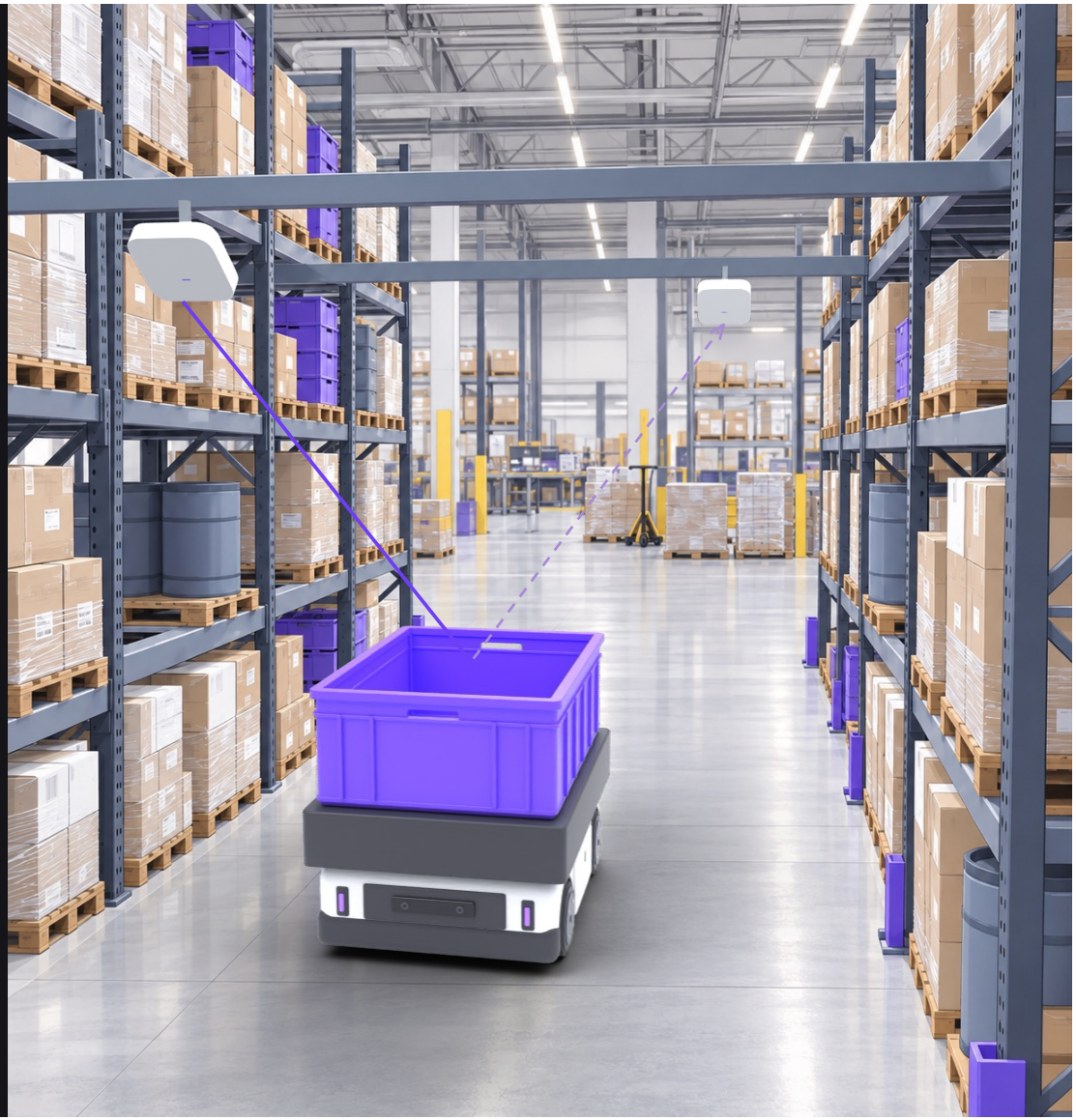
Wi-Fi Roaming in the Real World

Mika Hakala

sidos



sidos

Wi-Fi Roaming Fundamentals

Comparing cellular and Wi-Fi roaming

CELLULAR

Network Decides Roaming

Phone sends measurement reports; the network decides.

Target cell prepared before the move: resources reserved, keys derived, buffered data forwarded.

Even a hard handover: tens of ms and lossless.

WI-FI

Client Decides Roaming

Client evaluates its connection and candidate APs.

802.11k neighbor reports and 11v BTM provide hints.

Key pre-distribution only (11r); no context transfer or data forwarding. In-flight frames are lost.

The infrastructure cannot make a Wi-Fi roam happen. It can only make a good roam possible.

The cost of looking for a better AP

A single radio client leaves the serving channel to scan other channels.

Interruption duration ≈ channels visited × dwell time per channel

Client signals power-save (PM=1); the AP buffers downlink traffic while scanning.

While off-channel, the serving link cannot deliver traffic. Buffering may hide short interruptions.

What shrinks the search

802.11k

Neighbor report: tells the client which BSSIDs/channels are worth checking.

RNR

Advertises 6 GHz BSSs through 2.4/5 GHz beacons and probe responses.

6 GHz PSC

Preferred Scanning Channels reduce the in-band active scan search space.

These tools do not make roaming network-controlled; they reduce candidate-discovery cost.

Roam Triggers and Execution

sidos



What triggers a roam?

TRIGGER 1

RSSI

Falls below the client's threshold → scan → roam. Threshold crossing starts evaluation – not an automatic roam

TRIGGER 2

Link quality / retries

A strong signal can still be a bad link. Retries, loss or contention can cause roams even when RSS is strong

OTHER TRIGGERS

Policy, preference

11v BTM · Band/PHY preference
Channel/BSS load
AP deauth/disassoc · DFS event

Example client roaming thresholds:

iPhone / iPad	**≈ –70 dBm**
Mac	**≈ –75 dBm**
Zebra / Honeywell	**–65 dBm or configurable**
Older Honeywell	**–77 dBm**

Intel

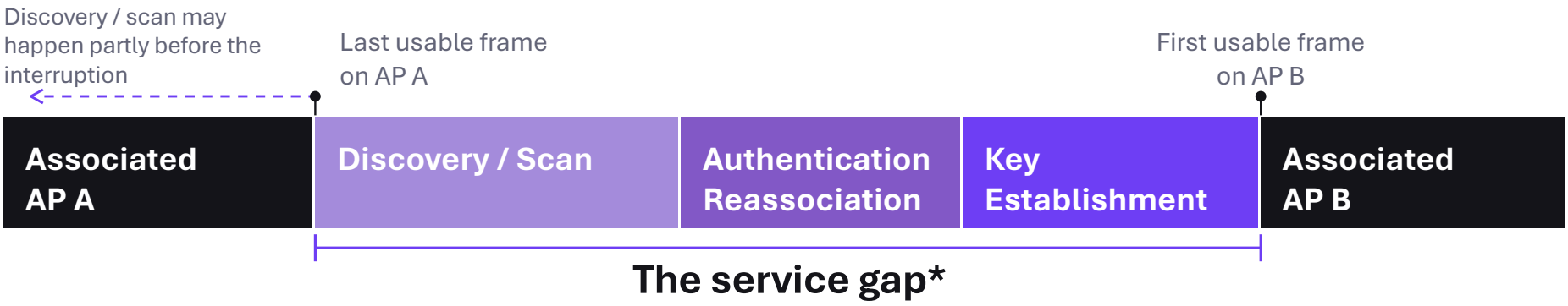
Roaming Aggressiveness controls when the adapter starts searching for another AP.

sidos

Sources: Apple Platform Deployment · Intel KB 000005546 · Zebra TechDocs · Mist WLAN Design Framework

Roaming creates a service gap

Gap: Time between the last usable data frame on AP A and the first usable data frame on AP B.



50ms VoIP target
Are we going to make it?

- WPA2-Personal (PSK) → Yes, **but** lost EAPOL 100ms - 1s+
- WPA2-Personal (802.11r FT) → **Yes**
- WPA2-Enterprise (full 802.1X) → **No**
- WPA2-Enterprise (caching / FT) → **Yes**

sidos

* Conceptual phases — may overlap or occur in a different order depending on the roaming method.

sidos

Why is it so hard to troubleshoot roaming issues?

Trifecta of challenges



Remote sites

Problems occur at remote sites. AP vendor tools can help, but they can’t see the client viewpoint.

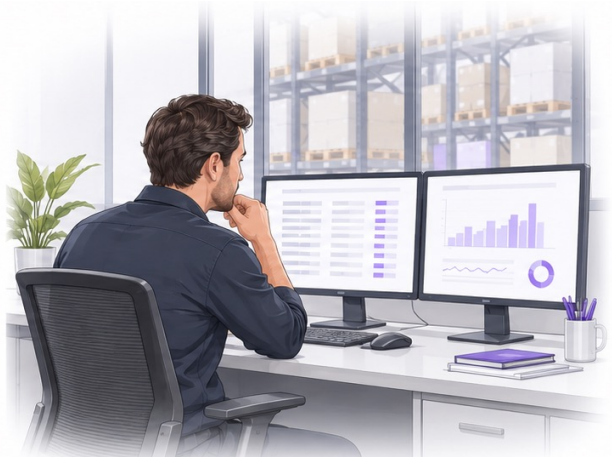


Sporadic failures

May take a long time to reoccur.

Complex capture setups.

Little visibility to client decisions.



Difficult analysis

Analyzing the captured data can be challenging.

sidos

Symptoms don’t reveal root cause

Sticky

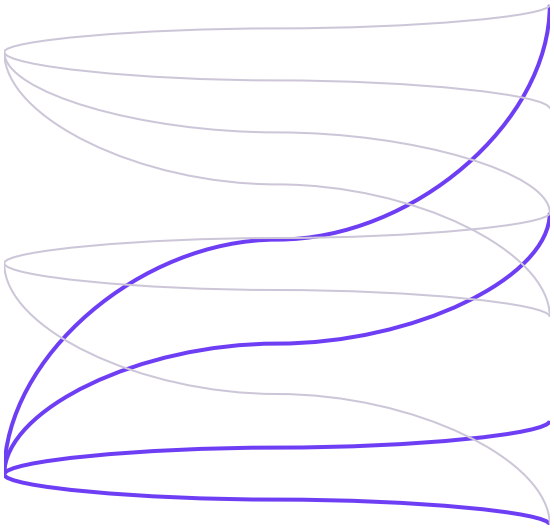
“It stays on the far AP.”

Ping-pong

“It keeps bouncing between APs.”

Drop

“Wi-Fi drops intermittently.”



Infrastructure rejected the roam

Reassoc failure · deauth/disassoc reason

Client rejected or ignored guidance

BTM response · target offered but not selected

No viable target

Candidate RSSI · channel · neighbor visibility

Client roaming decision

Roamed early · stayed too long · candidate dwell

Security transition failed or was slow

Full EAP · 4-way handshake ·EAPOL retransmissions

RF / channel event

Retry spike · beacon loss · DFS / CSA

Some resolve in one field in one frame: a rejection status or deauth reason. Most are patterns across many frames. Either way, you want the capture.

sidos

Survey, capture, move. Repeat.

Capture the serving channel and relevant candidate channels. A limited set of capture radios may not cover every candidate.

Identify nearby APs and channels, set the capture radios, infer the roam. Repeat at the next location.



Position 1
36 · 52 · 100 · 149

→



Position 2
52 · 100 · 116 · 157

→



Position 3
116 · 132 · 157 · 40

Illustrative channel sets. Availability varies by region.

If the client moves to an unmonitored channel, you are blind and must try again.

sidos

sidos

Now there is

a better way



Sidos Roaming micro-app

Following a client through the entire roaming process automatically

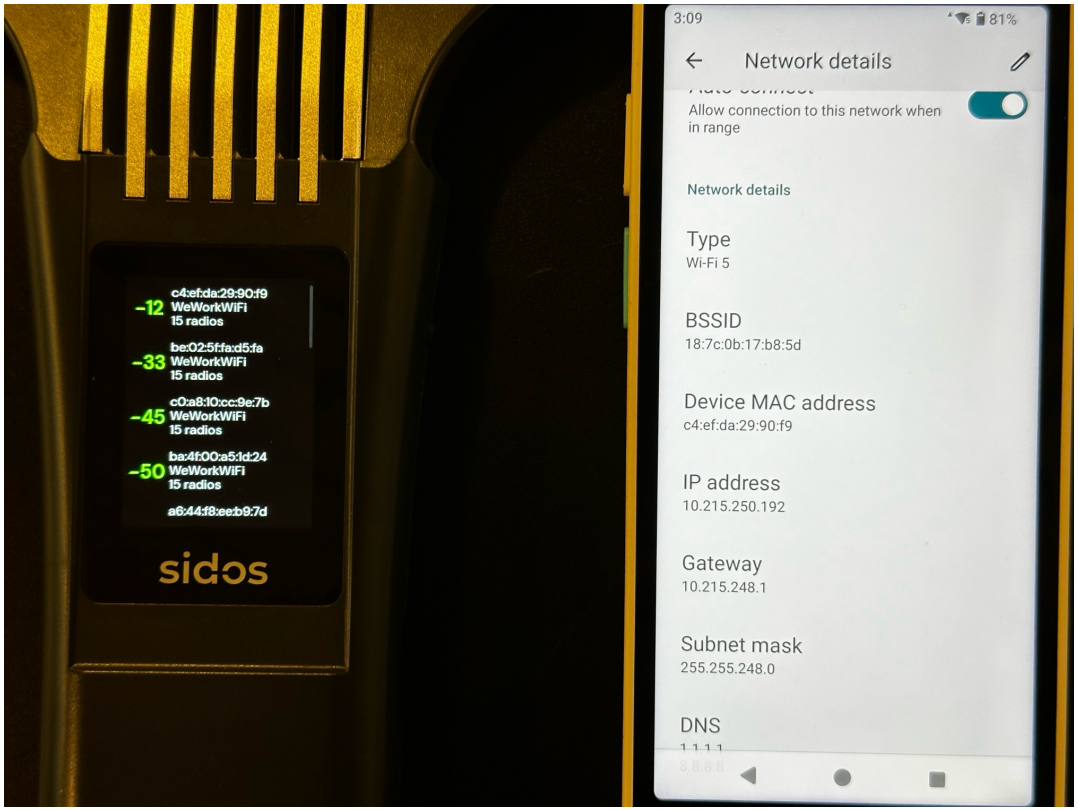


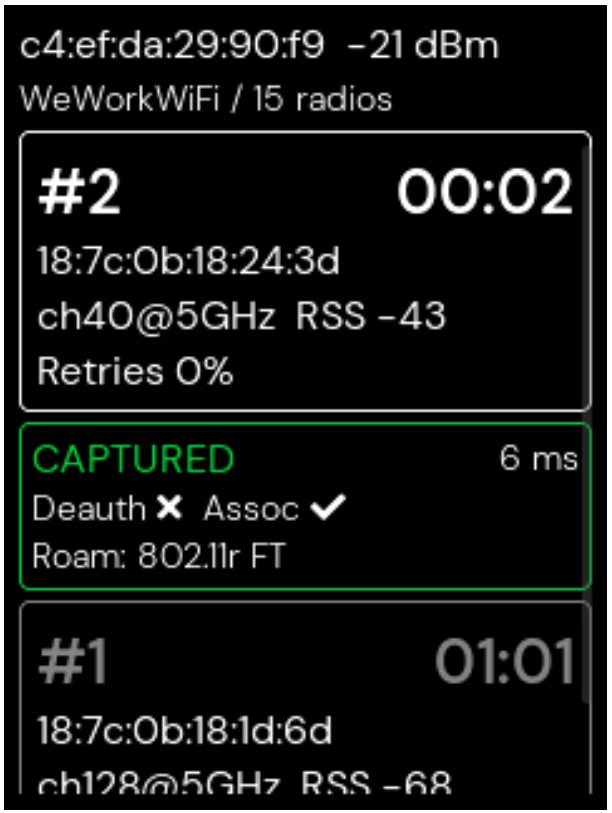
Select the client

Move with it

Analyze the data

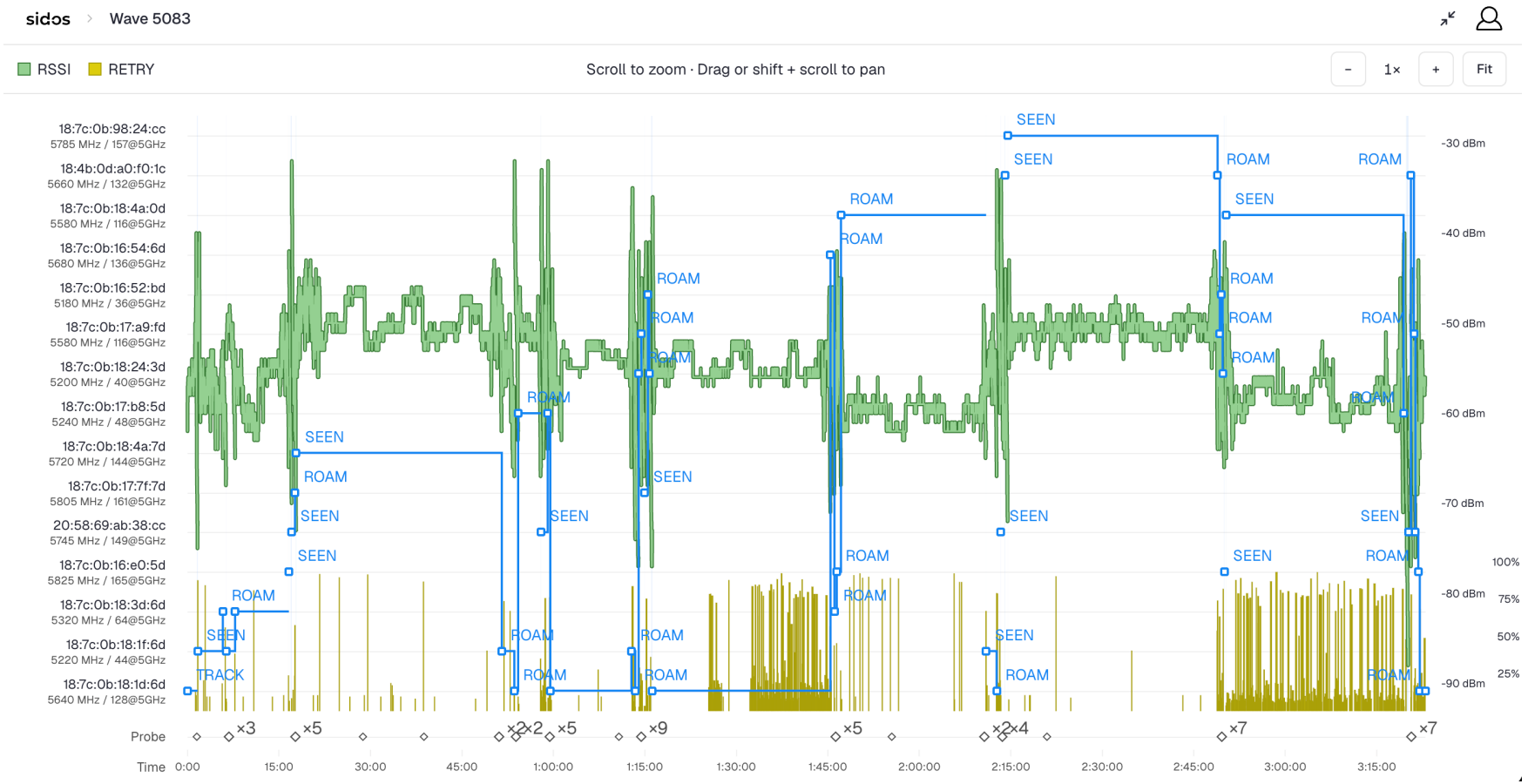
Honeywell CT37 – Meet Sidos Wave

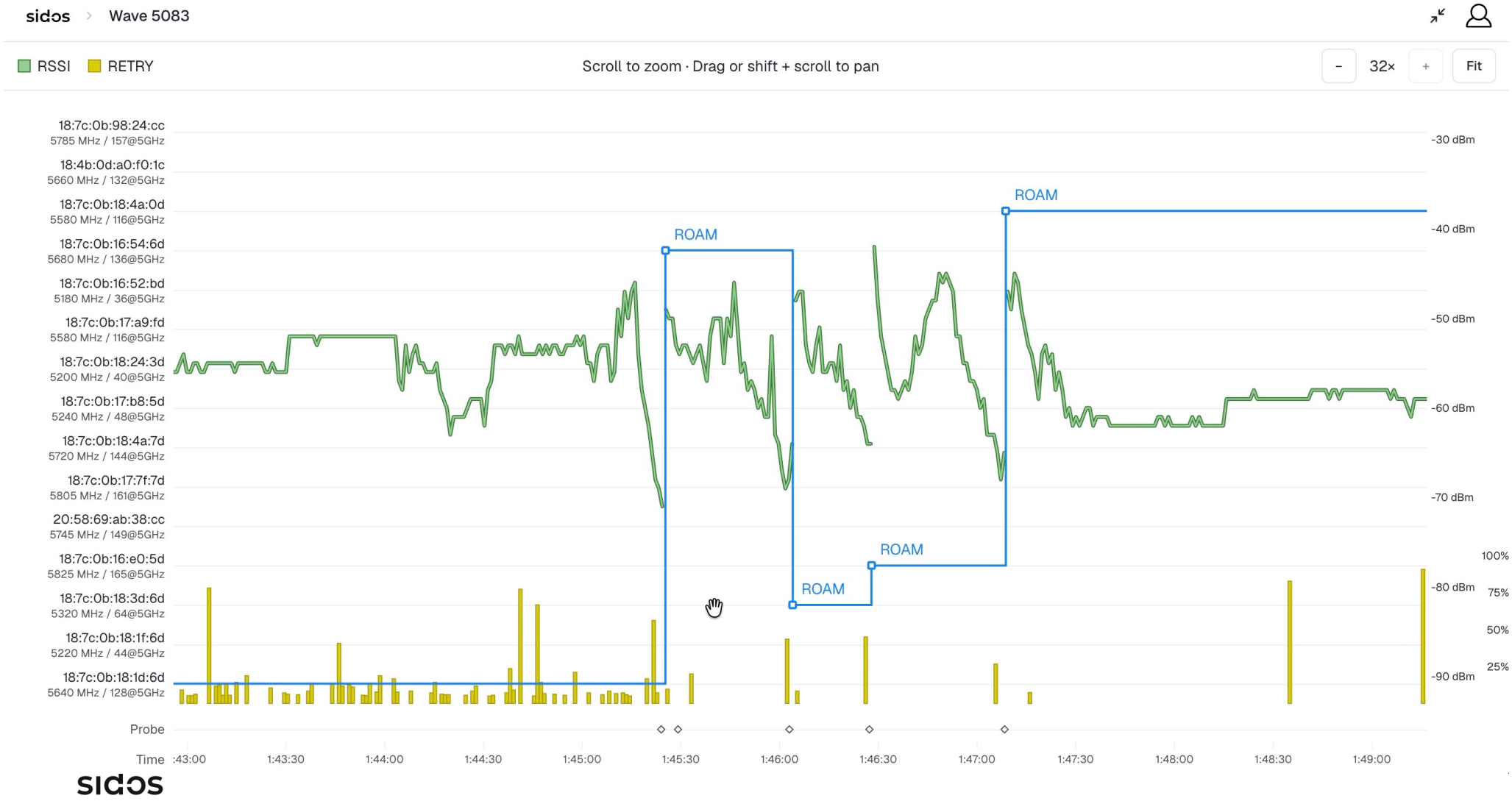


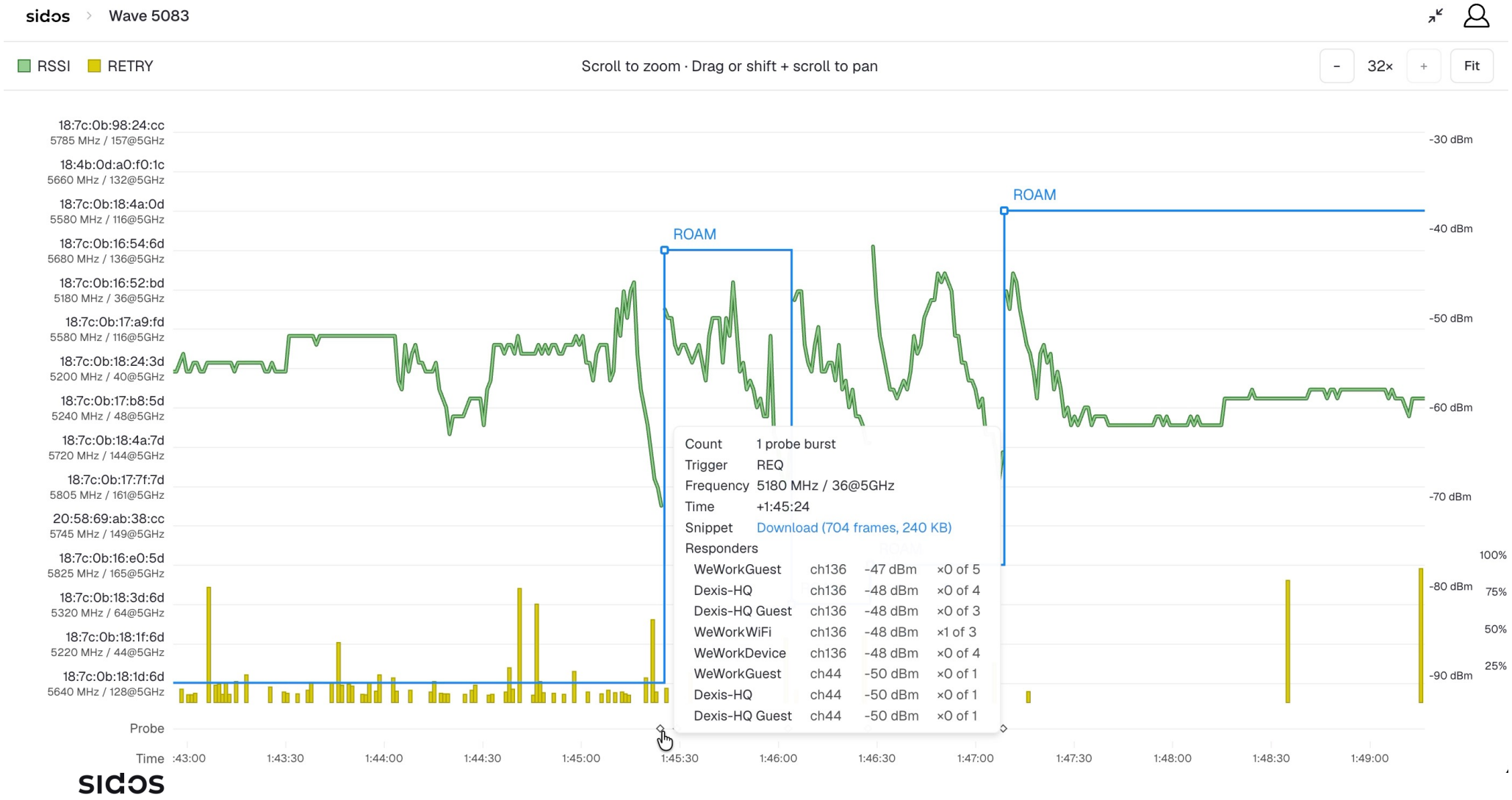


sidos

Honeywell CT37 roaming for 3 hours 20 mins




sidos
Wave 5083
RSSI
RETRY
Scroll to zoom · Drag or shift + scroll to pan
-
32×
+
Fit
18:7c:0b:98:24:cc
5785 MHz / 157@5GHz
18:4b:0d:a0:f0:1c
5660 MHz / 132@5GHz
18:7c:0b:18:4a:0d
5580 MHz / 116@5GHz
18:7c:0b:16:54:6d
5680 MHz / 136@5GHz
18:7c:0b:16:52:bd
5180 MHz / 36@5GHz
18:7c:0b:17:a9:fd
5580 MHz / 116@5GHz
18:7c:0b:18:24:3d
5200 MHz / 40@5GHz
18:7c:0b:17:b8:5d
5240 MHz / 48@5GHz
18:7c:0b:18:4a:7d
5720 MHz / 144@5GHz
18:7c:0b:17:7f:7d
5805 MHz / 161@5GHz
20:58:69:ab:38:cc
5745 MHz / 149@5GHz
18:7c:0b:16:e0:5d
5825 MHz / 165@5GHz
18:7c:0b:18:3d:6d
5320 MHz / 64@5GHz
18:7c:0b:18:1f:6d
5220 MHz / 44@5GHz
18:7c:0b:18:1d:6d
5640 MHz / 128@5GHz
ROAM
ROAM
ROAM
ROAM
-30 dBm
-40 dBm
-50 dBm
-60 dBm
-70 dBm
-80 dBm
-90 dBm
100%
75%
50%
25%
Probe
Time
:43:00
1:43:30
1:44:00
1:44:30
1:45:00
1:45:30
1:46:00
1:46:30
1:47:00
1:47:30
1:48:00
1:48:30
1:49:00
sidos


sidos
Wave 5083
RSSI
RETRY
Scroll to zoom · Drag or shift + scroll to pan
-
32×
+
Fit
18:7c:0b:98:24:cc
5785 MHz / 157@5GHz
18:4b:0d:a0:f0:1c
5660 MHz / 132@5GHz
18:7c:0b:18:4a:0d
5580 MHz / 116@5GHz
18:7c:0b:16:54:6d
5680 MHz / 136@5GHz
18:7c:0b:16:52:bd
5180 MHz / 36@5GHz
18:7c:0b:17:a9:fd
5580 MHz / 116@5GHz
18:7c:0b:18:24:3d
5200 MHz / 40@5GHz
18:7c:0b:17:b8:5d
5240 MHz / 48@5GHz
18:7c:0b:18:4a:7d
5720 MHz / 144@5GHz
18:7c:0b:17:7f:7d
5805 MHz / 161@5GHz
20:58:69:ab:38:cc
5745 MHz / 149@5GHz
18:7c:0b:16:e0:5d
5825 MHz / 165@5GHz
18:7c:0b:18:3d:6d
5320 MHz / 64@5GHz
18:7c:0b:18:1f:6d
5220 MHz / 44@5GHz
18:7c:0b:18:1d:6d
5640 MHz / 128@5GHz
Probe
Time
ROAM
ROAM
-30 dBm
-40 dBm
-50 dBm
-60 dBm
-70 dBm
-80 dBm
-90 dBm
100%
75%
50%
25%
:43:00
1:43:30
1:44:00
1:44:30
1:45:00
1:45:30
1:46:00
1:46:30
1:47:00
1:47:30
1:48:00
1:48:30
1:49:00
Count 1 probe burst
Trigger REQ
Frequency 5180 MHz / 36@5GHz
Time +1:45:24
Snippet Download (704 frames, 240 KB)
Responders
WeWorkGuest ch136 -47 dBm ×0 of 5
Dexis-HQ ch136 -48 dBm ×0 of 4
Dexis-HQ Guest ch136 -48 dBm ×0 of 3
WeWorkWiFi ch136 -48 dBm ×1 of 3
WeWorkDevice ch136 -48 dBm ×0 of 4
WeWorkGuest ch44 -50 dBm ×0 of 1
Dexis-HQ ch44 -50 dBm ×0 of 1
Dexis-HQ Guest ch44 -50 dBm ×0 of 1
sidos


sidos
Wave 5083
RSSI
RETRY
Scroll to zoom · Drag or shift + scroll to pan
-
32×
+
Fit
18:7c:0b:98:24:cc
5785 MHz / 157@5GHz
18:4b:0d:a0:f0:1c
5660 MHz / 132@5GHz
18:7c:0b:18:4a:0d
5580 MHz / 116@5GHz
18:7c:0b:16:54:6d
5680 MHz / 136@5GHz
18:7c:0b:16:52:bd
5180 MHz / 36@5GHz
18:7c:0b:17:a9:fd
5580 MHz / 116@5GHz
18:7c:0b:18:24:3d
5200 MHz / 40@5GHz
18:7c:0b:17:b8:5d
5240 MHz / 48@5GHz
18:7c:0b:18:4a:7d
5720 MHz / 144@5GHz
18:7c:0b:17:7f:7d
5805 MHz / 161@5GHz
20:58:69:ab:38:cc
5745 MHz / 149@5GHz
18:7c:0b:16:e0:5d
5825 MHz / 165@5GHz
18:7c:0b:18:3d:6d
5320 MHz / 64@5GHz
18:7c:0b:18:1f:6d
5220 MHz / 44@5GHz
18:7c:0b:18:1d:6d
5640 MHz / 128@5GHz
Probe
Time
:43:00
1:43:30
1:44:00
1:44:30
1:45:00
1:45:30
1:46:00
1:46:30
1:47:00
1:47:30
1:48:00
1:48:30
1:49:00
-30 dBm
-40 dBm
-50 dBm
-60 dBm
-70 dBm
-80 dBm
-90 dBm
100%
75%
50%
25%
ROAM
ROAM
ROAM
ROAM
Type ROAM
Current 18:7c:0b:16:54:6d
Previous 18:7c:0b:18:1d:6d
RSSI -49 dBm
Frequency 5680 MHz / 136@5GHz
Time +1:45:25
Snippet Download (704 frames, 240 KB)
sidos

Client Profiling by

No client roaming data from vendor? This is better - it's the roaming profile in *your* network

Metric	n	Mean	Std_dev
Old AP RSS at roam (dBm)	40	-64.9	5.4
Serving AP RSS at scan start (dBm)	33	-61.1	5.8
Scan-to-roam lead time (s)	33	3.7	5.3
New AP RSS after roam (dBm)	40	-52.2	6.3
Gain new-old (dB)	40	12.7	7.4

The client's logic reads as: **begin scanning around −61 dBm, commit around −65 dBm, needing a candidate ~12–15 dB better.**
This is client logic, not AP-side steering — confirmed by zero BTM requests, deauths or disassocs in any snippet. All captured roams are FT over-the-air (auth alg 2, MDIE/FTIE, AKM 3, no 4-way)

Default: Roaming RSSI Threshold = −65 dBm, Roaming RSSI Difference = 10 dB (Honeywell KB 000075100, covering CT4x/CT6x/CN80/EDA5x etc. on Android 8–14).

sidos

sidos

Do Different Clients Roam Differently?



Tracking iPhone 14, CT37 and MacBook M3




0:00.00
start
APs
AP-mainfloor-7
AP-mainfloor-6
AP-mainfloor-3
AP-mainfloor-4
AP-mainfloor-5
AP-mainfloor-2
AP-mainfloor-1
AP-mainfloor-8
AP-mainfloor-11
AP-mainfloor-9
AP-mainfloor-10
Y (m)
X (m)
14 roams total
Next ▶

Summary

- Roaming is client driven. Know your clients and make good roaming possible.
- Issues happen in the field. Get more data, ideally packet captures and L1 measurements.
- Failures are sporadic; symptoms don’t reveal root cause. Collecting the data can consume significant time → pure overhead.
- Analysis can be difficult, but that’s where the answers lie. AI can help when provided with enough of high-quality data.

sidos

Thank You!