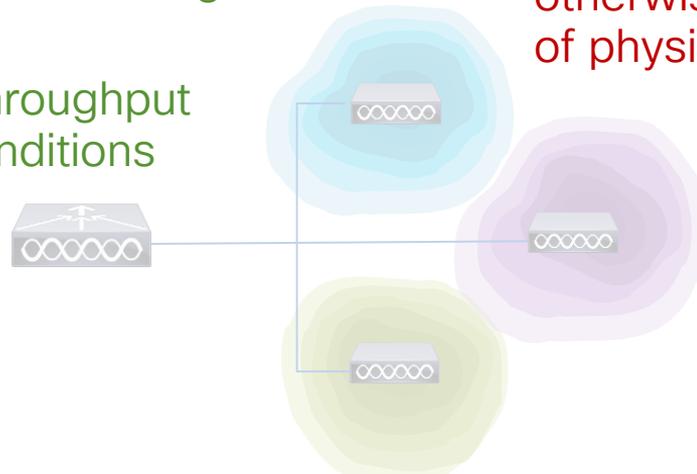
Dynamic Channel Allocation · Dynamic Bandwidth Selection · Transmit Power Control · Coverage Hole Detection

• What It Does

- Dynamically balances the RF environment and mitigates changes
- Monitor and maintain coverage for all clients
- Provides optimal throughput under changing conditions

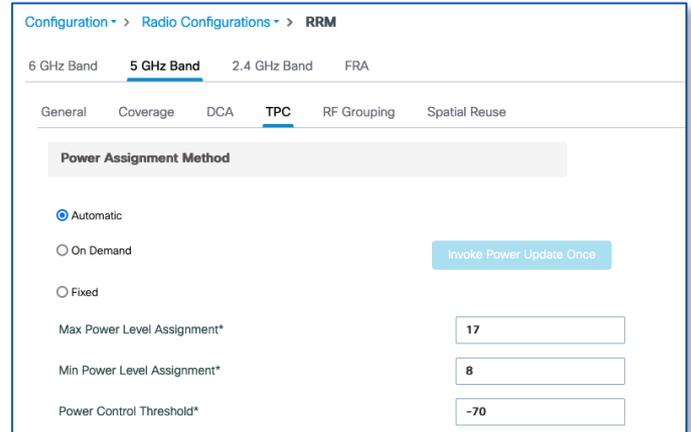
• What It Doesn't Do

- Substitute for a site survey
- Correct a poor RF design
- Manufacture spectrum or otherwise counteract the laws of physics...



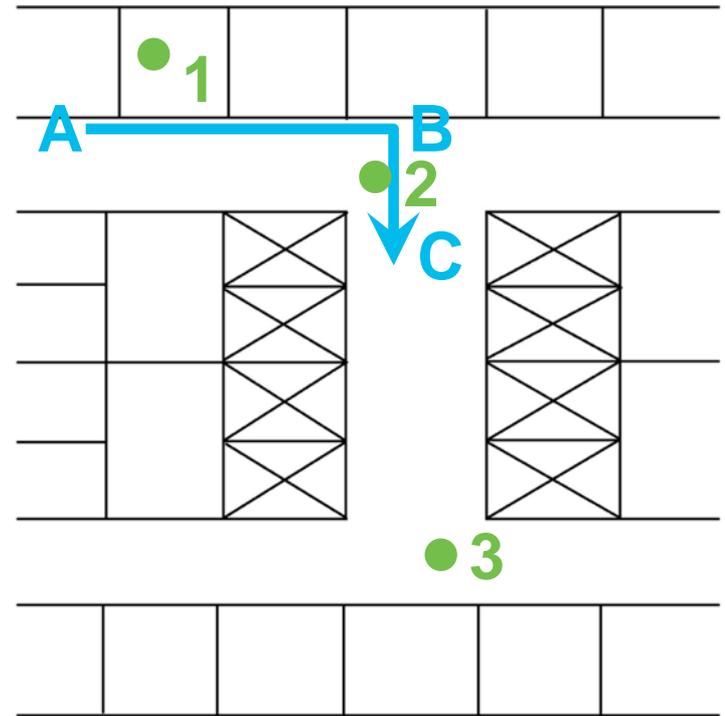
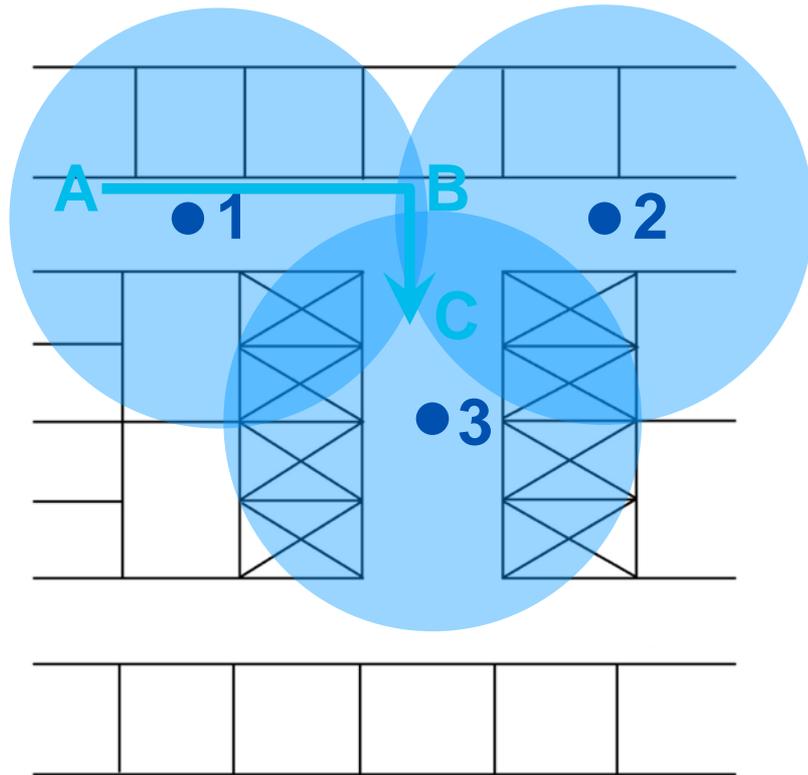
-66 dBm, but What is the AP Power?

- In short: right AP max power value is **at your worst client max power**
 - Laptops: 20-23dBm
 - Modern Phones and Tablets: 17dBm
 - Older and Cheaper Phones: 11-14dBm
- Experience shows you can allow a 3 dB margin
- For 5 GHz, assume worst clients are at 14 dBm, set your AP power to 17 dBm

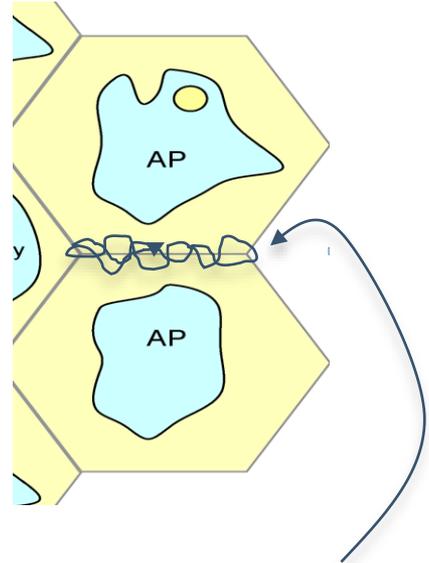
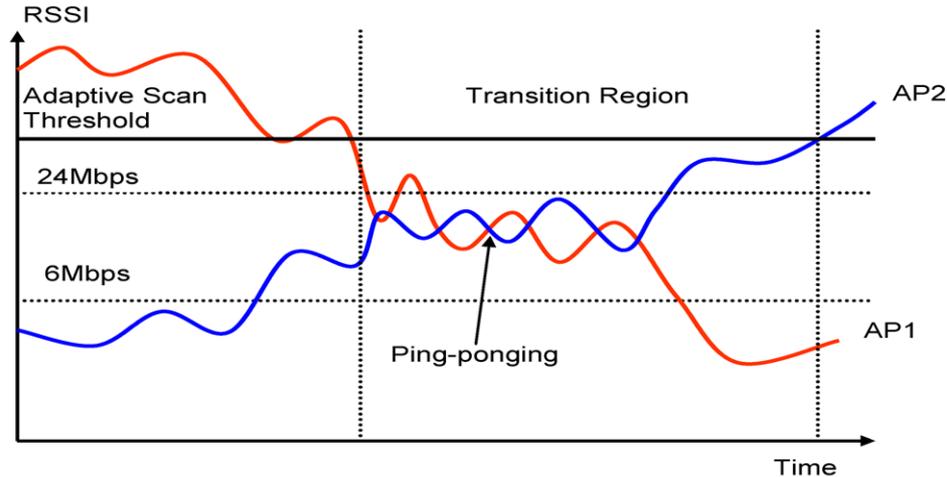


The screenshot shows the Cisco RRM configuration page for the 5 GHz Band. The 'TPC' (Transmit Power Control) tab is selected. Under the 'Power Assignment Method' section, the 'Automatic' option is selected. Below this, there are three input fields for power levels: 'Max Power Level Assignment*' is set to 17, 'Min Power Level Assignment*' is set to 8, and 'Power Control Threshold*' is set to -70. A blue button labeled 'Invoke Power Update Once' is also visible.

Use the Reports to Strategically Position Your Transition APs



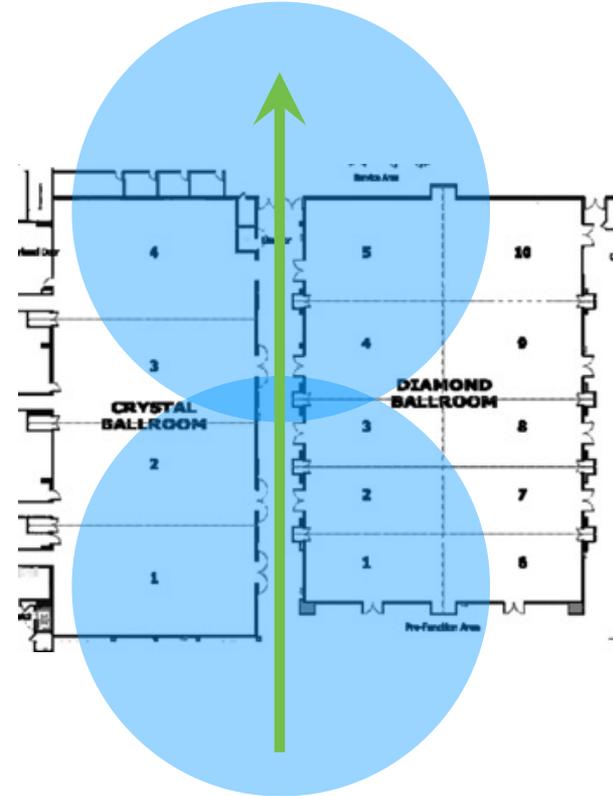
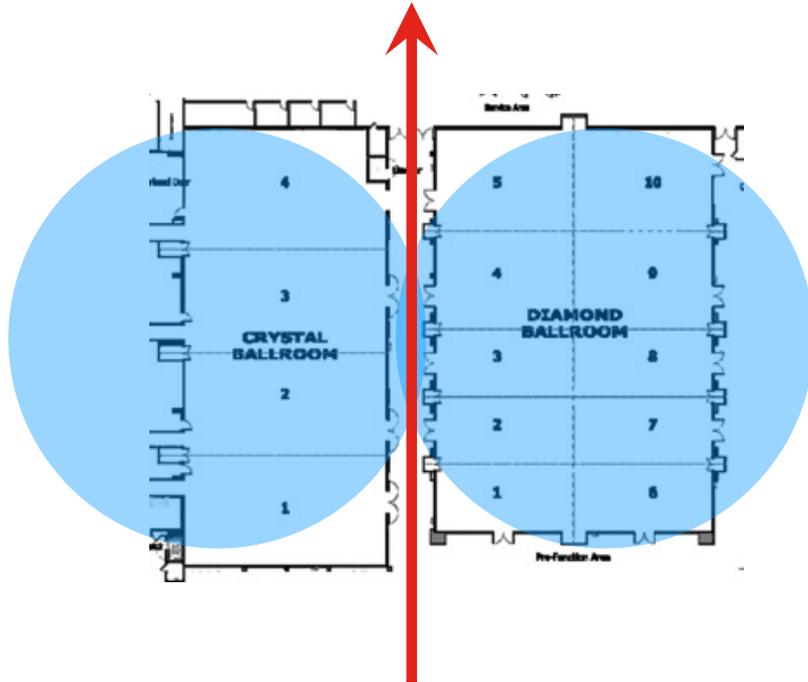
Avoid Ping Pong Zones



Client stays here

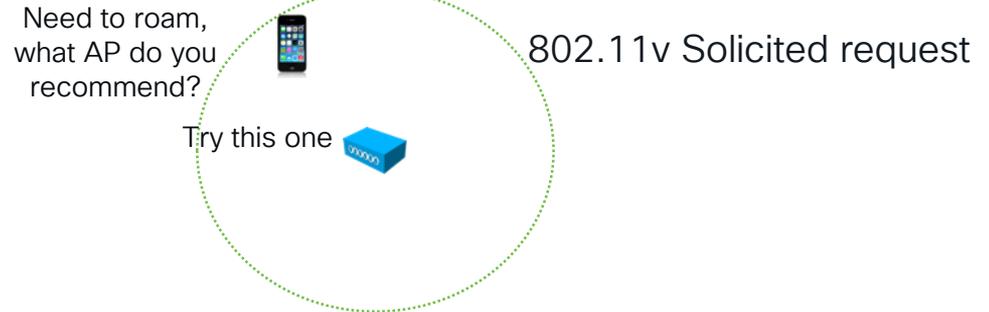
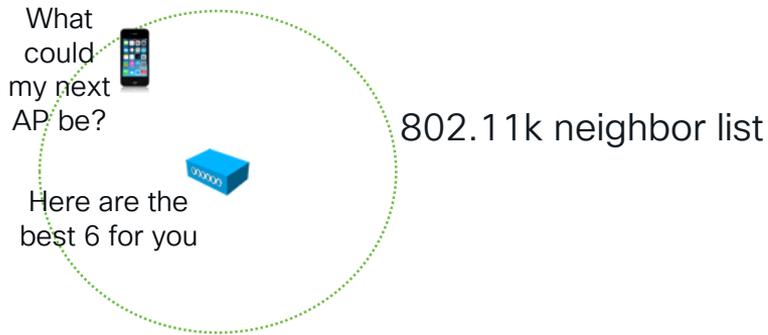
Ping-pong effect occurs when a wireless client is at the edge of two cells and hops between them.

Avoiding Ping Pong Zones



Tell your Clients About the Next (Best) Cell

- 802.11k and 802.11v BSS Transition Management



Enabling Support

- 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

The screenshot shows the 'Edit WLAN' configuration page with several sections highlighted by red boxes and annotated with blue arrows:

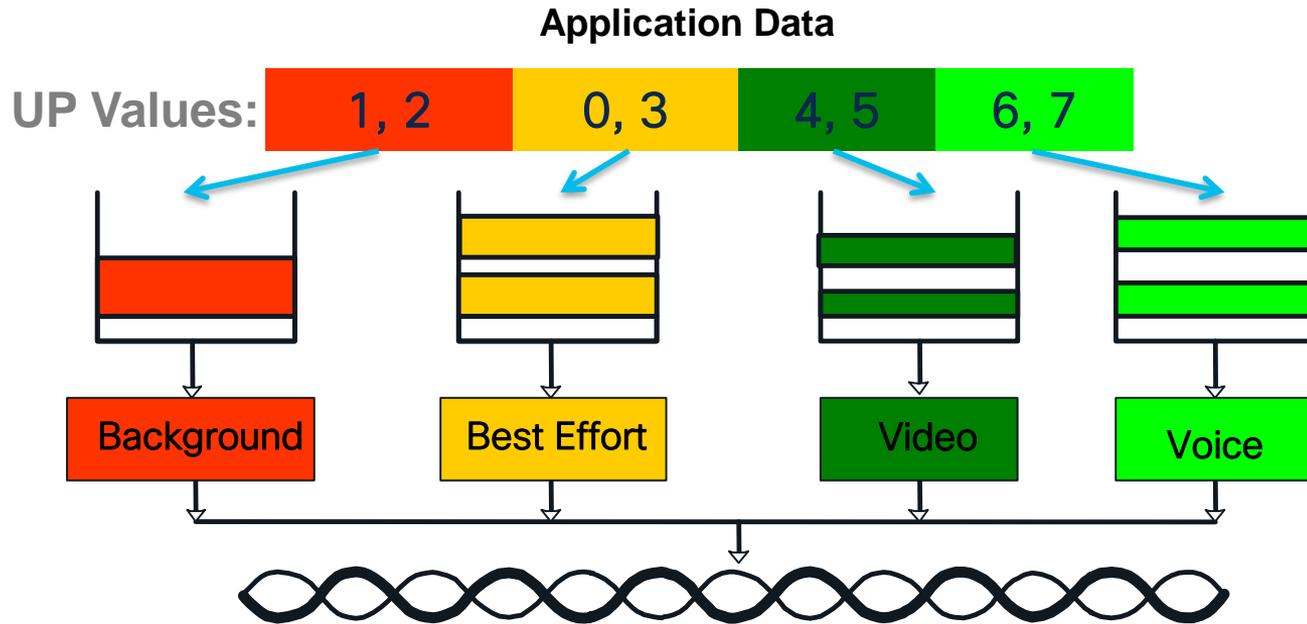
- Max Client Connections:** Per WLAN (0), Per AP Per WLAN (0), Per AP Radio Per WLAN (200).
- Assisted Roaming (11k):** Prediction Optimization (unchecked), Neighbor List (checked), Dual Band Neighbor List (unchecked).
- DTIM Period (in beacon intervals):** 5 GHz Band (1-255) (1), 2.4 GHz Band (1-255) (1).
- 11v BSS Transition Support:** BSS Transition (checked), Dual Neighbor List (unchecked), BSS Max Idle Service (checked), BSS Max Idle Protected (unchecked), Directed Multicast Service (checked). A note below states: "Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only".
- Device Analytics:** Advertise Support (checked), Advertise PC Analytics Support (checked), Share Data with Client (checked).
- 11k Beacon Radio Measurement Client Scan Report:** On Association (checked), On Roam (checked).

Annotations with blue arrows point from the following text to the corresponding settings:

- "Enables Samsung Analytics" points to "Advertise Support".
- "Enables Intel Analytics" points to "Advertise PC Analytics Support".
- "Shares with Samsung client(onboard ML optimizer)" points to "Share Data with Client".
- "Enables 11k reports (Samsung, Intel)" points to the "11k Beacon Radio Measurement Client Scan Report" section.

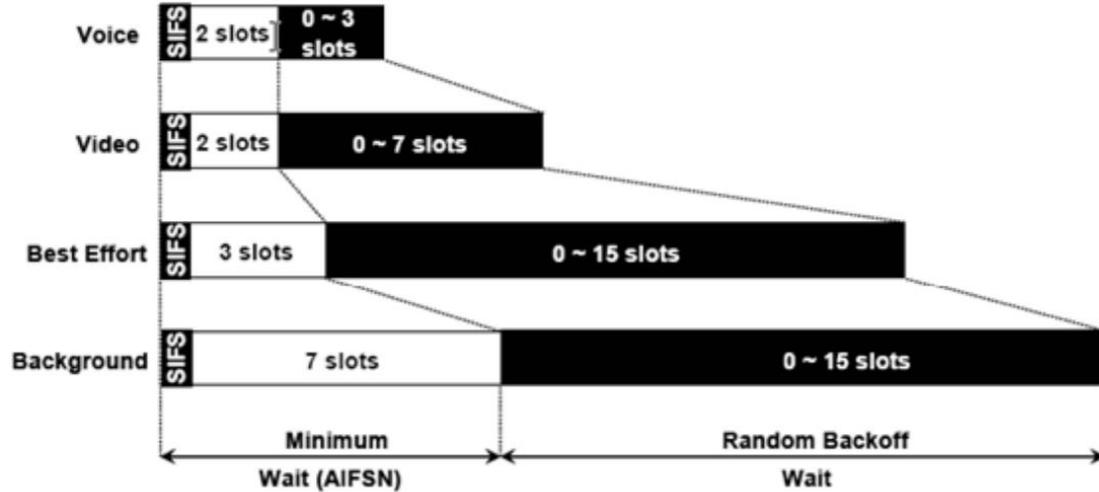
Roaming Faster Also Implies Good QoS

When wireless frames are transmitted, a 3-bit QoS value known as the **User Priority (UP)** is written into the 802.11 L2 frame

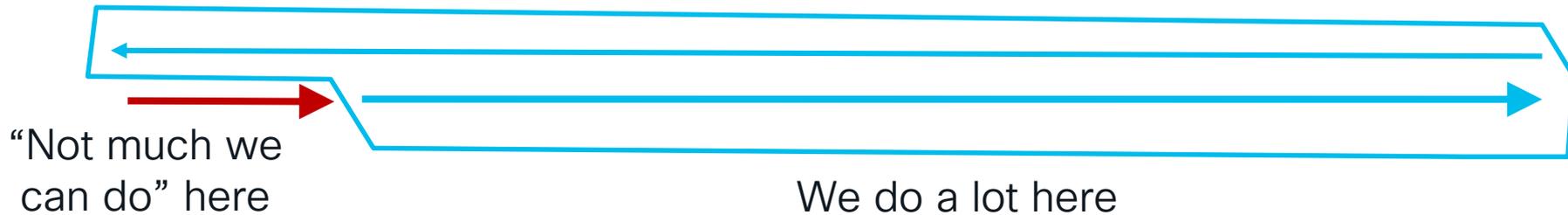
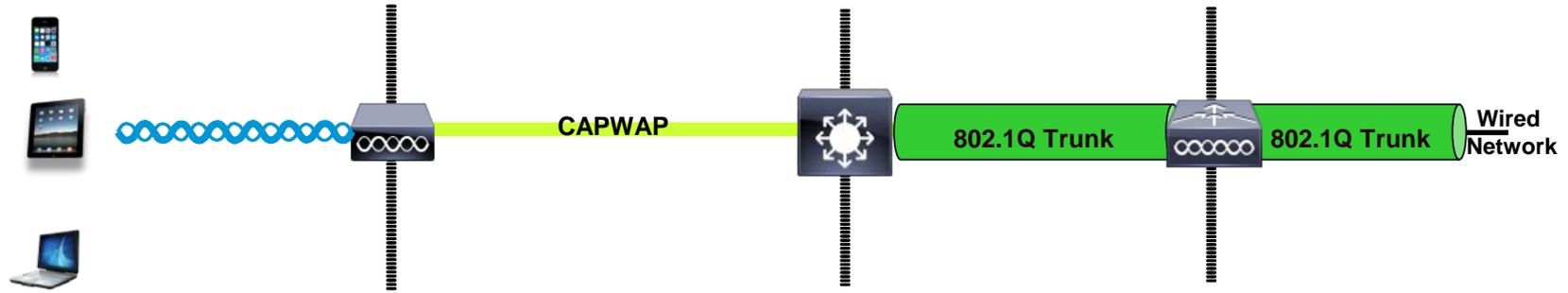


Results of the EDCA Timers

- By combining these timers, the theoretical probability of higher priority frames getting serviced first is greatly improved (but is not guaranteed in every case)
- Simply having a queue doesn't give you QoS – how you manage the queue is what matters.



Infrastructure QoS and Client QoS



L3 and L2 QoS

PROPOSED STANDARD

Internet Engineering Task Force (IETF)
Request for Comments: 8325
Category: Standards Track
ISSN: 2070-1721

T. Szigeti
J. Henry
Cisco Systems
F. Baker
February 2018

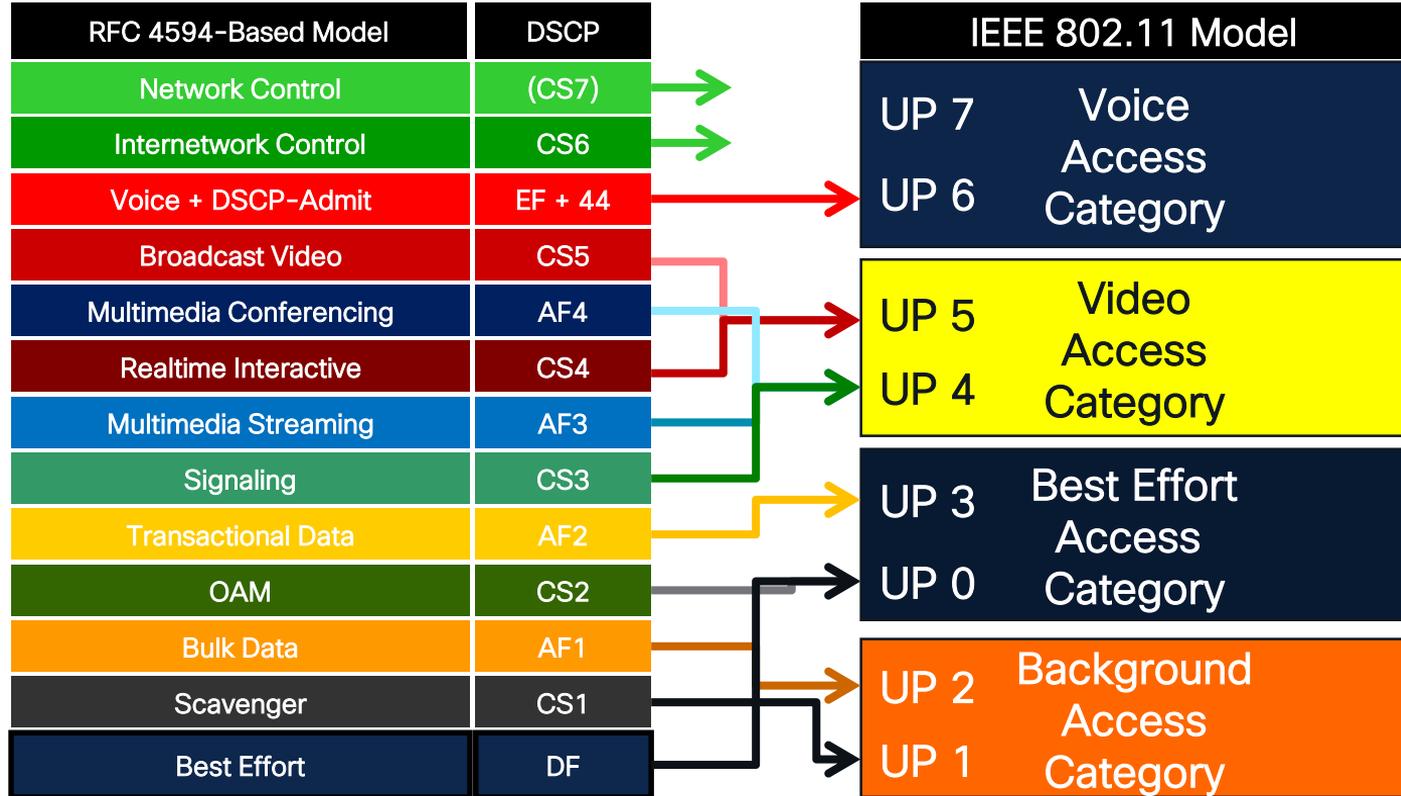
Mapping Diffserv to IEEE 802.11

Abstract

As Internet traffic is increasingly sourced from and destined to wireless endpoints, it is crucial that Quality of Service (QoS) be aligned between wired and wireless networks; however, this is not always the case by default. This document specifies a set of mappings from Differentiated Services Code Point (DSCP) to IEEE 802.11 User Priority (UP) to reconcile the marking recommendations offered by the IETF and the IEEE so as to maintain consistent QoS treatment between wired and IEEE 802.11 wireless networks.

RFC 8325

- ✓ Apple
- ✓ Samsung/Google
- ✓ Microsoft



CISCO Live!

QoS Partnerships

- **Windows:**
use Group Policies
- **Samsung:**
natively implements RC 8325
- **Other Android:**
test, they might support QoS
- **iOS:** use Fastlane

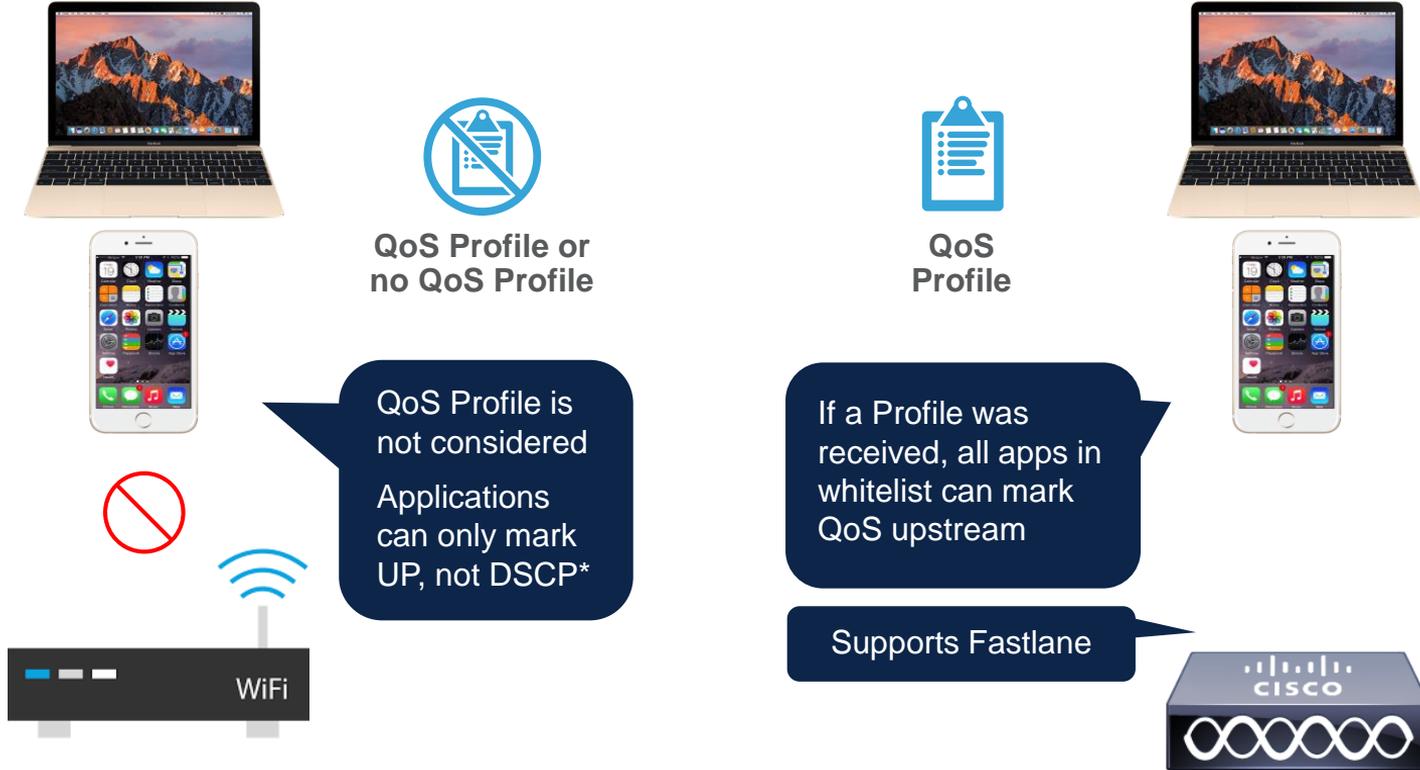
2015

Endpoint/Client	Voice (EF)	Video (AF41/42)	Control (CS3)
WMM Convention	6	4, 5	4
Audio (iOS)	5	5	0
Audio (Samsung)	5	5	0
Audio (OSX)	5	5	0
Audio (Windows 10)	5	4	3

Today

Endpoint/Client	Voice (EF)	Video (AF41/42)	Control (CS3)
WMM Convention	6	4, 5	4
Audio (iOS)	6	5	5
Audio (Samsung)	6	5	5
Audio (OSX)	6	5	5
Audio (Windows 10)	6	5	5

FastLane: Apple and Cisco



FastLane enables network administrator to prioritize applications per your environment

Supports Fast lane



Admin can provision Apple IOS device with a QoS profile*
Applications in whitelist get QoS marking**
Other applications get BE/BK

Supports Fast lane



My profile for this environment:
Minecraft = Real-time-interactive
Viber = BE

My profile for this environment:
Minecraft = BE
Viber = Voice



Supports FastLane

Supports FastLane



Fastlane – Who Does What



Application Developer

- Marks app flows appropriately



Network Administrator

- Accepts most Cisco configuration defaults
- Enables Fastlane on target SSIDs



Mobile Device Manager

- (Optional) Creates and deploy an iOS QoS profile to whitelist only mission-critical applications



End User

- (Optional) Receives the QoS profile

Cisco WLAN Network and Apple equipment recognize each other;
QOS marking is trusted end-to-end

Configure AVC to Ensure Marking Consistency

The screenshot displays the Cisco DNA Center interface for configuring AVC. The main view shows the 'Application Policy Name' configuration for 'cisco-jabber-audio'. A sidebar lists various application categories like 'authentication-services', 'backup-and-storage', and 'collaboration-apps'. A central navigation pane includes 'Dashboard', 'Monitoring', 'Configuration', 'Administration', and 'Troubleshooting'. Two 'Add QoS' dialog boxes are overlaid. The top dialog shows 'Auto QoS' disabled and a table with two entries:

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol cisco-jabber-audio,cisco-phone,ms-lync-audio	DSCP	46		Disabled	AVC	Interface
<input type="checkbox"/>	protocol cisco-jabber-video,ms-lync-video,webex-media,faceTime	DSCP	34		Disabled	AVC	Interface

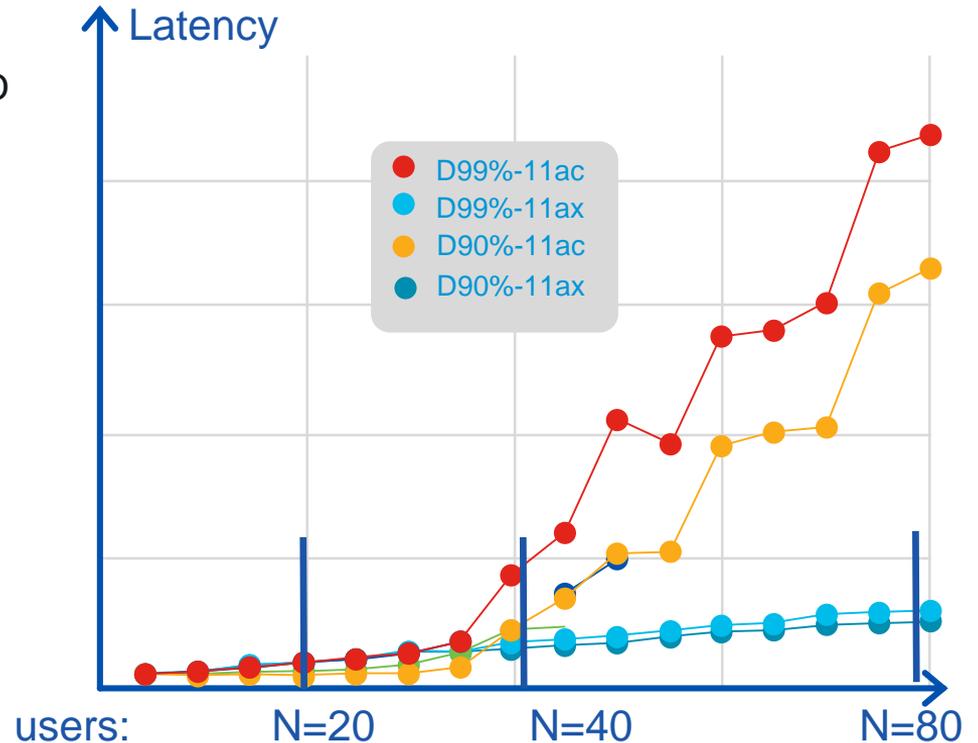
The bottom dialog shows 'Auto QoS' enabled and 'Auto Qos Macro' set to 'fastlane'. It includes a 'Police(kbps)' field with the value '8 - 10000000' and a search bar for profiles.

AVC provides traffic visibility... and ensures that marking stays consistent in both directions

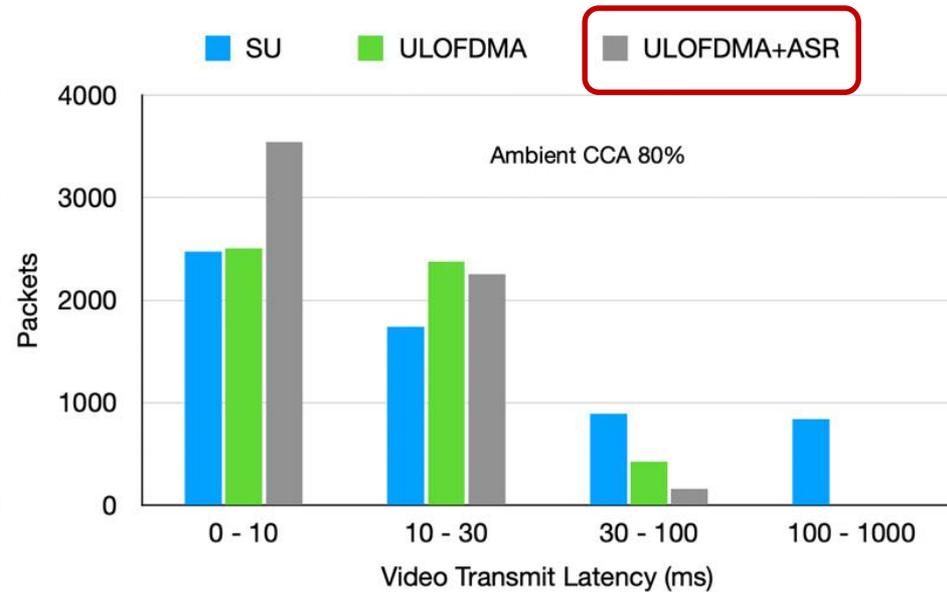
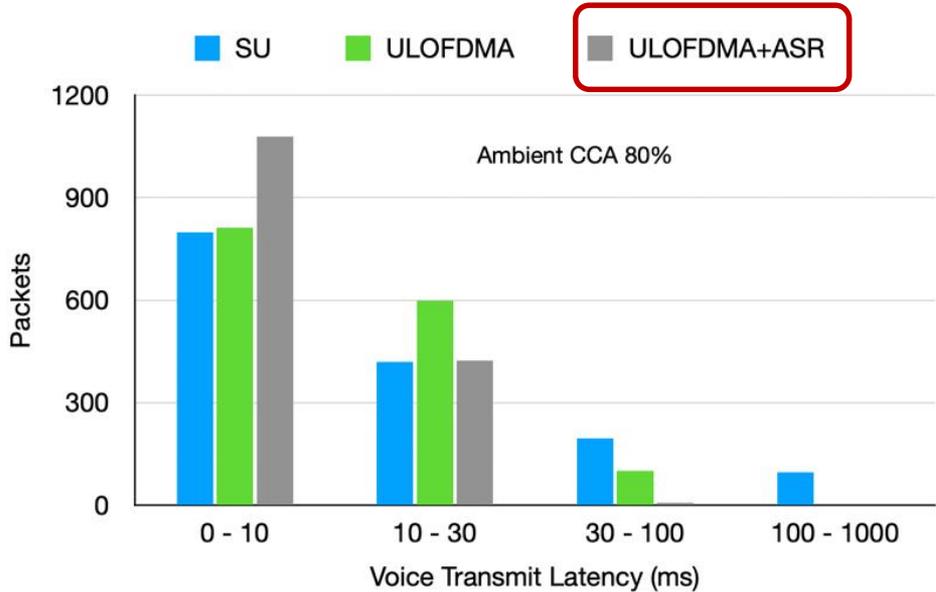


Reducing Roaming Latency Further: FastlanePlus

- FastLane is great... but we want to get rid of the profile need
- For 802.11ax, we developed FastLanePlus
 - The (11ax iOS 14 and up) client tells us in advance what traffic is going to come up
 - Uses an Advanced Service Request (ASR) frame
 - We pre-book resources, and allocate them as traffic flows

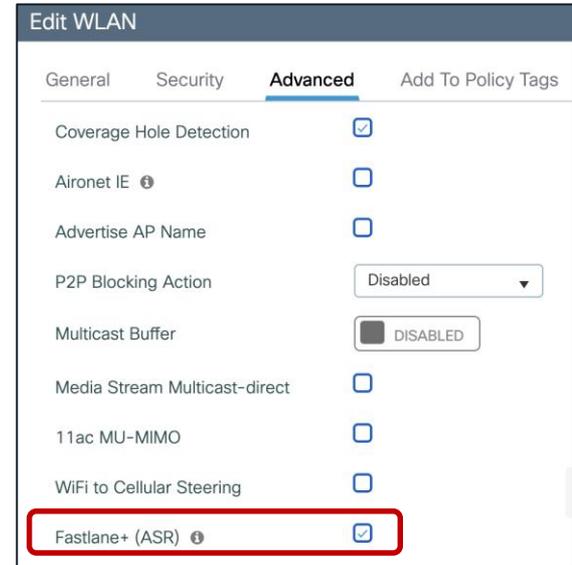


FastLanePlus (ASR) Effect on Latency



FastLane+ Configuration

- One checkbox...
- What about non-Apple clients?
 - We inserted FastLanePlus into 802.11be
 - > aka Wi-Fi 7
 - We also inserted client QoS policy (Fastlane) into Wi-Fi Alliance Optimized Connectivity Program
 - Clients get the QoS profile at association time
 - Coming to your other clients soon



Effect on Your Network Design

- Enable QoS (your clients use it!)
- Trust DSCP (CoS, 802.1p are things of the past)
- Enable FastLane Plus
- Use AVC if needed
- Only enable ACM if your real-time audio is predominantly on iOS and/or Cisco phones

Configuration > Radio Configurations > Media Parameters

6 GHz Band **5 GHz Band** 2.4 GHz Band

Voice

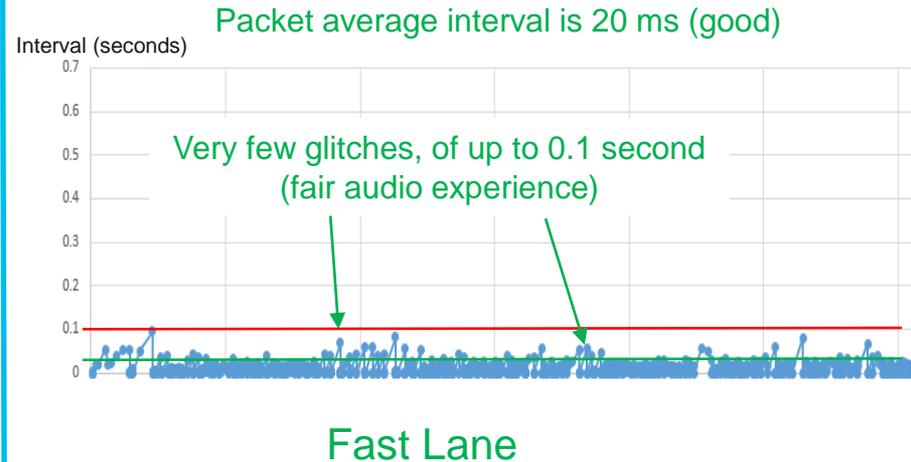
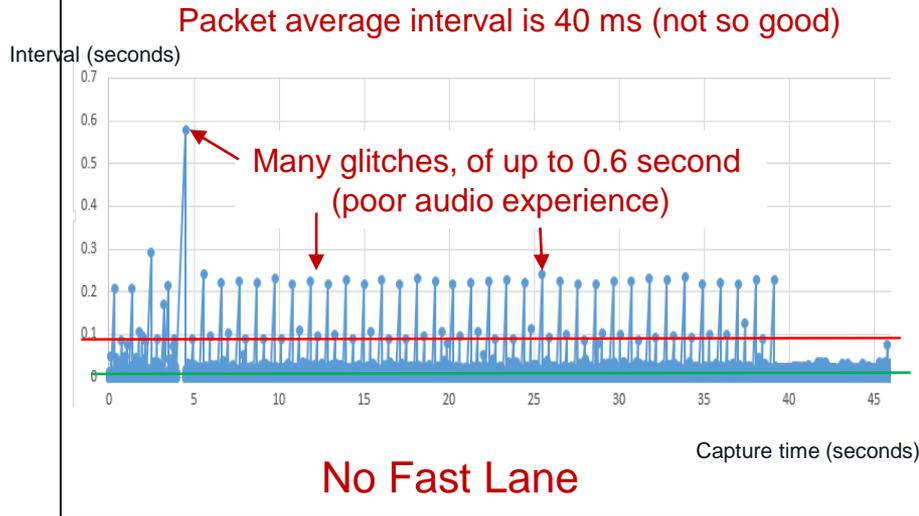
Call Admission Control (CAC)

Admission Control (ACM)



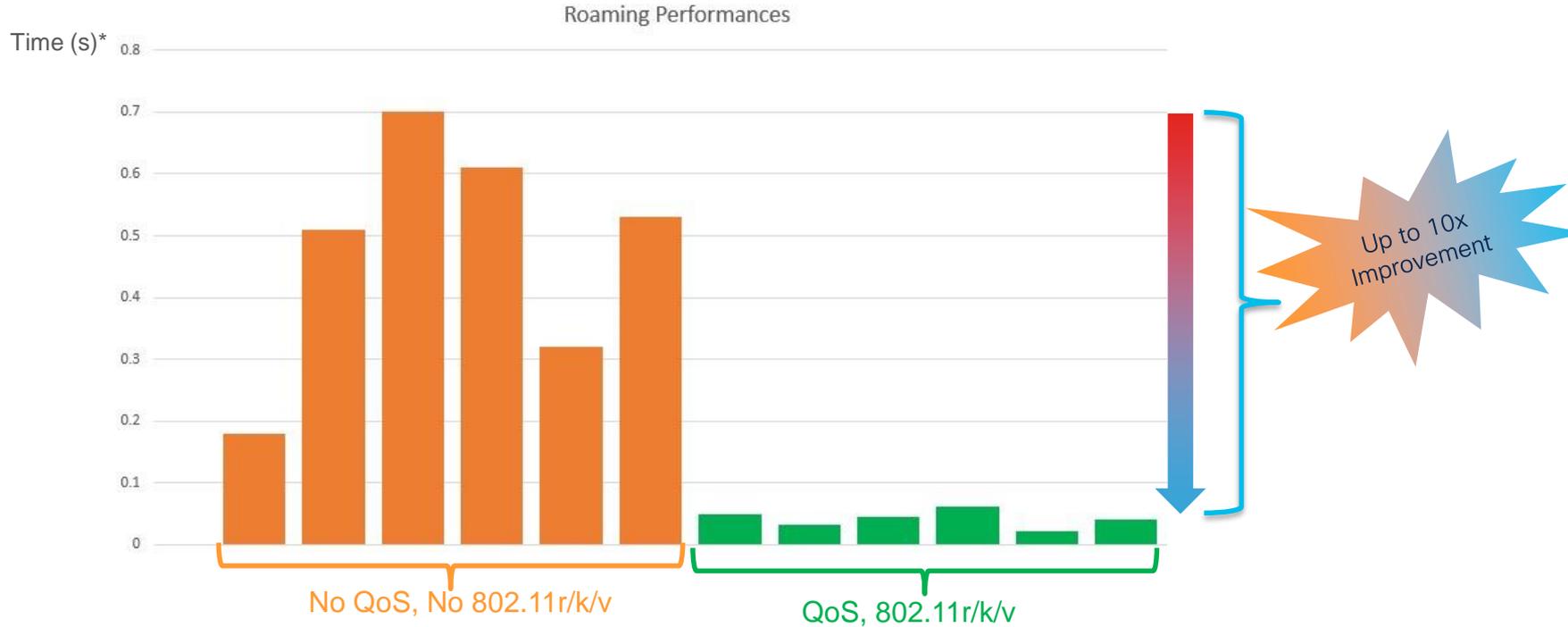
QoS Prioritization is Critical in Congested Scenarios

- In a congested environment, one voice packet is sent every 20 ms
- We measure the actual interval between voice packets in the upstream direction



Roaming Performance :

10x Better end-user Browsing and App Experience



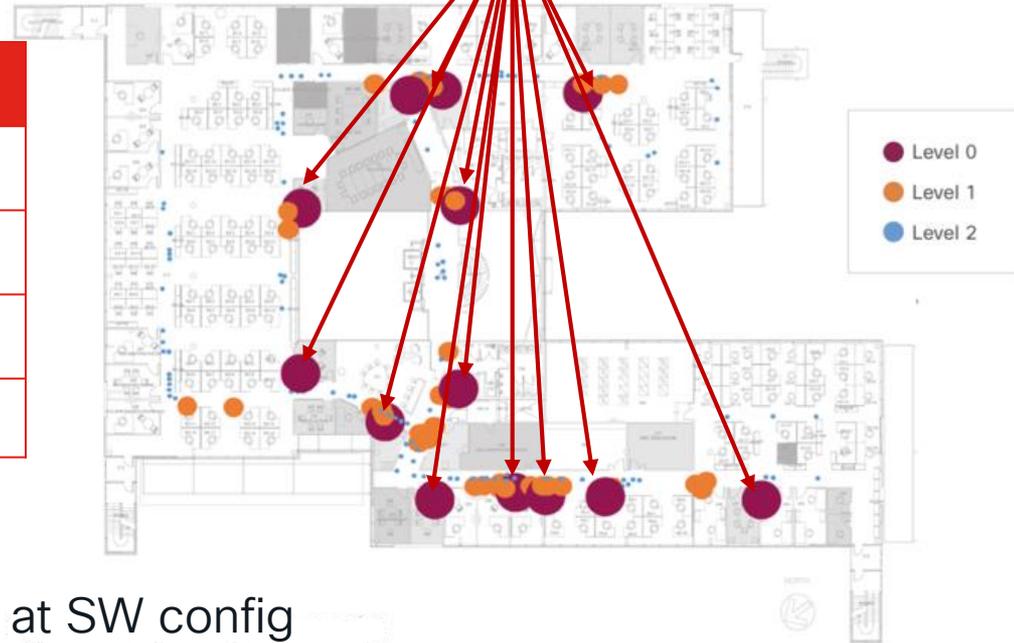
*Time Interval between last packet on previous AP, and first packet on next AP

An Example – Cisco Bedfont Lakes

Support requests – Wi-Fi issues during Video VoFi call

Roaming points

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

Before the Software Upgrade

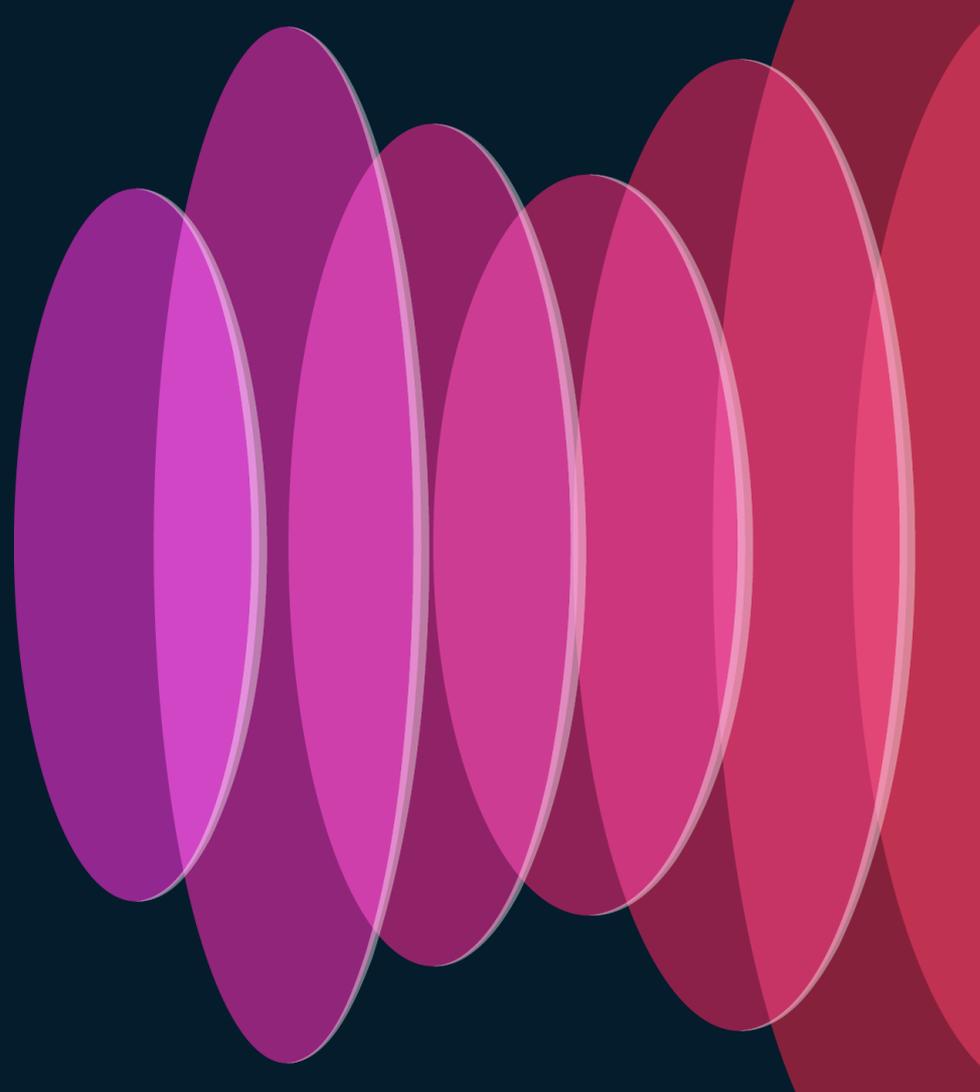


After the Software Upgrade



<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.*

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn **exclusive prizes!**



Complete your surveys in the **Cisco Live mobile app**.

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive