

AI Wireless Operation

CISCO Live !

When AI meets Cisco Meraki Wireless

Minse Kim
Product Manager, [@linkedin.com/in/minse-k](https://www.linkedin.com/in/minse-k)

Cisco Webex App

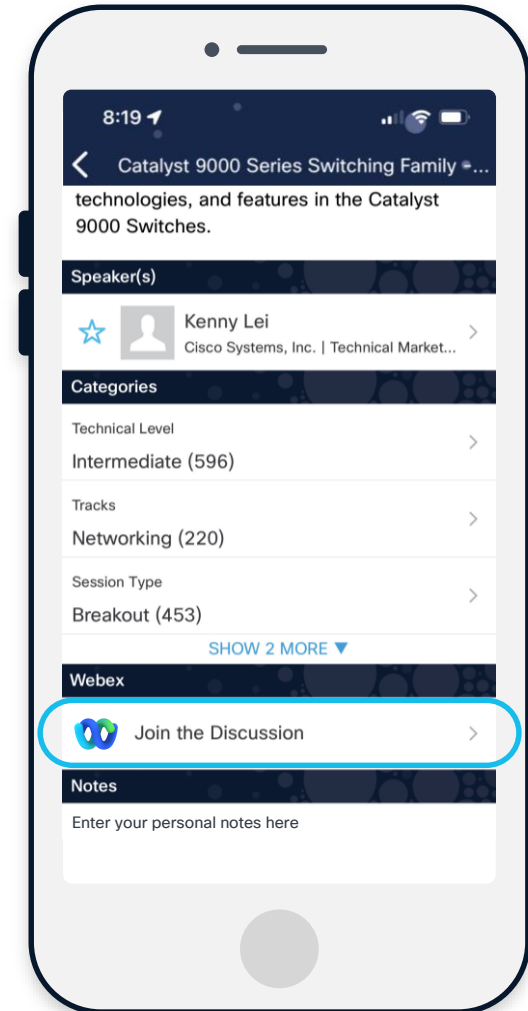
Questions?

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 13, 2025.



Agenda

- 01 Meraki Assurance Overview
- 02 Client Assurance
- 03 Wireless Device Assurance
- 04 RF Optimization
- 05 AP Refresh/Deployment
- 06 Cisco AI Assistant
- 07 Conclusion

Welcome Back to San Diego!

We've come a long way...



BRKEWN-2034



Cisco DNA Wireless Assurance

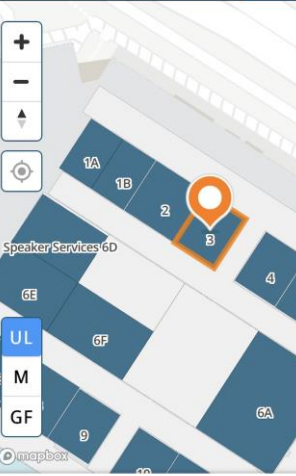
Isolate problems for faster troubleshooting

Min Se Kim, TME

Search 5G E 11:59 AM 59%

Location

Search



San Diego Convention Center, Floor

SHARE

Search LTE 6:55 AM 95%

Cisco DNA Assurance: Isolate wireless network problems for faster troubleshooting using AI and Machine learning

BRKEWN-2034 | SDCC - Upper Level, Room 3

INTERESTED IN THIS SESSION?

Remove Favorite

REGISTER FOR THIS SESSION

Mon 10 Jun, 04:00 PM - 05:30 PM

SDCC - Upper Level, Room 3

MAP

View Location

SPEAKER(S)

Min Se Kim

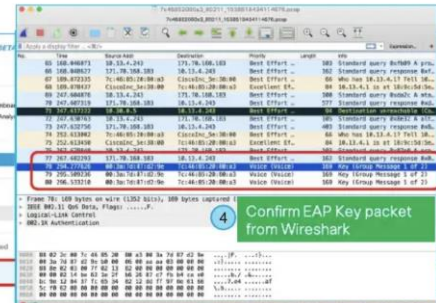




Intelligent Capture ~ Key Use-Cases

- VIP Assurance
- RF Scanner
- Automated PCAP*
- On-Demand PCAP (of Onboarding Frames)

From Network into Client Wi-Fi Onboarding failure



4 Confirm EAP Key packet from Wireshark



3 Download Onboard Packet

Meraki Assurance Overview

Four Stage of Assurance



Baseline and Detect

Monitor end-to-end digital experience from critical vantage points



Localize and Diagnose

Visualize, localize, and diagnose across every network segment



Mitigate and Remediate

Closed-loop actions across digital domains and teams



Predict and Optimize

Forecast disruptions, optimize path, and plan connectivity and migrations

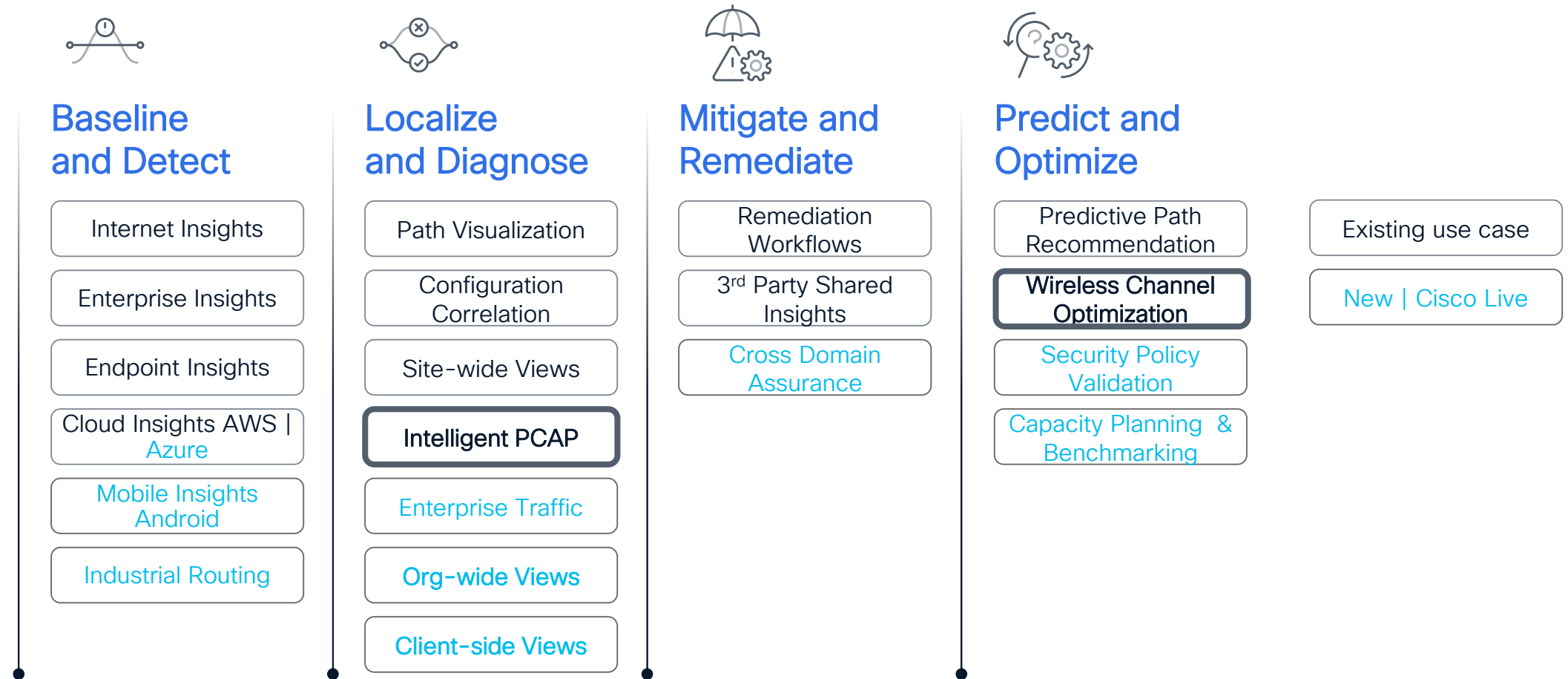


Assurance

Reactive monitoring

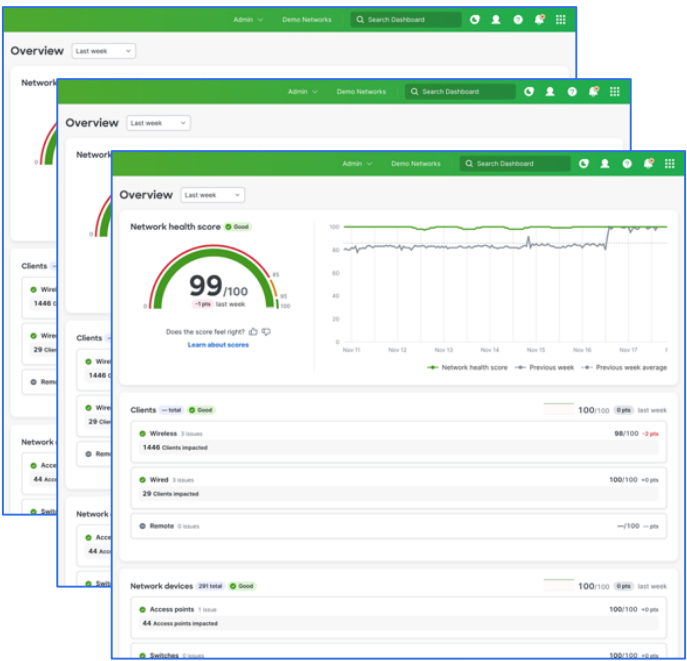
Executing Against Our Assurance Vision

Across and within network domains



Expanded assurance view to entire organization

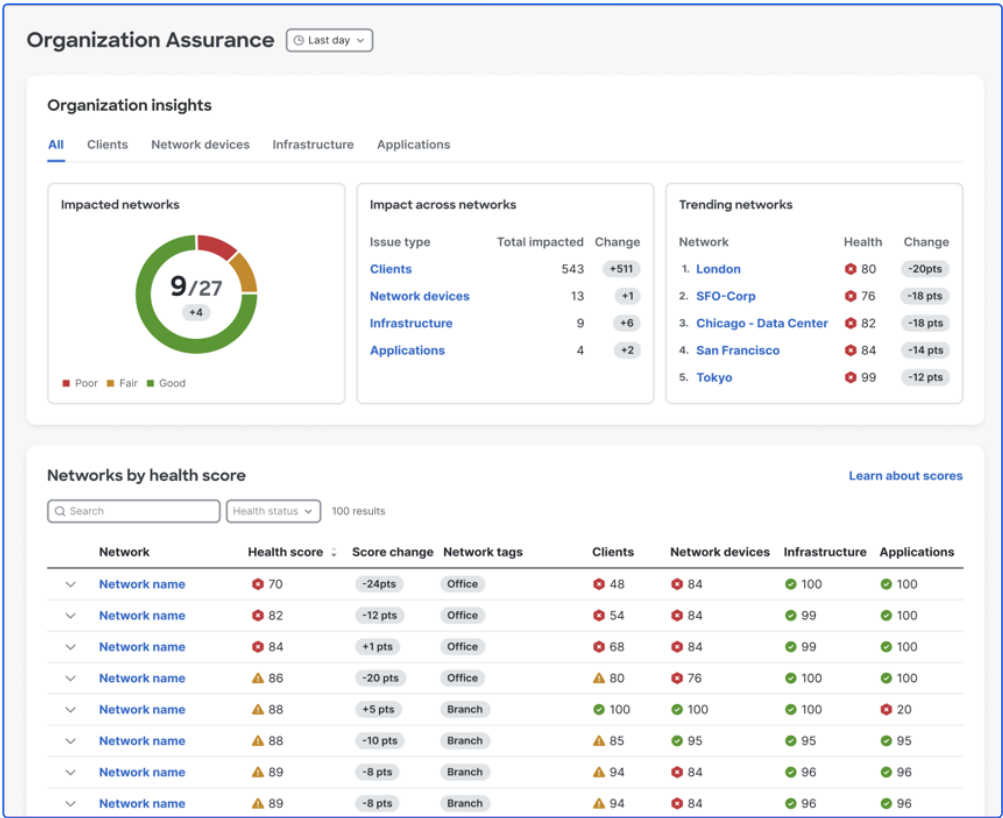
Network-wide Assurance



Network to -> Client or Device-level drill down

Org-wide Assurance

Production Beta



Org-level discovery workflow

Client Assurance

Client Event evolved overtime for explainability and correlated insights

Event log – catch all events

Event logfor access points

Access point:c4:14:a2:fb:3f:70Client:AnyBefore:06/08/202507:53(PDT)

Event type include:All client eventsEvent type ignore:None

SearchReset filters

Download as

Time (PDT)	Access point	SSID	Client	Category	Event type	Details
Jun 8 06:36:14	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	802.11	802.11 disassociation	unspecified reason more
Jun 8 06:34:18	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	Wireless problems	Connectivity problem	type: NO DHCP ack, associated: true, radio: 1, vap: 0
Jun 8 06:34:08	sfo12-4-ap-035	Meraki-Corp	eb08a3a536f8e2b217345adaef9a9e42	Wireless problems	Connectivity problem	type: NO DHCP ack, associated: true, radio: 1, vap: 0
Jun 8 06:33:55	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	Wireless problems	Association status	radio: 1, vap: 0, is_8021x: 1 more
Jun 8 06:33:53	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	802.1X	802.1X authentication	radio: 1, vap: 0, client_mac: 08-6A:C5-6A:14-27, identity: wallboard.sfo12
Jun 8 06:33:53	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	802.1X	Successful authentication (EAP success)	radio: 1, vap: 0, client_mac: 08-6A:C5-6A:14-27, identity: wallboard.sfo12
Jun 8 06:33:53	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	802.1X	RADIUS response	radio: 1, vap: 0, group: more
Jun 8 06:33:53	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	802.1X	RADIUS response	radio: 1, vap: 0, group: more
Jun 8 06:33:53	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	802.11	802.11 association	channel: 104, rssi: 35, band: 5 more
Jun 8 06:33:52	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	Wireless problems	Association status	radio: 1, vap: 0, is_8021x: 1 more
Jun 8 06:33:51	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.1X	802.1X authentication	radio: 1, vap: 0, client_mac: 08-6A:C5-5A:0E-BF, identity: wallboard.sfo12
Jun 8 06:33:51	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.1X	Successful authentication (EAP success)	radio: 1, vap: 0, client_mac: 08-6A:C5-5A:0E-BF, identity: wallboard.sfo12
Jun 8 06:33:51	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.1X	RADIUS response	radio: 1, vap: 0, group: more
Jun 8 06:33:51	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.11	802.11 association	channel: 104, rssi: 53, band: 5 more
Jun 8 06:33:49	sfo12-4-ap-035	Meraki-Corp	eb08a3a536f8e2b217345adaef9a9e42	Wireless problems	Association status	radio: 1, vap: 0, is_8021x: 1 more
Jun 8 06:33:47	sfo12-4-ap-035	Meraki-Corp	eb08a3a536f8e2b217345adaef9a9e42	802.1X	802.1X authentication	radio: 1, vap: 0, client_mac: 08-6A:C5-5C-55-8A, identity: wallboard.sfo12
Jun 8 06:33:47	sfo12-4-ap-035	Meraki-Corp	eb08a3a536f8e2b217345adaef9a9e42	802.1X	Successful authentication (EAP success)	radio: 1, vap: 0, client_mac: 08-6A:C5-5C-55-8A, identity: wallboard.sfo12
Jun 8 06:33:47	sfo12-4-ap-035	Meraki-Corp	eb08a3a536f8e2b217345adaef9a9e42	802.1X	RADIUS response	radio: 1, vap: 0, group: more
Jun 8 06:33:47	sfo12-4-ap-035	Meraki-Corp	eb08a3a536f8e2b217345adaef9a9e42	802.1X	RADIUS response	radio: 1, vap: 0, group: more
Jun 8 06:33:47	sfo12-4-ap-035	Meraki-Corp	eb08a3a536f8e2b217345adaef9a9e42	802.11	802.11 association	channel: 104, rssi: 49, band: 5 more
Jun 8 06:00:32	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.11	802.11 disassociation	client was deauthenticated more
Jun 8 06:00:22	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.11	802.11 association	channel: 104, rssi: 53, band: 5 more
Jun 8 06:00:21	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.11	802.11 association	channel: 104, rssi: 38, band: 5 more
Jun 8 06:00:16	sfo12-4-ap-035	Meraki-Guest	g0106f0552a34f56142a3d5c5b578aaf	Wireless problems	Association status	radio: 1, vap: 10, is_8021x: 1 more
Jun 8 06:00:15	sfo12-4-ap-035	Meraki-Guest	g0106f0552a34f56142a3d5c5b578aaf	802.1X	802.1X authentication	radio: 1, vap: 10, client_mac: 08-6A:C5-69-A4-A6
Jun 8 06:00:15	sfo12-4-ap-035	Meraki-Guest	g0106f0552a34f56142a3d5c5b578aaf	802.11	802.11 association	channel: 104, rssi: 50, band: 5 more
Jun 8 03:41:30	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.1X	802.1X authentication	radio: 1, vap: 0, client_mac: 08-6A:C5-5A:0E-BF more
Jun 8 03:41:30	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.1X	Successful authentication (EAP success)	radio: 1, vap: 0, client_mac: 08-6A:C5-5A:0E-BF more
Jun 8 03:41:30	sfo12-4-ap-035	Meraki-Corp	40aa88c199e91cc782ce9ddec75b711	802.1X	RADIUS response	radio: 1, vap: 0, group: more
Jun 7 21:01:54	sfo12-4-ap-035	Meraki-Corp	g3d78542fc1d0694b617553cec4795f1	802.11	802.11 disassociation	unspecified reason more

30 total

Client Timeline – descriptive client event logs

CLIENTSGalaxy-A12

OverviewConnectionsPerformanceRoamingTimelineStored captures

HistoryJun 7 08:00 to Jun 8 08:00

SSIDAll SSIDs

ACCESS POINTAll Access Points

BANDAll bands

CONNECTION STEPAll connections

STATUSAll statuses

PACKET CAPTUREAll

Jun 8 06:17:17

Roamed from access point sfo12-4-ap-044-elev then had a failed connection to SSID Meraki-Guest-OWE on access point sfo12-4-ap-013 during authentication because the client did not provide credentials.

CHANNEL52

BAND5 GHz

SNR43 dB

MERAKI REASON (CODE 101)EAPoL timeout

Download packet captureView in packet viewer

Jun 8 06:16:41

Successful connection to SSID Meraki-Guest-OWE for a few seconds on access point sfo12-4-ap-044-elev.

CHANNEL132

BAND5 GHz

SNR42 dB

TIME TO CONNECT490 ms

Jun 8 06:16:33

Roamed from access point sfo12-4-ap-020 then had a failed connection to SSID Meraki-Guest-OWE on access point sfo12-4-ap-044-elev during authentication because the client did not provide credentials.

CHANNEL132

BAND5 GHz

SNR41 dB

MERAKI REASON (CODE 101)EAPoL timeout

Jun 8 06:16:05

Successful connection to SSID Meraki-Guest-OWE for a few seconds on access point sfo12-4-ap-020, and then the client roamed to access point sfo12-4-ap-044-elev.

CHANNEL161

BAND5 GHz

SNR35 dB

TIME TO CONNECT450 ms

Jun 8 06:15:55

Roamed from access point sfo12-4-ap-014 then had a failed connection to SSID Meraki-Guest-OWE on access point sfo12-4-ap-044-elev during authentication because the client did not provide credentials, and then the client roamed to access point sfo12-4-ap-020.

CHANNEL11

BAND2.4 GHz

SNR46 dB

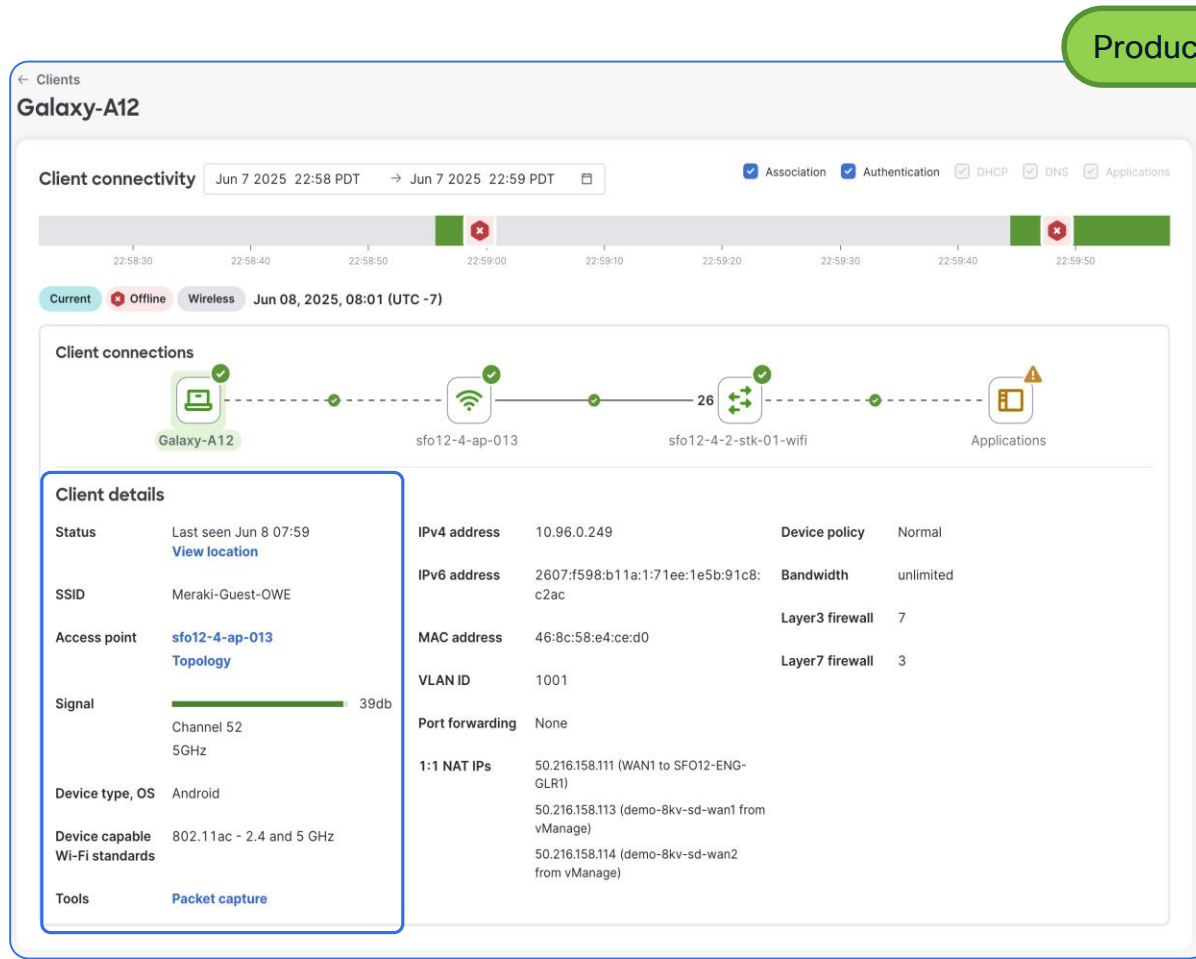
MERAKI REASON (CODE 101)EAPoL timeout

Packet capture

- Raw client event log
- Most detailed, Expert tool

- Various type filters
- Highlight the reason code and RF condition
- Proactive Packet Capture integrated

Client 360 – Brings all the internetworking level timeline view to the forefront of the client page



Client 360 for Meraki Dashboard

- Client connection and session history
- Network-wide client experience with timeline
- E2E network correlation and Topology
- Client connection details
- Easy chronical navigations of failed event
- Click to Zoom
- Integrated Tools access (e.g Packet capture, Ping)

Layer 2 Connectivity

Layer 3 Network info

Network Policy

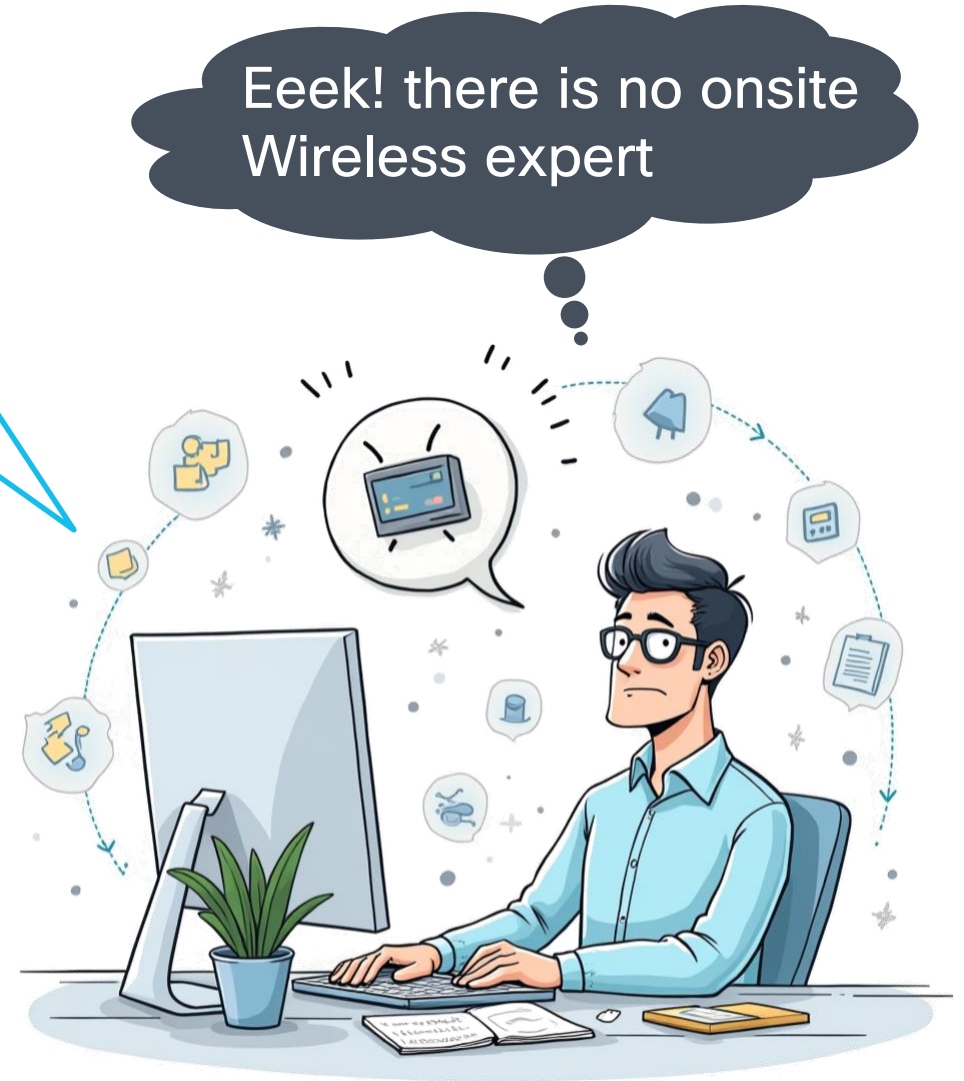
Case - Wireless disconnection issue reported

Complaint filed via corporate messenger channel, reported **Bad Wi-Fi experience yesterday**, in the San Diego Branch

Wait.. it's 3rd time reported from SD this month

Is this a network or client issue?

EEK! there is no onsite Wireless expert



Case - Wireless disconnection issue reported

Let's try to get
some PCAP



Let's try to get some PCAP

3rd Party Capture Tool

- Unknown Target AP channel
- Multi-Channel Bonding
- Encrypted Payload
- Multi PCAP file concatenation
- Multi-band/ Multi-radio capture
- Remote Capture
- Outdated PCAP Hardware

Sniffer/Promiscuous AP Packet capture

- Packets bundle to Network event correlation
- Incomplete, Partial PCAP
- Wired-Wireless PCAP



Dashboard Packet Capture

- Historical PCAP Access
- Missing Packet Payload
- Out of Order Packets
- Capture size limit
- Wi-Fi 7/MLO Packet Capture
- Difficult to share large PCAP files
- Failed to grasp failure moment
- No scheduled PCAP

Intelligent Capture

Next Generation Packet Capture Solution for Wired and Wireless

Meraki

Network-wide

Security & SD-WAN

Switch

Wireless

Systems Manager

Camera

Sensors

Insight

Organization-wide

Packet Captures

Capture Name (Analysis)

Packet capture

Time	Source	Destination	Protocol	Transaction ID	Transaction ID	Info
1 0.000000	192.168.128.2	192.168.129.45	DNS	0xef4f		Standard query 0xef4f A dns.msftncsi.com
2 0.398151	192.168.128.2	192.168.129.45	DNS	0xd1c7		Standard query 0xd1c7 A dns.msftncsi.com
3 0.780715	fe80::a1e8:b...	ff02::1:2	DHCP			Solicit XID: 0x8eaa32 CID: 000100012a84816b54e1a
4 1.405498	192.168.128.2	192.168.129.45	DNS	0xd1c7		Standard query 0xd1c7 A dns.msftncsi.com
5 1.686310	CiscoMer_eei...	Spanning-tree (for...	STP			RST, Root = 4096/0/e0:55:3d:c4:3d:78 Cost = 215
6 1.837274	192.168.128.2	192.168.129.45	DNS	0x642a		Standard query 0x642a A self.events.data.microso
7 2.014230	192.168.128.2	192.168.129.45	DNS	0xef4f		Standard query 0xef4f A dns.msftncsi.com
8 3.300038	CiscoMer_00:...	LCFCHefe_51:fa:5c	ARP			Who has 192.168.128.2? Tell 192.168.128.1
9 3.301814	LCFCHefe_51:...	CiscoMer_00:db:7b	ARP			192.168.128.2 is at 54:e1:ad:51:fa:5c
10 3.387856	192.168.128.2	192.168.129.45	ICMP			Echo (ping) request id=0x0001, seq=34/8704, ttl
11 3.414848	192.168.128.2	192.168.129.45	DNS	0xd1c7		Standard query 0xd1c7 A dns.msftncsi.com
12 3.697035	CiscoMer_eei...	Spanning-tree (for...	STP			RST, Root = 4096/0/e0:55:3d:c4:3d:78 Cost = 215
13 5.697478	CiscoMer_eei...	Spanning-tree (for...	STP			RST, Root = 4096/0/e0:55:3d:c4:3d:78 Cost = 215
14 5.888320	192.168.128.2	192.168.129.45	DNS	0xfd41		Standard query 0xfd41 A wpad.supportlab.ikarem.3
15 6.027472	192.168.128.2	192.168.129.45	DNS	0xef4f		Standard query 0xef4f A dns.msftncsi.com
16 6.373097	CiscoMer_eei...	CDP/VTP/DTP/PAGP/U...	UDLD			Device ID: 149F43EE4C60 Port ID: 11
17 6.888997	192.168.128.2	192.168.129.45	DNS	0xfd41		Standard query 0xfd41 A wpad.supportlab.ikarem.1
18 7.470200	192.168.128.2	192.168.129.45	DNS	0xd1c7		Standard query 0xd1c7 A dns.msftncsi.com

Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
Ethernet II, Src: LCFCHefe_51:fa:5c (54:e1:ad:51:fa:5c), Dst: CiscoMer_00:db:7b (0c:8d:db:00:db:7b)
Destination: CiscoMer_00:db:7b (0c:8d:db:00:db:7b)
Source: LCFCHefe_51:fa:5c (54:e1:ad:51:fa:5c)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.128.2, Dst: 192.168.129.45
User Datagram Protocol, Src Port: 58977, Dst Port: 53
Domain Name System (query)

Packet Capture Analysis

The packet capture analytics tool looks for 4/10 categories of possible issues in your packet capture. Please note that even if it does not show any issues in the results below it is only reporting on Rogue DHCP, ARP, DNS, and ICMP issues.

Packet capture analysis summary

Tests summary

Protocols

DHCP

DNS

ICMP

ARP

MAC address summary

Device summary

DNS

ARP

DHCP

ICMP

Proactive

Automated

Integrated

Last login

about 2 hours ago from your current IP address

© 2023 Cisco Systems, Inc.

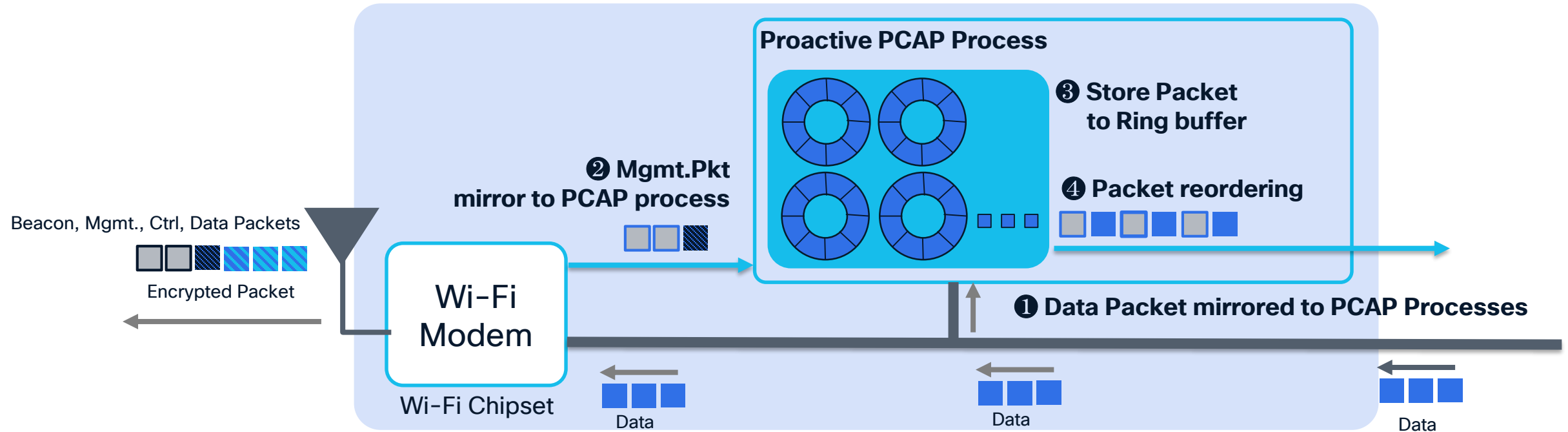
Privacy - Terms

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKEWN-2039

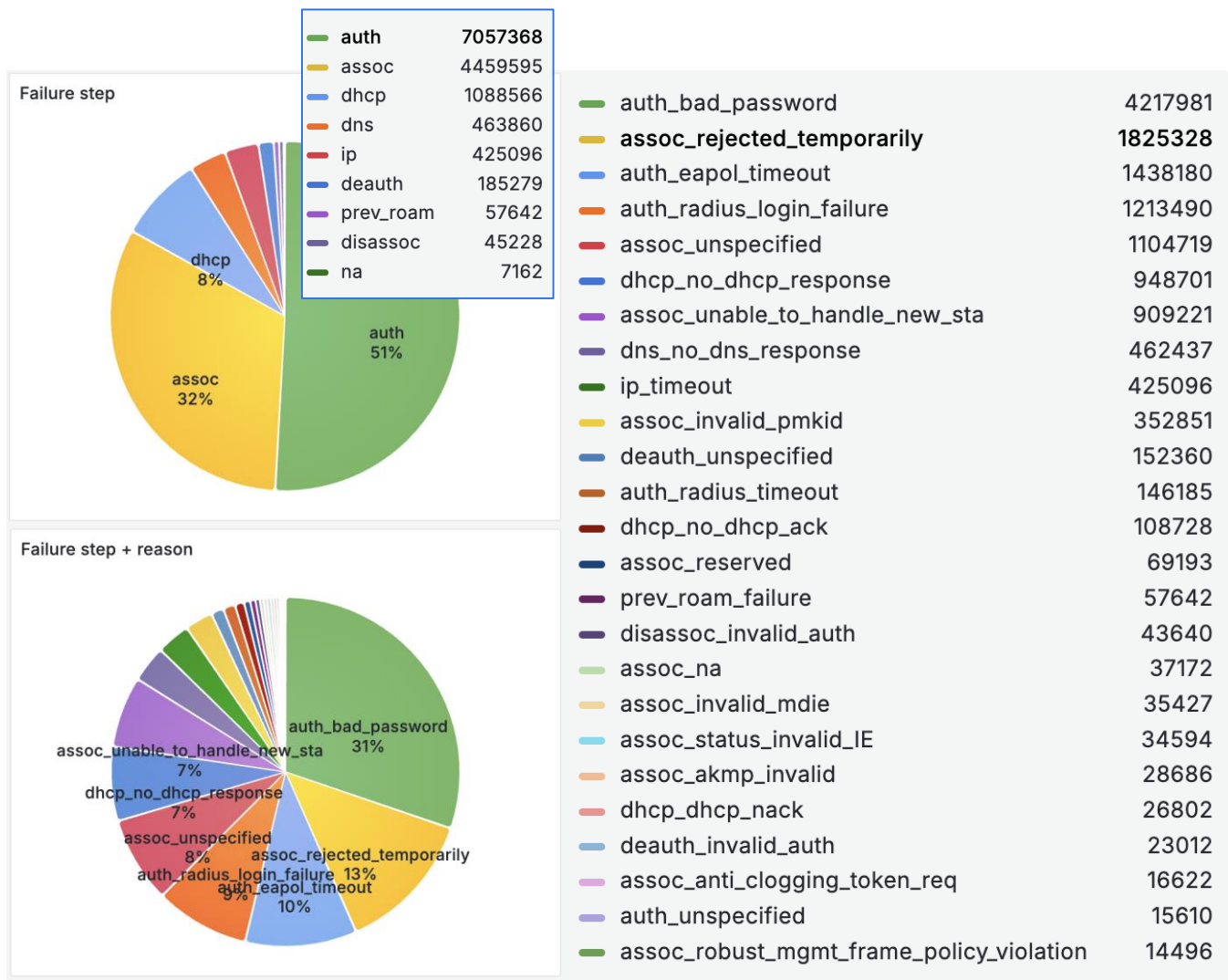
15

Purpose-Built Packet Capture Architecture



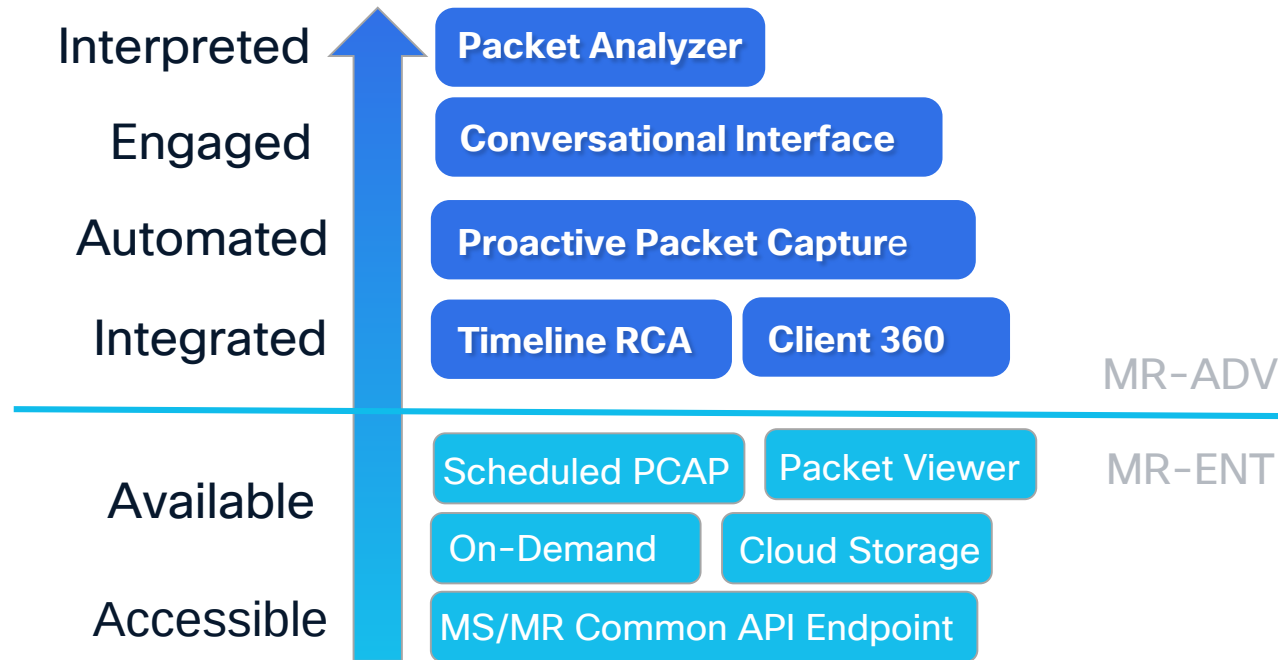
- Packet Capture doesn't change AP or radio mode and continue to serve client without any performance impact
- Management Frames from modem gets replicated and copied back into PCAP Buffer
- Resequencing packet capture frame between Data Frame and Management frame in the right order
- Per-Client Ring Buffer for Proactive PCAP enabled concurrent packet capture

Proactive Packet automatically take a PCAP on all of client failures conditions



- Proactive PCAP automatically collect Wireless PCAP All the time at every connection failure
- including “unknown failure” cases
- PCAP includes Mgmt, Control and Client connection payload

Intelligent Capture – Meraki Wireless



- Every client connection failure condition leaves Packet as evidence
- Packet Viewer shows exact reason why client failed to connect

Intelligent Capture

For access points

New capture Stored captures Proactive PCAP Enablement

← All captures

e6:09:90:60:f9:d4_CK5zjY_auth_eapol_timeout

source	Destination	Transmitter	Receiver	Protocol	PHY type	Length	Info	QBSS Utilization
ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	802.11	802.11b (HR/DSSS)	78	Authentication, SN=3885, FN=0, Flags...	
e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	802.11	802.11b (HR/DSSS)	263	Reassociation Request, SN=3584, FN...	
ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	802.11	802.11b (HR/DSSS)	92	Action, SN=6, FN=0, Flags=p...	
ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	802.11	802.11b (HR/DSSS)	92	Action, SN=6, FN=0, Flags=p...	
e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	802.11	802.11b (HR/DSSS)	263	Reassociation Request, SN=3584, FN...	
ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	802.11	802.11b (HR/DSSS)	74	Deauthentication, SN=3886, FN=0, Fla...	
e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	802.11	802.11b (HR/DSSS)	91	Authentication, SN=3585, FN=0, Flags...	
ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	802.11	802.11b (HR/DSSS)	78	Authentication, SN=3887, FN=0, Flags...	
e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	802.11	802.11b (HR/DSSS)	263	Reassociation Request, SN=3586, FN=...	
ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	802.11	802.11b (HR/DSSS)	252	Reassociation Response, SN=0, FN=0,...	
e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	e6:09:90:60:f9:d4	ca:9c:3e:f7:d8:90	EAPOL	802.11b (HR/DSSS)	224	Key (Message 2 of 4)	

> Frame 58: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits)
 > Radiotap Header v0, Length 48
 > 802.11 radio information
 > IEEE 802.11 Reassociation Request, Flags:R...
 > IEEE 802.11 Wireless Management
 > Fixed parameters (10 bytes)
 > Tagged parameters (181 bytes)
 > Tag: SSID parameter set: "msnjs2023e"
 > Tag: Supported Rates 11(B), 12, 18, 24, 36, 48, 54, [Mbit/sec]
 > Tag: Power Capability Min: -7, Max: 22
 > Tag: Supported Channels
 > Tag: RSN Information
 > Tag: RM Enabled Capabilities (5 octets)
 > Tag: HT Capabilities (802.11n D1.10)

Requirement

- FW version: MR 31.x or newer
- AP HW : Wi-Fi 6 or later MR & CW APs



Demo – Client Assurance

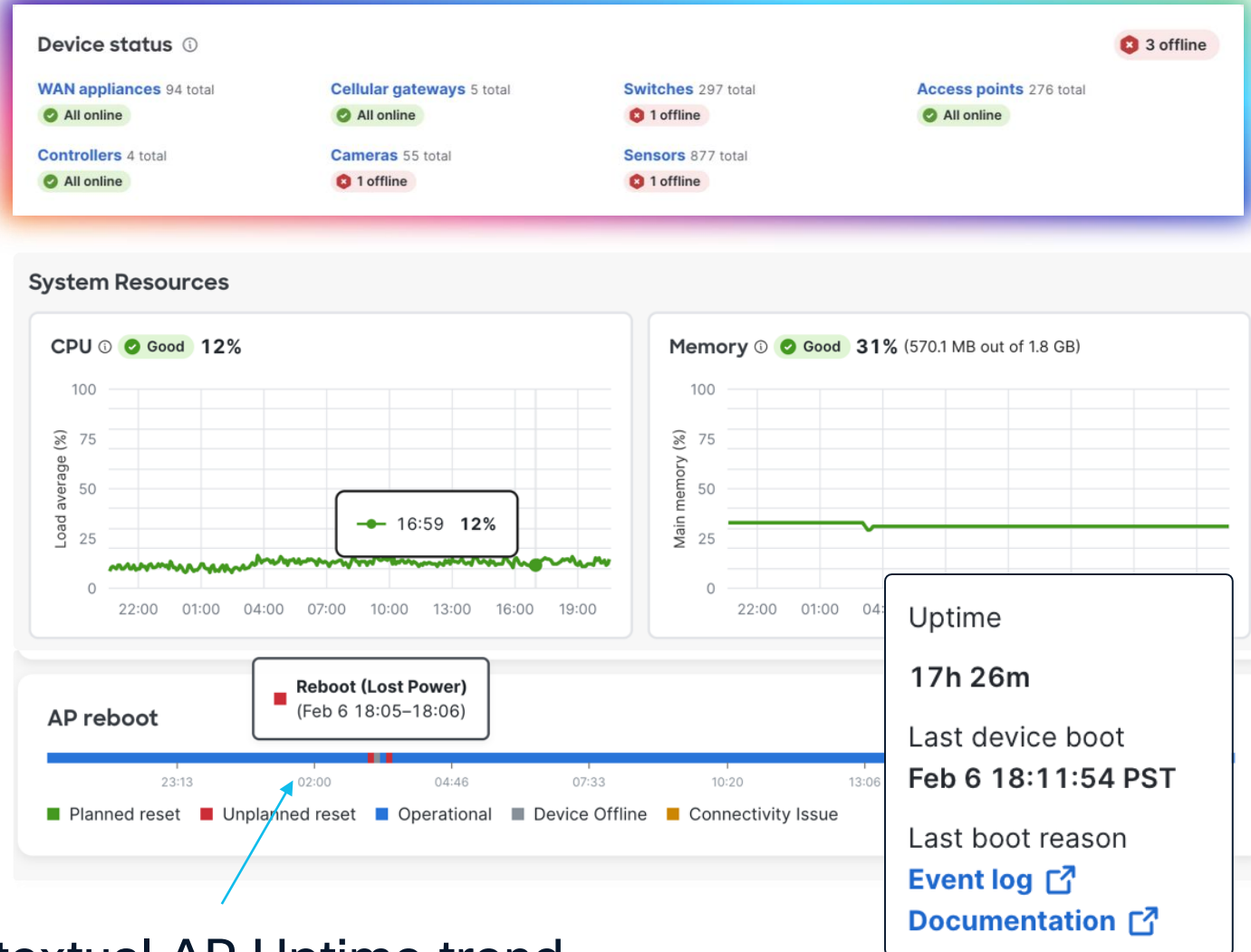
Wireless Device Assurance

AP Device Health

Don't forget the basic

- Device availability
- CPU and Memory utilization – latest & trend
- Detect Memory leak or CPU spikes
- PoE / Power monitoring
- Build your Own Dashboard, Org-Wide API Ready!

/organizations/{organizationId}/wireless/devices/system/cpu/load/history



Contextual AP Uptime trend

Suggested actions for assisted device alert remediation

The image displays three overlapping screenshots of the Cisco Network Traffic Analysis (NTA) interface, illustrating suggested remediation actions for network alerts.

Top Screenshot: "Unplanned low power mode"

- Alert: **Unplanned low power mode** (Active)
- Device: OC-Yamaha-PoE-Interop_CW62_802.3af-PoE-Injector
- Time: Jun 6 2025 at 22:07 PDT
- Tab: **Suggested actions** (1)
- Action 1: **1. Check PoE budget**

Middle Screenshot: "Ethernet uplink speed degrade"

- Alert: **Ethernet uplink speed degrade**
- Details: The data rate from MS120-1 / 3 is capped at 100 Mbps
- Time: May 28 2025 at 21:55
- Tab: **Suggested actions** (3)
- Action 1: **1. Cable test**
- Action 2: **2. Update link negotiation settings**
- Details: The link negotiation is set to **100 Megabit half duplex (forced)** may solve the problem.
- Warning: A manual override of the link negotiation on the switch on the wired uplink.
- Device Name: MS120-1
- Port: 3
- Capability: 1000 Mbps
- Link Negotiation: 100 Megabit half duplex (forced) → 100 Megabit half duplex (forced)
- Buttons: View port configuration, Confirm changes
- Action 3: **3. Cycle port on switch**

Bottom Screenshot: "Unplanned low power mode"

- Alert: **Unplanned low power mode** (Active)
- Time: Jun 9 2025 at
- Tab: **Suggested actions** (5)
- Text: These steps are prioritized, but can be done in any order.
- Actions:
 1. Cable test
 2. Check that LLDP is running
 3. Cycle port on switch
 4. Check PoE budget
 5. Run LLDP packet capture
- Warning: Certain admin privileges are required to perform this action. Please contact your admin or support team.
- Text: Run a packet capture to collect forensics of LLDP negotiation failures.
- Button: Run packet capture

RCA Framework features

- Automated RCA workflows eliminated unlikely root causes
- Support MS Switches for integrated remediations steps
 - Cable test
 - Switch port config check
 - PoE type check
 - Port cycle
 - LLDP packet capture
- 3rd Party switch LLDP Packet Analysis

New AP Alert RCA – Access point became repeater

The screenshot displays the Cisco Meraki dashboard interface. On the left, a sidebar shows the 'Access points' section with a filter for 'Alerting repeater'. The main content area shows an alert titled 'Access point became repeater' for the access point 68:49:92:98:ae:70. The alert message states: '68:49:92:98:ae:70 has switched to repeater mode to avoid losing internet connection. 68:49:92:98:ae:70 · z-pdumouli-wireless · Jun 2 2025 at 10:11 PDT'. Below the alert, a map shows the location of the access point. The 'Details' tab is selected, showing the 'Suggested actions' section. The first action is '1. Resolve misconfigured VLAN', which explains that the access point has been assigned to a VLAN that isn't configured to connect to the Meraki cloud. The recommended solution is to match the native VLAN settings of the repeater and gateway access points. A table compares the configuration of the repeater (68:49:92:98:ae:70) and the gateway (68:49:92:f9:a3:30). The table shows that the repeater's Native VLAN is 3, while the gateway's Native VLAN is 1 (Recommended). At the bottom of the table, there are buttons for 'Edit manually' and 'Accept recommendation'.

This is a Cisco internal organization.

← Access points ←

68:49:92:98:ae:70 Alerting repeater

CW9166I 68:49:92:98:ae:70

Access point became repeater.

Map data ©2025 Google

Address

SSIDs

Firmware

Firmware version locked, please contact support

Access point became repeater Active

68:49:92:98:ae:70 has switched to repeater mode to avoid losing internet connection.
68:49:92:98:ae:70 · z-pdumouli-wireless · Jun 2 2025 at 10:11 PDT

Details Suggested actions 1

1. Resolve misconfigured VLAN

The access point has been assigned to a VLAN that isn't configured to connect to the Meraki cloud. The recommended solution is to match the native VLAN settings of the repeater and gateway access points.

Access point	68:49:92:98:ae:70 (repeater)	68:49:92:f9:a3:30 (gateway)
IPv4 address(es)	—	10.30.104.119
IPv6 address(es)	—	—
Connected switch	Switch_automation/1	Switch_automation/5
Type	trunk	trunk
Allowed VLANs	1-1000	1-1000
Native VLAN	3	1 Recommended

Edit manually Accept recommendation

- Detect AP which became repeater.
- RCA Engine lists all the possible scenario and provides active RCA steps to corresponding root cause.
 - Lost gateway connectivity
 - DHCP doesn't serve IP address to it's wired uplink port
 - Config change (Config management)
 - AP firmware mismatch
 - Last resort, force AP reboot

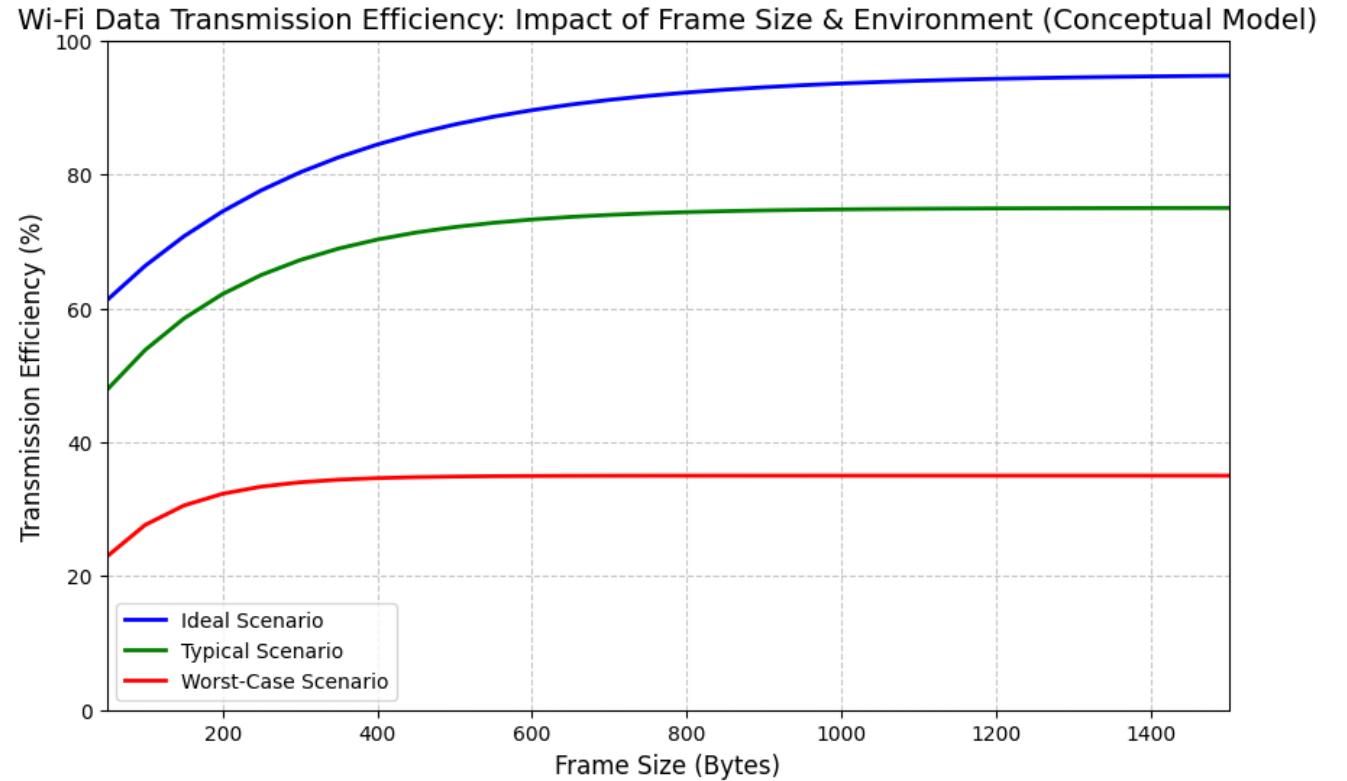
Demo – Device Assurance

RF Optimization

How's my Wi-Fi doing? It depends...

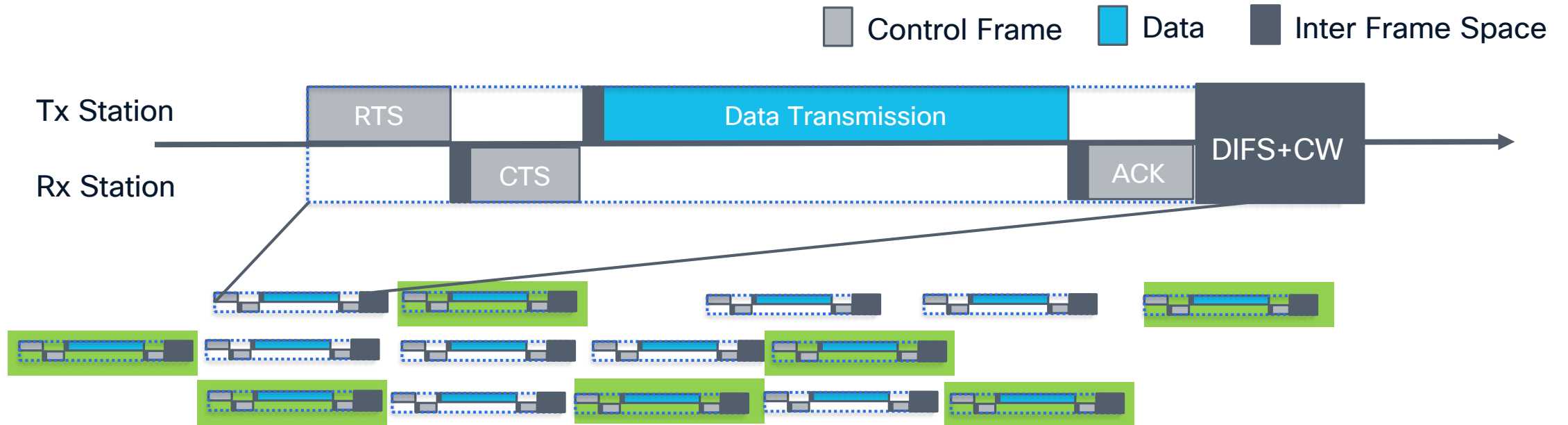
Wireless performance are depending on many factors as Wi-Fi relies on transport conditions and clients that are unique on each type

- Uncertainly of transport quality
- Over the air resource availability
- Varied client capabilities



Wi-Fi Performance is determined many factors and there is no single rule of thumbs

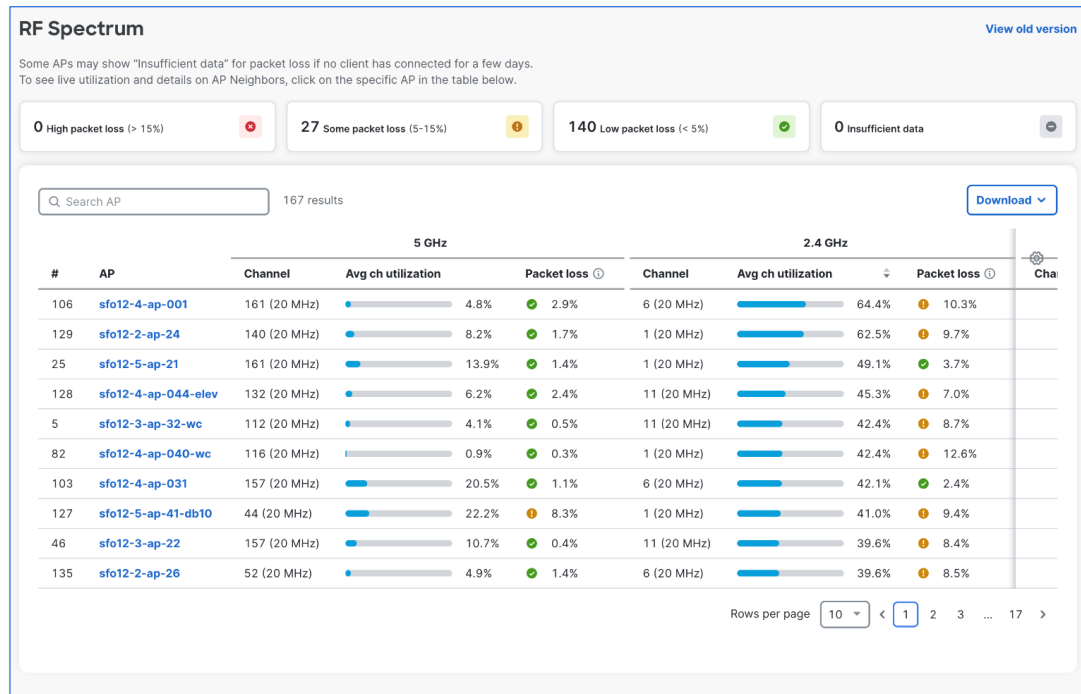
Wi-Fi designed to avoid collision, higher the Channel utilization goes, longer the waiting time has become



- Wi-Fi designed as CSMA/CA system – Carrier Sense Multiple Access / Collision Avoidance
- Half-Duplex system, Tx and Rx can't happen same time
- Overhead can be anywhere between 20% to 80%, average ballpark of 40-50%
- Duty Cycle of each frame is varied as each frame uses own MCS (Encoding size) and distance (RTT)

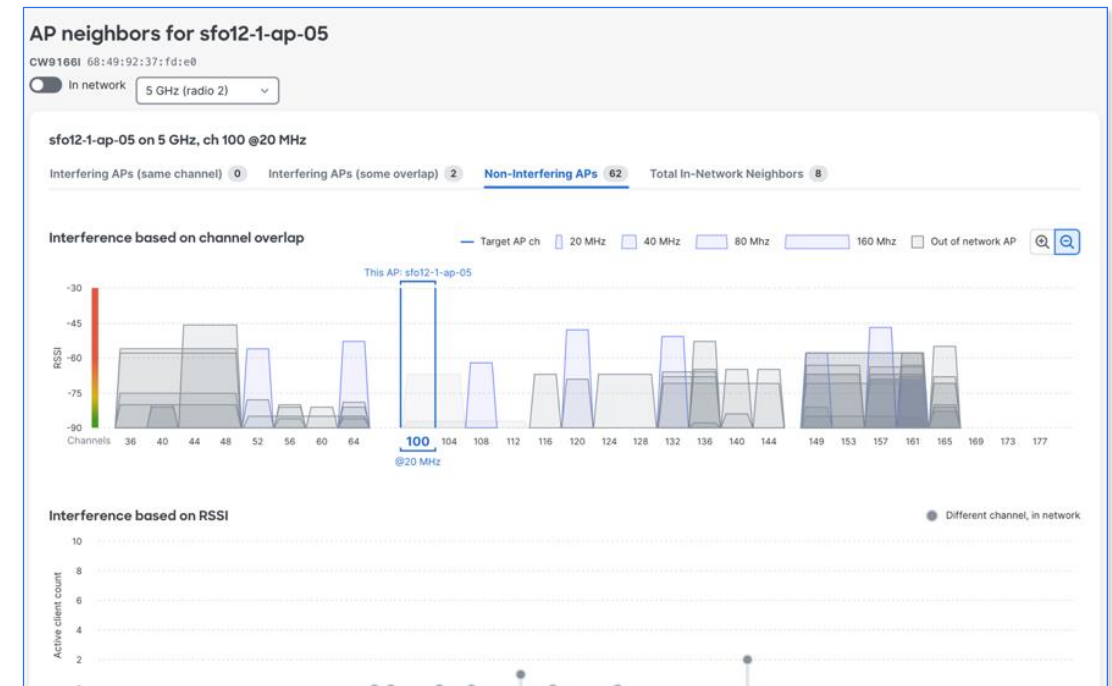
RF Spectrum evolved to provide both top-down discovery as well as bottom-up real-time RF neighbors

Long-term, trend-based Top-N list view



- Monitor RF Utilization and Packet Loss
- Proactive, discovery workflow to detect AP with persistent problem

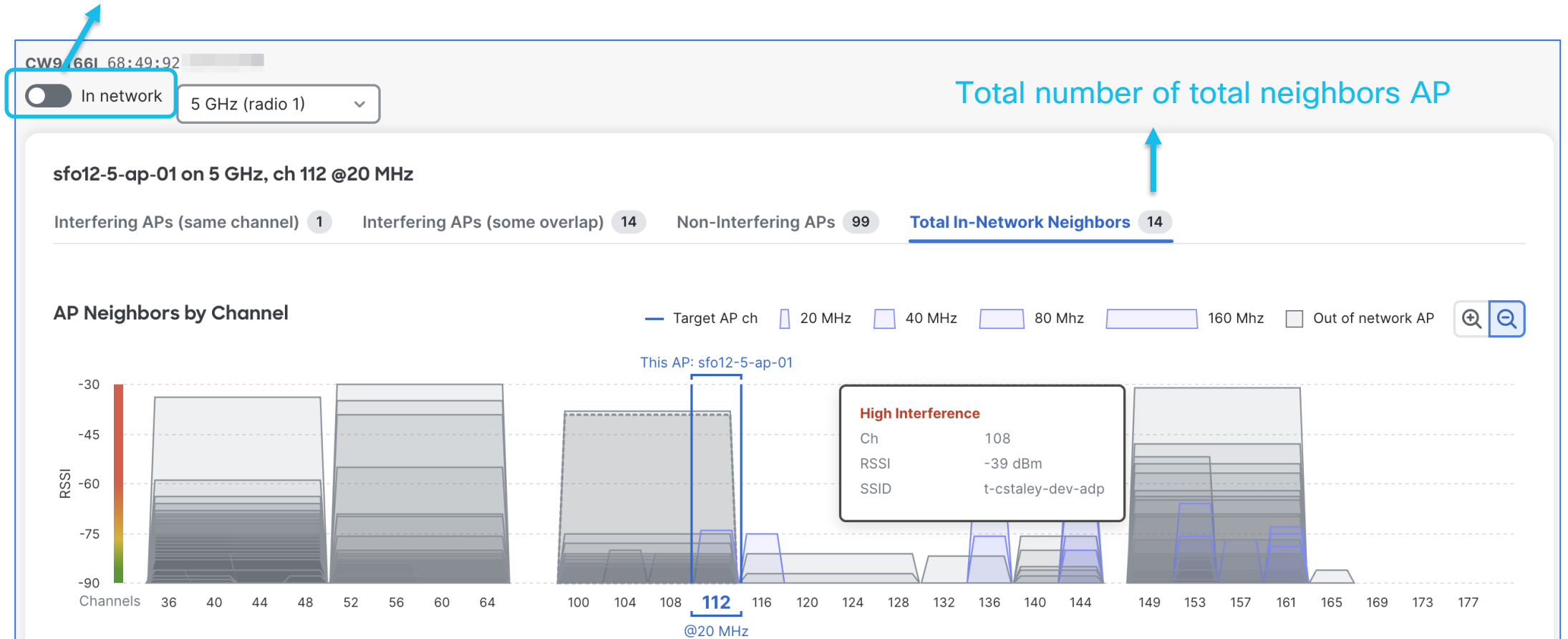
Real-time RF Neighbors



- Full-channels Wi-Fi analyzer while AP is in service using scanning radio
- Offers workflow from RF health and RF overview list

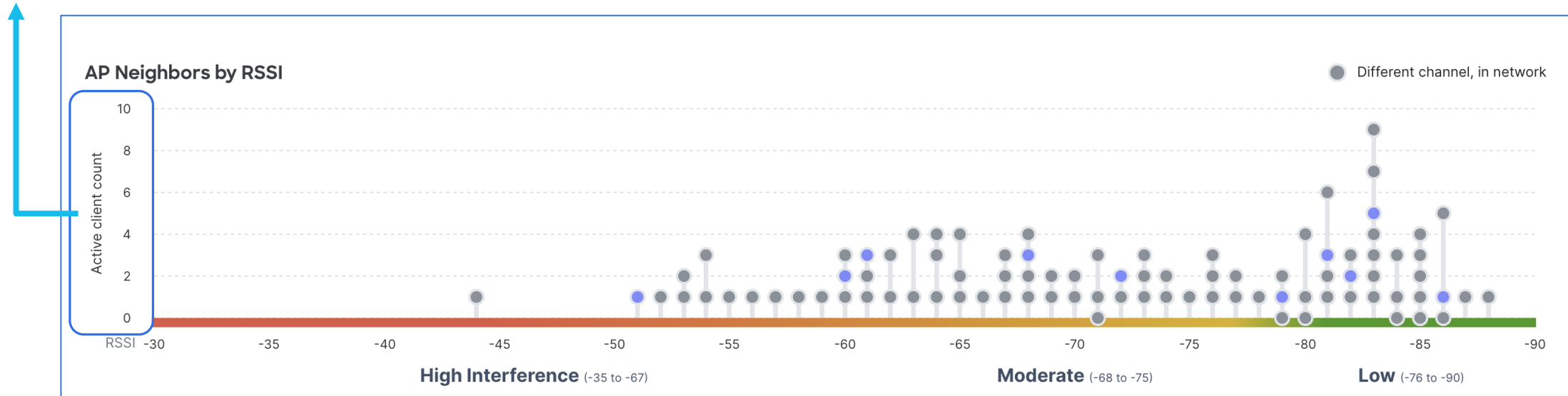
AP neighbor view makes remote troubleshooting easy and powerful – Whole band scanning and real-time updates

In network toggle to enable/disable neighboring, out of network APs/BSSIDs



AP neighbor view makes remote troubleshooting easy and powerful – AP Neighbors by RSSI

Shows neighboring APs with active clients



- Lists all neighboring APs from current radio
- Not a rogue AP view
- Showing all APs across band
- Client counts shows possible channel consumption contributions

- Lists all neighboring APs from current radio
- Not a rogue AP view
- Showing all APs across band

AP neighbor view makes remote troubleshooting easy and powerful – AP Neighbors by RSSI

These three tabs are available from In-Network APs

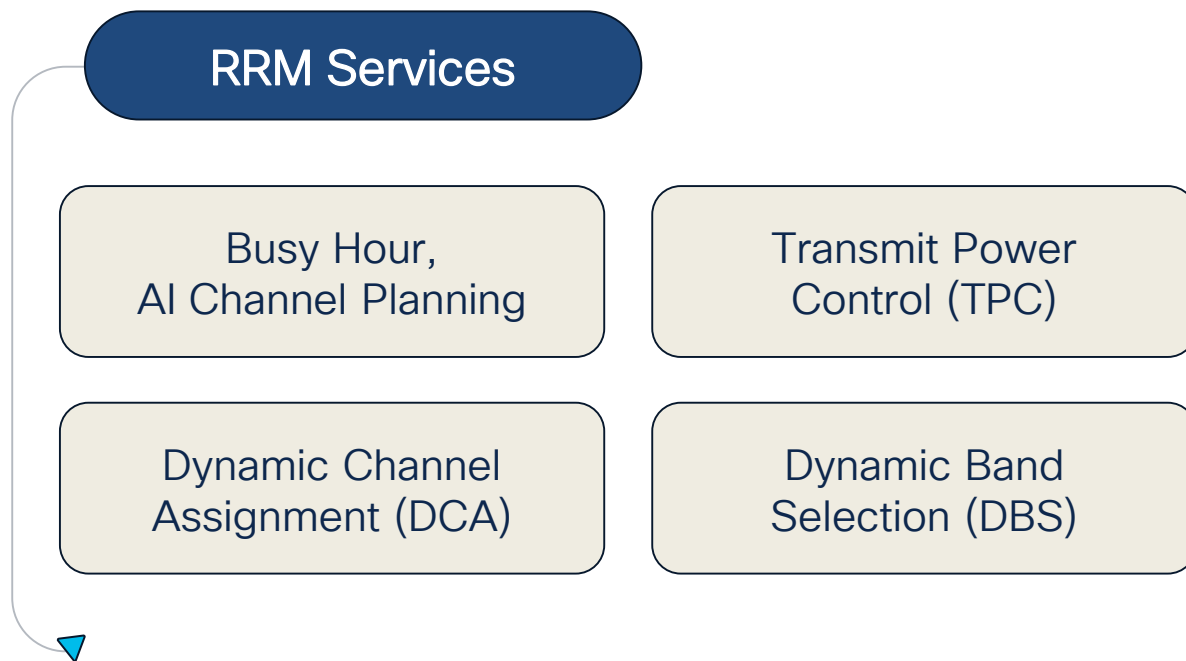
#	Interference	AP neighbor		RSSI (dBm)	Ch	Ch utilization	Active clients	Tx power (dBm)	SSIDs
1	✔ None	32:8d:cb:b3:fa:5c		-30	52 (80 MHz)	—%	0		erich_mr
2	✔ None	8e:15:54:ab:ac:5c		-31	149 (80 MHz)	—%	0		t-whauser-brid, t-whause
8	✔ None	0e:8d:cb:6d:f2:f2		-54	153 (80 MHz)	—%	0		KEITH_SFO12_MG_WORKBENCH WiFi
9	✔ None	b2:88:91:51:47:a0		-54	153 (80 MHz)	—%	0		COPY THIS NETWORK - wireless WiF
10	✔ None	a6:18:98:00:fb:2a		-59	44 (80 MHz)	—%	0		devel 3 - wireless WiFi
11	✔ None	sfo12-5-ap-02		-61	136 (20 MHz)	5.4%	1	5	Meraki-Corp, Meraki-Guest, avalanche_openroaming, blizzard
12	✔ None	sfo12-5-ap-07		-62	144 (20 MHz)	9.11%	0	5	Meraki-Corp, Meraki-Guest, avalanche_openroaming, blizzard

Interferences type -  Overlapping  Same ch  None

Multiple BSSIDs from same AP are combined

What is radio resource management?

RRM is a Radio config optimization features that constantly update wireless's RF configurations to improve wireless performance.



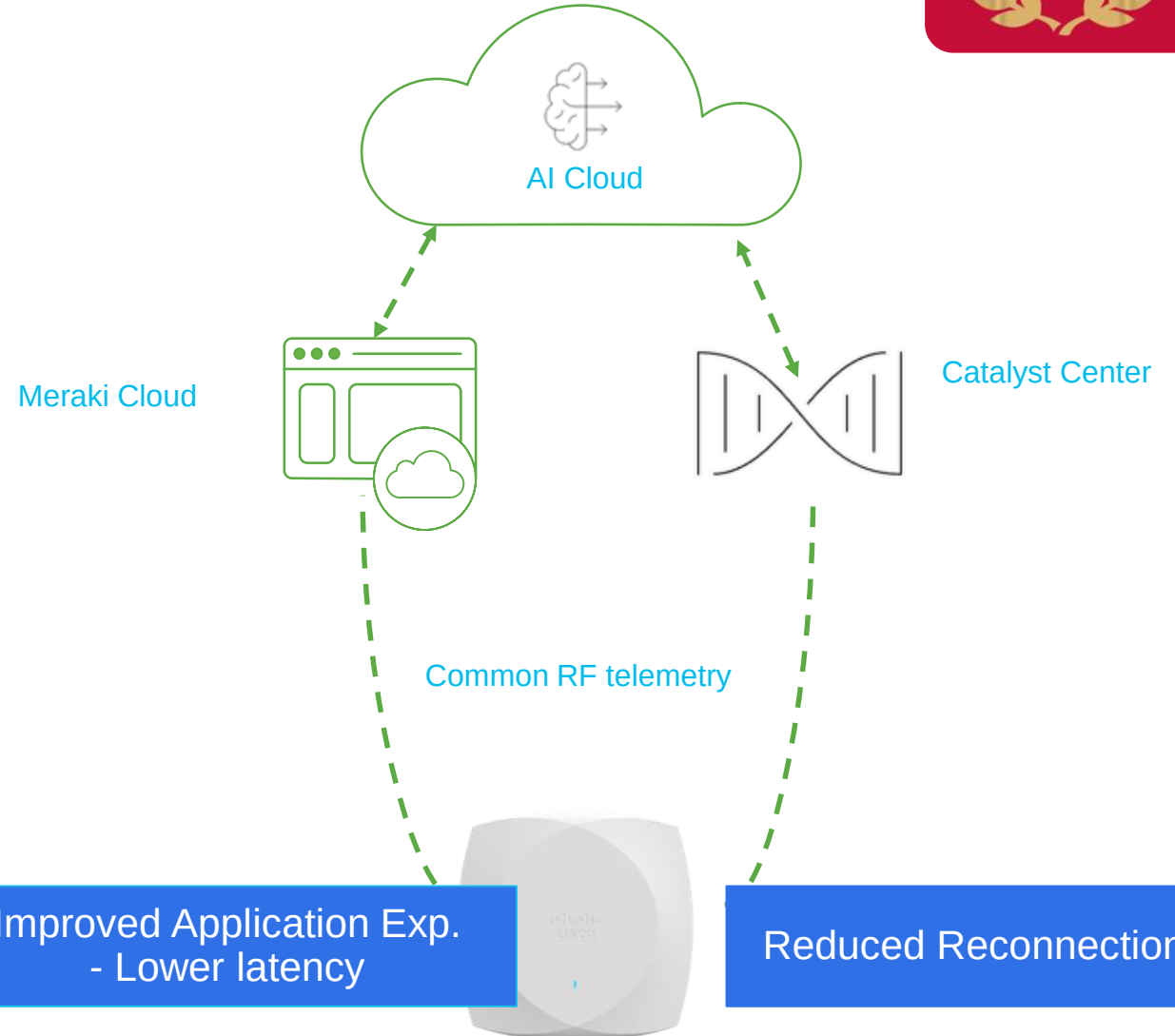
First Unified AI Wireless Service – AI-RRM

Path to autonomous Wi-Fi



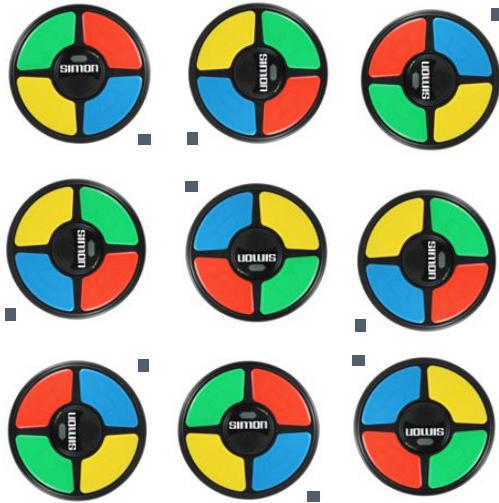
RF Intelligence powered by the unified AI cloud

- Interferences reduction
- Reduced Channel Changes
- Client Experience Improvement
- Wi-Fi Performance Improvement



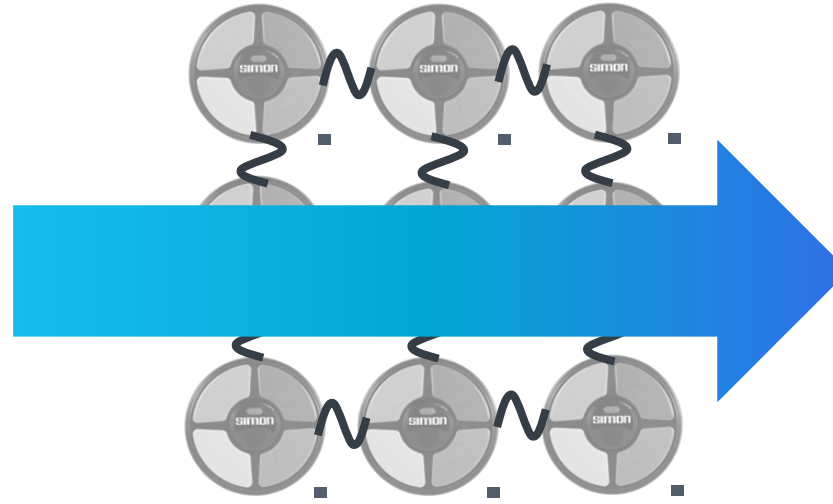
AI-RRM leapfrogs decades of innovations

Gen.1 Per AP RRM



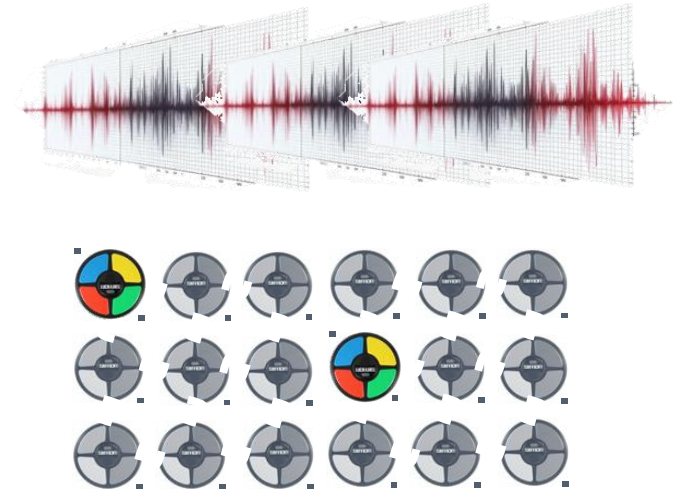
- Each AP makes own RF changes independently, at own timing
- Cascading RF changes could introduce infinite change-loops

Gen.2 Snapshot RRM



- All APs in the same RF group makes RRM decision all at once
- No cascading effect
- 10~15min, RF scanning duration for RF change

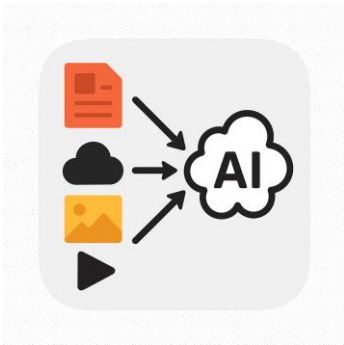
Gen.3 Trend-based, AI-RRM



- Long-term Trend-based RF telemetry pre-processing
- Minimal RF change from AI Busy Hour
- AI-RRM Dashboard

AI-RRM AI process pipelines

Multi-type data Ingestion



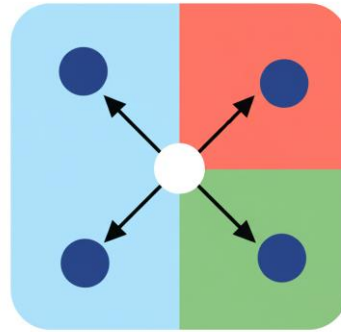
- AP Device Info
- RF Config/Profile
- RF Neighbor info
- Client Telemetry
- RF Events

Normalization



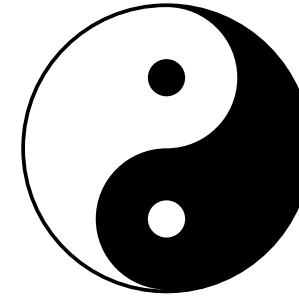
- Baselining
- Remove transient event
- Minimum 2 week of RF telemetry data

Classification



- KNN Classification
- Identify Busy Hour
- Apply different RF optimization weights by busy or non-busy hour
- Per-Network model

Reinforced Learning



- Feedbacks from RF Score
- Updates AI-RRM model using RF evaluations outcome
- Automated & RLHF

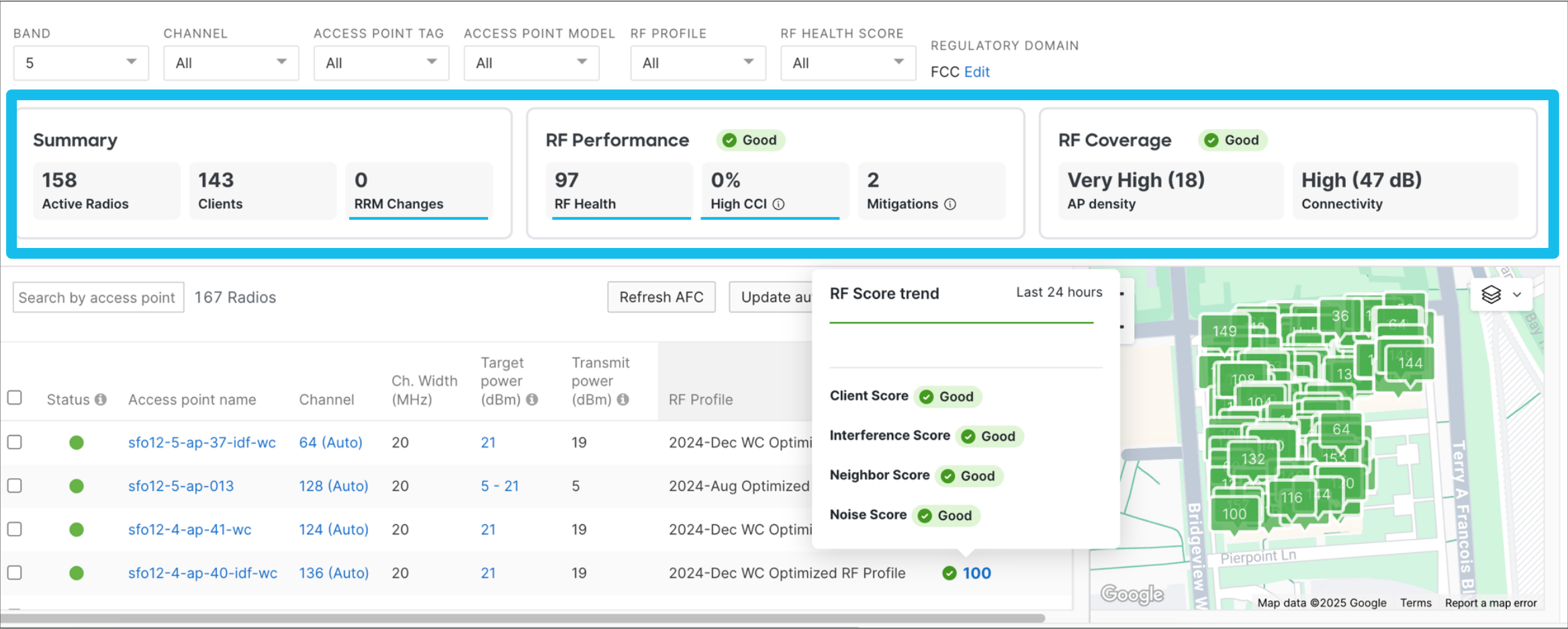
Digital Twins



- RF Simulation using Digital Twin
- “What if” results on updated RF config recommendations

Closed-loop RF configuration and optimization with AI Insight

Connected workflow of radio configure, assess and optimize

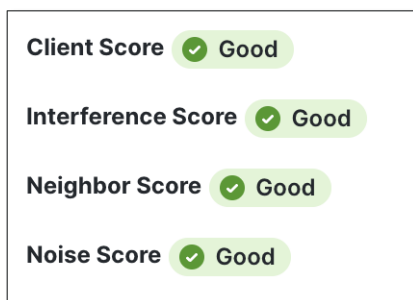


What defines better Wireless Network from the RF Point of view



RF Health

- RF Health algorithm debuted 2018 by Javier Contreras, Principal Engineer from Cisco.
- RF Health calculated from 9 RF metrics, takes worst score from which ever metric – Neighbor, Interference, Noise and Client



Co-Channel Interference

Interference can make your Wi-Fi slow or unreliable. AI-RRM calculated below factors

- Impact Score
- Highest CCI dBm
- Duty Cycle from Interferers

✓ Good

0%
High CCI ⓘ



Channel Changes

When AP changes channel, client can follow new AP channel if it supports 802.11h (CSA) and on 5GHz SSID.

If client doesn't support 802.11h, client may experience network delay or disruption

Minimize Ch. Change will avoid sudden wireless connection disruption or delay

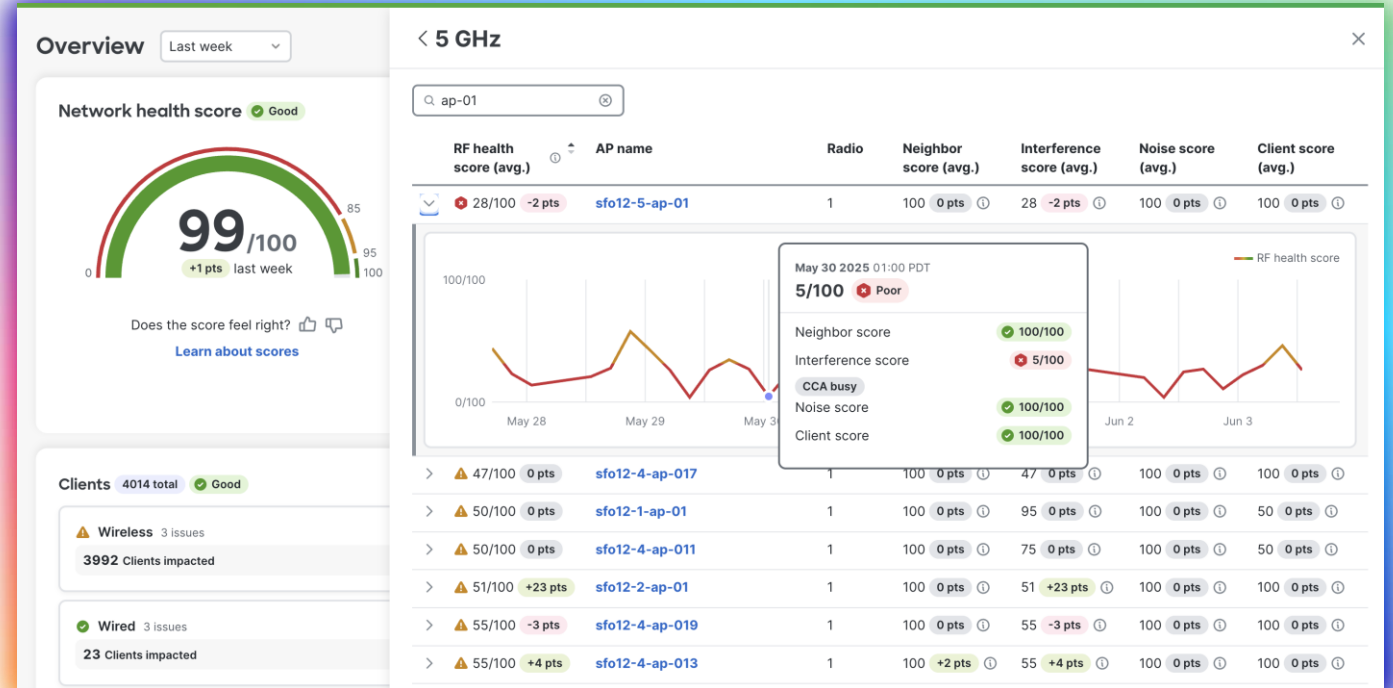
0
RRM Changes

RF Health – Barometers for Over-the-Air RF Spectrum quality assessment tool



RF Health – Always On Wi-Fi Audit

- Highlights problematic band and point in time view, identify what's the persistent or transient issue
- Provide per-radio RF scoring, the same algorithm used for AI-RRM
- Provides further scoring and insights on critical RF categories –neighbors, interference, noise, and client connectivity



Discover source of interferences and quantify the impact

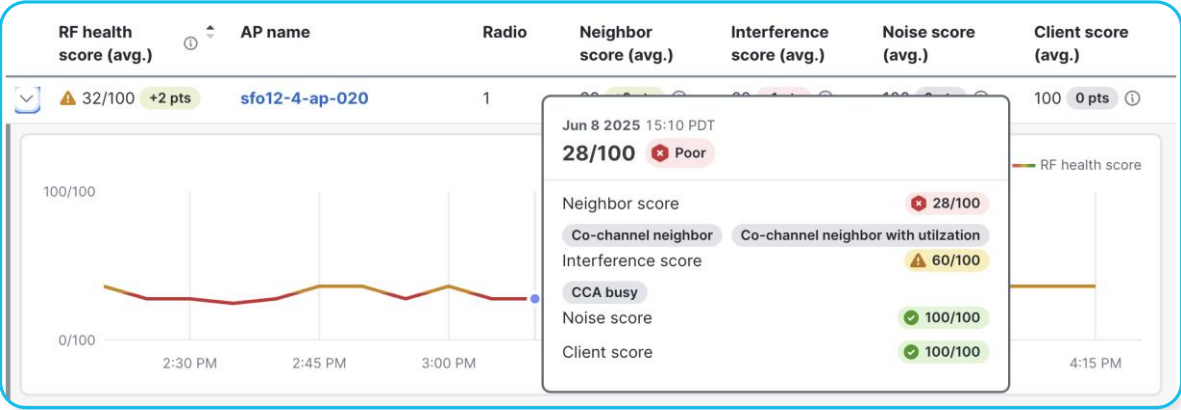
RF Settings/ Overview



Health score tier

- 61– 100 : Good
- 31– 60 : Fair
- 0– 30 : Poor

Assurance Overview / RF Health

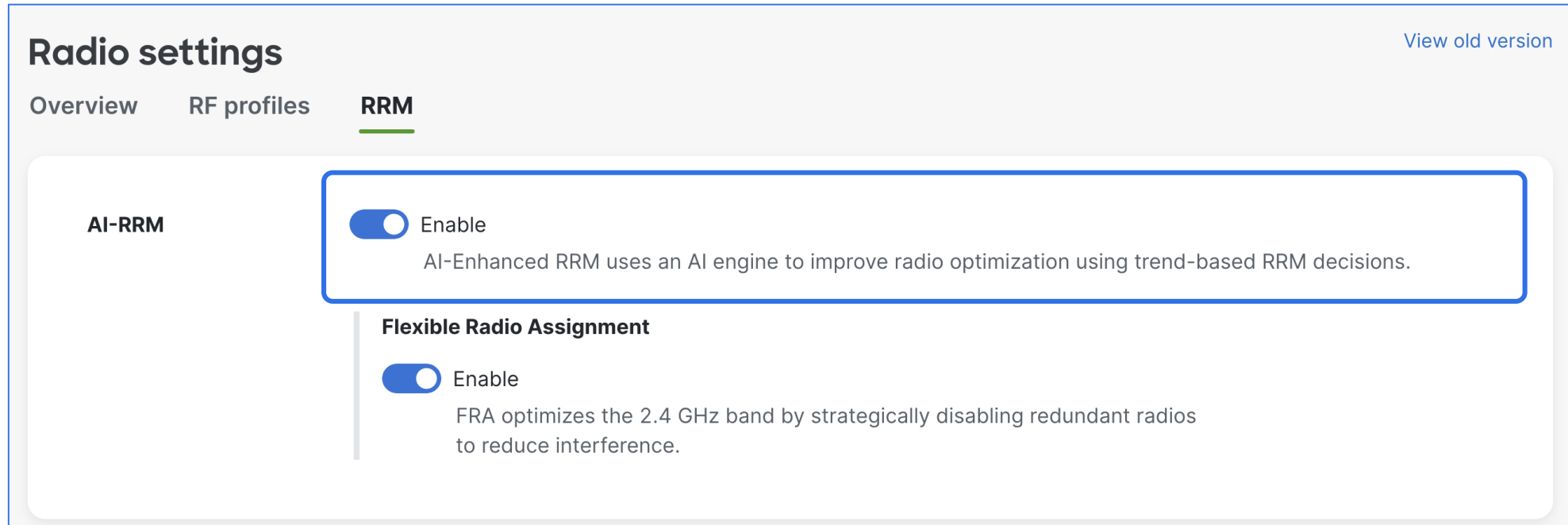


Most common RF score impacting KPI

Reason	Causes
Co-channel neighbors	High channel reuse
Co-channel neighbor with utilization	High ch. reuse with busy neighbor AP
CCA Busy	Too many Rogue APs

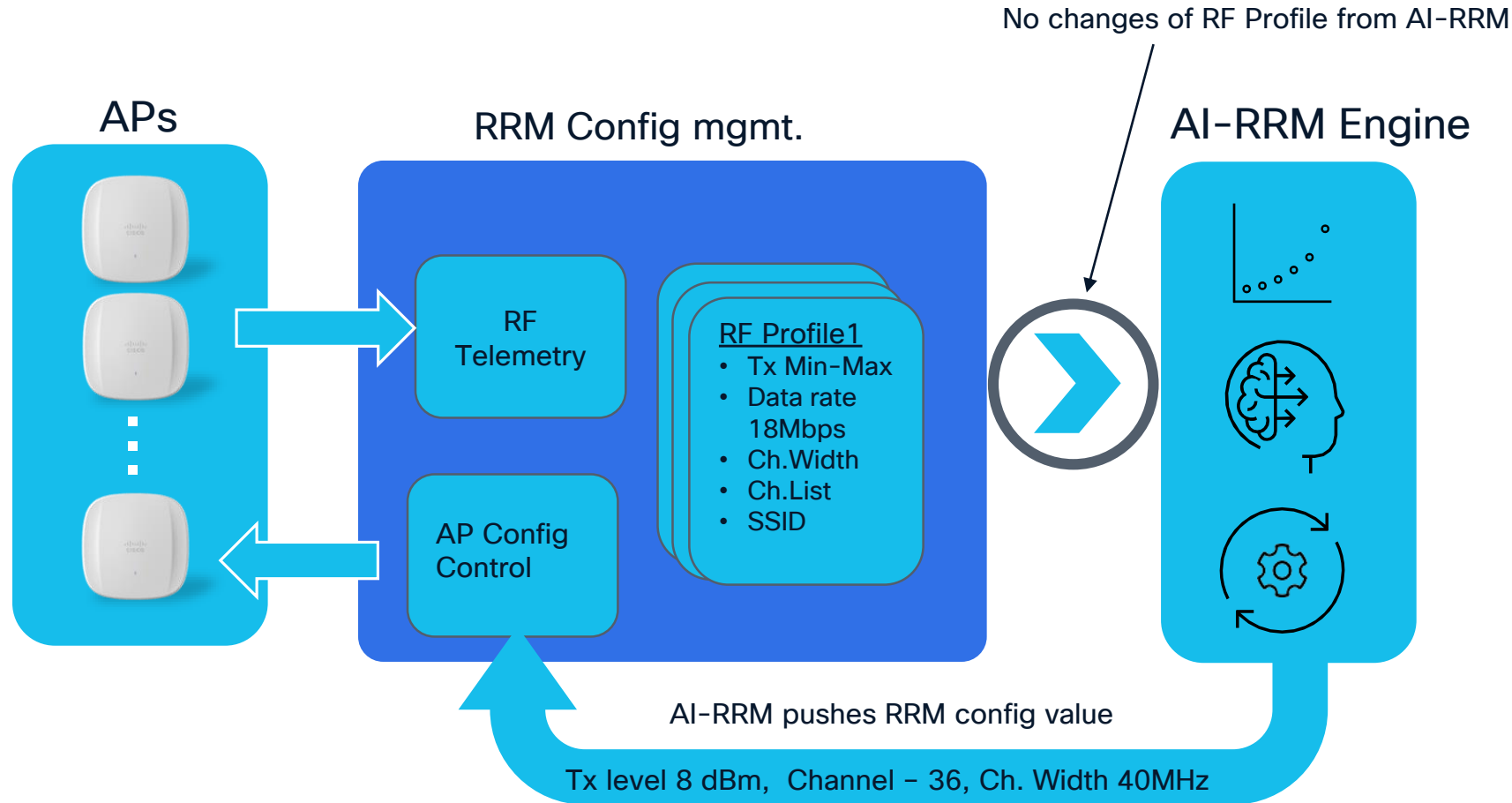
AI-RRM UX/UI Principal

Insanely Simplified, seamless RF Brain transplant



- Just one click to turn on AI-RRM
- Keep Everything else – RF Profiles or any other existing configs “as-is”
- No separate config page or changes required.

AI-RRM provides the best outcome within given RF Profile settings



- No Changes in the existing RF Profile
- AI-RRM optimize RF configuration within the RF profile policy
- RF Health and performance evaluation will happen all the time
- Unlikely scenario, AI-RRM service failure, RF optimization will fall back to traditional RRM

AI-RRM provides clear reasons of what and why

Meraki Dashboard

Network > Event log > **All AI-Enhanced RRM** event type

Auto Channel Update « hide		Auto Channel Update « hide	
New_Channel	153/20	New_Channel	56/20
Old_Channel	136/20	Old_Channel	161/20
Band	5	Band	5
Radio	1	Radio	1
Event_Reason	-Interference -82 in new channel is less than old channel interference -78	Event_Reason	-Duty cycle(rogue traffic amount) 1% in new channel is less than old channel duty cycle 3%

Time (PDT)	Access point	SSID	Client	Category	Event type	Details
Jun 9 01:18:22	sfo12-2-ap-27			AI-Enhanced RRM	AI-Driven Channel Change	Auto Channel Update « hide New_Channel 153/20 Old_Channel 136/20 Band 5 Radio 1 Event_Reason -Interference -82 in new channel is less than old channel interference -78
Jun 9 01:18:22	sfo12-4-ap-030			AI-Enhanced RRM	AI-Driven Channel Change	Auto Channel Update more » Auto Channel Update « hide New_Channel 56/20 Old_Channel 161/20 Band 5 Radio 1 Event_Reason -Duty cycle(rogue traffic amount) 1% in new channel is less than old channel duty cycle 3%
Jun 9 01:18:22	sfo12-2-ap-37			AI-Enhanced RRM	AI-Driven Channel Change	Auto Channel Update « hide New_Channel 56/20 Old_Channel 161/20 Band 5 Radio 1 Event_Reason -Duty cycle(rogue traffic amount) 1% in new channel is less than old channel duty cycle 3%

Event type include:

All AI-Enhanced RRM

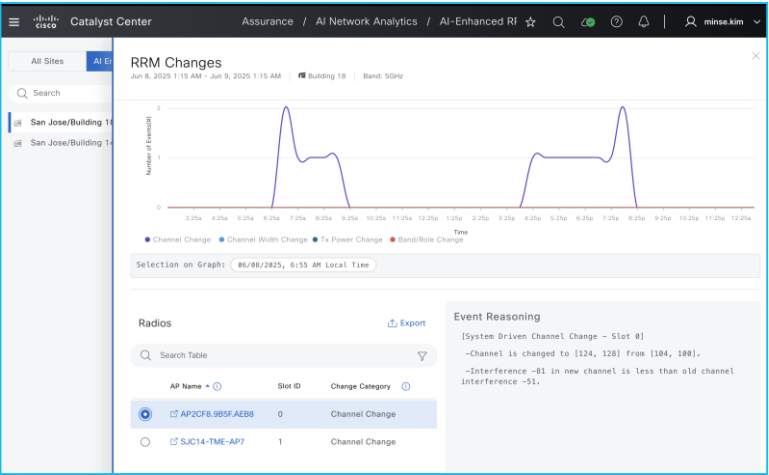
x

Catalyst Center

Assurance > AI Network Analytics
> **Building** > **RRM changes**

Event Reasoning

[System Driven Channel Change - Slot 0]
-Channel is changed to [124, 128] from [104, 100].
-Interference -81 in new channel is less than old channel interference -51.



AI-RRM vs. RRM networks

AI-RRM uses **x1,344** times larger RF statistics data to calculate next best channel

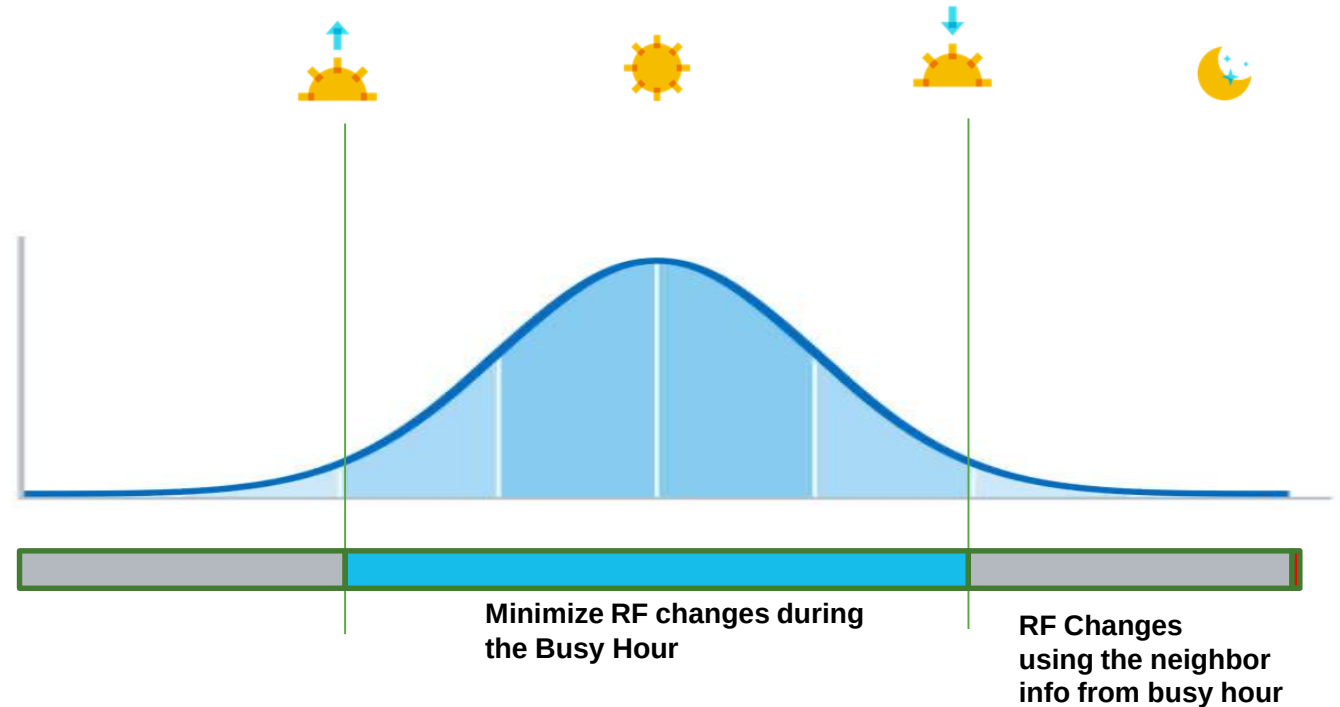
	RF config model	Base RF Optimization	Base RF Optimization duration	Advanced Optimization	Assurance	Architecture	License Tier
AI-RRM	RF Profile	Trend-based	2 Weeks = 20,160 min	- Enhanced Busy Hour - AI Channel Planning - Flexible Radio Assignment	- RF Health - RF Dashboard - Before-After analytics - Peer Comparison	Unified AI-RRM Cloud	- MR-ADV - Advantage Subscription
RRM (autoRF)	RF Profile	Snapshot-based	15 min	- Busy Hour - AI Channel Planning	RF Health	Meraki Cloud hosted	- MR-ENT - Essential Subscription

- RRM and AI-RRM uses common RF Profile configuration
- Switching between AI-RRM and RRM happens seamlessly
- AI-RRM services is available for MR-ENT customers as a trial services

Minimize Channel-Change in Busy Hour

AI Busy Hour

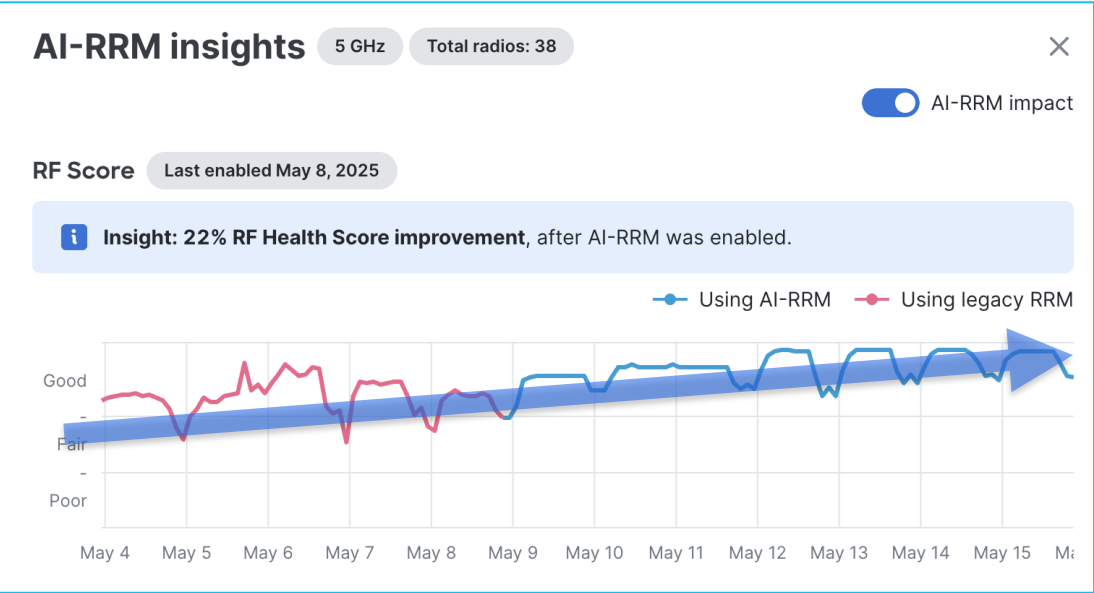
- Busy Hour can be either automatically or manually configured
- Every Changes are done off hour, using busy hour data.
- Avoid client disconnection or roaming due to channel change



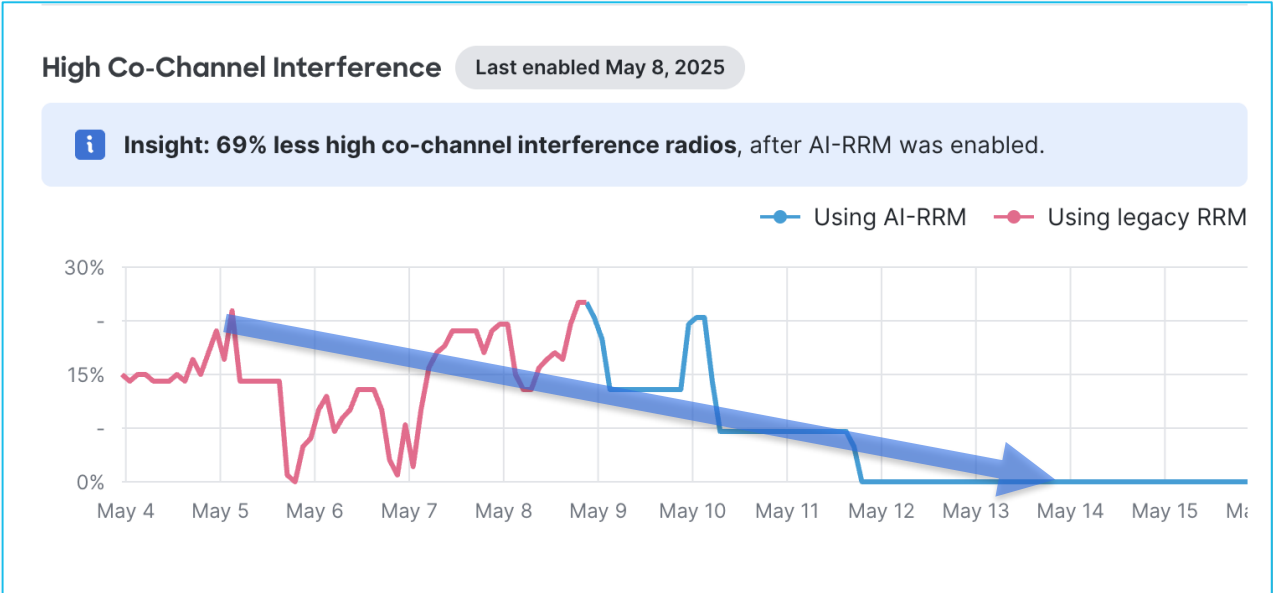
AI-RRM Before & After – Measurable AI Advantage

Typical Network examples with medium network density – (AP Density of 9)

+22% RF health score improvements



-69% less High Co-Channel Interference

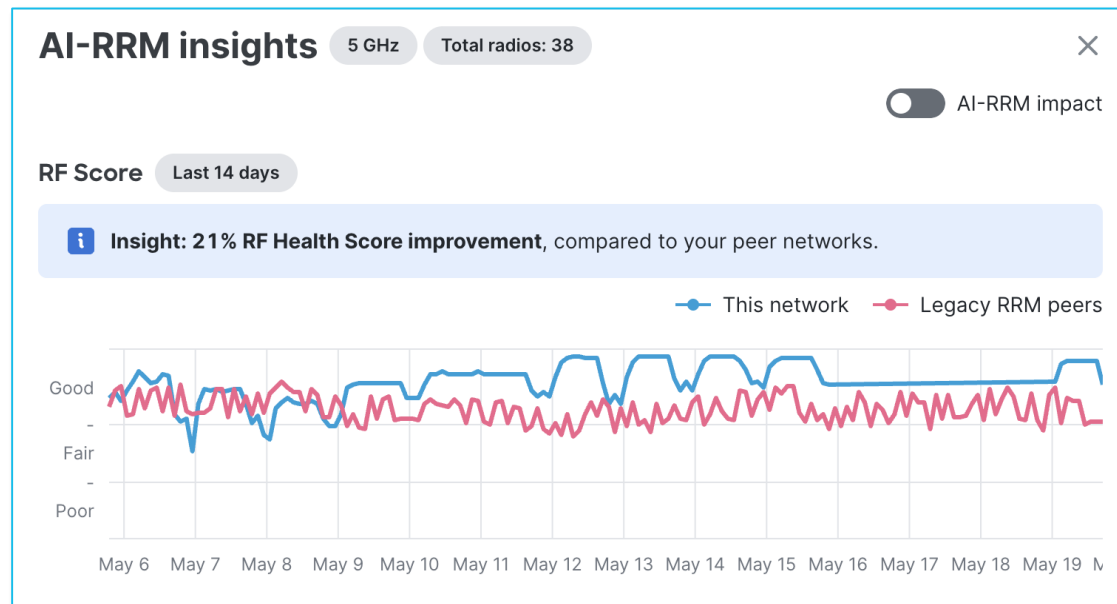


- Red Before AI-RRM gets enabled, using legacy RRM (autoRF)
- Blue After customer enabled AI-RRM

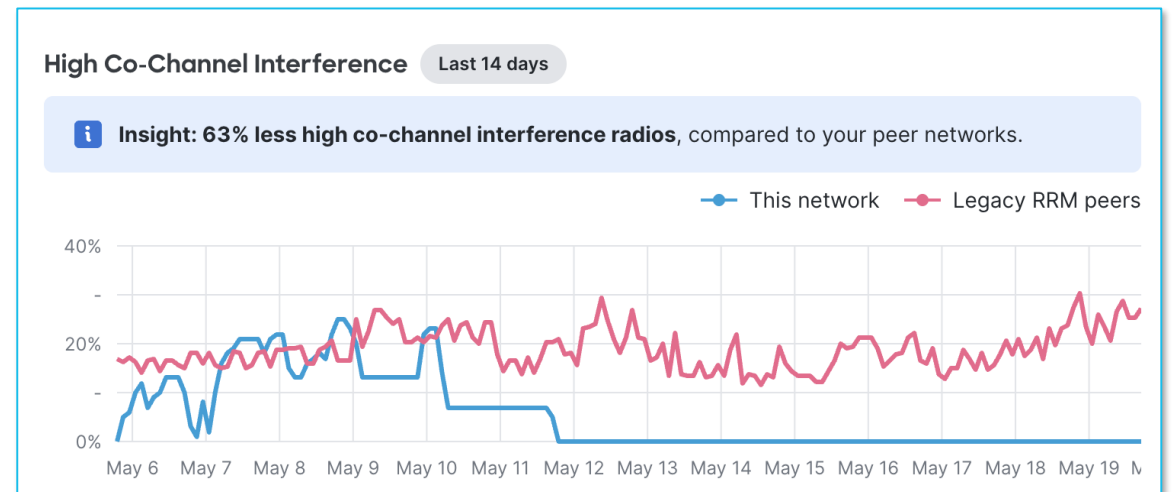
Comparison with peer networks that has same AP density as my network

Typical Network examples with medium network density – (AP Density of 9)

+21% RF health score improvements



-63% less High Co-Channel Interference



Red

Before AI-RRM gets enabled, using legacy RRM (autoRF)

Blue

After customer enabled AI-RRM

Demo – RF Optimization

AP Refresh/Deployment

AP provisioning steps for replace/upgrade case

Existing AP Refresh workflow



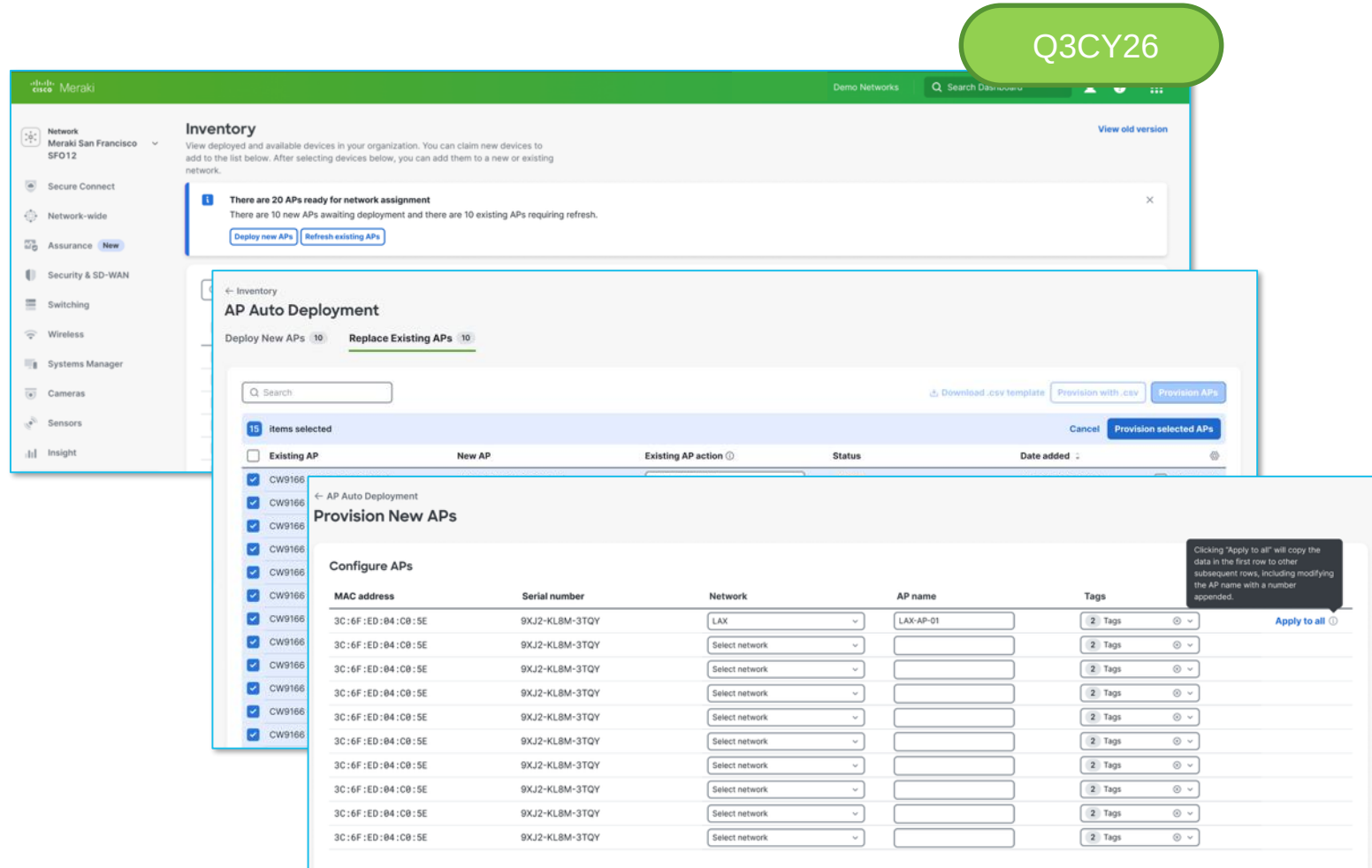
1. Claim new AP
2. Search claimed AP's installed network
3. Manually assign AP to right network
4. Go to old AP detail page, rename previous AP to old_AP Name
5. Search newly added AP, go to new AP detail page, change default AP to planned AP name
6. Add Tags to AP to assign SSID
7. Go to Configure>RF setting, Assign RF profile to newly added AP
8. Remove old AP from the network
9. Unclaim old AP from inventory to not waste cloud license
10. Connect AP to the network, wait for AP to come up online (DHCP, Cloud connectivity, FW updates)
11. Place AP to the floor using AP auto locate and/or third-party tool (e.g. Ekahau, Hamina)

Repeat all steps for each new AP installation - 100s to 1000s times per network

New - AP Zero-Touch Refresh

- Fully automated, Brownfield AP migrations
 - Automated Network discovery and assignment
 - Auto Discovery of AP location and configuration using “any” switch in the network. Cisco Switch (MS or Cat) or 3rd party switch
 - Switch doesn’t need to be added to the network to get discovered
 - Support both Wireless network and Combined Network
- New AP takes the identity of the old AP
- New Bulk AP provisioning CSV and API workflows as well
- Save time and \$\$\$ when you upgrade APs with Cisco !!

Q3CY26



The screenshot illustrates the Meraki dashboard interface for AP Zero-Touch Refresh. It shows the 'Inventory' page with a notification for 20 APs ready for network assignment. The 'AP Auto Deployment' page is active, showing a list of 10 items selected for replacement. The 'Provision New APs' page is also visible, showing a table for configuring APs with columns for MAC address, Serial number, Network, AP name, and Tags. An 'Apply to all' button is visible at the bottom right of the table.

MAC address	Serial number	Network	AP name	Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	LAX	LAX-AP-01	2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags
3C:6F:ED:04:C0:5E	9XJ2-KLBM-3TQY	Select network		2 Tags

Simplified AP Provisioning process

New! AP Refresh workflow



1.Claim new AP

Just confirm the AP config migration with a single click

10.Connect AP to the network, wait for AP to come up online (DHCP, Cloud connectivity, FW updates)

11.Place AP to the floor using AP auto locate and/or third-party tool (e.g. Ekahau, Hamina)

Bulk AP provisioning, 1000s of AP configurations in just single click action.

Admin

[View old version](#)

 The new onboarding experience for cloud-managed Catalyst switches is now available. Easily onboard your Catalyst switches into hybrid or cloud operating mode. [Learn more](#)

Adaptations

status

Download ▾

+ Claim devices

Demo – AP Zerotouch Refresh

Cisco AI Assistant

- Wireless use-case

Cisco AI Assistant

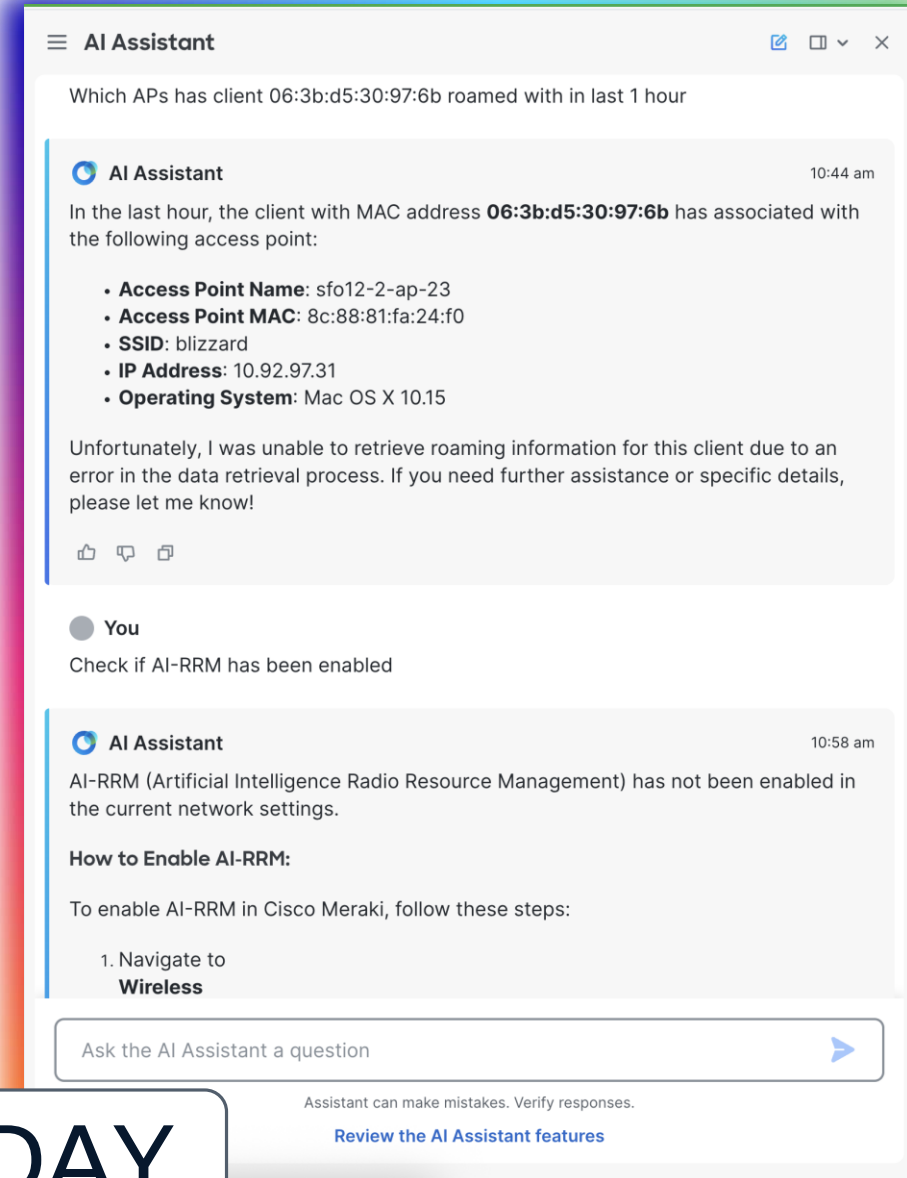
Native, GenAI-based Agentic Network Interface

- Understand Wireless, Wired, WAN and Internet networking experience
- Understand unique network contexts such as Network Telemetry, Configuration, Firmware
- Answers dynamic network inquiries and answers
- Dynamic query parameter derivations and composite

Documentation and Best Practice Recommendations

- Acknowledge existing network configuration and provide the best practice network configuration

Available TODAY



Cisco AI Assistant Use-cases

Top-down discovery

- Uncertainly to certain
- Proactive Discovery
- Org-wide or Network-wide inquiries and reply

Monitoring

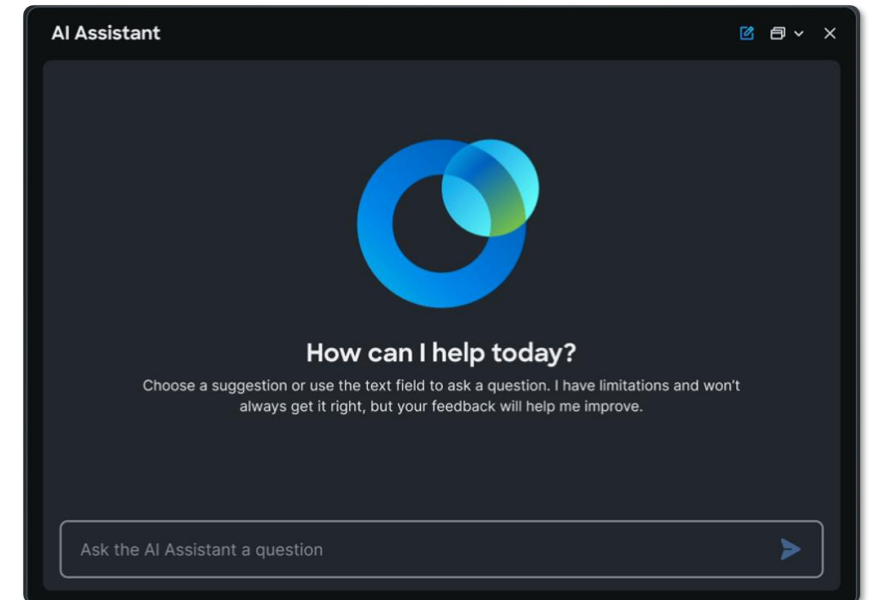
- Various quires and ad-hoc questions around all things such as inventory, device & Network configuration check, Firmware, device and client log, events, statistics and many more!

Bottom-up troubleshooting

- Notification Driven
- Client Troubleshooting
- Drill-Down deep into the RCA

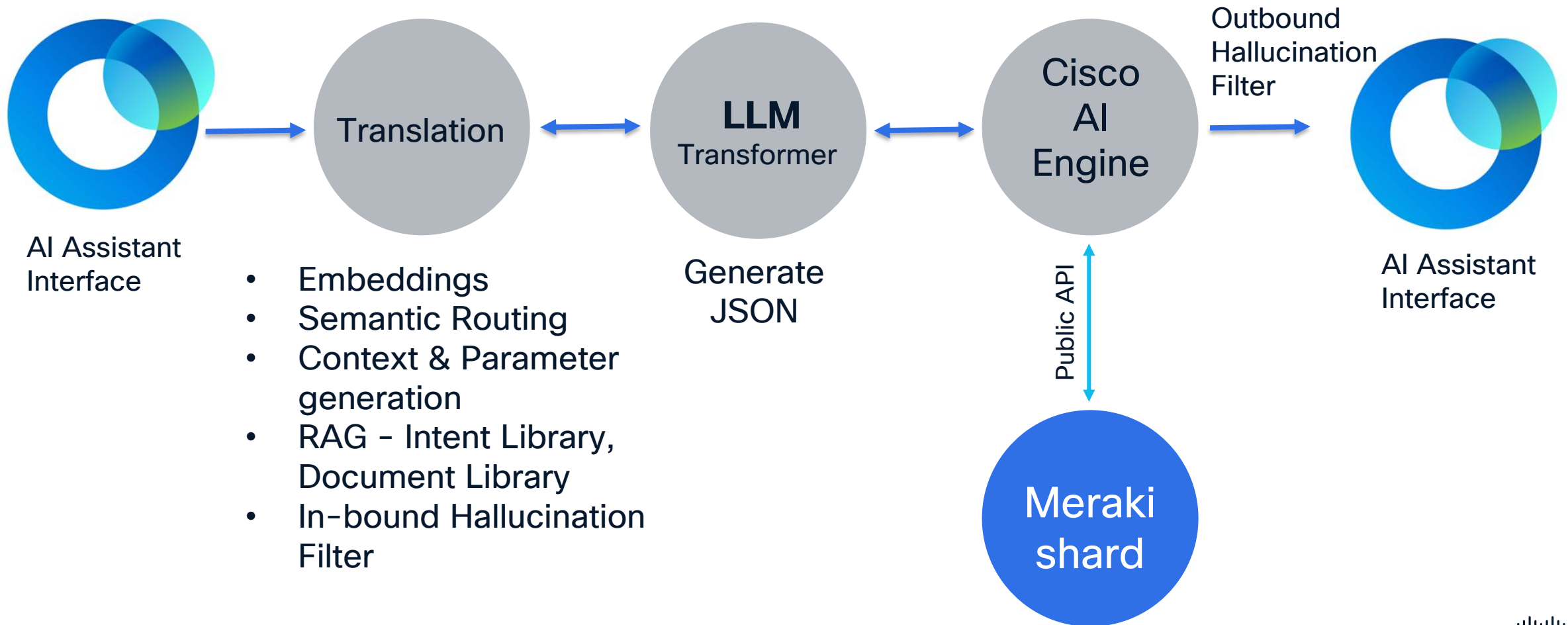
Configuration

- Guided workflows by Agentic Intelligence.
- Enable AI-driven multi-step and multi-system Workflows
- All based on Cisco's validated designs.
- Create a WLAN Network to RADIUS configurations



AI Assistant for Networking Architecture

In a nutshell

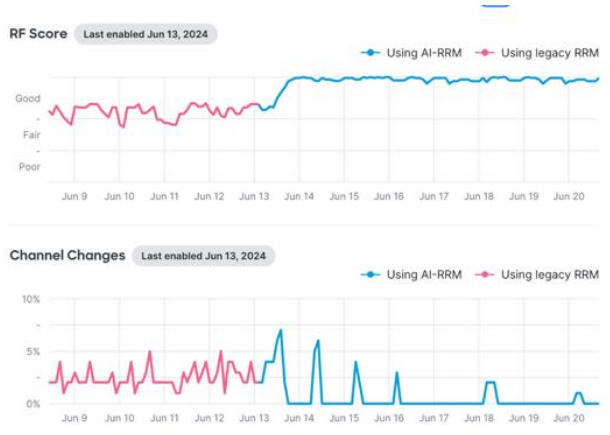


Demo – Cisco AI Assistant

Wireless use-case

Conclusion

Conclusion: AI Wireless designed to offer productivity operation efficiency



Visible impact of Before & After AI-RRM

Time	Source	Destination	Protocol	Details
1 0.000000	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A dns.mstncl.com
2 0.390151	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A dns.mstncl.com
3 0.780715	fe80::1a2b:1b1b:1b1b:1b1b	ff02::1:2	DHCP	Solicit XID: 0x00000000 ID: 000100012a041054e1
4 1.485498	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A dns.mstncl.com
5 3.981512	CiscoMer_00:00:00:00:00:00	192.168.129.45	HTTP	GET / Root = 00000000000000000000000000000000
6 1.837274	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A self.events.data.micr
7 2.014238	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A dns.mstncl.com
8 3.380030	CiscoMer_00:00:00:00:00:00	192.168.129.45	HTTP	Who has 192.168.128.2? Tell 192.168.128.1
9 3.381814	LCF0HfE_S1:fa5c	CiscoMer_00:00:00:00:00:00	ARP	192.168.128.2 is at 54:1ad:51:fa:5c
10 3.387856	192.168.128.2	192.168.129.45	ICMP	Echo (ping) request id=0x0001, seq=34/8784, ttl=
11 3.414848	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A dns.mstncl.com
12 3.897815	CiscoMer_00:00:00:00:00:00	192.168.129.45	HTTP	GET / Root = 00000000000000000000000000000000
13 4.007818	CiscoMer_00:00:00:00:00:00	192.168.129.45	HTTP	GET / Root = 00000000000000000000000000000000
14 5.080320	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A vpad.supportlab.iharen
15 6.027472	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A dns.mstncl.com
16 6.139917	CiscoMer_00:00:00:00:00:00	192.168.129.45	HTTP	Device ID: 14974324008 Port ID: 11
17 6.080997	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A vpad.supportlab.iharen
18 7.470000	192.168.128.2	192.168.129.45	DNS	Standard query 0x00000000 A dns.mstncl.com

Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: LCF0HfE_S1:fa5c (54:1ad:51:fa:5c), Dst: CiscoMer_00:00:00:00:00:00 (8c:8d:00:00:00:00)
Destination: CiscoMer_00:00:00:00:00:00 (8c:8d:00:00:00:00)
Source: LCF0HfE_S1:fa5c (54:1ad:51:fa:5c)
Type: IPv4 (0x0000)
Internet Protocol Version 4, Src: 192.168.128.2, Dst: 192.168.129.45
User Datagram Protocol, Src Port: 58977, Dst Port: 53
Domain Name System (query)

AI Assistant

Which APs has client 06:3b:d5:30:97:6b roamed with in last 1 hour

AI Assistant 10:44 am

In the last hour, the client with MAC address **06:3b:d5:30:97:6b** has associated with the following access point:

- Access Point Name: sfo12-2-ap-23
- Access Point MAC: 8c:88:81:fa:24:f0
- SSID: blizzard
- IP Address: 10.92.97.31
- Operating System: Mac OS X 10.15

Unfortunately, I was unable to retrieve roaming information for this client due to an error in the data retrieval process. If you need further assistance or specific details, please let me know!

AI-RRM

- Using AI to tune and select channels best suited for your network
- Learning your network usage patterns to auto determine busy hours
- Optimizing to enhance client experience

Intelligent Captures

- Complex troubleshooting made simple
- Save expensive issue recreation cycles

AI Assistant

- Conversational Interface.
- Multi-domain Cisco AI Assistant

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 2026.



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.

Q> I want to learn more. Where to go next?

BRKEWN-3007

AI-RRM Under the hood
Technical AI Deep-dive

FULL CONFERENCE

IT LEADERSHIP

Demystifying the Role of AI in Your Cisco Wireless Deployments - BRKEWN-3007



Vishal Desai, Principal Wireless Architect, Cisco



Schedule

Monday, Jun 9 | 2:30 PM - 3:30 PM PDT | SDCC - Upper Level, Room 6B



BRKXAR-2028

Cisco AI Assistant
Technical Deep dive

FULL CONFERENCE

IT LEADERSHIP

AgenticOps in Motion: AI Agents Powering a Unified Cisco Experience - BRKXAR-2028



Richard Jang, Cisco - Distinguished Speaker



Schedule

Tuesday, Jun 10 | 2:00 PM - 3:30 PM PDT | SDCC - Mezzanine Level, Room 14A



BRKEWN-2399

Meraki Troubleshooting
Deep dive from Practitioner

FULL CONFERENCE

IT LEADERSHIP

Meraki Wireless from a Troubleshooter Perspective - BRKEWN-2399



Jakub Talalaj, Customer Escalations Engineering Technical Leader, Cisco

Schedule

Thursday, Jun 12 | 10:30 AM - 11:30 AM PDT | SDCC - Upper Level, Room 6B



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

Contact me at: @linkedin.com/in/minse-k

Thank you

CISCO Live !

