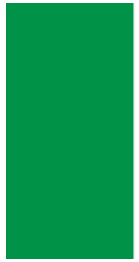
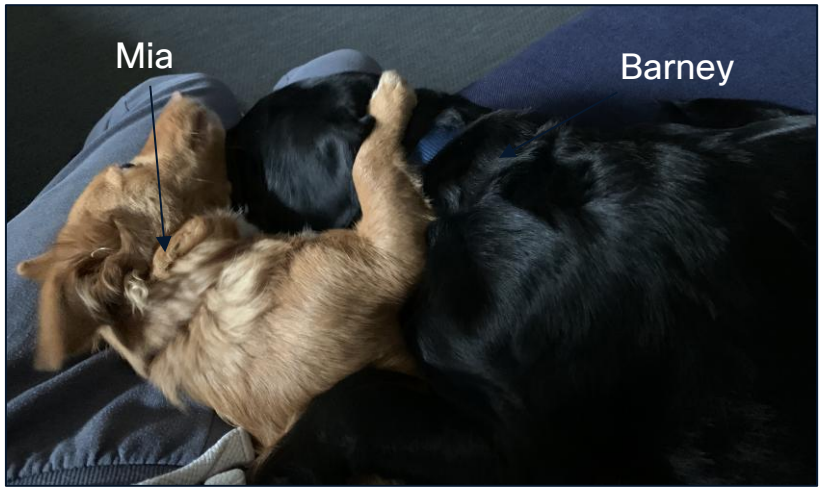
Design and Deploy Cisco Cloud Managed Enterprise Wireless Networks

Simone Arena
Distinguished TME, Cisco Wireless

Session ID: BRKEWN-2046

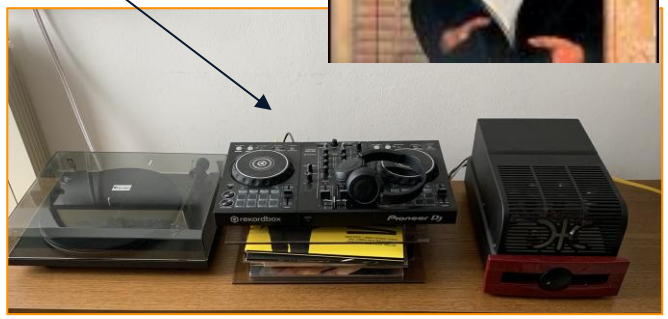
Who Am I?





The Boss, what else??

Tube amplifier



Le Pergole Torte Montevertine, 2020

Fiorentina soccer fan

Cisco Webex App

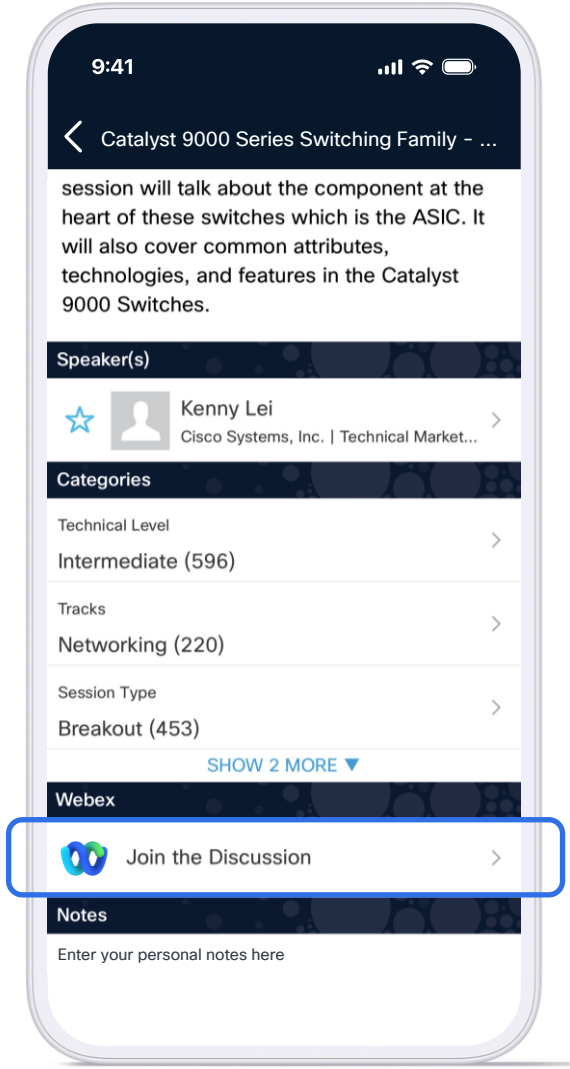
Questions?

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 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKEWN-2046**

Agenda

Cisco IT use case

01 Wireless Network Deployment

- 1.1 APs Deployment
- 1.2 RF Design
- 1.3 WLAN Design

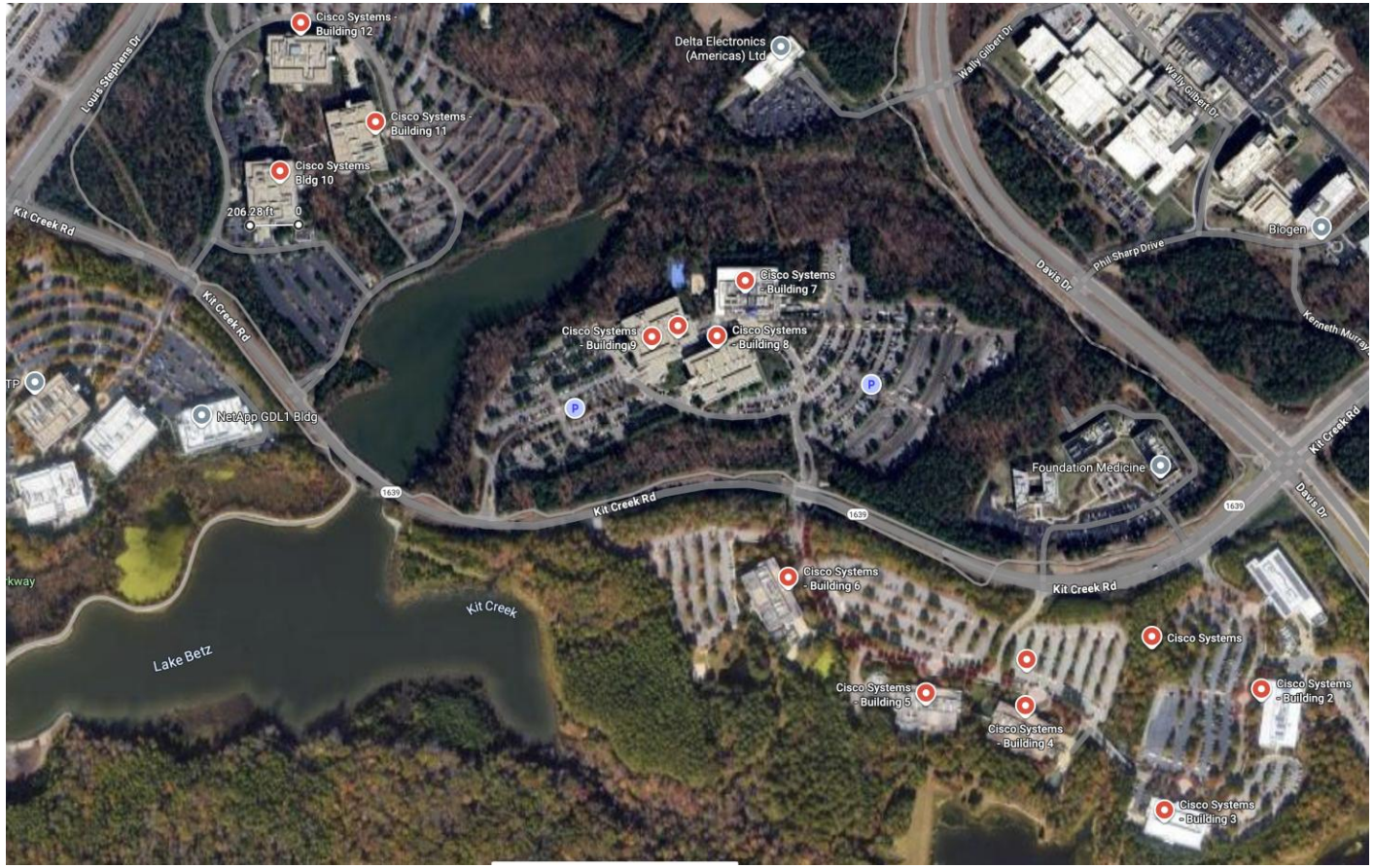
02 Wireless to Wired Design

- 2.1 Distribute or Centralize (the data plane)?
- 2.2 Best Practices

03 Monitoring and Troubleshooting

02 Conclusions

Research Triangle Park (RTP) Campus



- RTP is Raleigh, North Carolina
- Second largest Campus after San Jose
- Total 10 buildings. Each building is 60k sq. ft. (5600 sq. mt) and has three floors
- 1300 APs, peak of 4k clients per day
- Two SSIDs: Corporate and Guest
- Catalyst switch infrastructure
- Cisco ISE is used as AAA server

Reference use case: RTP Campus

Guess who lives here? Oh yes, it's TAC and CX

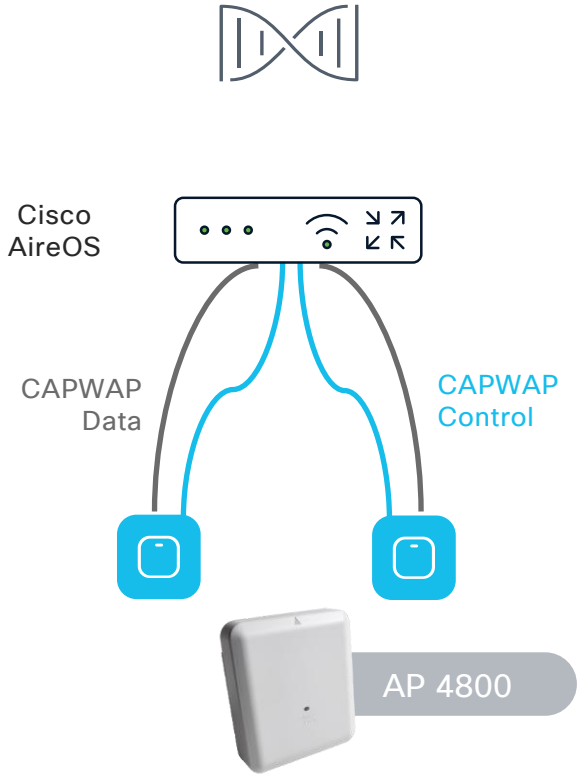
Top applications by usage

Application	Usage	% Usage
iperf	8.51 TB	23.08%
Encrypted TCP (SSL)	6.81 TB	18.46%
Apple services	3.04 TB	8.25%
Webex Video	2.55 TB	6.91%
DNS	1.35 TB	3.66%
Local Network SSL	1.35 TB	3.66%

RTP Campus – Cloud Management adoption

On-Prem

Cisco Catalyst Center

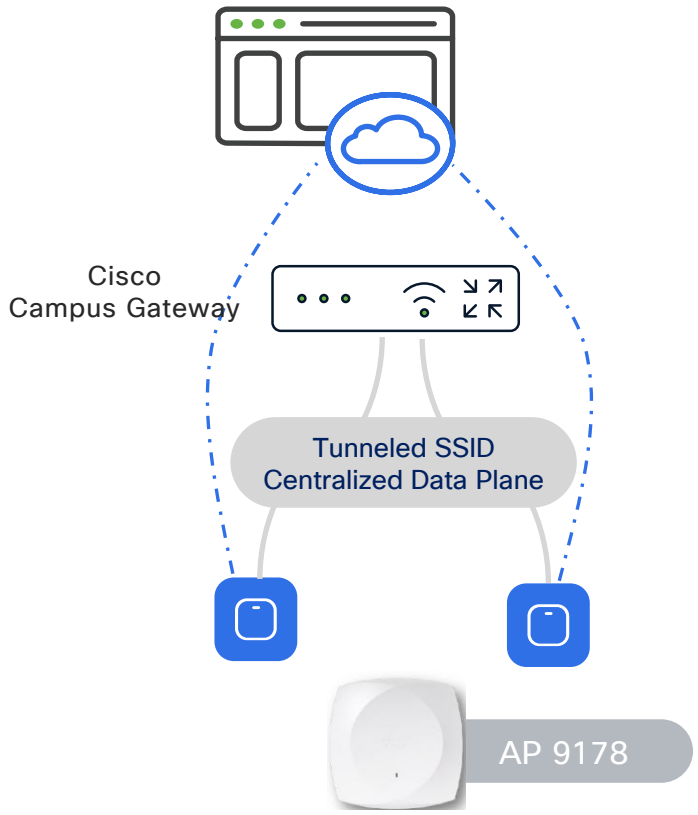


WHY? And WHY now?

- Wireless up for refresh
- Cloud Managed to streamline IT operations
- ”Eating our own dog food”
- Need Campus Gateway for scale
- Need some “Enterprise” features

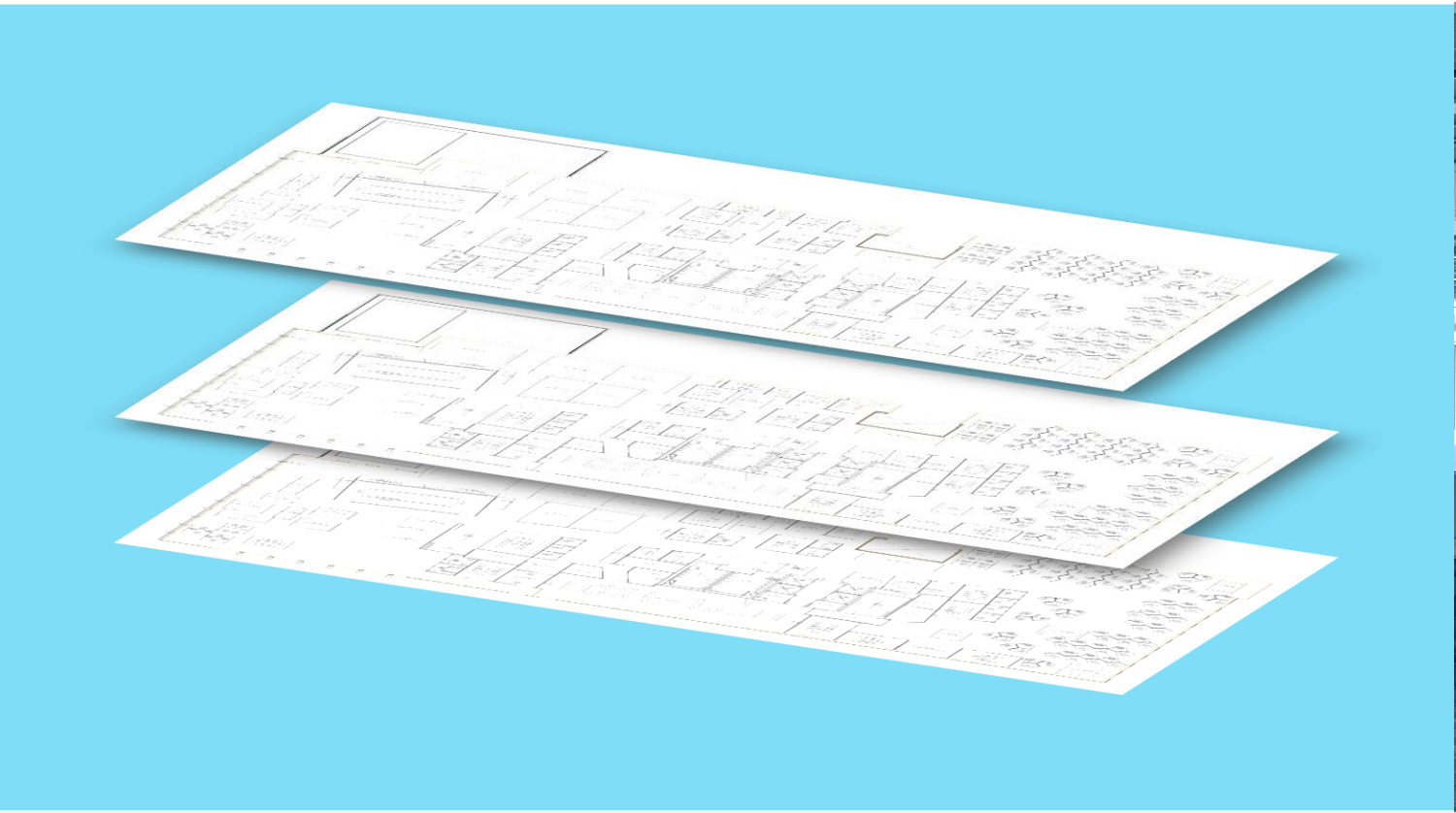
Cloud Management

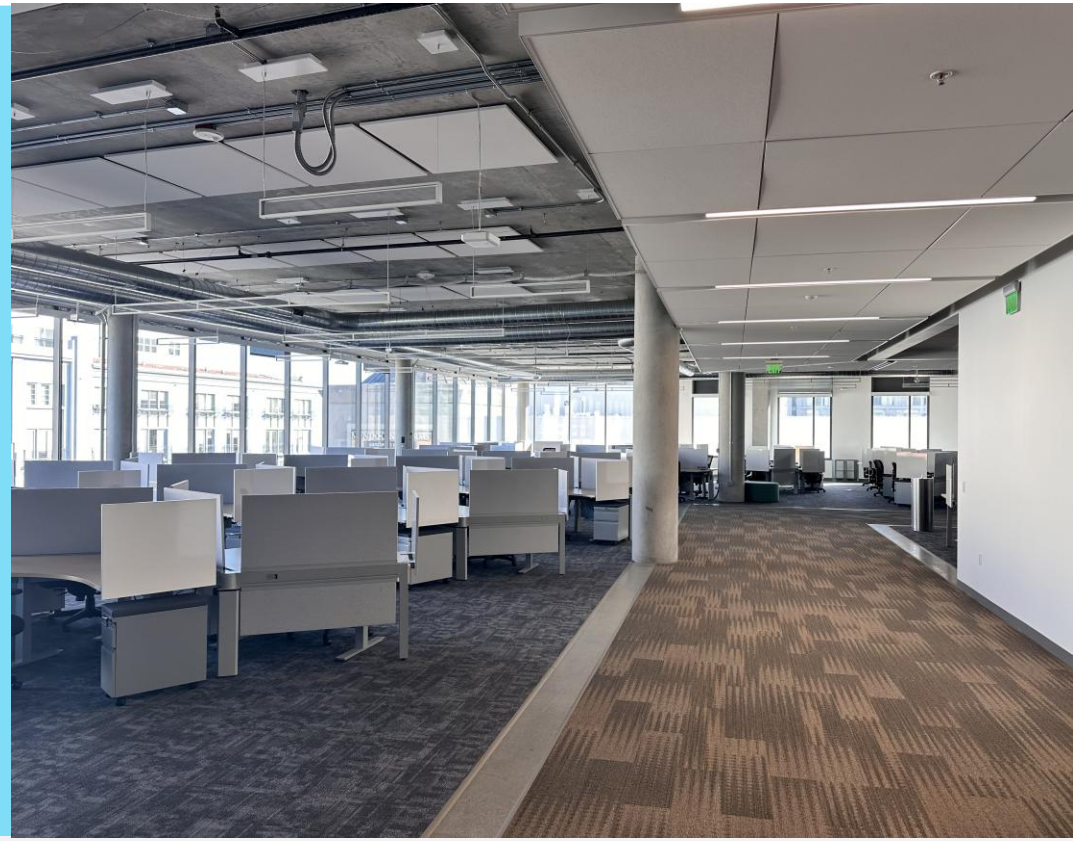
Meraki Dashboard



Wireless Network Deployment

RTP Buildings





Typical carpeted office: mix of open spaces and offices
Three floors, very similar layout across floors. Medium client density

Wi-Fi 7: what AP model?

CW9172H

6 Spatial Streams

Hospitality

CW9174E

8/10 Spatial Streams

External antennas

Dec 2025

CW9176D1

12 Spatial Streams

Integrated Directional

UWB

CW9179F

16 Spatial Streams

LPV/Stadium

CW9171I

4 Spatial Streams

Omnidirectional

Dec 2025

CW9172I

6 Spatial Streams

Omnidirectional

CW9174I

8/10 Spatial Streams

Omnidirectional

Dec 2025

CW9176I

12 Spatial Streams

Omnidirectional

UWB

CW9178I

16 Spatial Streams

Omnidirectional

UWB

Wi-Fi 7 | Global Use AP | Unified License | AI Optimized

cisco

Cisco Wireless 9178 Access Point

Cisco® Wireless 9178

Global Use AP, Tri-Radio with 16 Spatial Streams!

Hexa-Radio Architecture

- 2.4 GHz Serving Radio 4x4:4SS
- 5 GHz Serving Radio 4x4:4SS
- 5 GHz Serving Radio 4x4:4SS*
- 6 GHz Serving Radio 4x4:4SS
- Dedicated Tri-band scanning Radio (AI/ML)
- 2.4 GHz IoT Radio

** 5GHz – Single or Dual Radio, Default Operation – Single 5GHz Radio*

- 10 Gig Dual Ethernet
- PoE & Link Redundancy

- Omni directional: 2.4 GHz: 4dBi, 5 GHz: 5 dBi, 6GHz: 6dBi
- Built-in UWB, GPS/GNSS Location capabilities
- External GPS/GNSS Antenna Port*
- IoT: 2.4 GHz IoT Radio, Application Hosting Technology
- Built-in USB Port: 9W of output power

Same model for Cloud and On-prem!

Cisco Wireless 9178 Access Point

Hexa-Radio Architecture

- 2.4 GHz Serving Radio 4x4:4SS
- 5 GHz Serving Radio 4x4:4SS
- 5 GHz Serving Radio 4x4:4SS*
- 6 GHz Serving Radio 4x4:4SS
- Dedicated Tri-band scanning Radio (AI/ML)
- 2.4 GHz IoT Radio

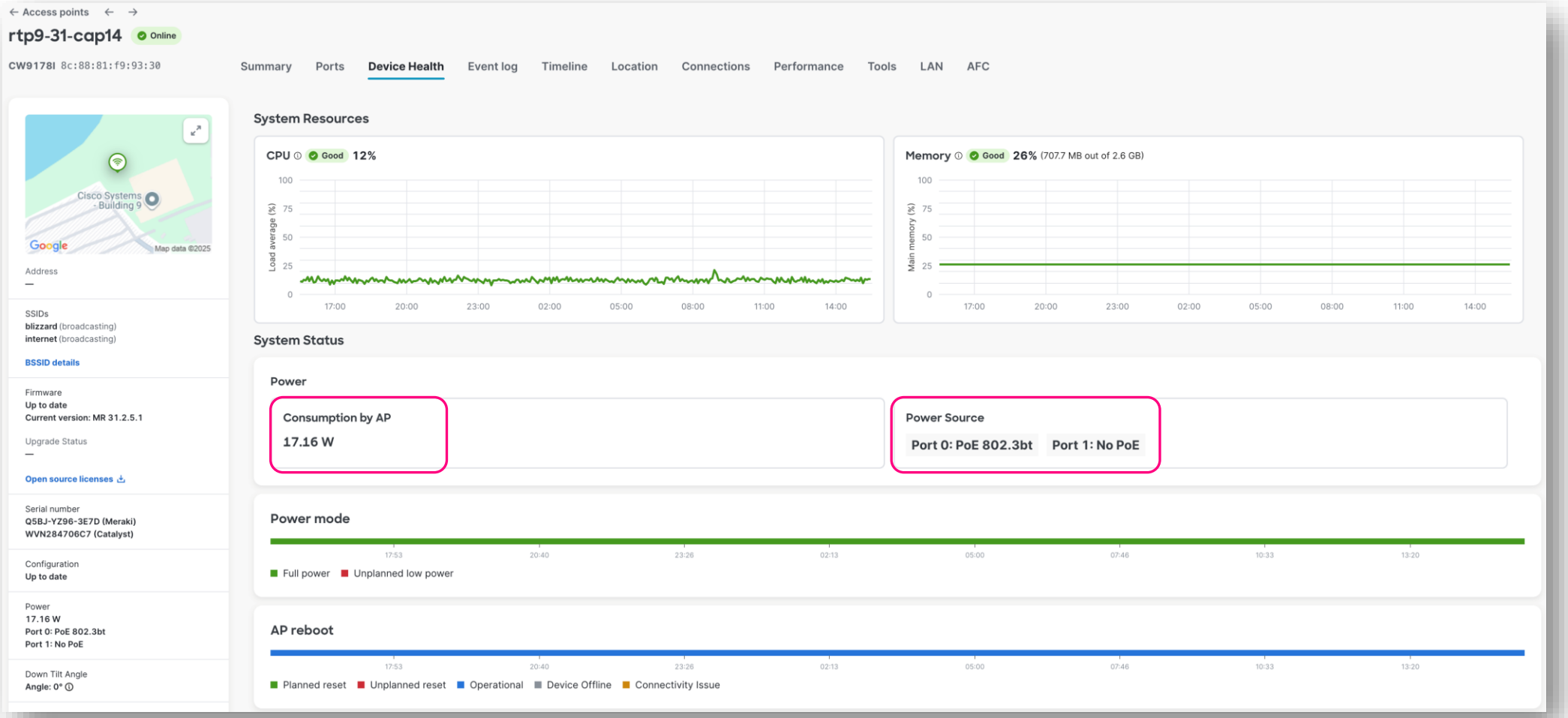
** 5GHz – Single or Dual Radio*

- 10 Gig Dual Ethernet
- PoE & Link Redundancy

- Omni directional: 2.4 GHz: 4dBi, 5 GHz: 5 dBi, 6GHz: 6dBi
- Built-in UWB, GPS/GNSS Location capabilities
- External GPS/GNSS Antenna Port*
- IoT: 2.4 GHz IoT Radio, Application Hosting Technology
- Built-in USB Port: 9W of output power

Wi-Fi 7: Enough power on the switch?

New Device Health tab will tell you...



CW9178I Power over Ethernet

Default Configuration (Fixed Power profile)

Power source	Number of spatial streams	2.4-GHz radio (slot 0)	Primary 5-GHz radio (slot 1)	Secondary 5-GHz radio (slot 2)	6-GHz radio (slot 3)	mGig PHY 0 link speed	mGig PHY 1 link speed	USB	IoT/GPS/UWB Scan Radio
802.3af (PoE)	NA	Disabled	Disabled		Disabled	1G	Disabled	Disabled	Y
802.3at* (PoE+) (Quad Radio)	8**	2x2	2x2 (LB)	2x2(HB)	2x2	2.5G	2.5G	Disabled	Y
802.3at* (PoE+) (Tri Radio)	8**	2x2	4x4(FB)	Disabled	2x2	2.5G	2.5G	Disabled	Y
802.3bt (PoE++/UPOE)	16	4x4	4x4(LB)	4x4(HB)	4x4	10G	10G	Yes/9W	Y

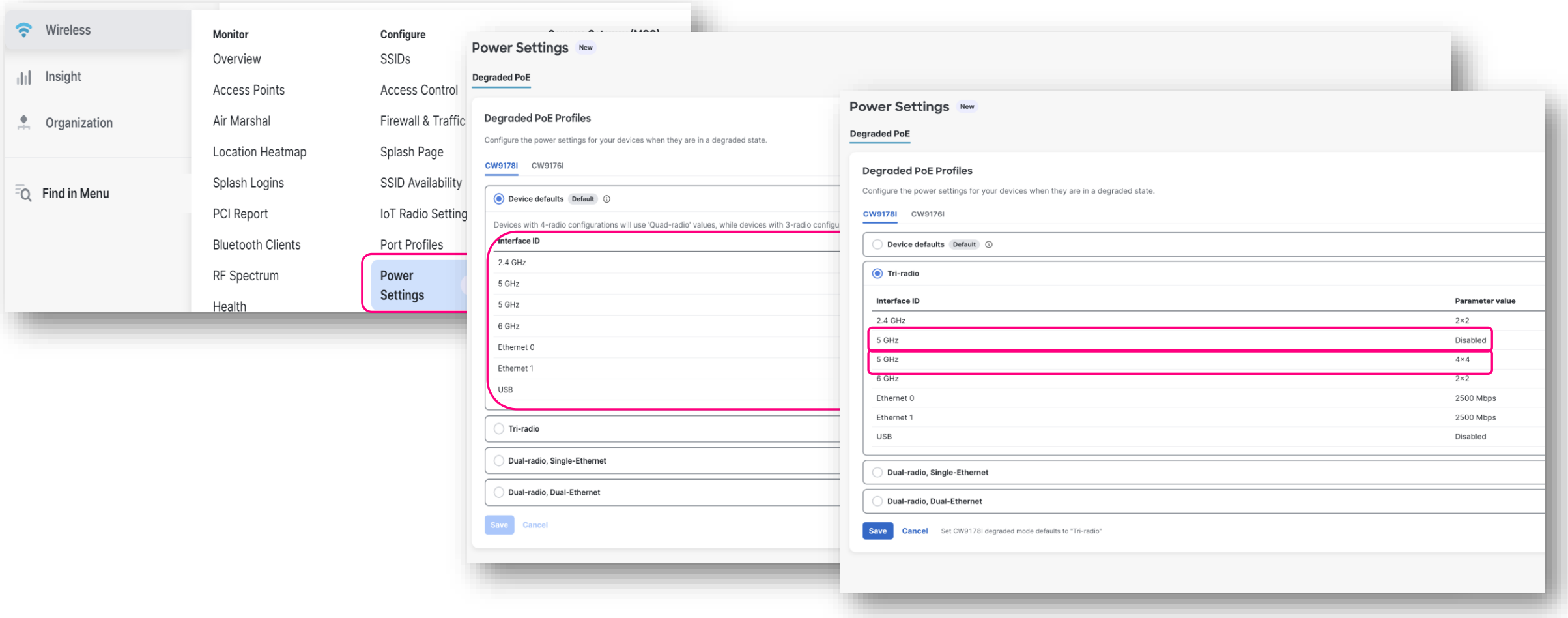
Note:

1. *For full radio operation – AP needs more than 30W of power with Type 3 IEEE 802.3bt/ Class 6
2. **Starting IOS-XE 17.15.3 release, 6 spatial streams support in IOS-XE 17.15.2, with 2x2:2 on 2.4/5/6 GHz radios
3. CW9178I can operate as a Tri-Radio with 5 GHz radio operating in 4x4 Full Band (or) operate as Quad-Radio with 5 GHz in Slot 1 as 4x4 Lower Band (UNII-1 &2) and Slot 2 as 4x4:4, Higher Band (UNII-2C&3)
4. CW-INJ-8, AIR-PWRINJ7, MA-INJ-6 are Cisco's 802.3bt power injectors

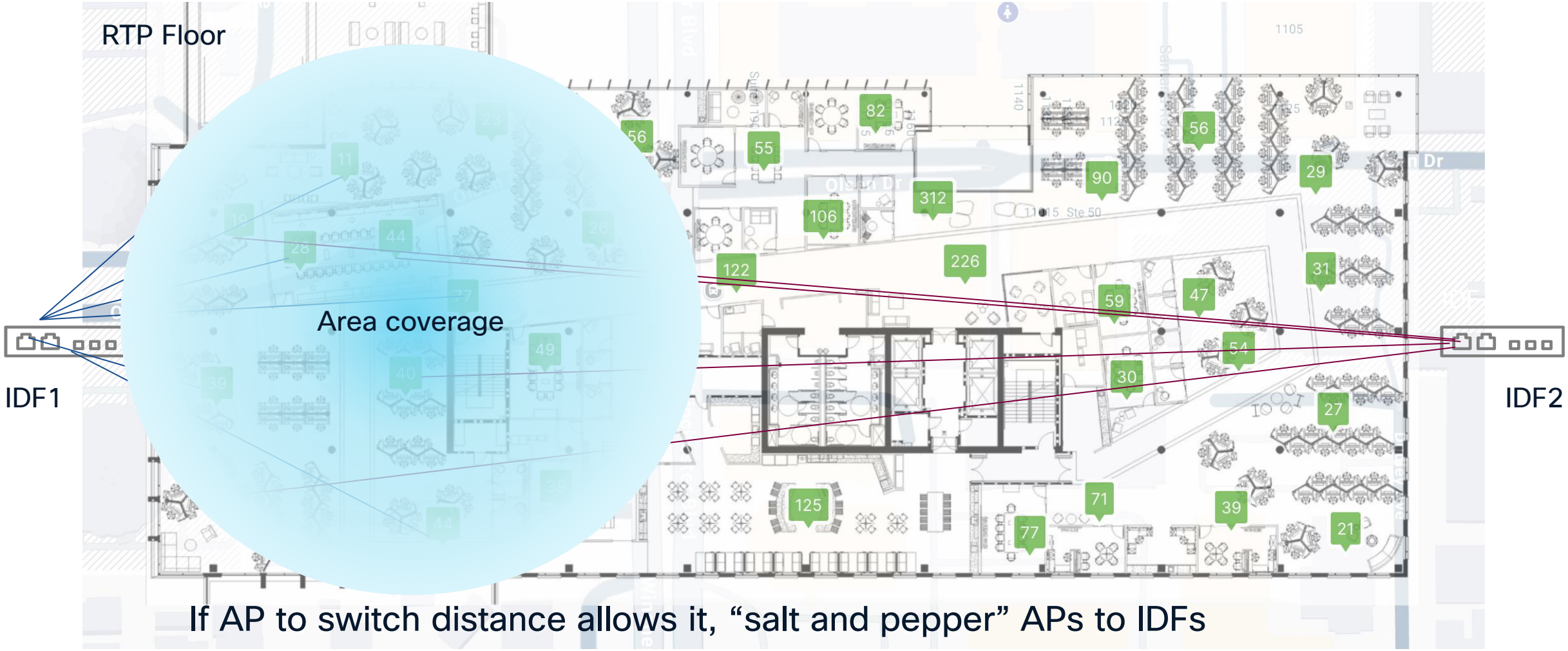
PHY = Physical layer
PoE = Power over Ethernet
UPoE = Universal Power over Ethernet
FB: Full 5Ghz band
LB: Lower 5Ghz band
FB: Higher 5Ghz band

Wi-Fi 7 – Enough power on the switch?

If you don’t have enough power, then you can use Power Profiles to decide what to power...

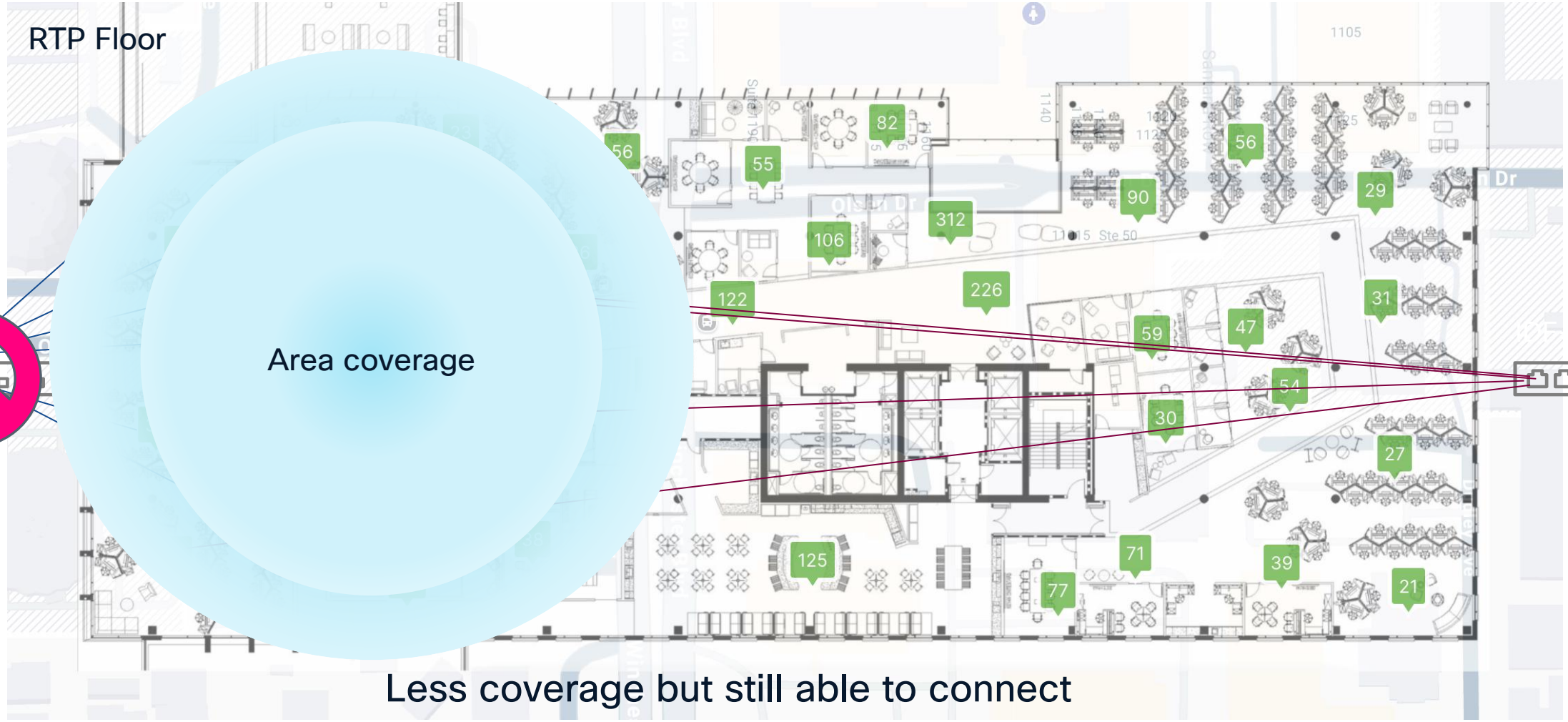


AP’s connection to the access switch



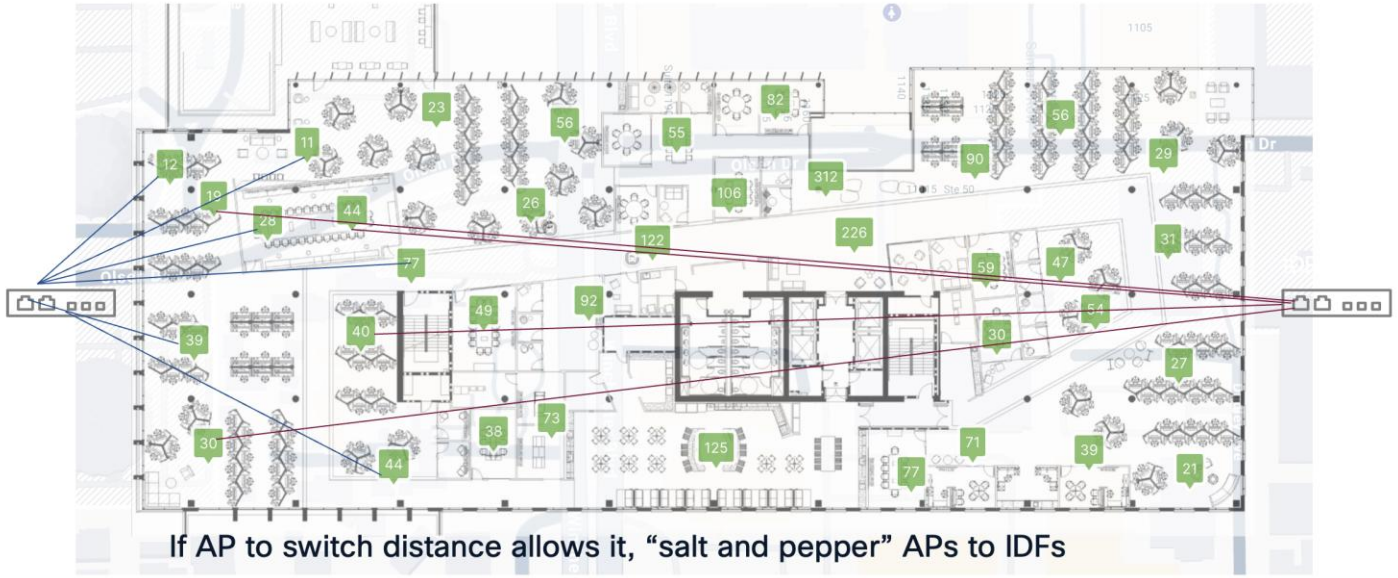
If AP to switch distance allows it, “salt and pepper” APs to IDFs

AP’s connection to the access switch



Less coverage but still able to connect

AP’s connection to the access switch

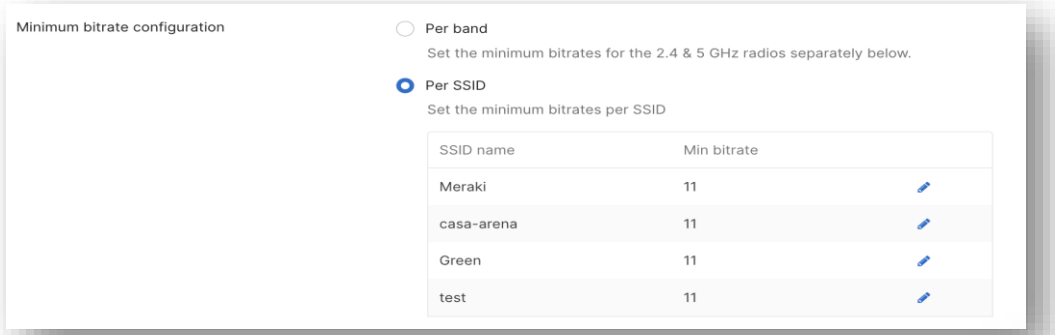


About “Salt and Pepper”

- Every other AP connected to a different switch or IDF
- Increases overall redundancy and high availability of the solution
- If one IDF goes down, coverage in an area of the floor is not lost, but capacity is reduced
- Should consider cable length and cost for wiring the APs to different IDFs
- For distributed data plane design (bridge mode) need same AP and client VLANs in both IDFs

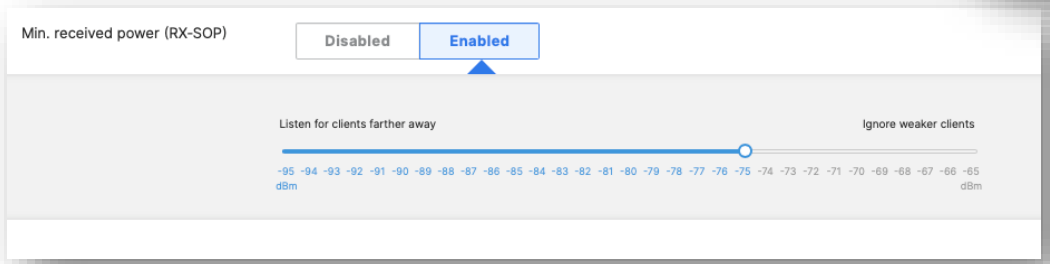
RF Design

Advanced RF features used

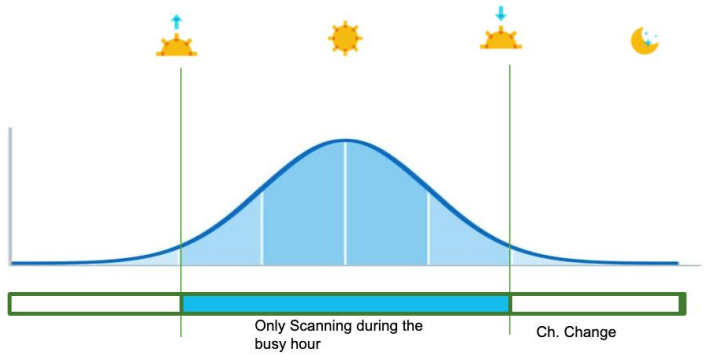


Per band vs per SSID settings

TX Power & Bit rate control

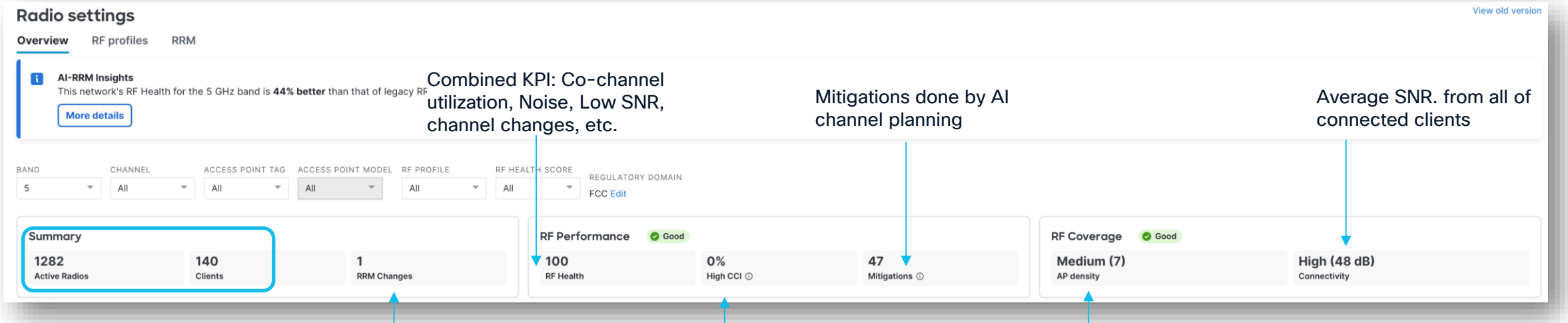


Fine tune with RX-SOP



AutoRF (RMM) > AI Enhanced RRM

RTP Campus - RF Profile



Combined KPI: Co-channel utilization, Noise, Low SNR, channel changes, etc.

Mitigations done by AI channel planning

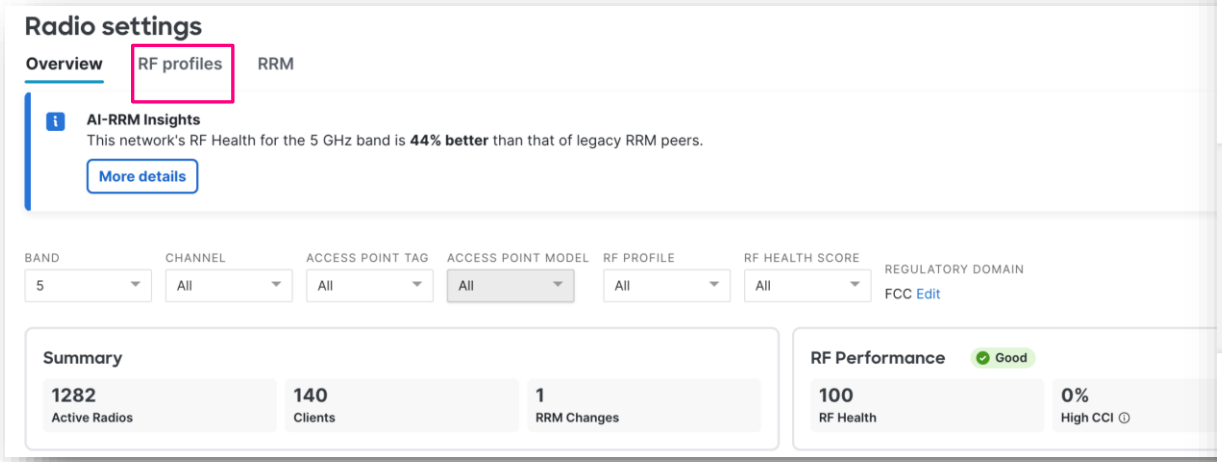
Average SNR. from all of connected clients

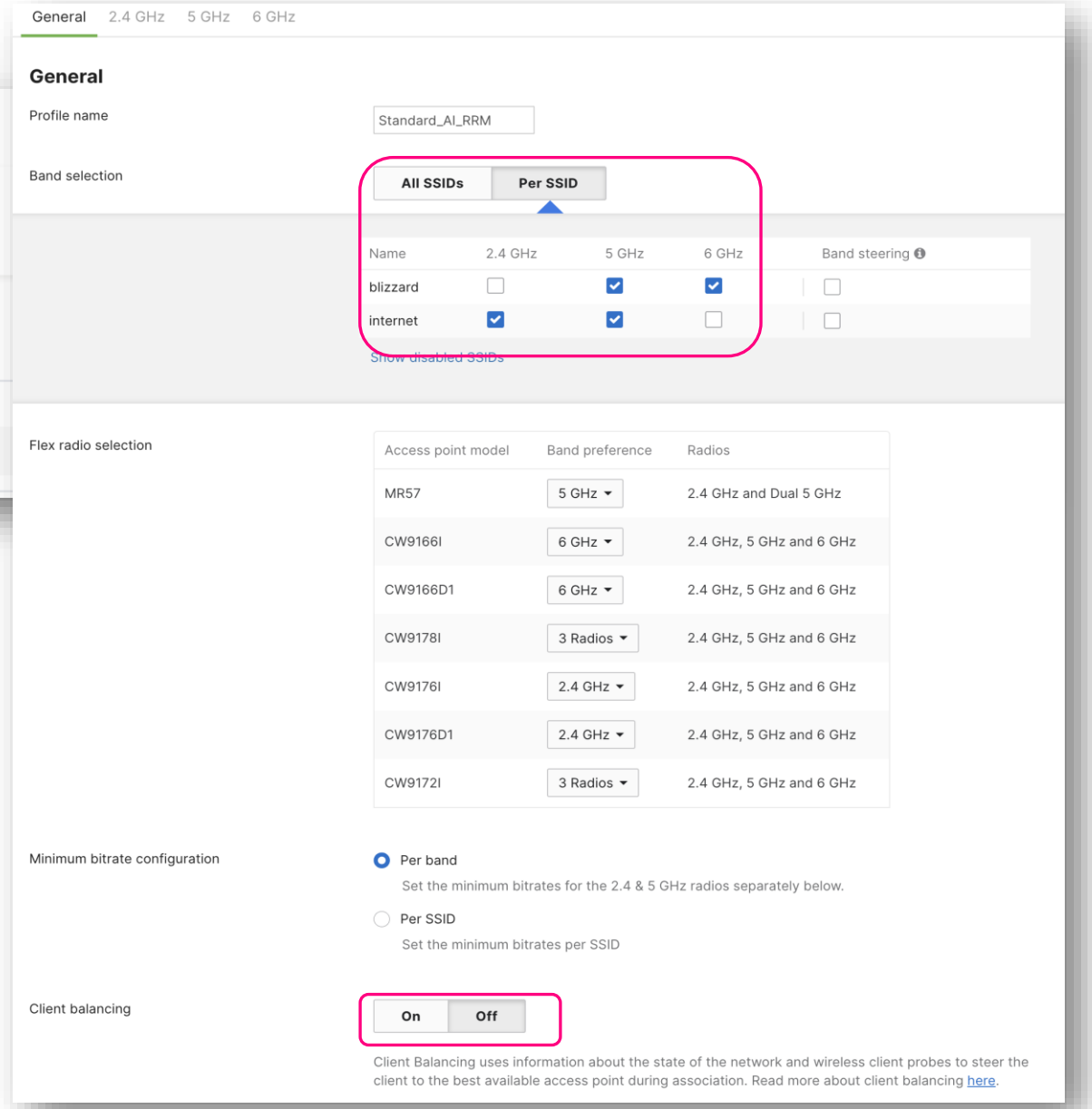
AI driven RRM changes

% APs with poor co-channel interference

Number of AP neighbors seen at or above -70 dBm

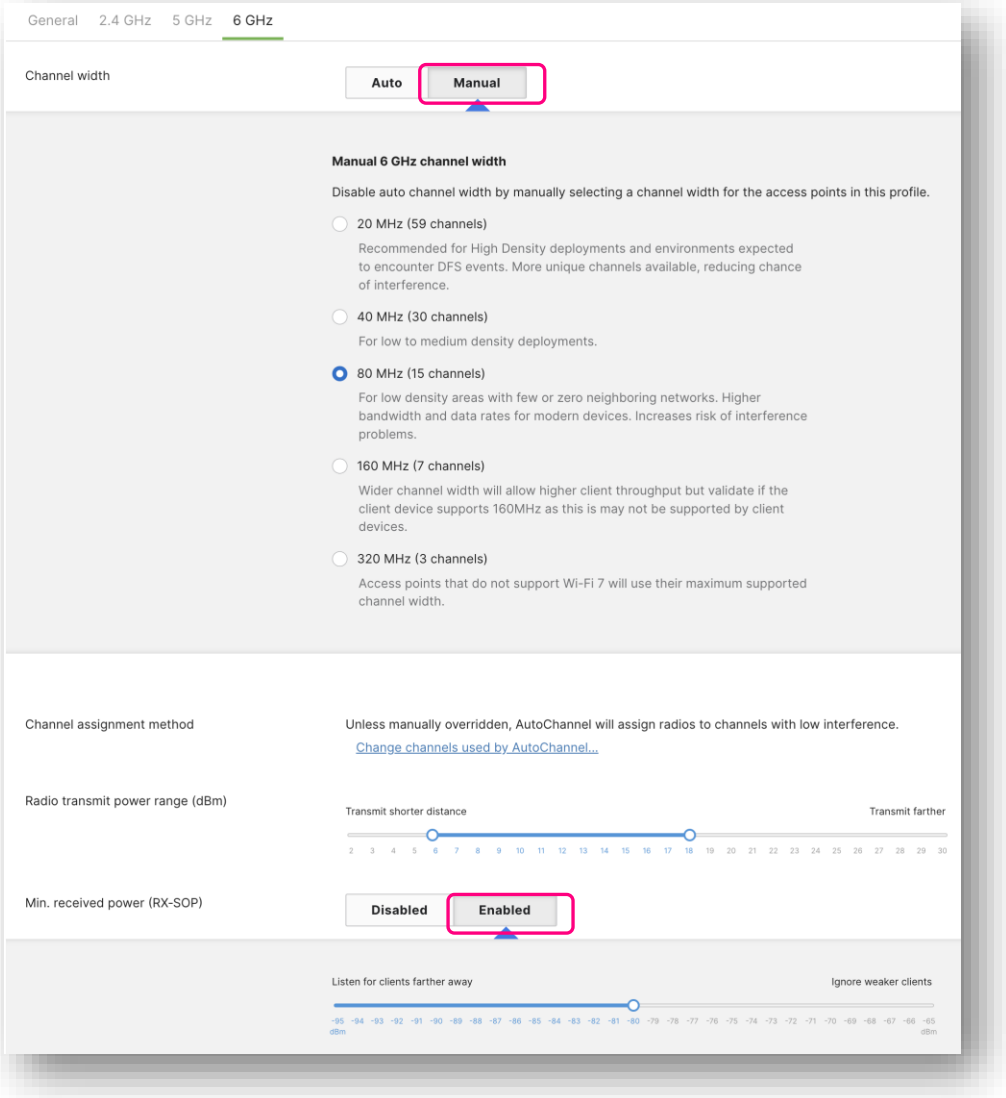
RTP Campus - RF Profile





- One RF profile for all indoor APs
- Band selection per SSID:
  - Employee SSID on 5/6 GHz
  - Guest on SSID on 2.4/5Ghz
- Client Load Balancing is OFF

RTP Campus - RF Profile



- Channel Width set to 40 MHz on 5GHz
- Channel Width set to 80 MHz on 6GHz
- 24 Mbps min data rate across all bands
- Min. received power (RX-SOP) at -80 dbm

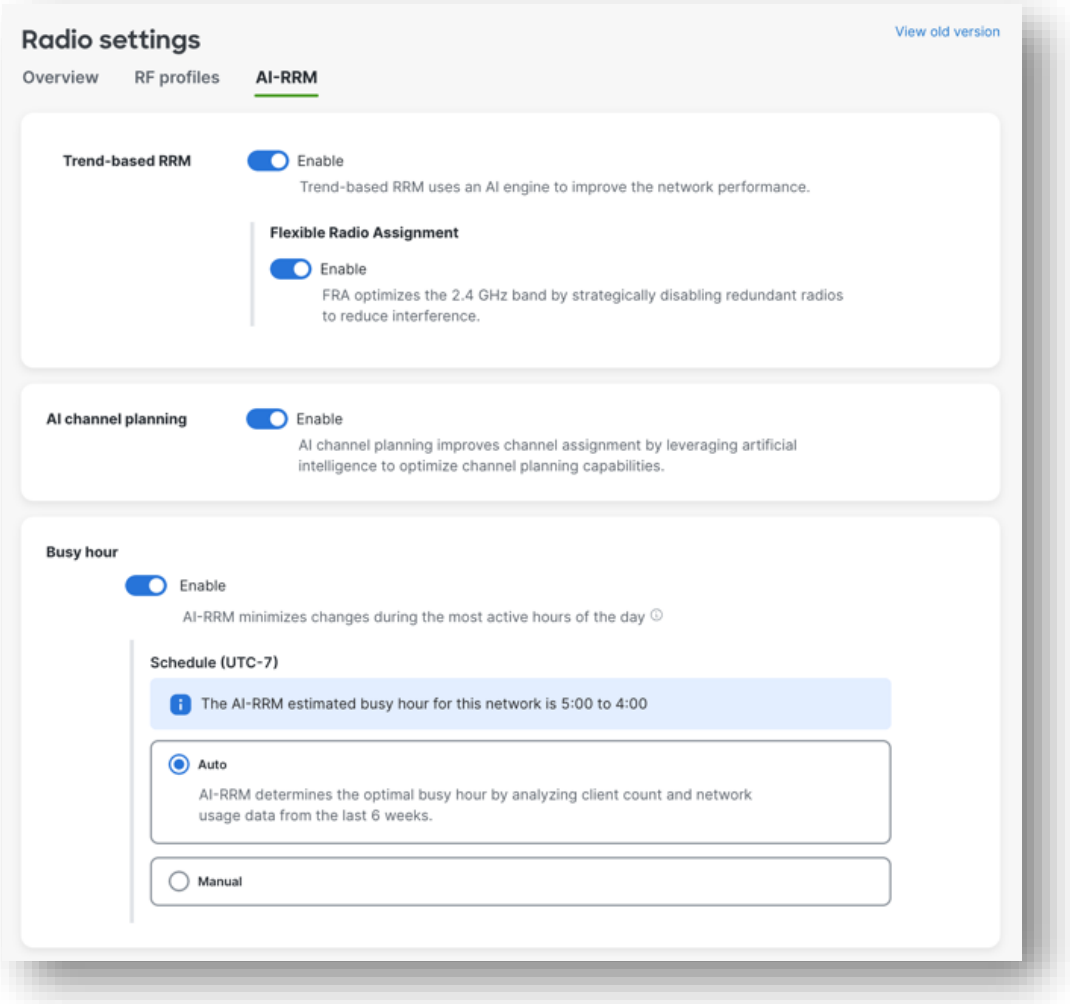
AI-Enhanced RRM

AI-Enhanced RRM improves wireless reliability

Trend-Based RRM
Optimize RF with weeks of historical analysis

Flexible Radio Assignment
Optimize band selection to minimize 2.4 GHz interference

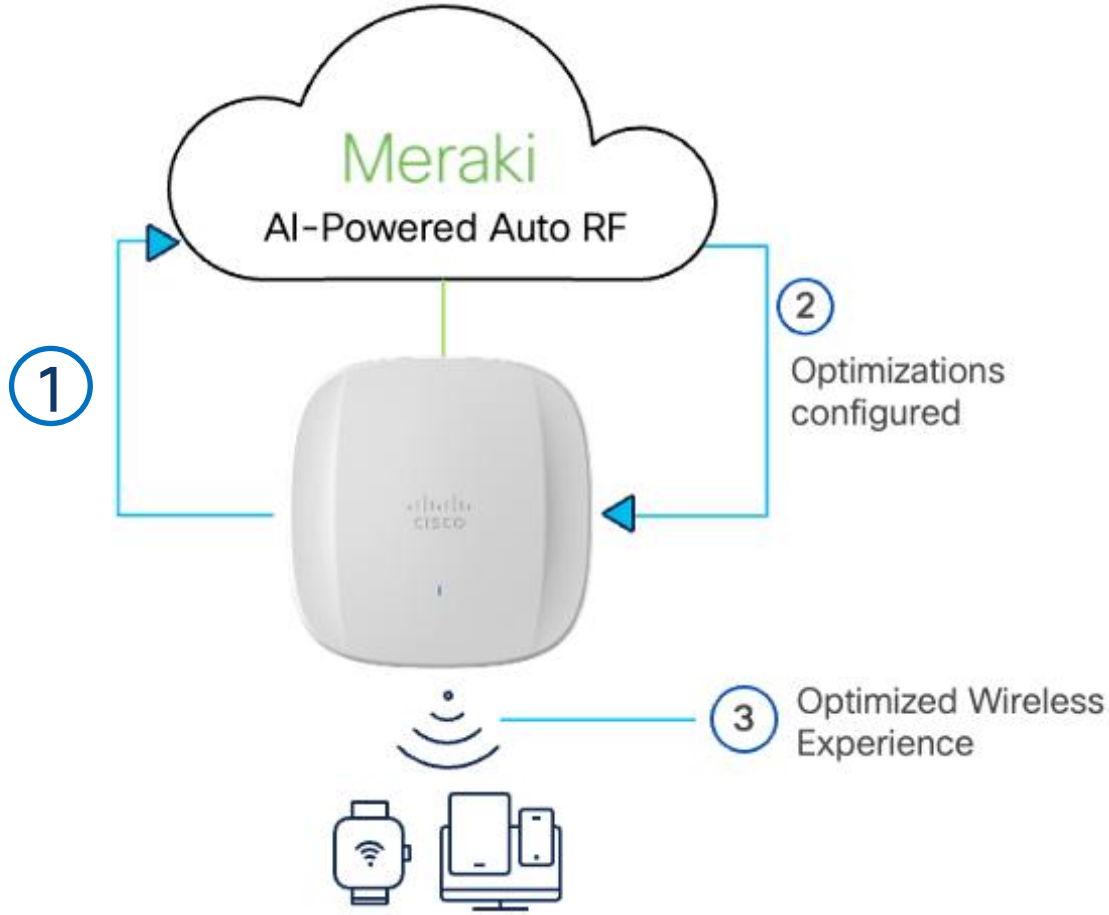
Busy Hour Aware
Minimize disruptive changes during the critical times of day



AI-Enhanced RRM: how does it work?

New telemetry data is now sent from APs to the Meraki Cloud for enhanced RRM decisions.

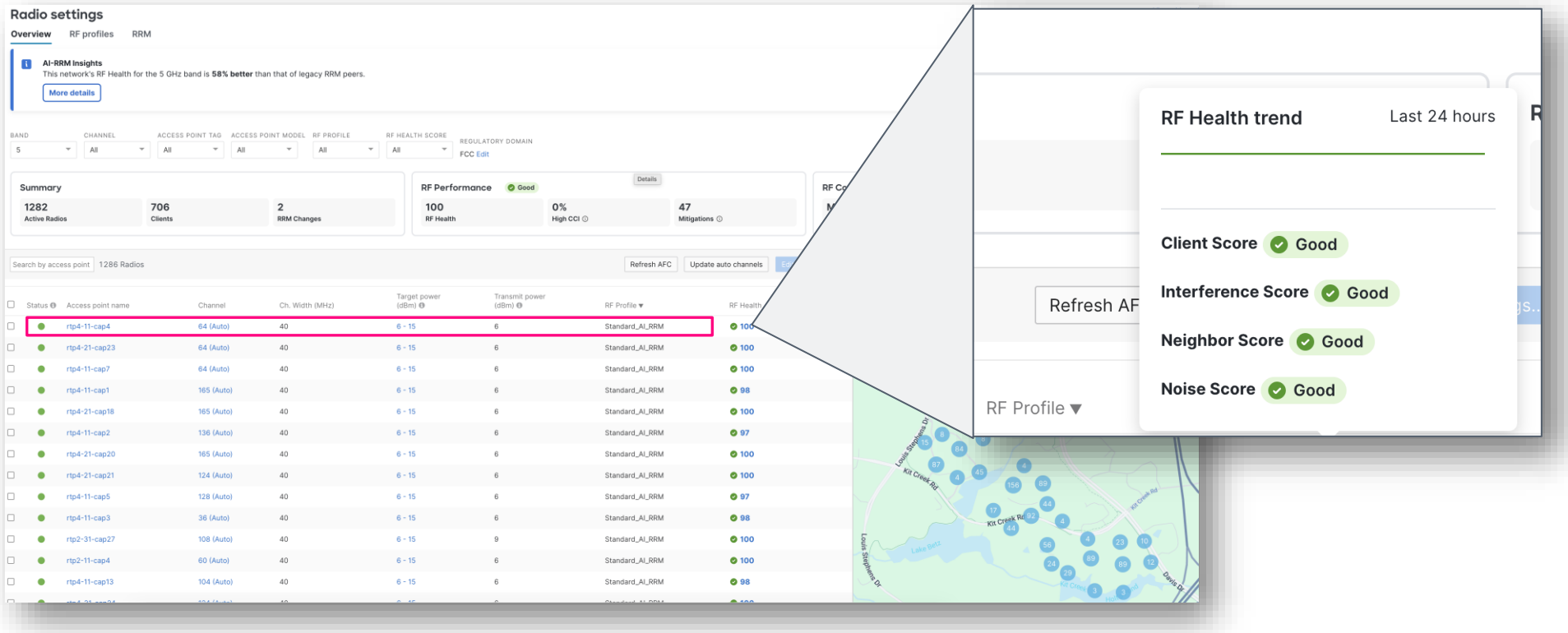
NEW
- Neighbor Discovery Protocol
- Interference Duty Cycle
- Noise Floor
- Channel Utilization
- AP Neighbor
- AP Radio Channel Power
- AP Radio
- AP Channel
- RRM Measurement Interference
- RRM Measurement Noise
- RRM Coverage Client Info
- RRM Measurement Load



AI-RRM on Dashboard – Now GA

Wireless > Radio Settings: RF Health score

- Originated from Wireless Config Analyzer tool*
- Now available across all networks on AI-RRM and Non-AI-RRM networks

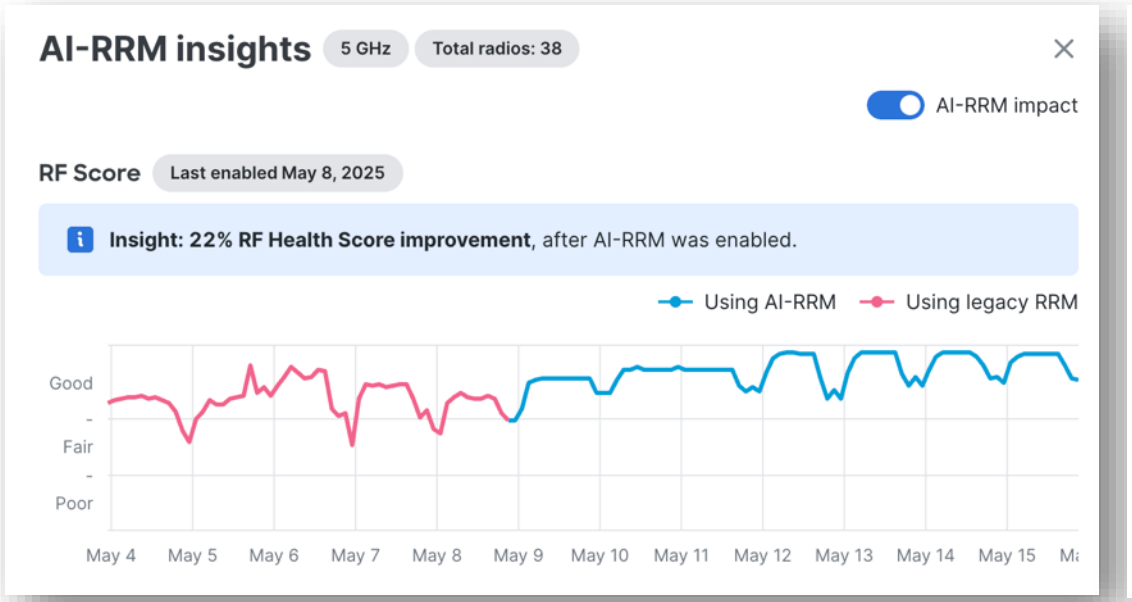


* https://developer.cisco.com/docs/wireless-troubleshooting-tools/wireless-config-analyzer/

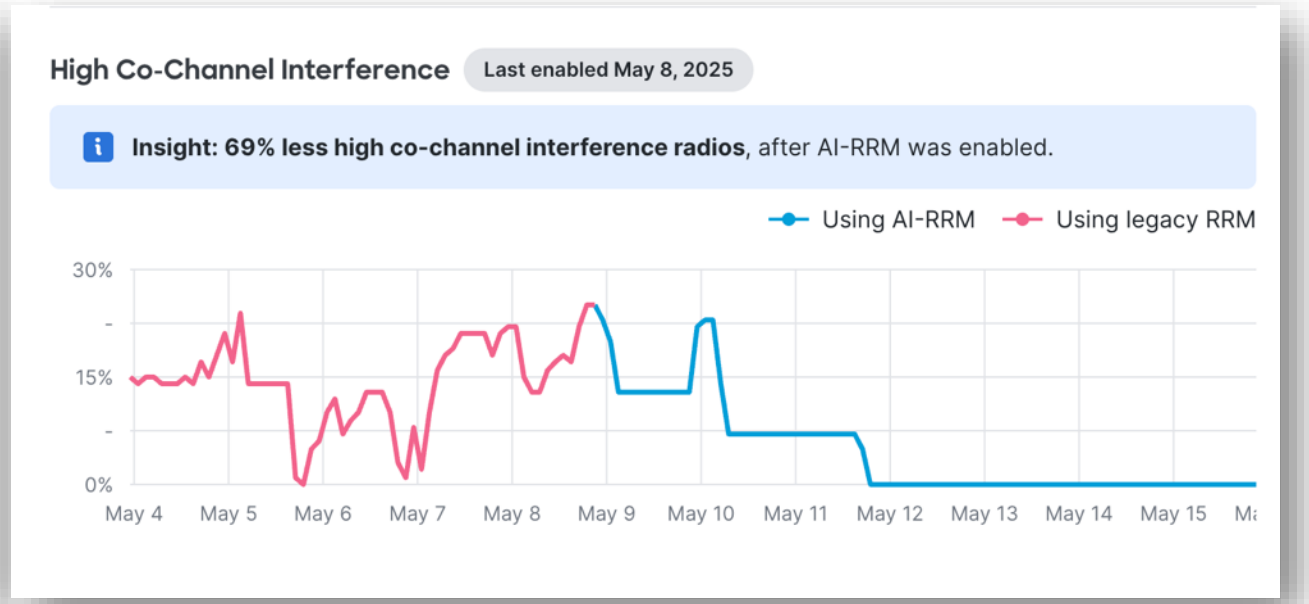
AI-RRM: Before & After – Measurable AI Advantage

Typical Network example with medium network density

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

AI-RRM vs RRM*: what you need to know

	RRM (AutoRF)	AI-RRM
RRM algorithm	Runs on last 15 mins of data Per-AP optimization	Trend based algorithm. 14 days augmented telemetry (NDP, Noise, Channel Utilization, etc.) per-Network optimization
AI Channel Planning	Marks and avoid DFS/RF Jammed channels	No changes
Busy hour	RF changes are based on last 15 mins of data	RF changes optimized for busy hours using trend-based telemetry. Busy hour collection, off-peak changes

**AutoRF is rebranded as RRM*

AI-RRM vs RRM*: what you need to know

	RRM (AutoRF)	AI-RRM	MR-ENT	MR-ADV
RRM algorithm	Runs on last 15 mins of data Per-AP optimization	Trend based algorithm. 14 days augmented telemetry (NDP, Noise, Channel Utilization, etc.) per-Network optimization	autoRF based	AI-RRM based
AI Channel Planning	Marks and avoid DFS/RF Jammed channels	No changes	No changes	No changes
Busy hour	RF changes are based on last 15 mins of data	RF changes optimized for busy hours using trend-based telemetry. Busy hour collection, off-peak changes	autoRF based	AI-RRM based

**AutoRF is rebranded as RRM*

WLAN Design

WLAN Design for 6Ghz (Wi-Fi 6E & 7)

6GHz
Wi-Fi 6E

WPA3/Enhanced Open
Mandatory

Protected Management
Frame (PMF) Mandatory

Wi-Fi 7
add-on

Enhanced ciphers for
WPA3-SAE & OWE*
New AKM support for
WPA3-SAE*

* (AKM: 24 & 25), (Cipher: GCMP 256)

Beacon Protection
(WPA3 mandatory for
11be MCS rates & MLO)

Wi-Fi 6E & 7 Security

Enterprise

WPA Type	AKMs*	802.11w	CCMP	GCMP256	Compatibility	Notes
WPA3 Enterprise	802.1x-SHA256	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	
WPA3 Enterprise	802.1x-SHA256	✓	✓	✗	Wi-Fi 6E	
WPA3 Transition	802.1x, 802.1x-SHA256	Optional	✓	✓	Wi-Fi 6 Wi-Fi 6E Wi-Fi 7	Allows legacy clients in 2.4/5 GHz bands
WPA3 192bit Security	SUITE-B-192	✓	✗	✓	Wi-Fi 6 Wi-Fi 6E Wi-Fi 7	
WPA2	802.1x	Optional	✓	✗	Wi-Fi 6, Legacy	Allows legacy clients in 2.4/5 GHz bands

**Implicitly enabled (no explicit configuration needed)*

AP Beacon Protection enabled with 11be

AKM = Authentication and Key Management
SHA-256 = Secure Hash Algorithm (SHA) 256 bit
CCMP (Counter Mode Cipher Block Chaining Message Authentication Protocol)
GCMP (Galois Counter Mode Protocol)

Wi-Fi 6E & 7 Security

Personal

WPA Type	AKMs*	802.11w	CCMP	GCMP256	Compatibility	Notes
WPA3 Personal	SAE, SAE-EXT-KEY	✓	✓	✓	Wi-Fi 6 Wi-Fi 6E Wi-Fi 7	Allows Wi-Fi 6 Clients in 2.4/5 GHz
WPA3 Personal	SAE	✓	✓	✗	Wi-Fi 6 Wi-Fi 6E	Allows Wi-Fi 6 Clients in 2.4/5 GHz
WPA3 Transition	PSK, SAE, SAE-EXT-KEY	Optional	✓	✓	Wi-Fi 6 Wi-Fi 6E Wi-Fi 7	Allows PSK clients in 2.4/5 GHz bands
WPA3 Transition	PSK, SAE	Optional	✓	✗	Wi-Fi 6 Wi-Fi 6E	Allows PSK clients in 2.4/5 GHz bands
WPA2	PSK	Optional	✓	✗	Wi-Fi 6, Legacy	Allows legacy clients in 2.4/5 GHz bands

*Implicitly enabled (no explicit configuration needed)

AP Beacon Protection enabled with 11be

AKM = Authentication and Key Management
SHA-256 = Secure Hash Algorithm (SHA) 256 bit
CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
GCMP (Galois Counter Mode Protocol)

cisco

Wi-Fi 6E & 7 Security

Enhanced Open

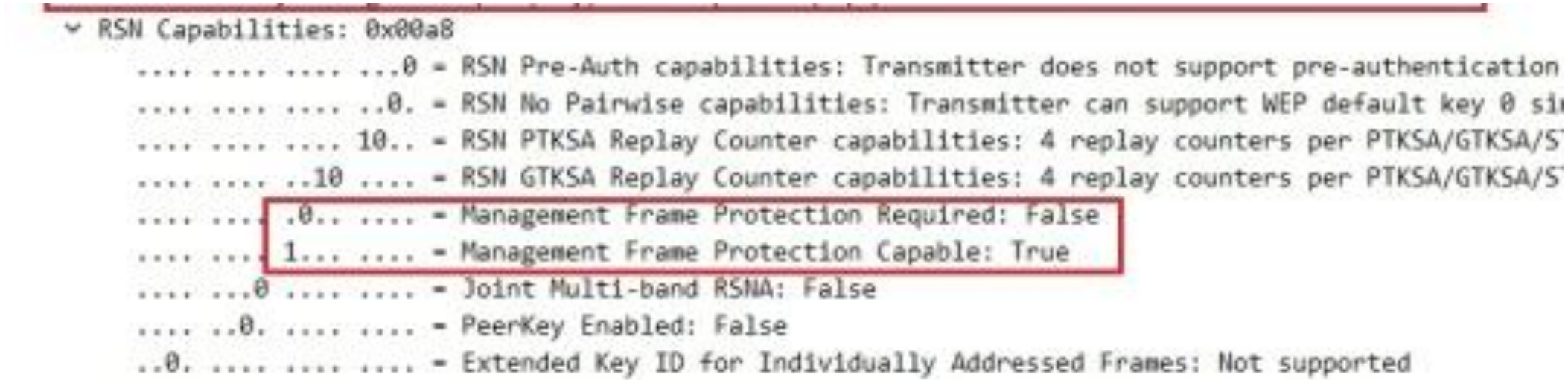
WPA Type	AKMs	802.11w	CCMP	GCMP256	Compatibility	Notes
Enhanced Open	OWE	Required	✓	✓	Wi-Fi 6 Wi-Fi 6E Wi-Fi 7	Allows Wi-Fi 6 Clients in 2.4/5 GHz
Enhanced Open	OWE	Required	✓	✗	Wi-Fi 6 Wi-Fi 6E	6 GHz supported. Wi-Fi 6 Clients in 2.4/5 GHz
Enhanced Open (Transition)	OWE	Required	✓	NA	Wi-Fi 6	No 6 GHz, No Wi-Fi 7 Requires 2 SSIDs Legacy clients in 2.4/5 GHz

*Implicitly enabled (no explicit configuration needed)

AP Beacon Protection enabled with 11be

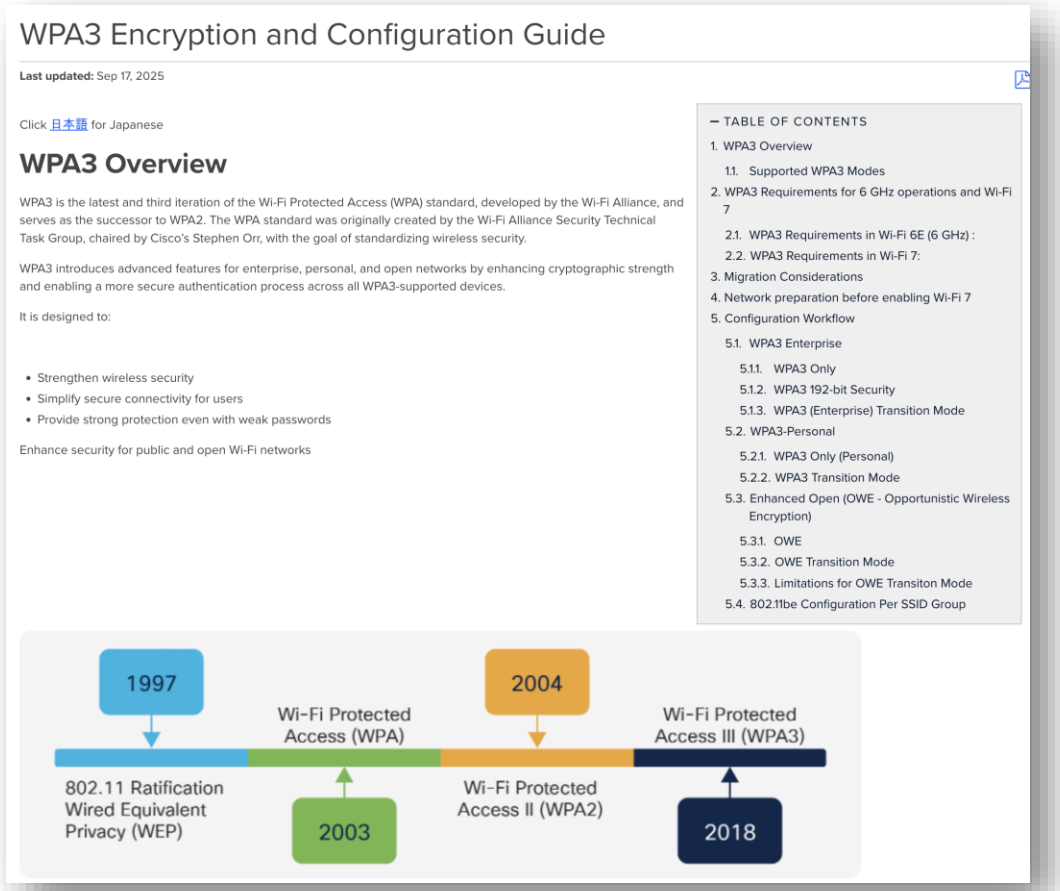
AKM = Authentication and Key Management
SHA-256 = Secure Hash Algorithm (SHA) 256 bit
CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
GCMP (Galois Counter Mode Protocol)

WPA3 Transition mode



- WPA3 Transition mode is about advertising one SSID with both WPA2 and WPA3 Authentication Key Methods (AKMs) and PMF set to optional, in both 2.4 and 5Ghz
- WPA3 capable clients can join using WPA3
- Note: Some older clients and OS can get confused by the multiple AKMs in the beacons. Whenever possible, important to test.

6GHz and Wi-Fi security requirements



- WPA3 + Protected Management Frame (PMF, 802.11w) is mandatory for 6Ghz
- Transition mode is a valid option to move clients to a more secure Wi-Fi on 2.4 and 5GHz
- WPA3 Enterprise Transition mode is supported starting MR 31.1.1
- WPA3 Personal Transition mode is supported starting MR 31.1.6
- Note: Transition mode is not an option for OWE as clarified in WPA3 v3.4
- Deployment guide recently updated https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

WLAN Design for 6Ghz and WPA3 (Wi-Fi 6E & 7)

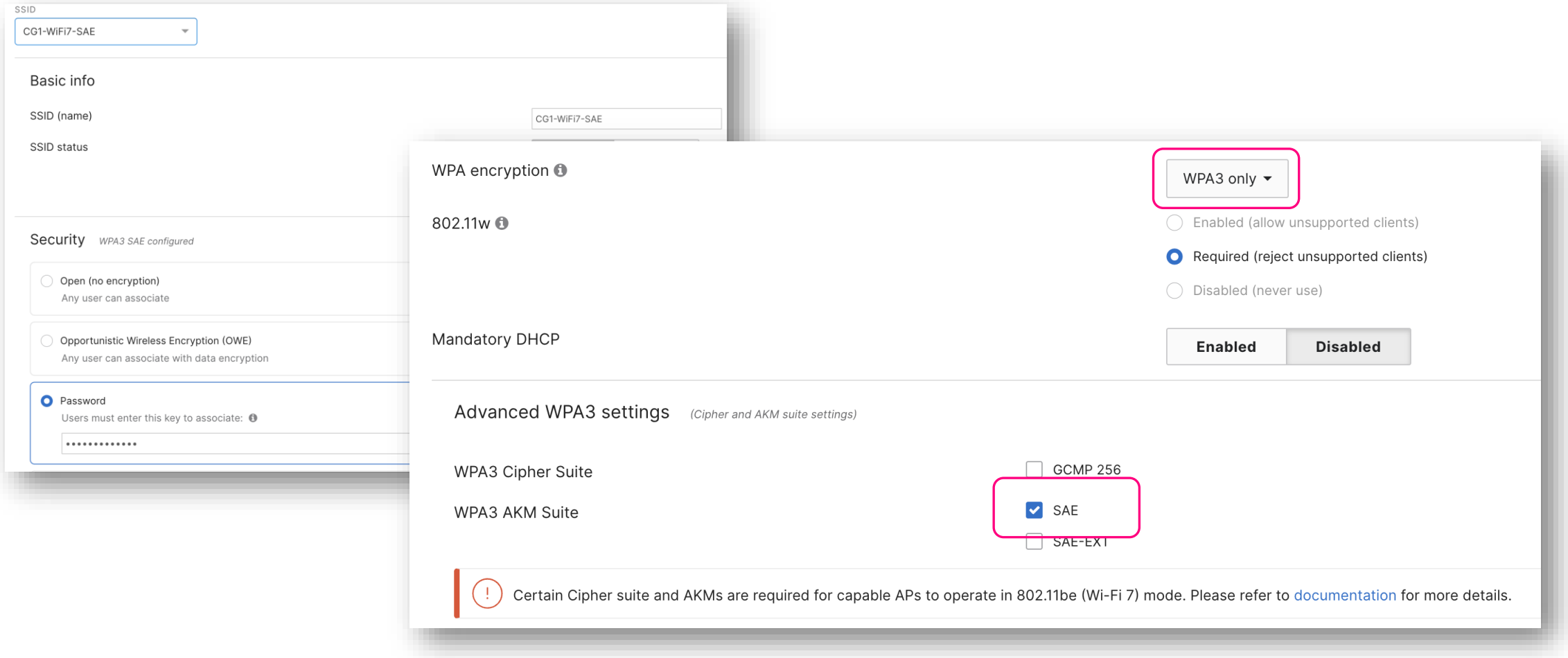
What options would you have?

1. **"All-In"**: Reconfigure the existing WLAN to WPA3, one SSID for all radio policies (2.4/5/6 GHz) – **Most Aggressive**
2. **"Multiple SSIDs"**: Redesign your SSIDs, adding SSID/WLAN with specific security settings – **Most Flexible**
3. **"Transition mode SSID"**: Use Transition Mode in 2.4 and 5GHz to support multiple security in different bands – **Most Conservative**

If you CANNOT control clients, Transition Mode is a viable option

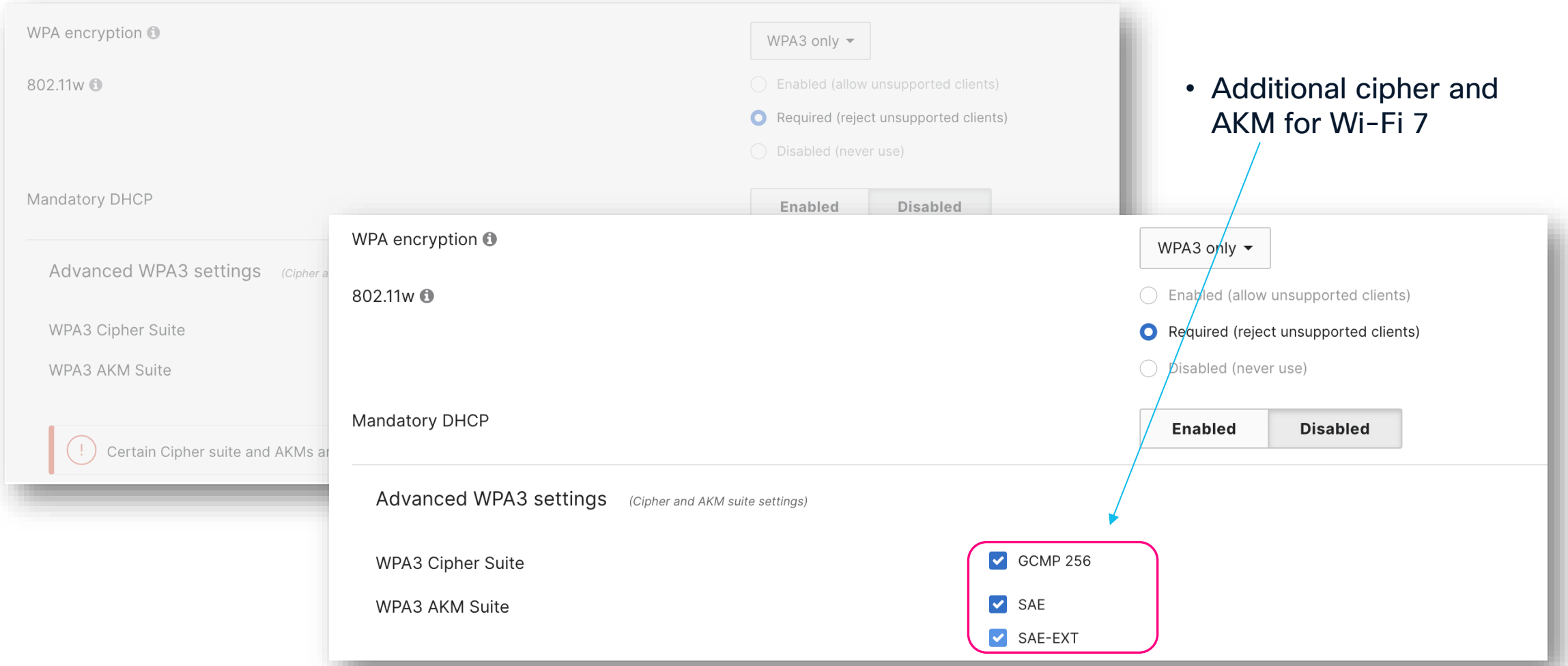
Wi-Fi 7 security requirements

This is a valid SSID security configuration for broadcasting it in 6Ghz (Wi-Fi 6E)



Wi-Fi 7 security requirements

This is a valid SSID security configuration for broadcasting it in 6Ghz (Wi-Fi 6E)



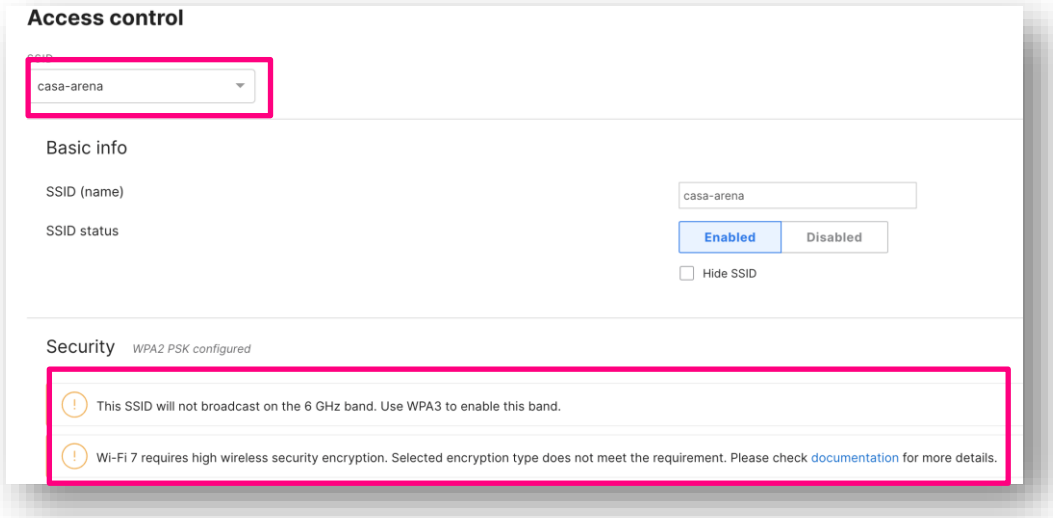
- Additional cipher and AKM for Wi-Fi 7

Wi-Fi 7 security compliance

Use Case	Security encryption today	Wi-Fi 7 compliant SSID
Guest access	Open	OWE
Corporte/Secure/RADIUS auth	WPA2	WPA3 OR WPA3 transition (Enterprise)
IoT/OT/Guest (PSK based)	WPA2	WPA3 OR WPA3 transition (SAE)

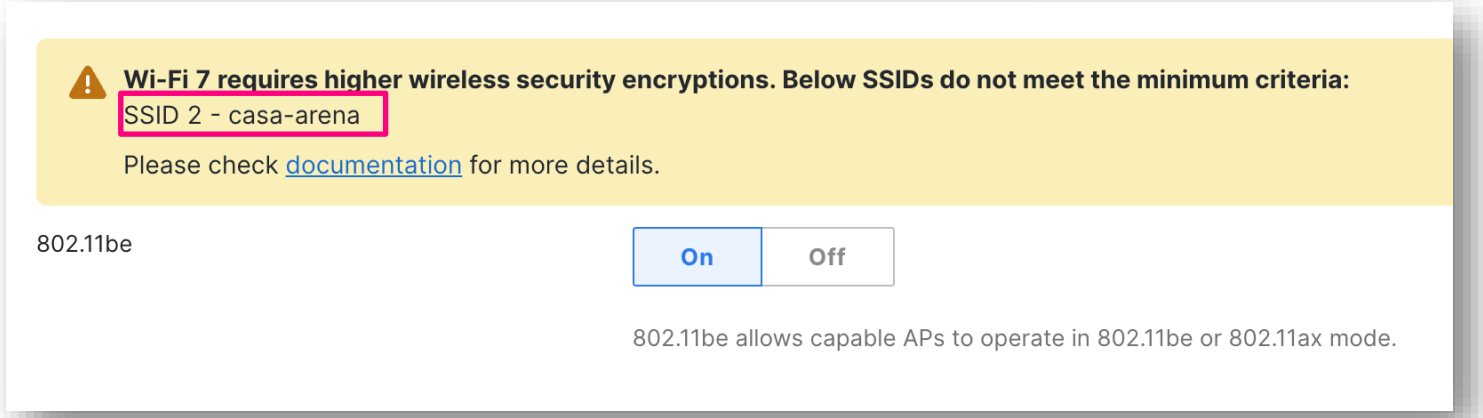
- IMPORTANT: For MR 31.1.x, all SSIDs on the Dashboard network must be Wi-Fi 7 compliant to enable Wi-Fi 7 via RF profiles
- Workaround: Only enabled SSIDs are considered for Wi-Fi 7 compliance. Use SSID availability tags to prevent Legacy SSIDs to be broadcasted on Wi-Fi 7 APs.
- **Note:** Support for per-SSID Wi-Fi 7 enablement is in R32.1.4 (now in Beta)

Wi-Fi 7 compliance requirements: Workaround



This SSID is WPA2 > doesn't meet the requirement for 6GHz and Wi-Fi 7

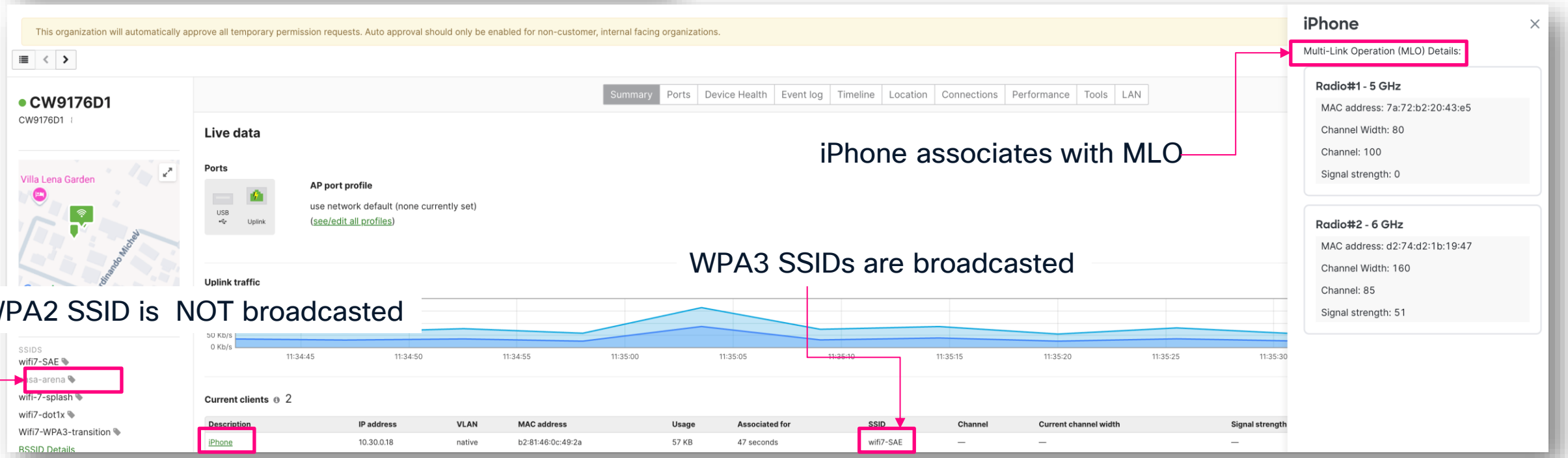
Wi-Fi 7 SSIDs are not broadcasted on the Wi-Fi 7 AP



Wi-Fi 7 compliance requirements: Workaround

Use device Tag to Enable WPA2 SSID only on older APs

Wi-Fi 7 SSIDs are now broadcasted on Wi-Fi 7 APs



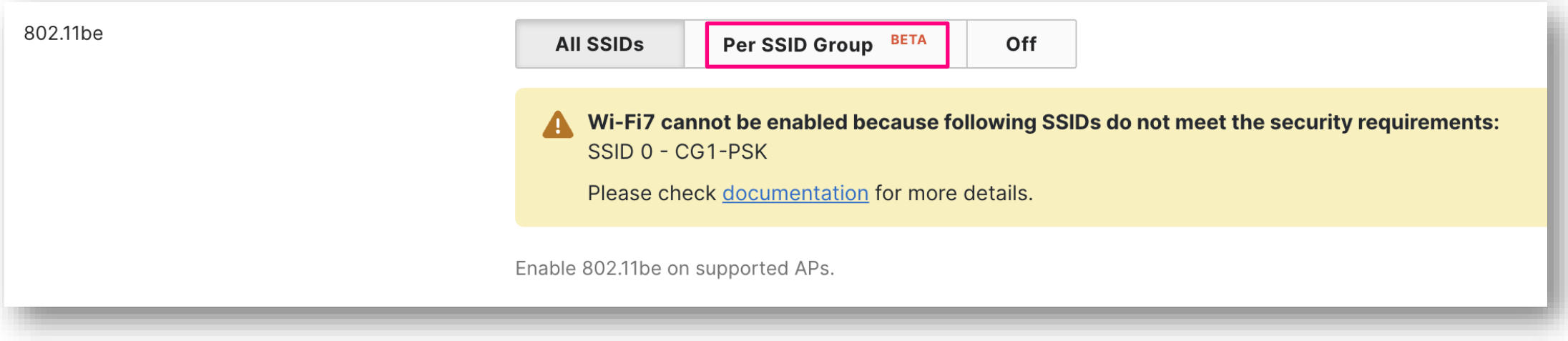
iPhone associates with MLO

WPA3 SSIDs are broadcasted

WPA2 SSID is NOT broadcasted

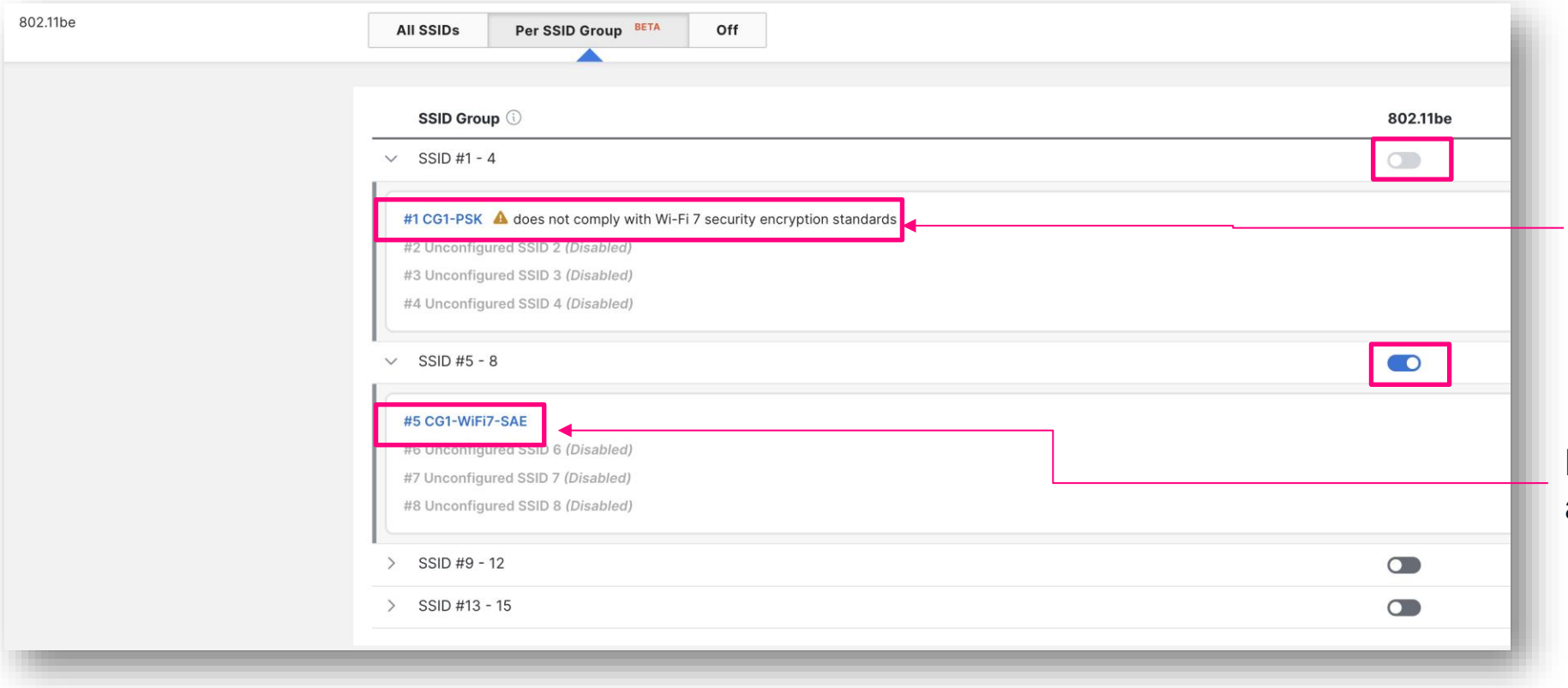
Wi-Fi 7 security compliance: what changes in 32.1.4?

- Wi-Fi 6E and Wi-Fi 7 introduced MBSSID (Multiple SSID), which allows groups of four SSIDs to be advertised within a single Beacon or Probe Response frame in the 6 GHz band.
- The dashboard supports four MBSSID groups (SSID Group), each containing four SSIDs.
- In earlier releases, all SSIDs transmitted by the AP were required to be Wi-Fi 7 compliant.



Wi-Fi 7 security compliance: what changes in 32.1.4?

- Per-group SSID configuration is available starting in MR 32.1.4.
- For an AP to advertise a group's Wi-Fi 7 capability, all SSIDs in that group must be Wi-Fi 7 compliant. If any SSID in the group is not compliant, the group's capability is reduced to Wi-Fi 6.

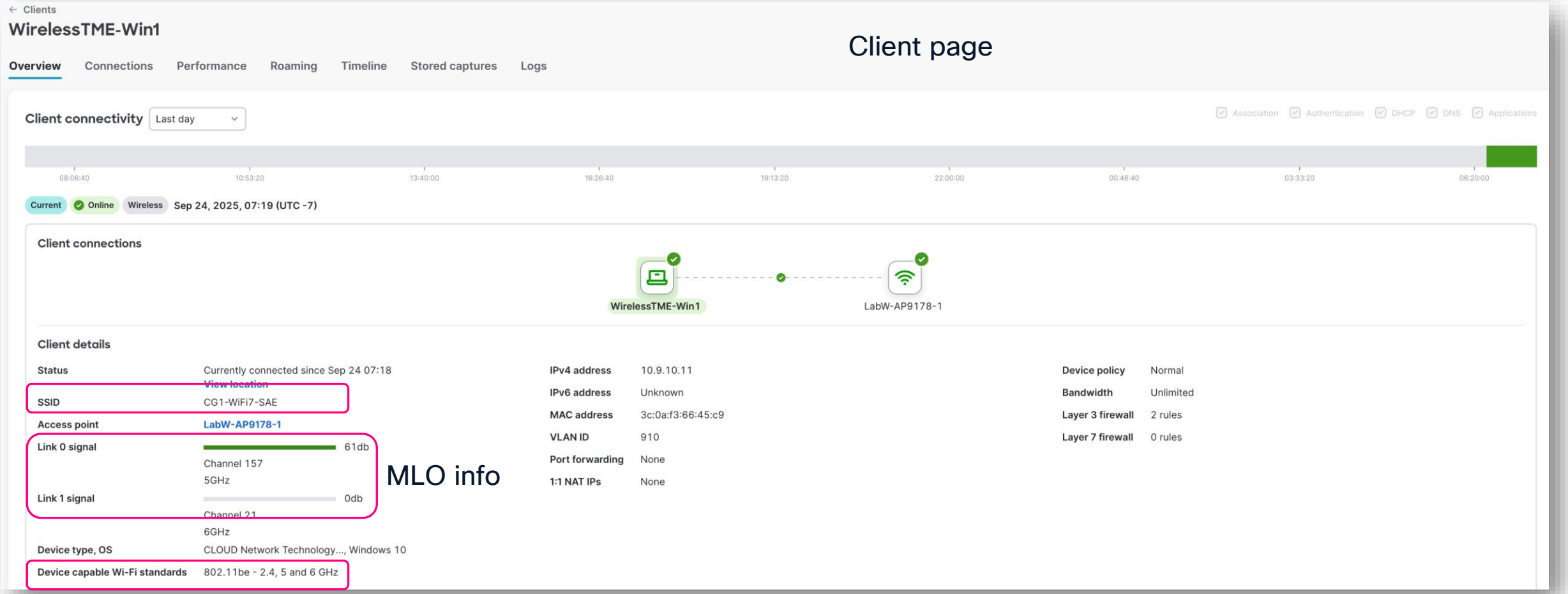


SSID not complaint, WI-Fi7 not advertised

Fully compliant, SSID advertised as Wi-Fi 7

Wi-Fi 7 security compliance

Wi-Fi 7 capable client can now connect at 802.11be rates and with MLO (Multi Link Operations)



RTP Campus – WLAN Design: #2 SSIDs

Employee

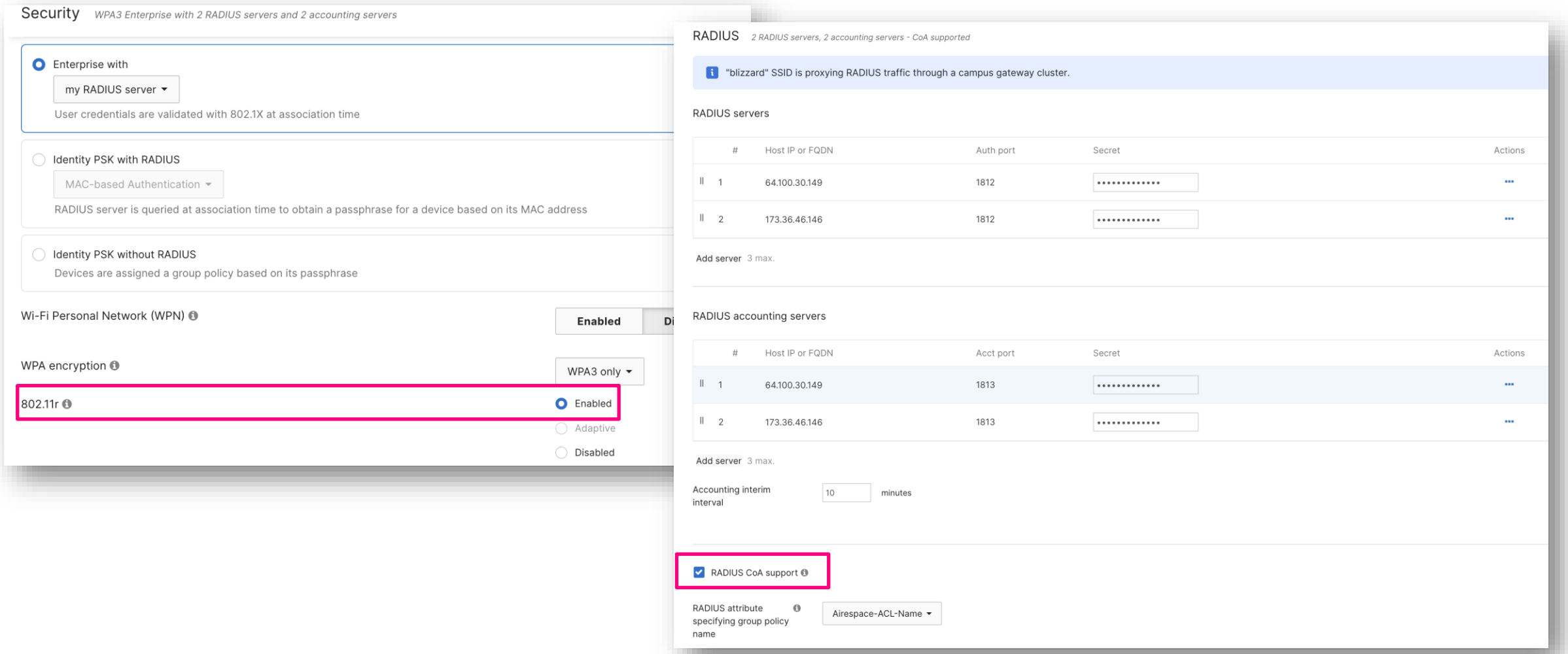
- WPA3 ”All IN” approach
- WPA3 Enterprise Only
- Broadcasted on 5 & 6 GHz
- Certificate based
- No BYOD allowed
- Mandatory DHCP
- 802.11r enabled
- AAA override
- CoA enabled
- No mDNS
- QoS: Webex with DSCP 46

Guest

- CWA (MAB + ISE portal)
- Broadcasted on 2.4 & 5 GHz
- Open (no OWE yet)
- BYOD SSID
- Mandatory DHCP
- 802.11r disabled
- AAA override
- CoA Enabled
- No mDNS
- QoS: remark all to DSCP 0

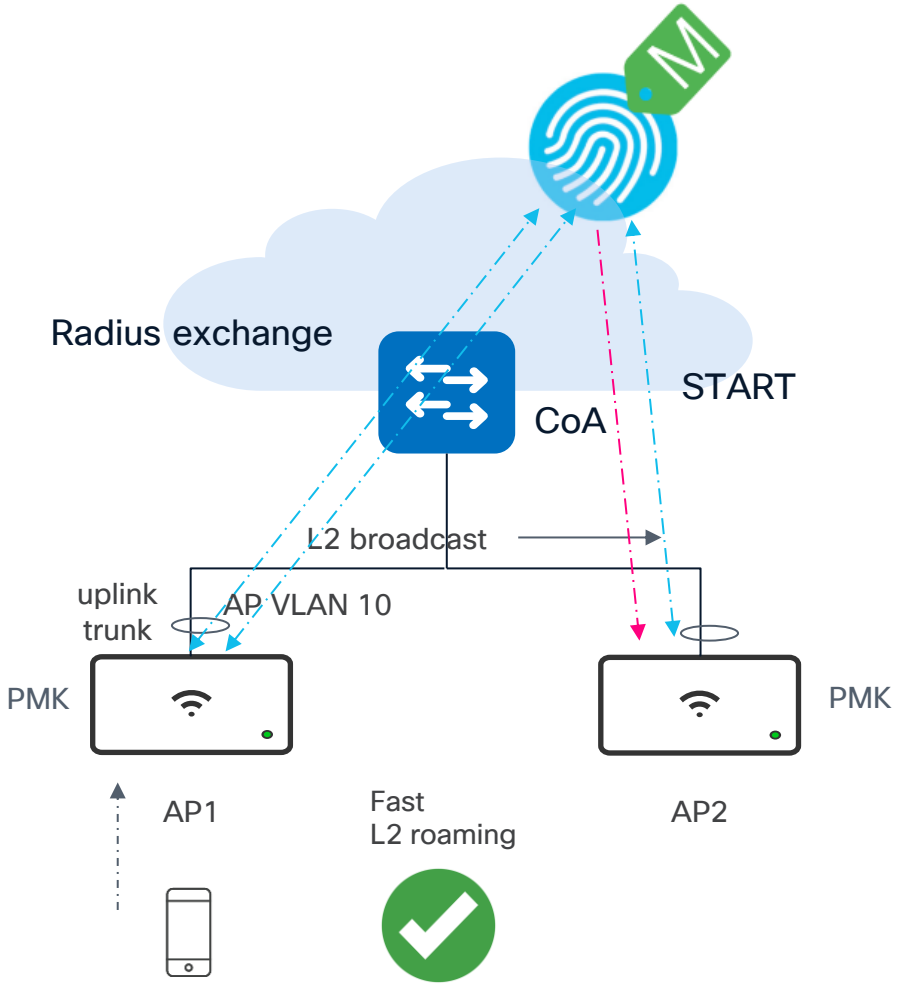
RTP Campus – WLAN Design: CoA + 11r

802.11r/OKC + CoA is supported starting 32.1



RTP Campus – WLAN Design: CoA + 11r

802.11r/OKC + CoA is supported starting 32.1



How?

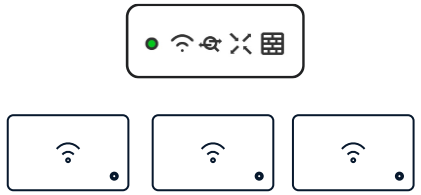
- Client authenticates to an SSID with 802.11r/OKC and PMK is derived > The Network Access Server (NAS) is the first AP that client authenticates with (AP1 in this case)
- PMK is shared via L2 broadcast and the client roams with 802.11r and no re-auth is sent to the AAA
- Roam-from AP sends an Accounting STOP
- Roam-to AP sends an Accounting START
- Accounting START message updates the NAS at the AAA, as it contains the same calling-station-ID (AVP Code 31)
- When, after the client roamed, AAA issues a CoA: the CoA is delivered to the roam-to AP
- Note: ISE 3.3 Patch 5 is required

Wireless to Wired Network Design

Distribute or Centralize?
THAT is the Design Question

Distribute or Centralize?

Large, Medium Campus
> Centralized Data Plane architecture



km^2/mi^2

E.g., University Campus

Distribute Enterprise: Branch, Small Campus
Large, Medium Campus with Fabric
> Distributed Data Plane architecture

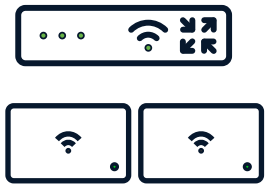
m^2/ft^2

e.g., Retail

Distribute or Centralize? Cisco Architecture Flexibility

Architecture

Centralized



Distributed

Cloud Managed

Campus Gateway

AP Bridged mode
(with or without Fabric*)

** Public Beta at the end of Nov 2025*

cisco

Distribute or Centralize? What to consider...

Use cases/Features

Services

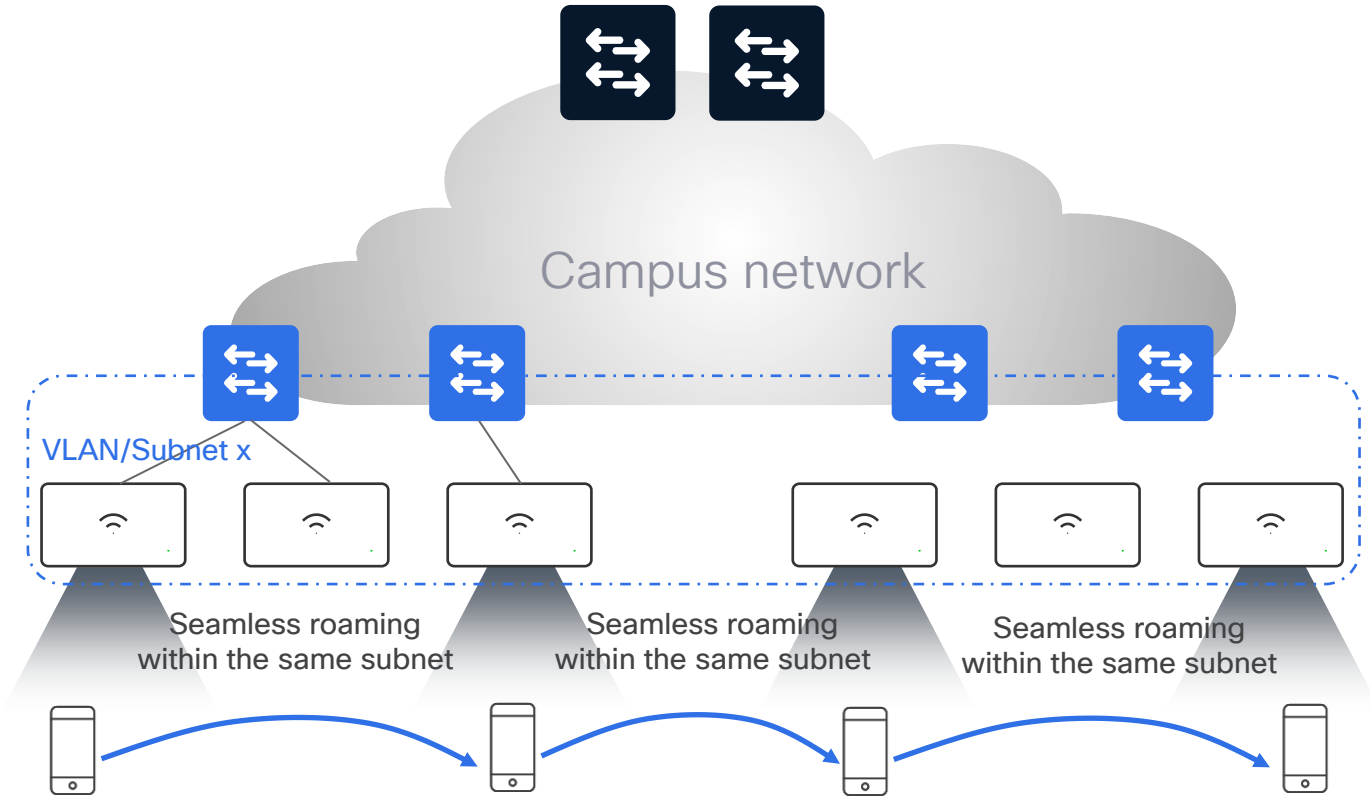
Wired Network Design

Performances

Policy

Scale

Distribute or Centralize? Seamless Roaming



Seamless roaming domain: keep same IP and policy as client roams > same VLAN/L2 broadcast domain

How can you create a L2 roaming domain?

- Spanning VLAN everywhere

Q: How big can be the L2 roaming domain?

A: Need to consider the type of layer 2 and Layer 3 switches and their MAC/ARP tables size, the impact of spanning tree (SPT), the DHCP scope design, etc.

How big can be the L2 roaming domain?

Let’s start with client considerations:

A **Single Dual Stack Host** will have **1 x IP**v4 address, and

at least 3 x IPv6 Addresses

(IPv4 Unicast, IPv6 Link Local, IPv6 Unique Local, IPv6 Global Unicast)

Windows 11: up to 16 IPv6 IP addresses (!!)

How big can be the L2 roaming domain?

Let’s identify a roaming domain in terms the number of APs:

Layer 2 switch = Catalyst 9200L (or MS equivalent)

MAC addresses table limit: 16,000

- Each wireless device will take a MAC address entry
- If we consider Random MAC, this number can be higher
- If we assume 40 clients per AP > 16,000/40 = **max 400 APs per L2 roaming domain**

How big can be the L2 roaming domain?

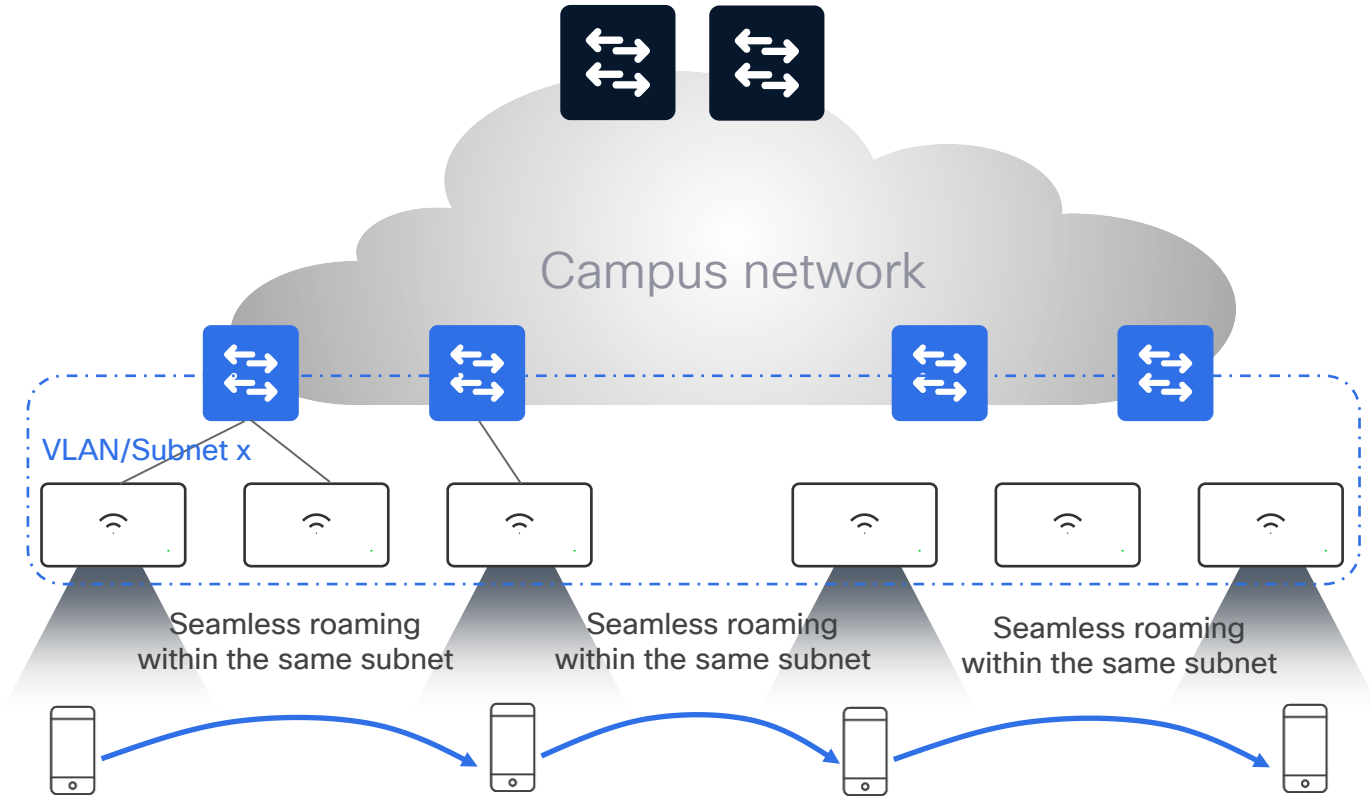
Let’s identify a roaming domain in terms the number of APs:

Layer 3 switch = Catalyst 9300 (or MS equivalent)

ARP entries: 32,000

- For dual stack clients, the scale numbers are divided by at least 4 (one entry for IPV4 and three entries for IPv6) > For 9300 the max number of clients is 32k/4 = 8k
- If we assume 40 clients per AP > 8,000/40 = **max 200 APs L2 roaming domain**

Distribute or Centralize? Seamless Roaming



Seamless roaming domain: keep same IP and policy as client roams > same VLAN/L2 broadcast domain

How can you create a L2 roaming domain?

- Spanning VLAN everywhere

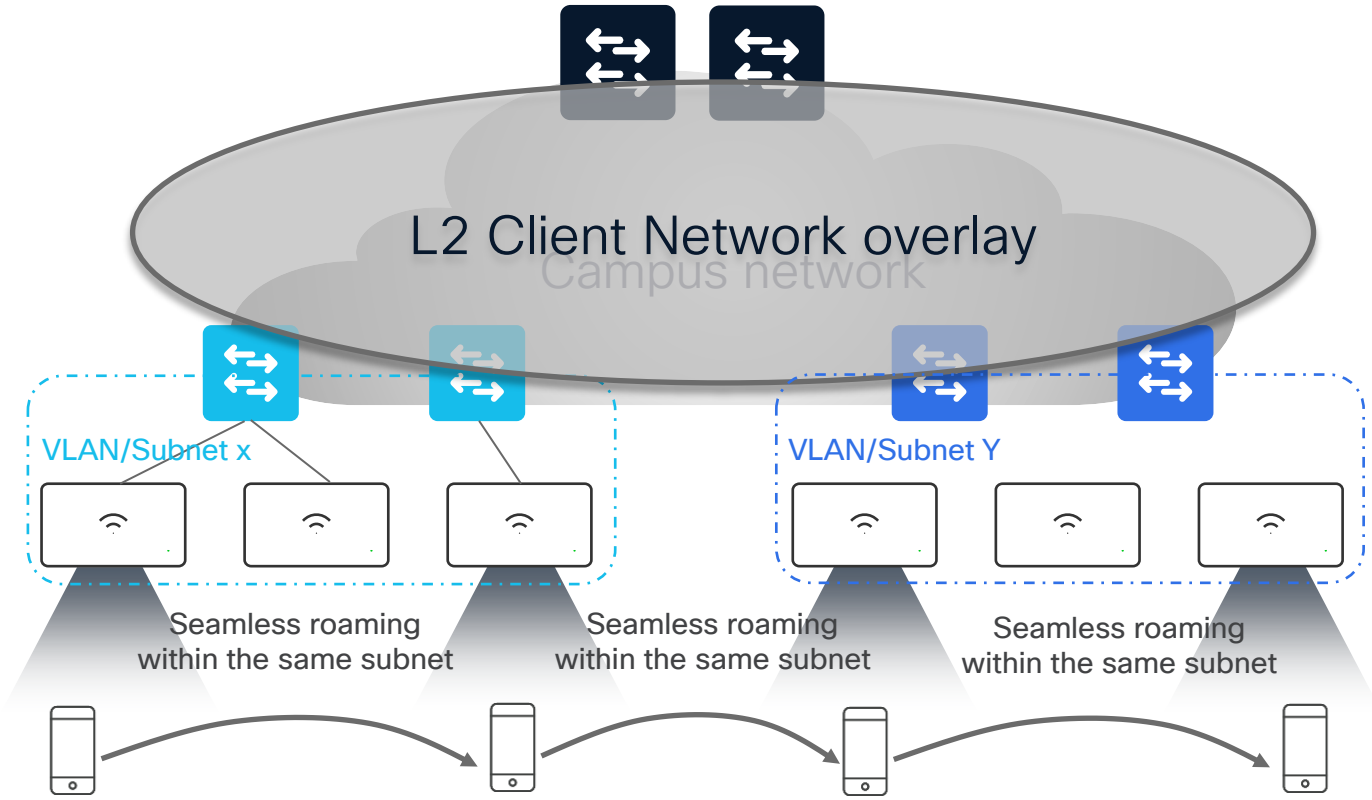
Q: How big can be the L2 roaming domain?

A: 200/300 APs, 8k clients as a reference, but anyway there is a limit...

Q: How to scale more?

A: you need seamless roaming across L3 boundaries > create L2 overlay

Distribute or Centralize? Seamless Roaming



How can you create the L2 overlay?

1. Wired Fabric

- Need to create a L2 overlay on top of the underlay campus network
- How? For example, with the new Cloud Managed Campus Fabric
- APs can be in bridge mode, distributed data plane

cisco

Cisco Cloud-Managed Campus Fabric

Multi-Network Cloud-Managed Fabric

Beta

Simplified management as a **single logical entity**

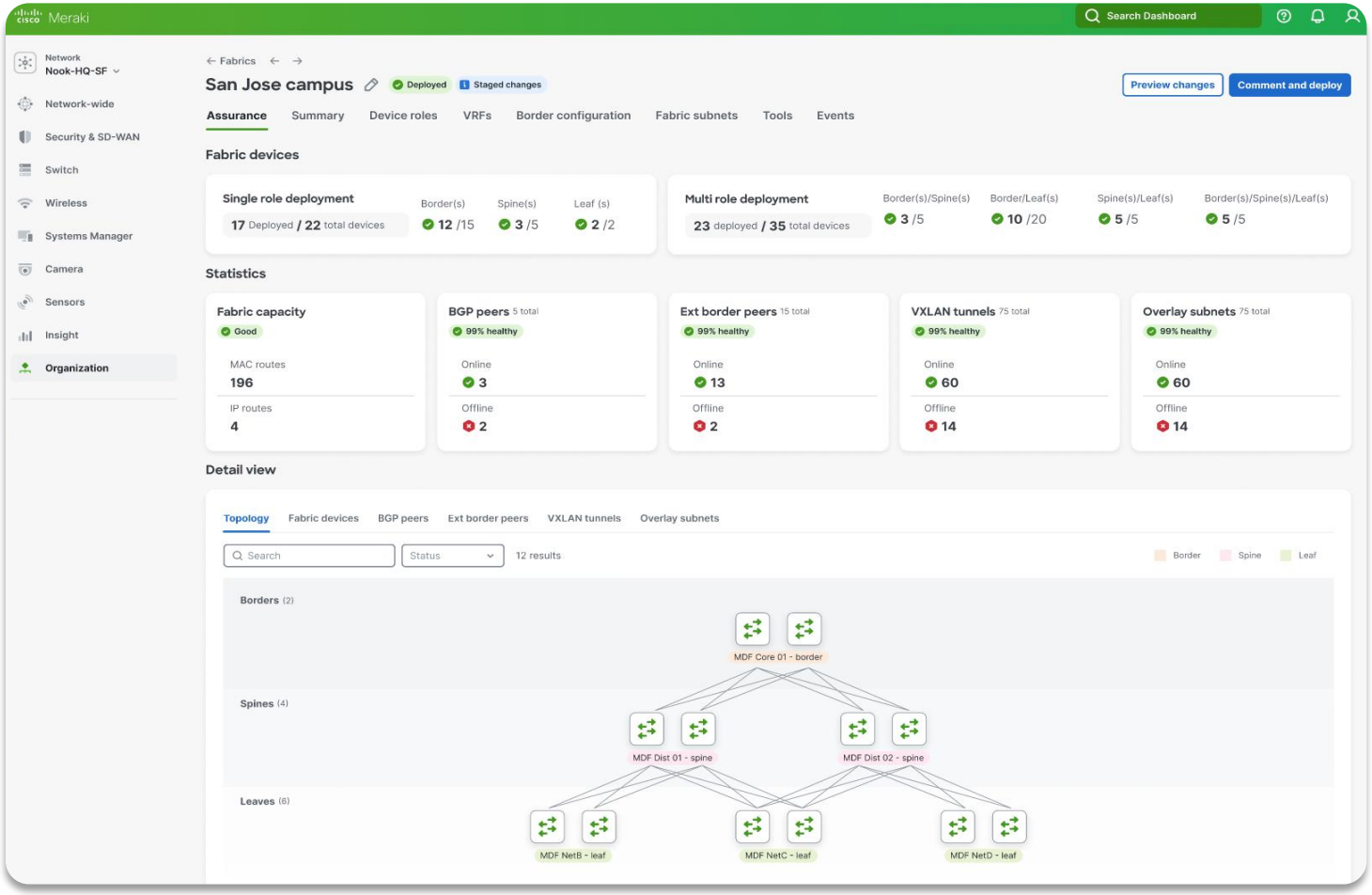
Focused on **brownfield migration**

Flexible deployment and staging

Securing the network with Adaptive Policy

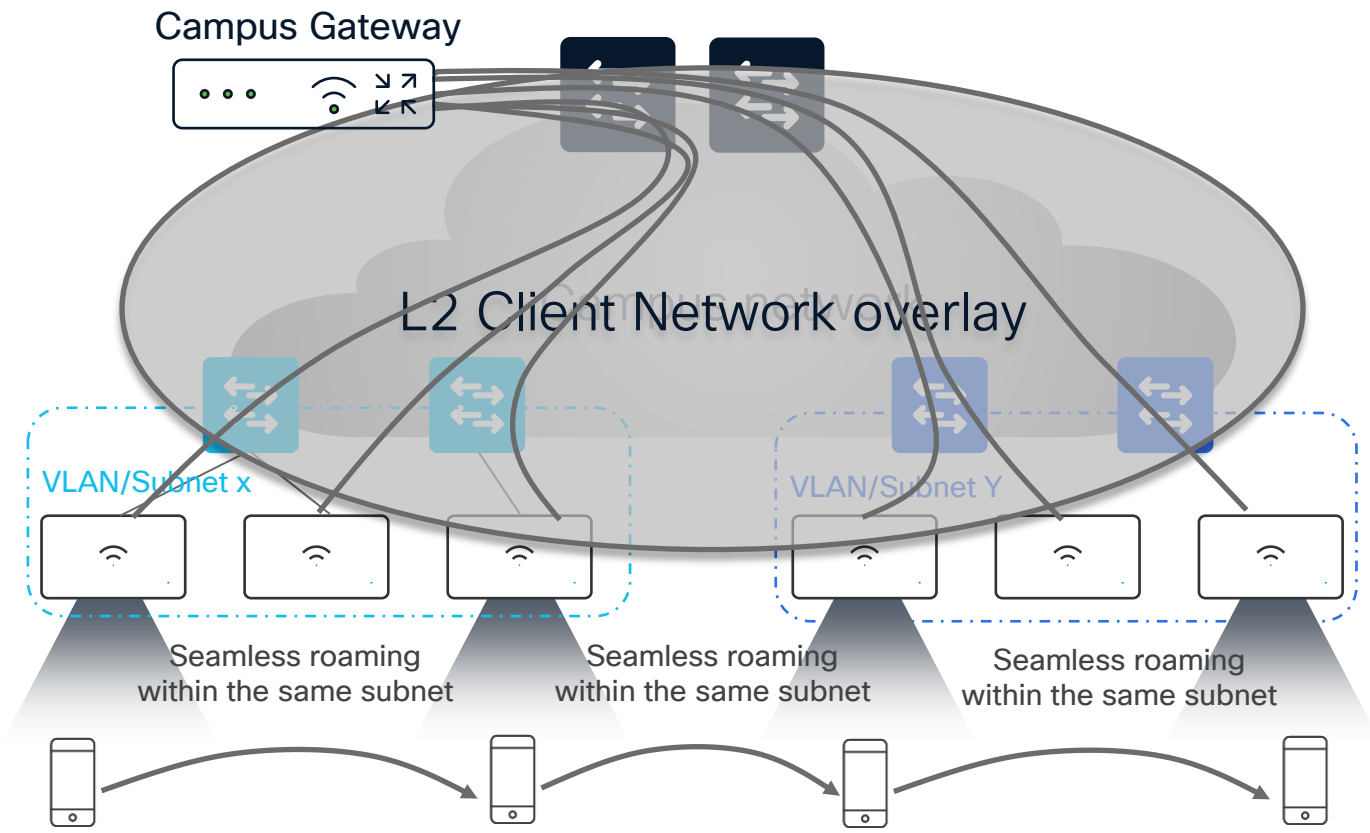
Optimized L2 extension

Day-2 Operational Assurance



More info? TechField Day session https://www.youtube.com/watch?v=I80zlNv3Zyk

Distribute or Centralize? Seamless Roaming

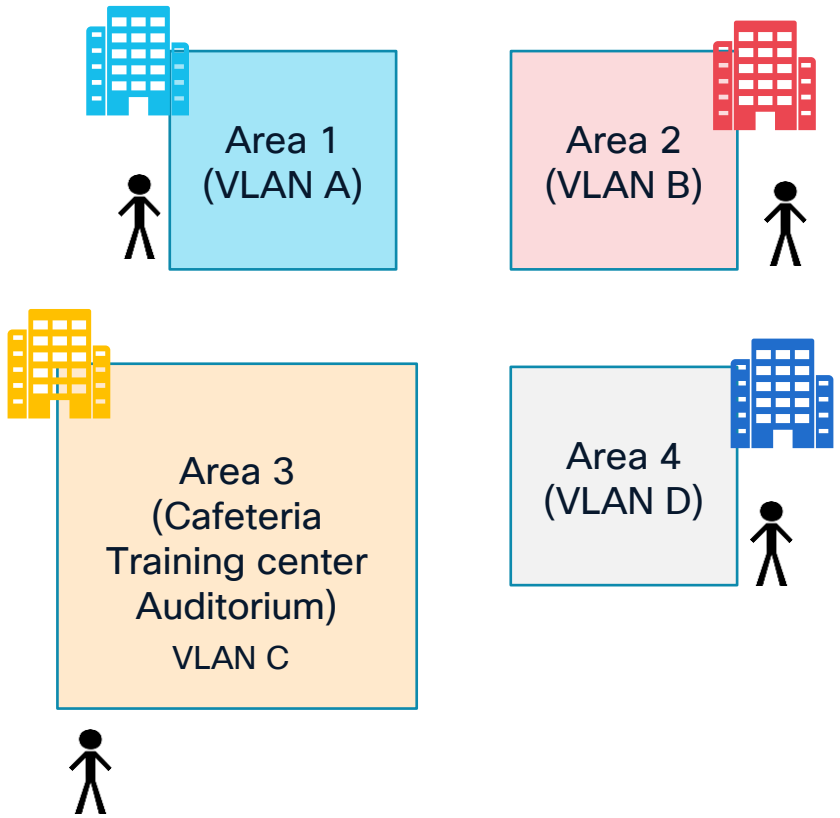


How can you create the L2 overlay?

1. Wired Fabric
2. Centralized Tunneling (VXLAN)

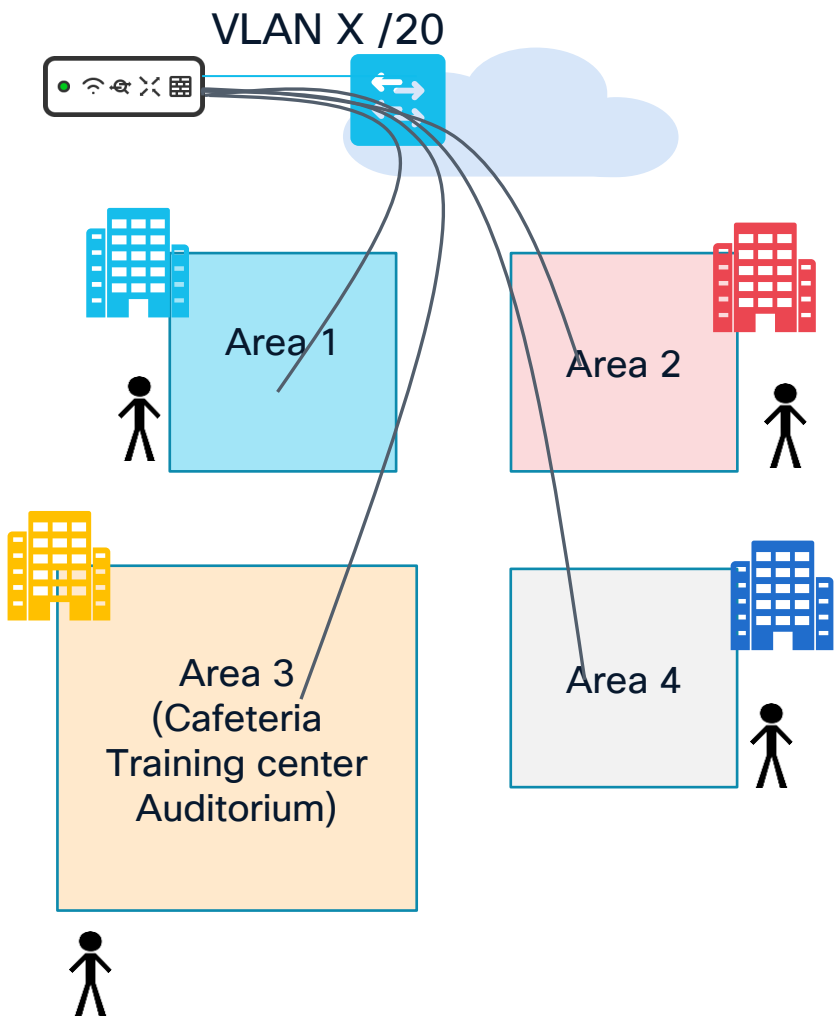
- Traffic is centralized, client VLANs exist only between Campus Gateway and distribution/core switch

Distribute or Centralize? VLAN/DHCP considerations



- For Distributed data plane deployment consider that any new SSID means new VLAN/Subnet that you need to add on the trunk port for every AP
- Also additional VLAN/subnet means defining the L3 interface, routing and the related DHCP scope
- Size your DHCP scope considering all the possible devices that could join in that area but also roaming devices from other areas. This is important to prevent DHCP scope starvation

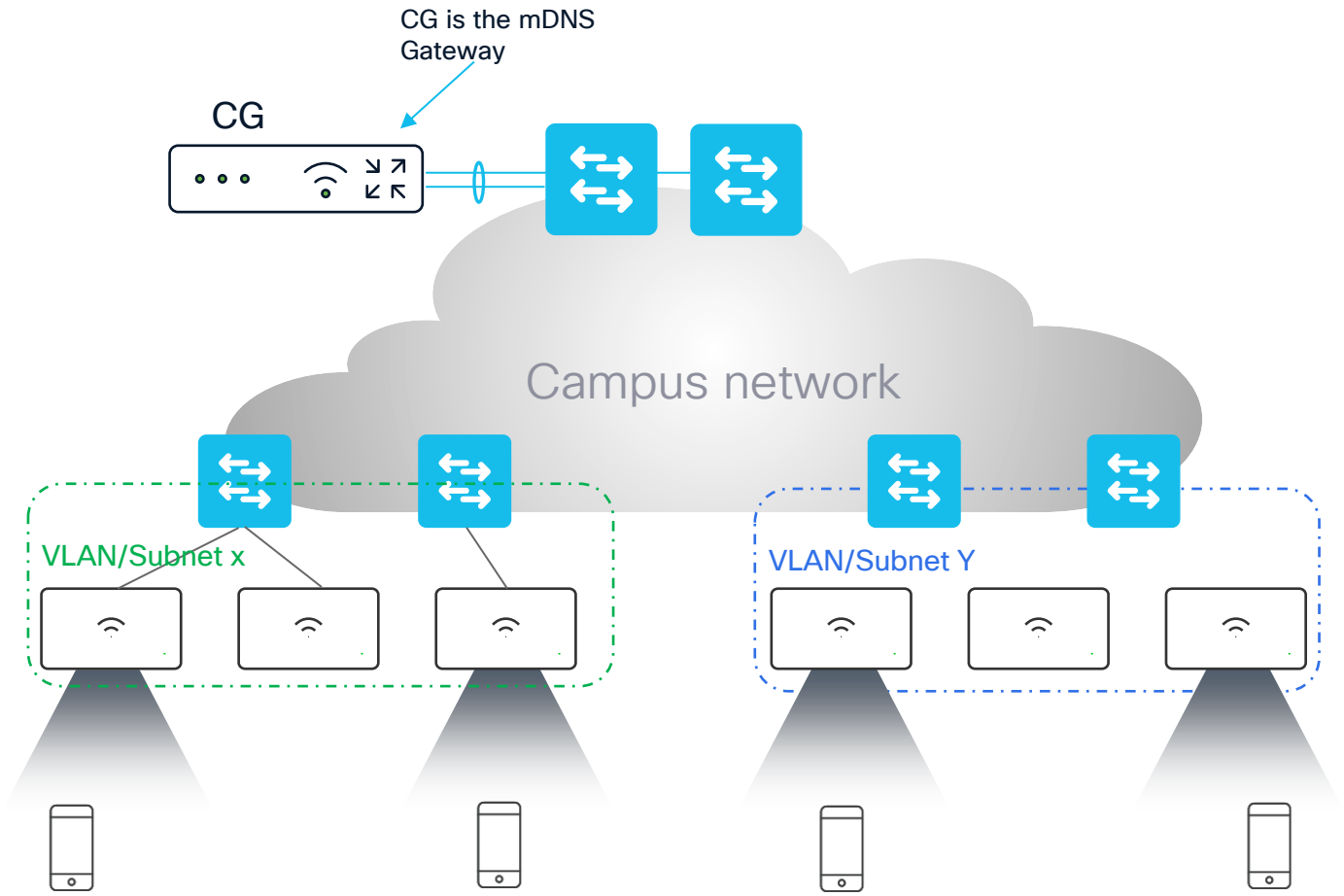
Distribute or Centralize? VLAN/DHCP considerations



- For Distributed data plane deployment consider that any new SSID means new VLAN/Subnet that you need to add on the tru trunk port for every AP
- Also additional VLAN/subnet means defining the L3 interface, routing and the related DHCP scope
- Size your DHCP scope considering all the possible devices that could join in that area but also roaming devices from other areas. This is important to prevent DHCP scope starvation

- For Centralized data plane it's easier as as you just need to add the VLANs in one place, on the connection between edge and distribution switch
- For DHCP scope, you can simply have one large subnet (/20, /16 are typical in high scale deployments) and call it the day
- Of course, you need to make sure that the distribution/core switch/es can scale to the number of MAC and ARP entries for the clients supported by Campus Gateway.

Distribute or Centralize? mDNS considerations



mDNS

- If you need mDNS at scale, you need to work across VLANs and you need a filtering function > You need mDNS Gateway function
- There is no mDNS gateway function for Meraki Bridged mode
- To scale, you need to deploy mDNS Gateway as a centralized function in Campus Gateway

Campus Gateway

Campus Gateway

Available now!

Enterprise-class cloud functionality

Support critical campus wireless services with cloud management and real-time control plane

Deploy without redesign

Deploy Campus Gateway with little to no redesign of the on-premises wireless network architecture

Seamless roaming at scale

Scale for up to 50,000 client devices and 5,000 access points with a single Campus Gateway

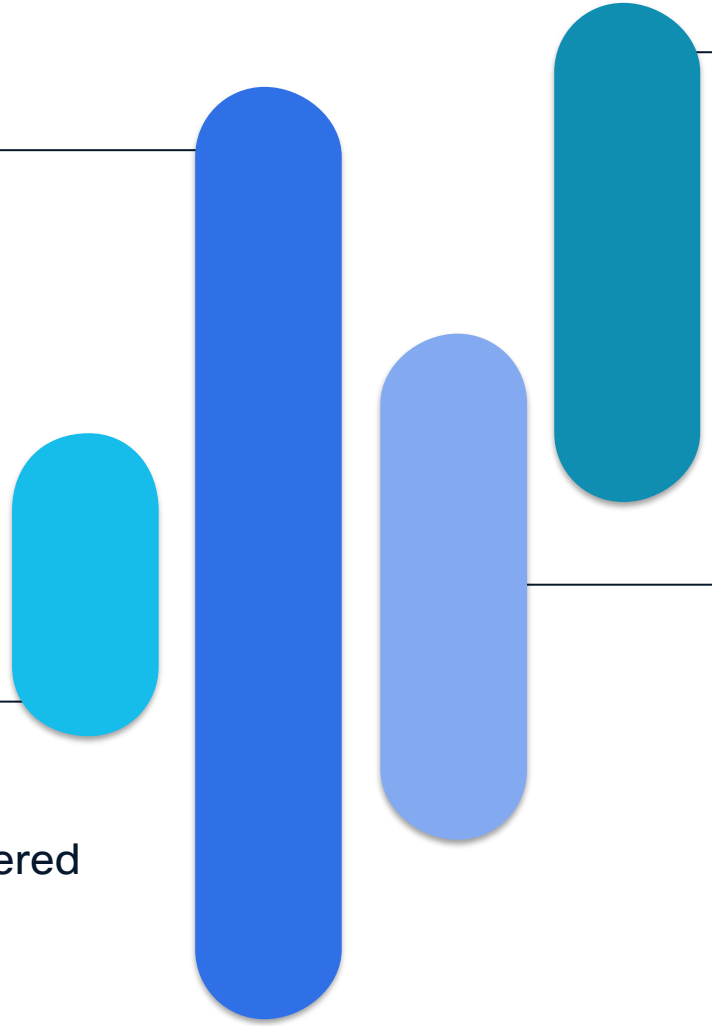
Campus Gateway: Feature set at launch

Infrastructure

ARP proxy
Active- Active Redundancy
LAG support
VLAN pooling
Tunnel configuration per SSID
Client isolation/P2P Blocking
BUM traffic blocking
IPv6 client support

Performance & Scale

Scale to 5,000 APs and 50,000 Clients
100Gbps throughput & 200Gbps Clustered



Security

Radius Proxy
AAA Override & CoA
Named VLAN override
L3 and URL ACLs
Adaptive Policy(SGTs)

Services

QoS (DSCP marking UP/DW)
Traffic Inspection & Classification at AP
mDNS Gateway
Wi-Fi Personal Network (WPN)

Campus Gateway: Hardware Platform

SKU	CW9800H1-MCG	
Throughput	up to 100 Gbps	
Number of APs	5,000	
Number of clients	50,000	
Data ports	8 x 1 GE / 10 GE SFP	4 x 25 GE ports

Campus Gateway – Supported Access Points

Supported Access Points

Wi-Fi 6
MR44, MR36, MR36H MR46, MR46E, MR56, MR76, MR78, MR86

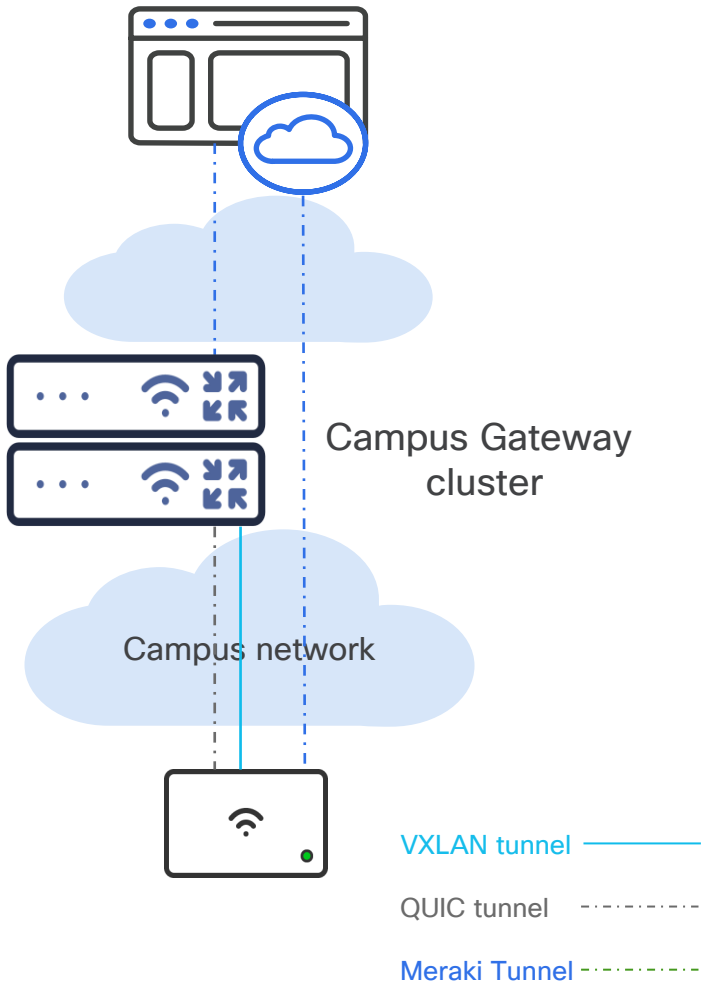
Wi-Fi 6E
MR57, CW9162, CW9163, CW9164, CW9166

Wi-Fi 7
CW9178, CW9176, CW9172i, CW9172H

Minimum Software

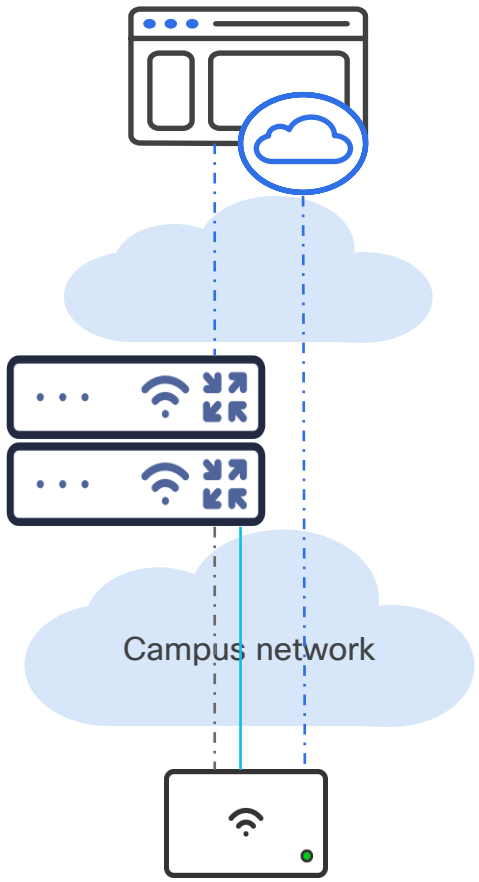
MR Release R31.2

Campus Gateway Architecture



- Campus Gateway and AP are directly managed by Meraki Dashboard like any other cloud managed node
- Campus Gateway adopt a centrally switched architecture, using tunneling, to create a L2 overlay for client traffic
- Tunneling to CG is configured on a per SSID basis
- At FCS, some architecture limitations apply:
  - Campus Gateway and AP need to be part of the same Meraki Network (new or existing Network)
  - Campus Gateway and AP should be part of the same geo location (RTT<20ms) > Focus at FCS is on Campus deployments
  - Only one Campus Gateway cluster is supported per Meraki Network
  - Two Campus Gateway nodes per Cluster

Campus Gateway Architecture



Meraki Dashboard

Management Plane
- Configuration management
- Monitoring & Troubleshooting
- Software management
- Licensing. etc.
- Serviceability/debugging

Non-real time Control Plane
- RRM (AI-RRM)
- AirMarshall
- Rogues
- etc.

Campus Gateway

Data Plane
- Data plane termination
- VLAN termination
- mDNS Gateway

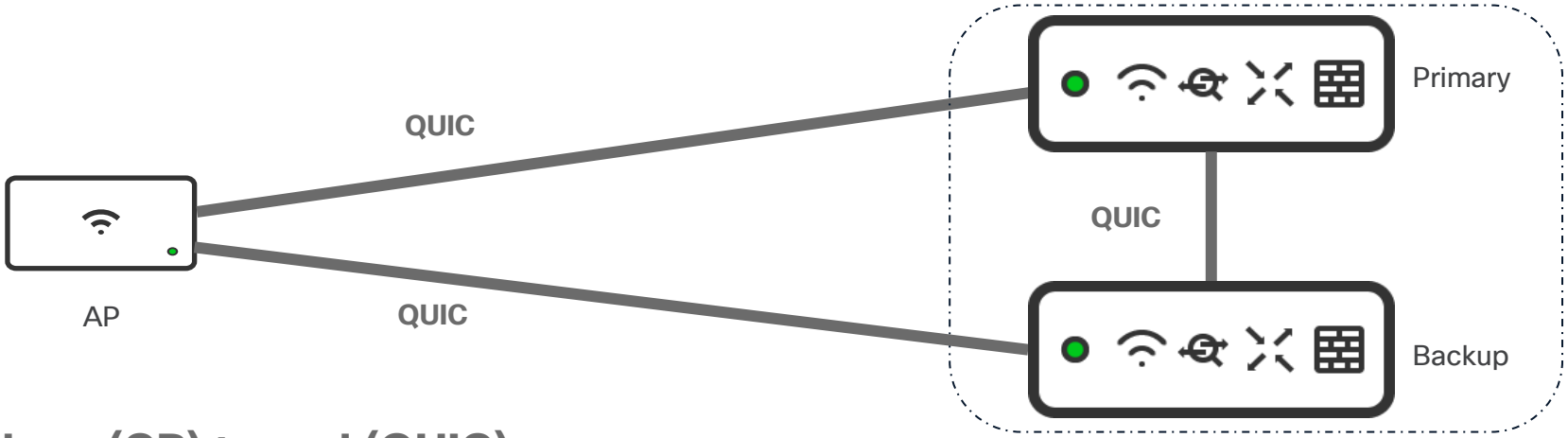
Real time Control Plane
- AAA Proxy
- Roaming - Key management
- Dstore (client DB)

Access Point

Data Plane
- Bridge local SSIDs
- Tunnel central SSIDs
- QoS
- Rate Limit
- Adaptive policy tagging

Real time Control Plane
- Client Authentication
- Client state machine
- Telemetry

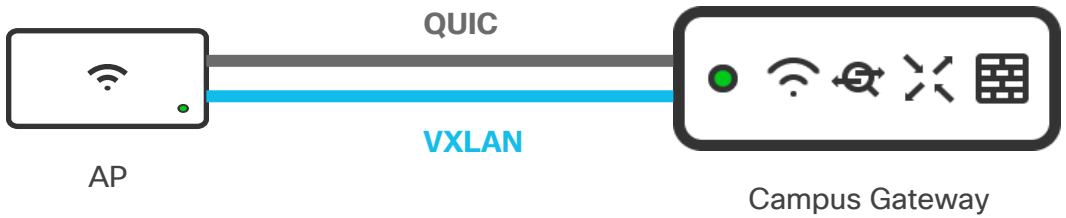
Campus Gateway -> Control Plane Tunnel



Control Plane (CP) tunnel (QUIC)

- Each AP establishes two QUIC tunnels to both Primary and Backup Campus Gateway
- CP tunnel is based on QUIC protocol. UDP based, Reliable tunnel (keepalives to check reachability)
- CP traffic is always encrypted (TLS 1.3) using Dashboard-provisioned keys or certificates
- Used for carrying CP messages such as AP registration, client anchoring, etc.
- Also used for special packets such as HA messages and inter-Campus Gateway control messages
- On a stable network, the QUIC tunnel is expected to consume few kbps

Campus Gateway -> Data Plane Tunnel

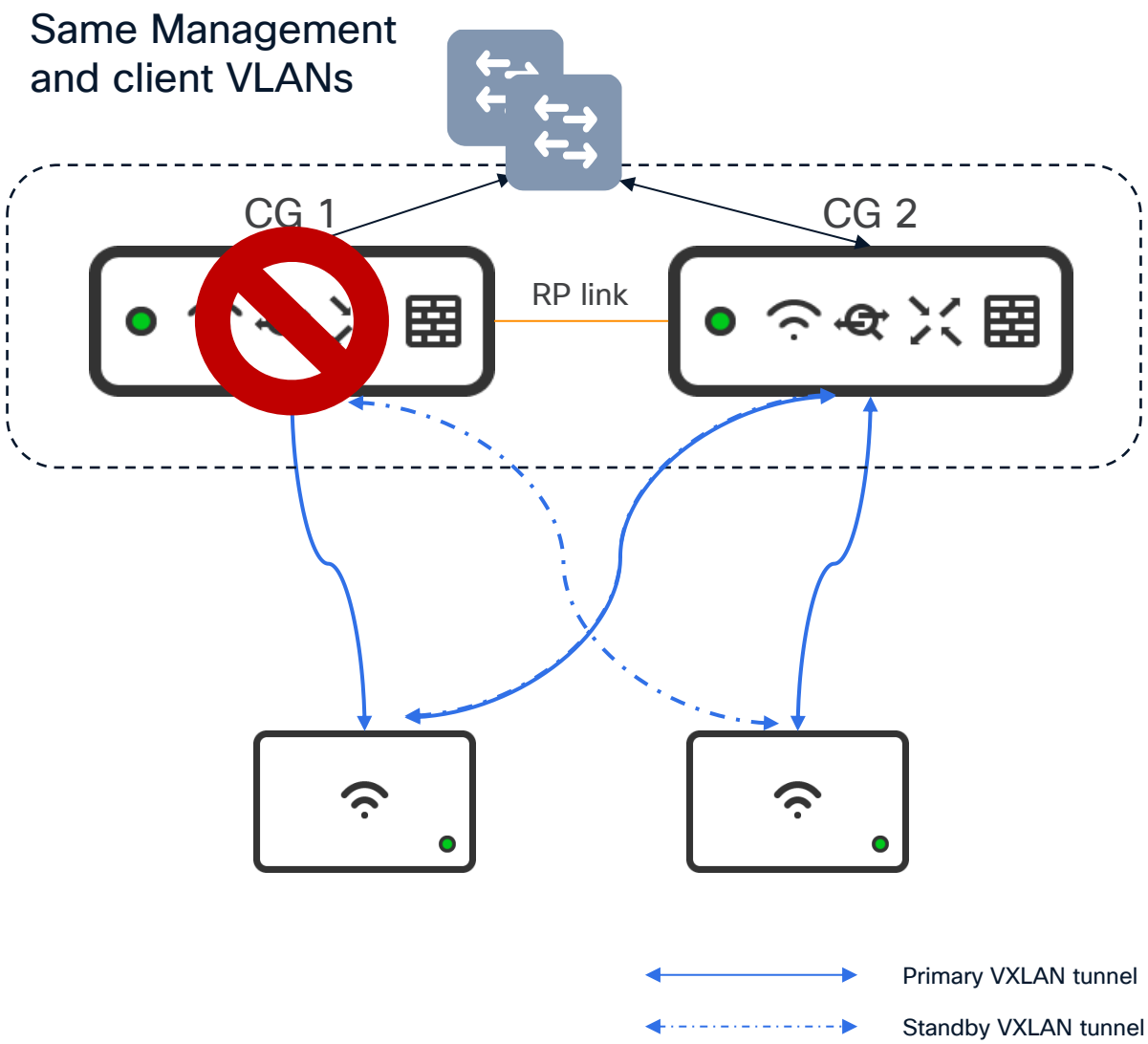


Data Plane (DP) tunnel (VXLAN)

- Each AP has one VXLAN tunnel to the primary Campus Gateway
- Used for carrying client data packets which are bridged onto the client VLANs at Campus Gateway
- Leverages standard VXLAN encapsulation
- QoS and policy information (e.g., DSCP, SGT, VRF) carried in the tunnel header
- RADIUS messages are also carried inside VXLAN tunnel

At FCS, only SGT segmentation is supported via Adaptive Policy. VRF support is not yet on a committed roadmap

Campus Gateway – Active/Active High Availability



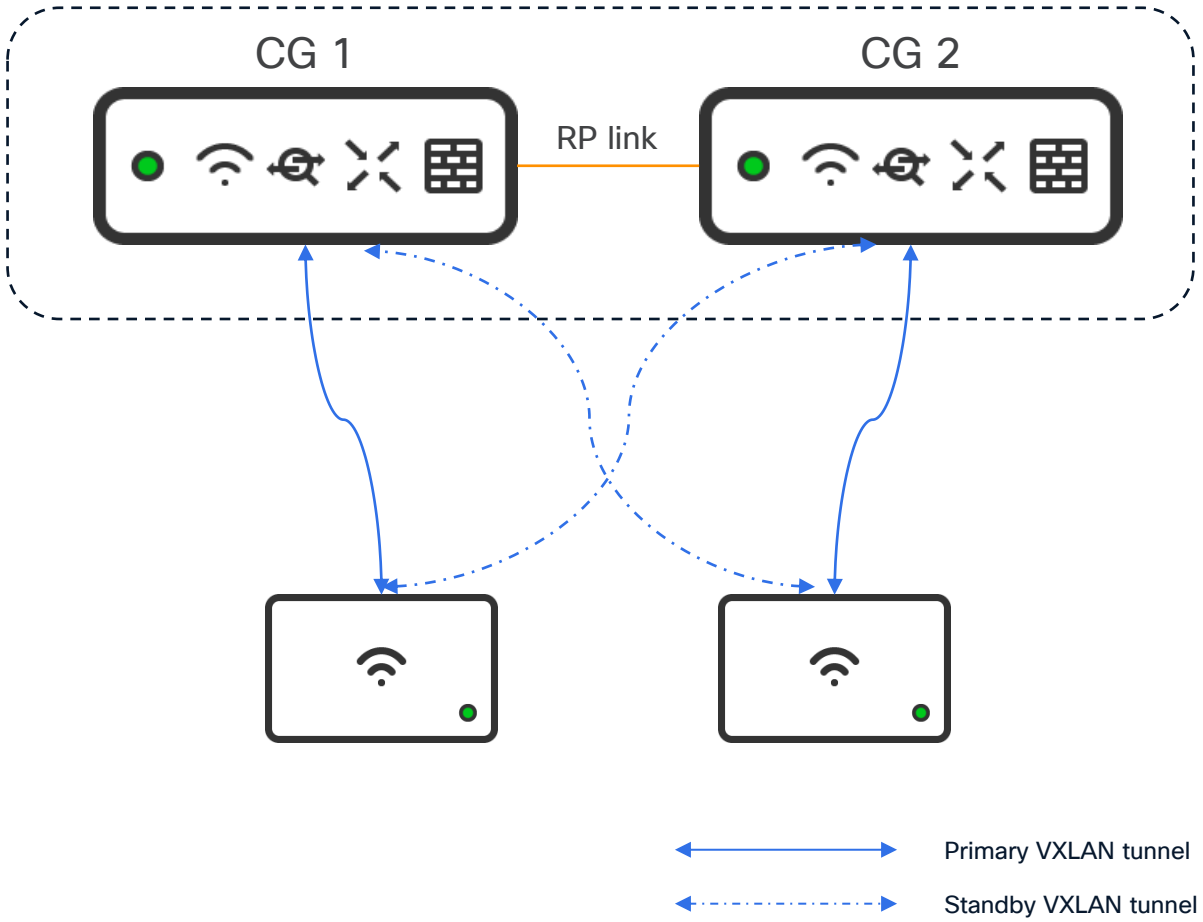
A cluster represents a group of CG with connectivity to a common set of VLANs.

Active-Active High Availability, with APs load balanced across the CGs in the cluster

Each AP is configured with a Primary and Preferred Backup Campus Gateways

When Primary CG node fails, the connected APs automatically failover to the Backup CG

Campus Gateway – Active/Active High Availability



Campus Gateway supports stateful, zero downtime failover for single node failure

If the dedicated Redundancy Port (RP) port is connected, Client and AP state are statefully synced between the CGs

RP port need to be connected via a L2 link (copper or fiber), either direct or through a dedicated VLAN

RP link is also used for fast keepalives 100ms. RP link latency <80 ms, Bandwidth > 60 Mbps and MTU >= 1500B

When should you consider a Campus Gateway?

Services @scale

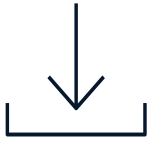
- Roaming across L3 boundaries
- Fast Roaming across a large domain (> 200/300 APs)
- mDNS Gateway function

Wired Network Design

- Want to simplify VLAN/Subnet design at the access layer
- Want to simplify DHCP scope design
- Don’t want to touch the underlay wired design

Policy

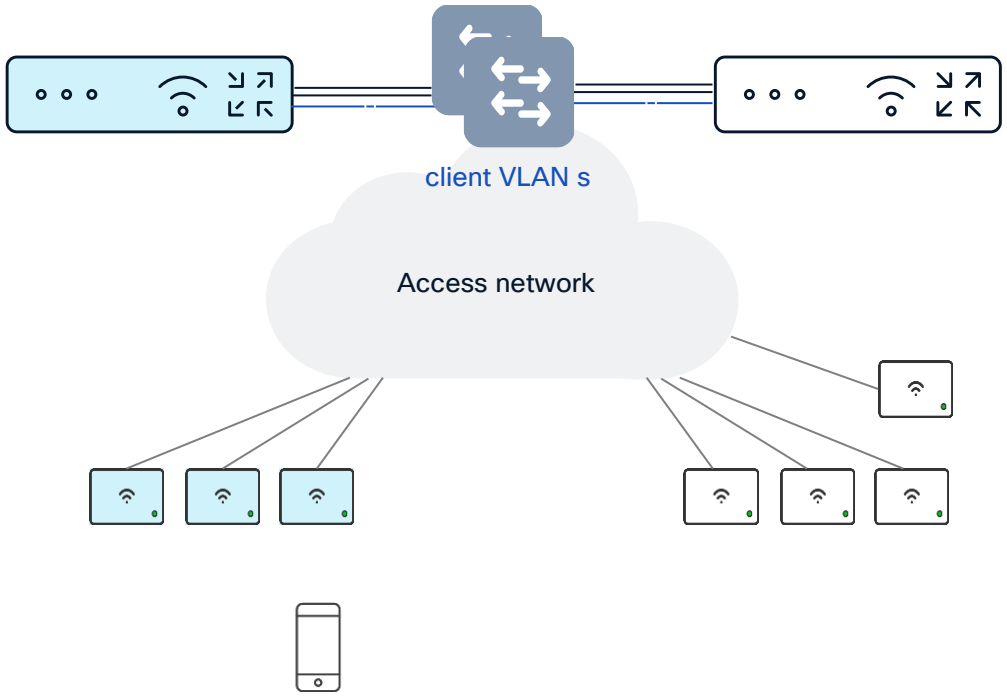
- Single policy (QoS, ACL, etc.) enforcement point for wireless traffic
- Single NAS to be configured in AAA server
- Simple way to handle BUM traffic



Performance

- Optimized for North-South traffic
- Centralized aggregator is not a bottleneck
- No latency impact for the “trombone” network effect

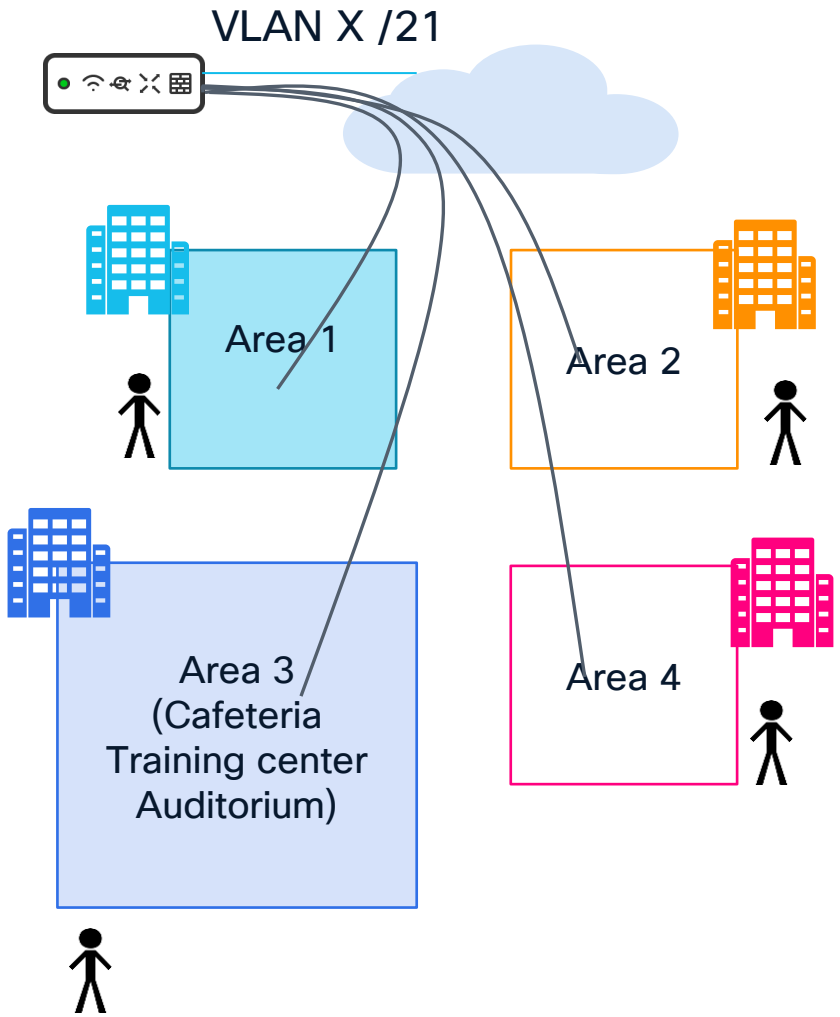
WLC to Campus Gateway migration



- Customers have a WLC deployment with Wi-Fi 6/6E and 7 and older APs. How to deploy Campus Gateway to migrate to a cloud native solution?
- Steps to migrate:
  - Install CG into the network: use same client VLANs > connect to the same L3 distribution switch. Add Campus Gateway as NAS in AAA server
  - Migrate compatible APs to the same Meraki Network as Campus Gateway. Refresh older APs and add the new ones to Campus Gateway network
- Recommendations:
  - Use same SSIDs mapped to the same VLANs (statically or dynamically) to allow for seamless roaming
  - Roaming will require a full re-auth so it will not be fast roam
  - Migrate an area/roaming domain at the time (if possible)
  - Disable DHCP Required / Mandatory DHCP for the roaming to be faster

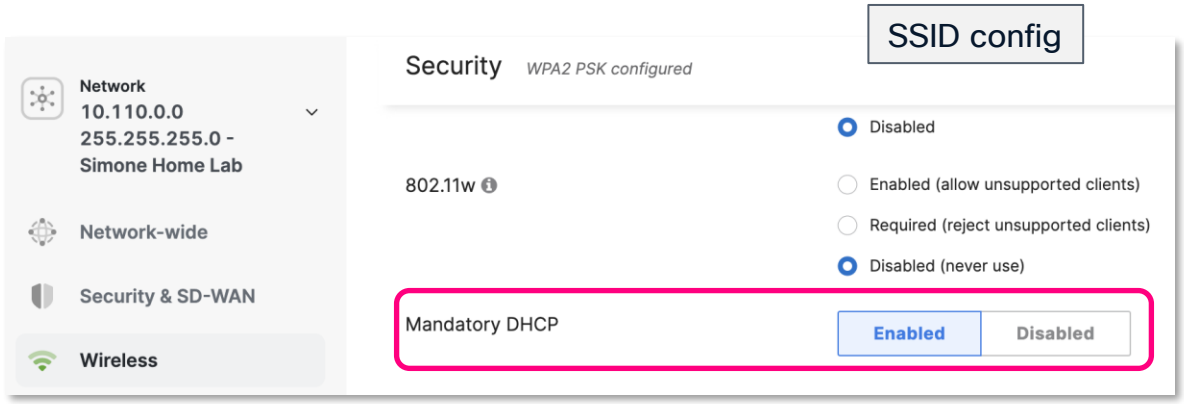
Design Best Practices

DHCP Lease design considerations



- Independently of Distributed or Centralized data plane deployment DHCP Lease is very important to reduce the load on DHCP server, prevent starvation and security issues.
- The recommendation for DHCP lease: Align it to the the average dwell time in that environment. For example:
  - Set it to 12 hours for normal office deployments
  - Set it to 8 hours for Universities
  - Set it to 1 hour for Retailers
  - Set it very low (e.g., 30 mins) for security reasons (reduced unauthorized time) but there is an impact on the DHCP server. Also consider Random MAC > keep DHCP lease lower to avoid starvation

DHCP Mandatory

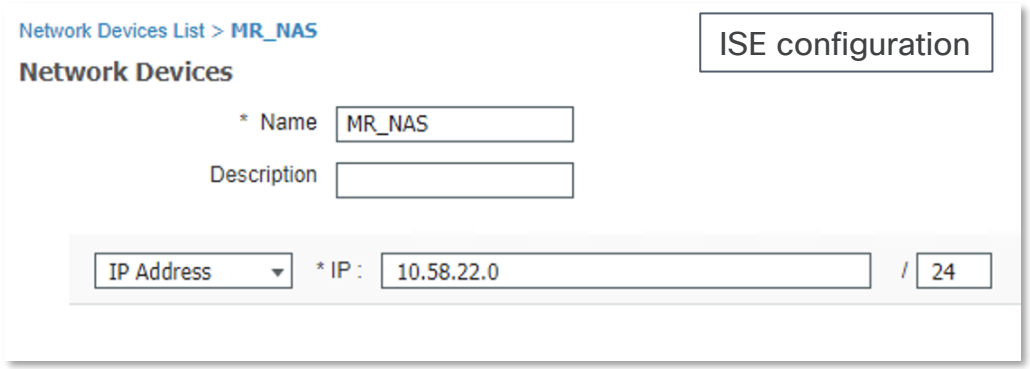


- Set DHCP Mandatory on your SSID access policy, if you don't need Static IP assignment.
  - DHCP Mandatory is a good security practice as system learns and records IP to MAC binding for each client
  - DHCP Mandatory automatically turns on Dynamic ARP inspection (DAI) and IP Source Guard which help in protecting the network from certain "man-in-the-middle" attacks and IP spoofing, respectively.
  - If few clients with static IPs need to be supported, consider DHCP reservation on the DHCP server
- Important: Not supported for IPv6 only clients. For dual stack IPv4/v6 please deploy r32.1.x or above

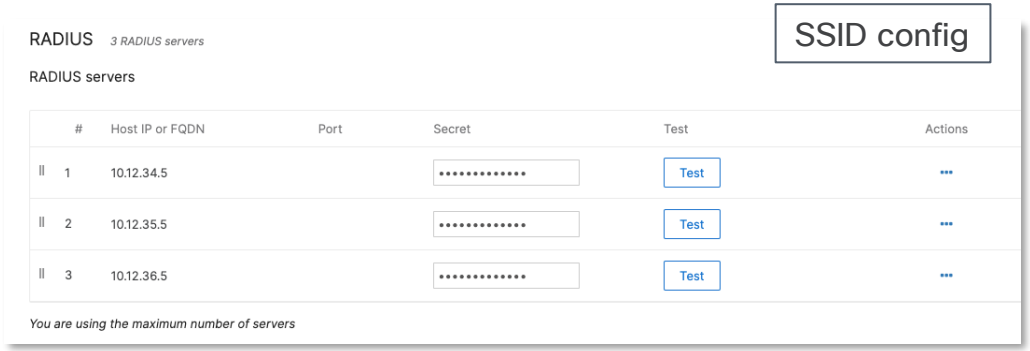
Did you disable Mandatory DHCP because you saw roaming issues?

- Note: Fixed in Dashboard starting June 2024. For existing SSIDs please disable and re-enable the feature. Fix is automatically applied for new created SSIDs

Security design considerations



ISE configuration



SSID config

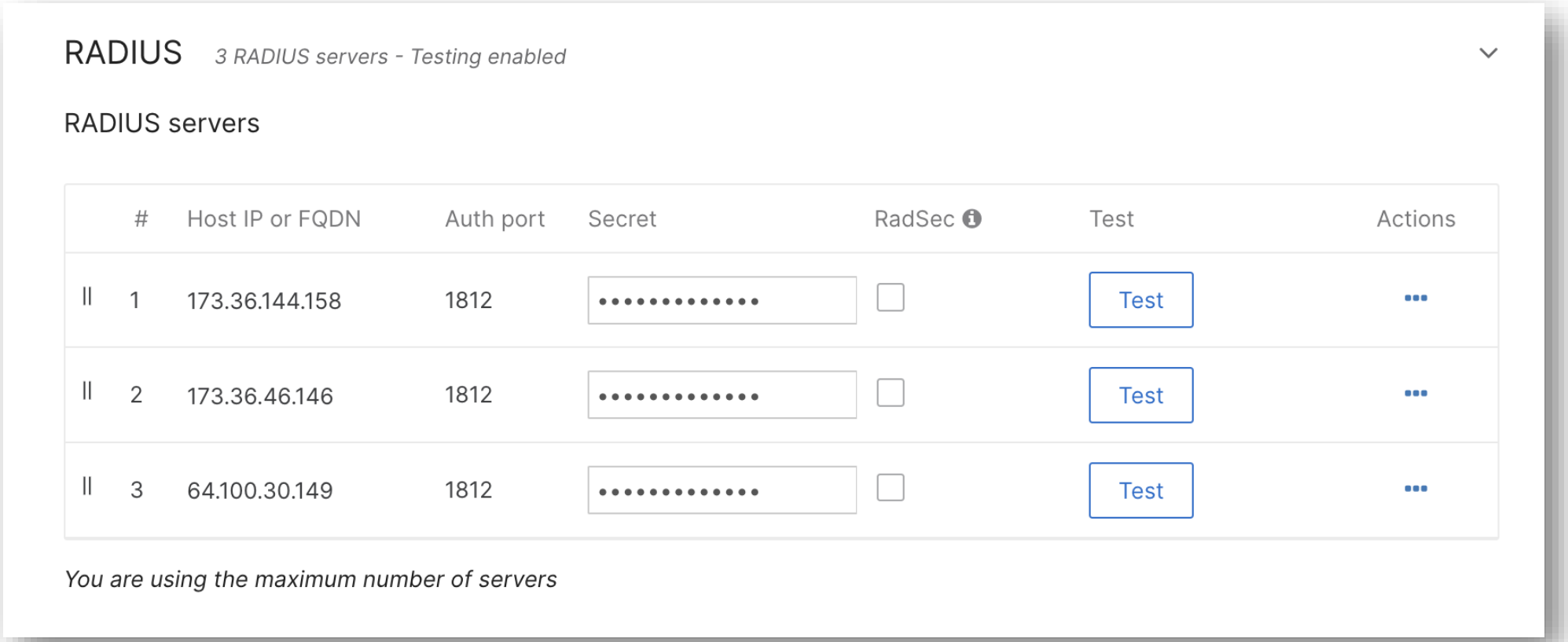
- For Bridged SSIDs, each AP talks to AAA server for 802.1x authentication and must be configured as Network Access Server (NAS); to avoid entering each AP's IP address, majority of the AAA servers on the market allow the definition of a subnet as NAS. **Recommendation**: Make sure you design the APs subnets to be summarized in a larger one

- Meraki has a limit of max #3 AAA servers per SSID. Usually this is not a constrain. For large, high-density deployments, you might consider placing a load balancer in front of the AAA servers. Configure source based sticky load balance, to make sure that each client session always talk to the same AAA if alive.

Security design considerations

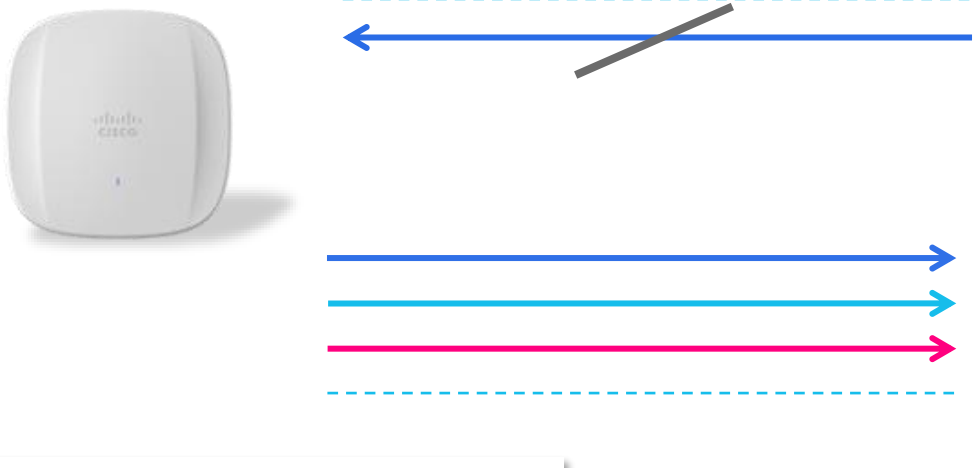
Radius server load balancing policy

APs support only strict priority order load balancing policy

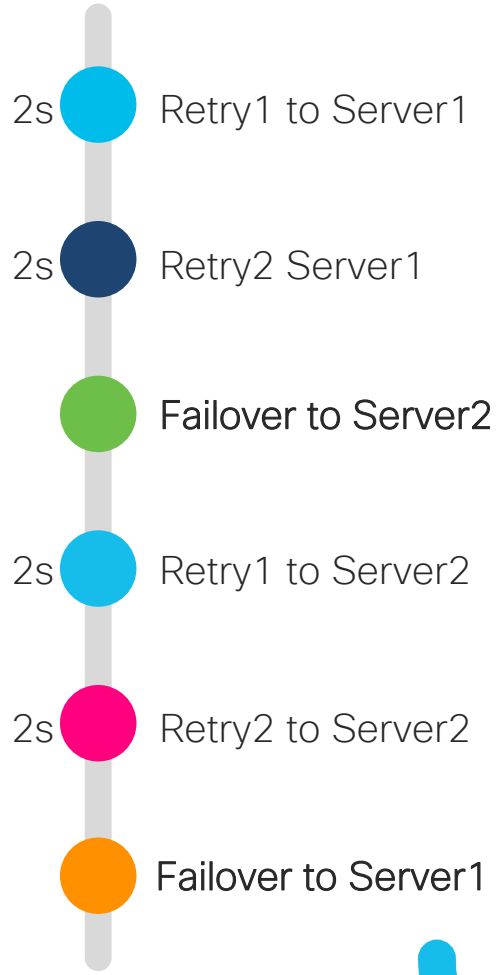


Security design considerations

RADIUS messages will be sent to servers in a top-down order

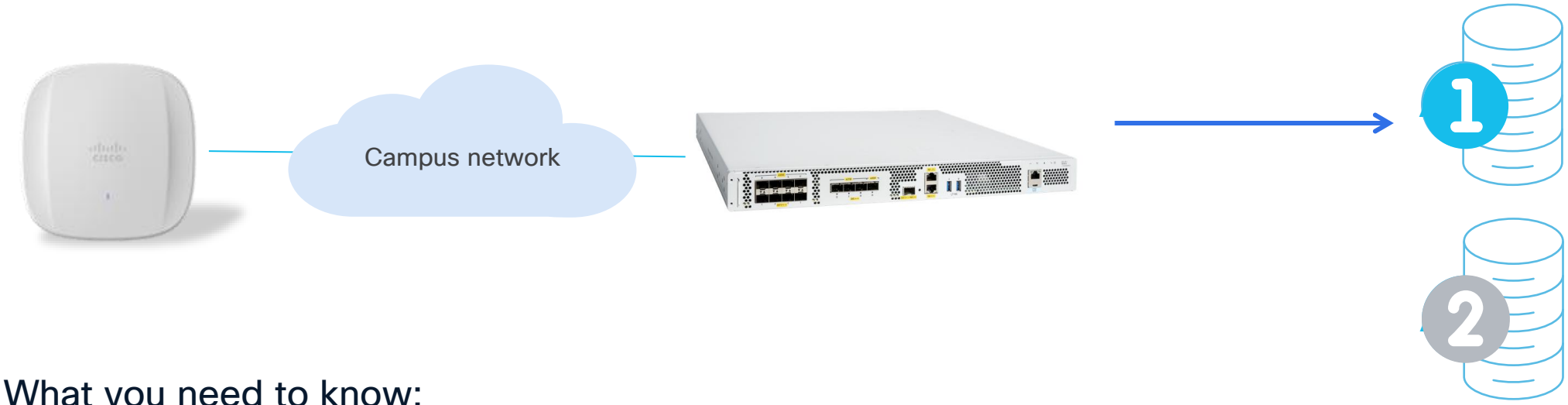


Server timeout	2	second(s)
Retry count	2	



Security design considerations

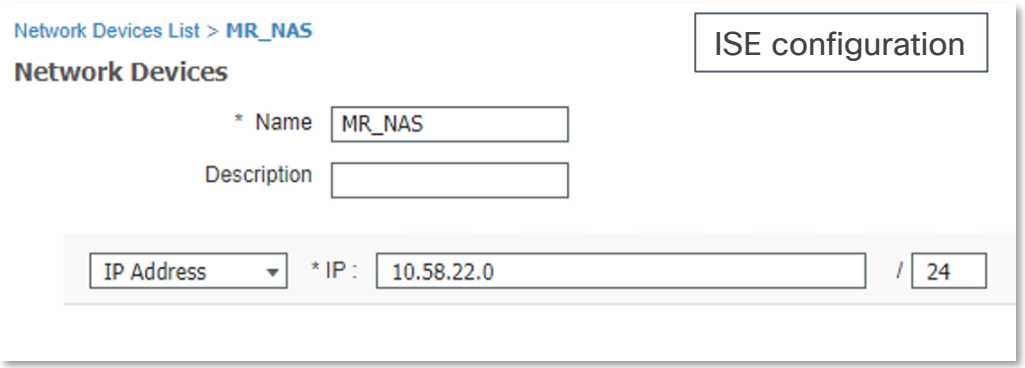
CG as Radius proxy



What you need to know:

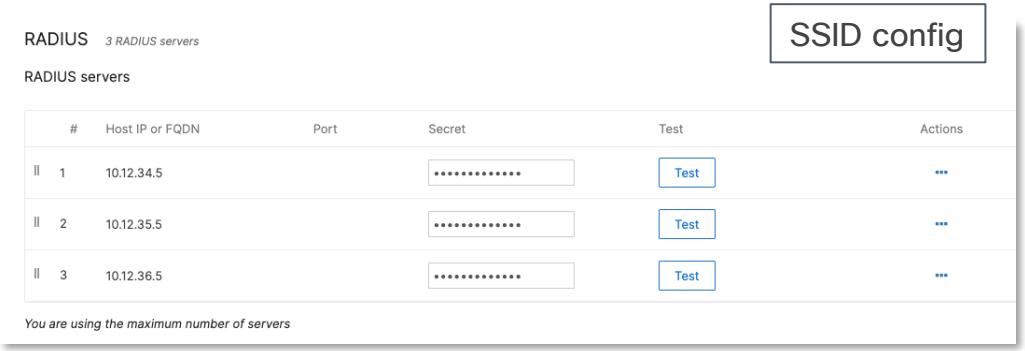
- APs always talk Radius to CG, doesn't do any load balancing and doesn't know about the external servers
- CG acts as proxy Radius > one NAS for the entire Network
- By default, CG has the same load balancing mechanism of APs, priority order. Round-robin load balancing can be configured via Meraki Support
- Since there is only one AAA server per CG, if you have multiple SSIDs with different Advanced RADIUS settings (NAS ID, Called-station-ID, timers, etc.), the settings from the first defined AAA server would be honored
- Note: at FCS, the test command to verify user credentials is not available on SSID with CG

Security design considerations



ISE configuration

- For Bridged SSIDs, each AP talks to AAA server for 802.1x authentication and must be configured as Network Access Server (NAS); to avoid entering each AP's IP address, majority of the AAA servers on the market allow the definition of a subnet as NAS. **Recommendation**: Make sure you design the APs subnets to be summarized in a larger one



SSID config

- Meraki has a limit of max #3 AAA servers per SSID. Usually this is not a constrain. For large, high-density deployments, you might consider placing a load balancer in front of the AAA servers. Configure source based sticky load balance, to make sure that each client session always talk to the same AAA if alive.

Session timeout

- Session timeout is the maximum time for a client session to remain active before requiring reauthorization.
- This is set to 2 days (172800s) and cannot be changed in Dashboard. Call Meraki support if need to change it on the SSID
- Or use AAA to set it dynamically on a per user/client session

Monitoring and Troubleshooting

Simplify, Accelerated NetOps through AI

Cisco AI Assistant and AI Canvas

Context-aware conversational interfaces, universal interface across multi-domain Cisco solutions

Automated RCA

Proactive, Systematic RCA and remediation

AI Packet Analyzer

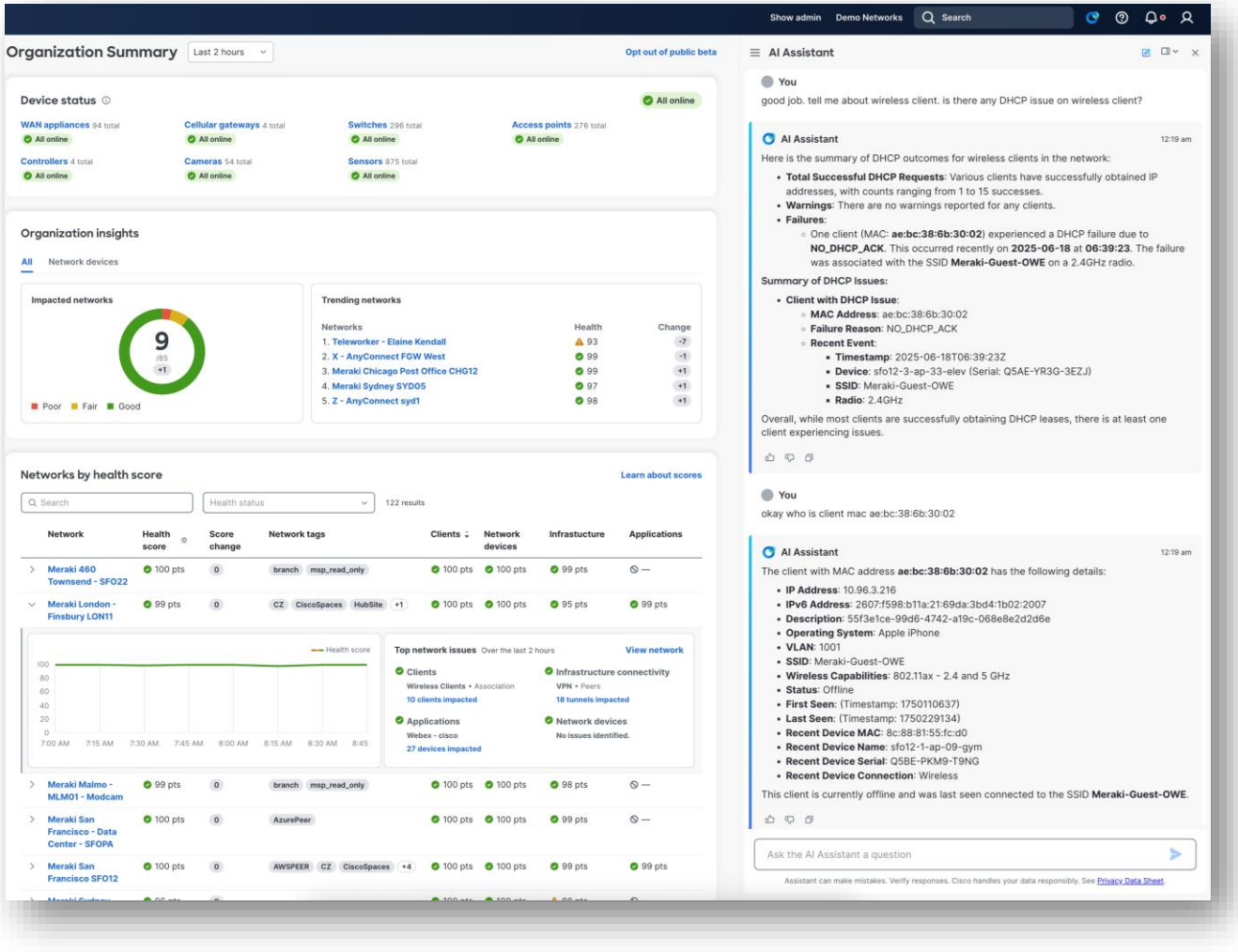
Root Cause Analysis (RCA) for failed client connection

Wireless Synthetic client

Proactive Issue detection from client perspective E2E Visibility

AI Radio Resource Mgmt.

Optimize RF for better wireless performance by reducing interference and channel changes



Cisco AI Assistant

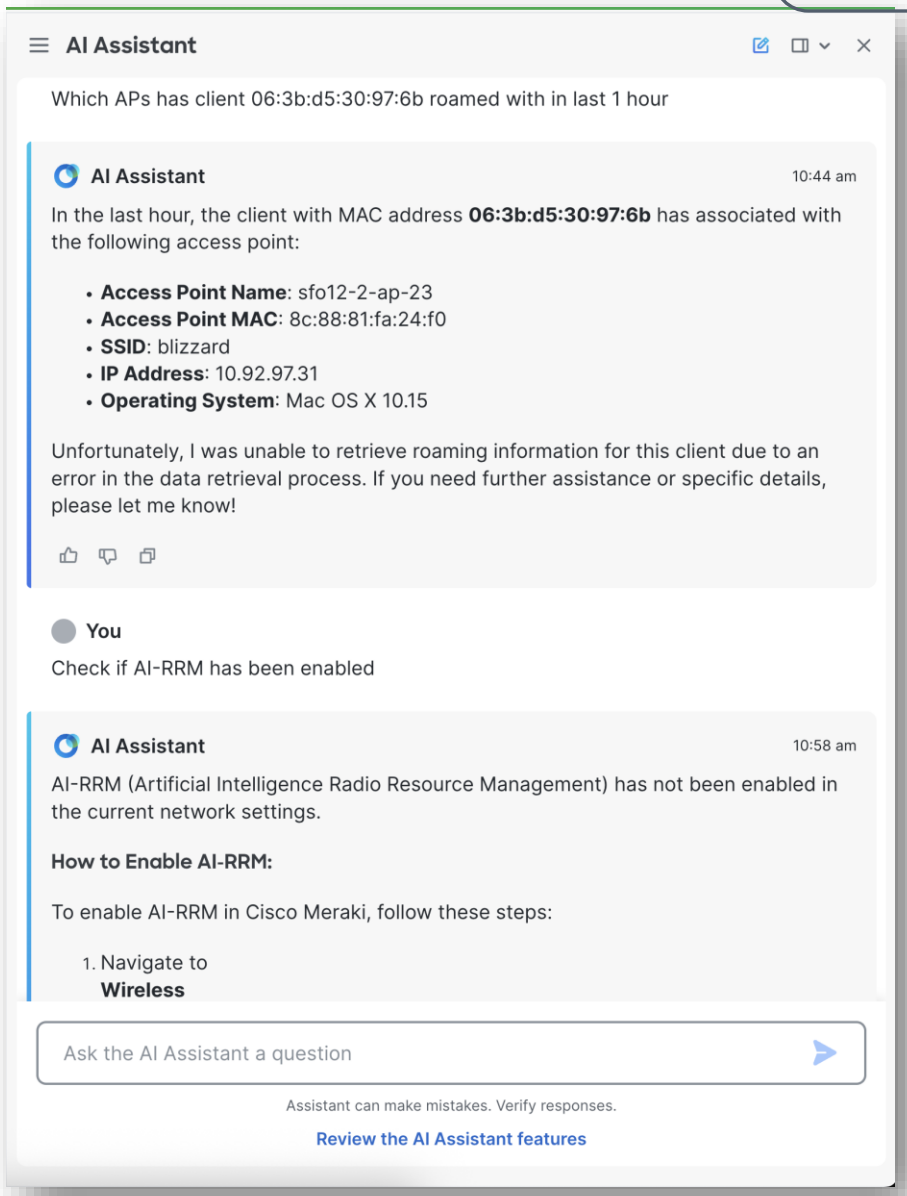
MR-ENT

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

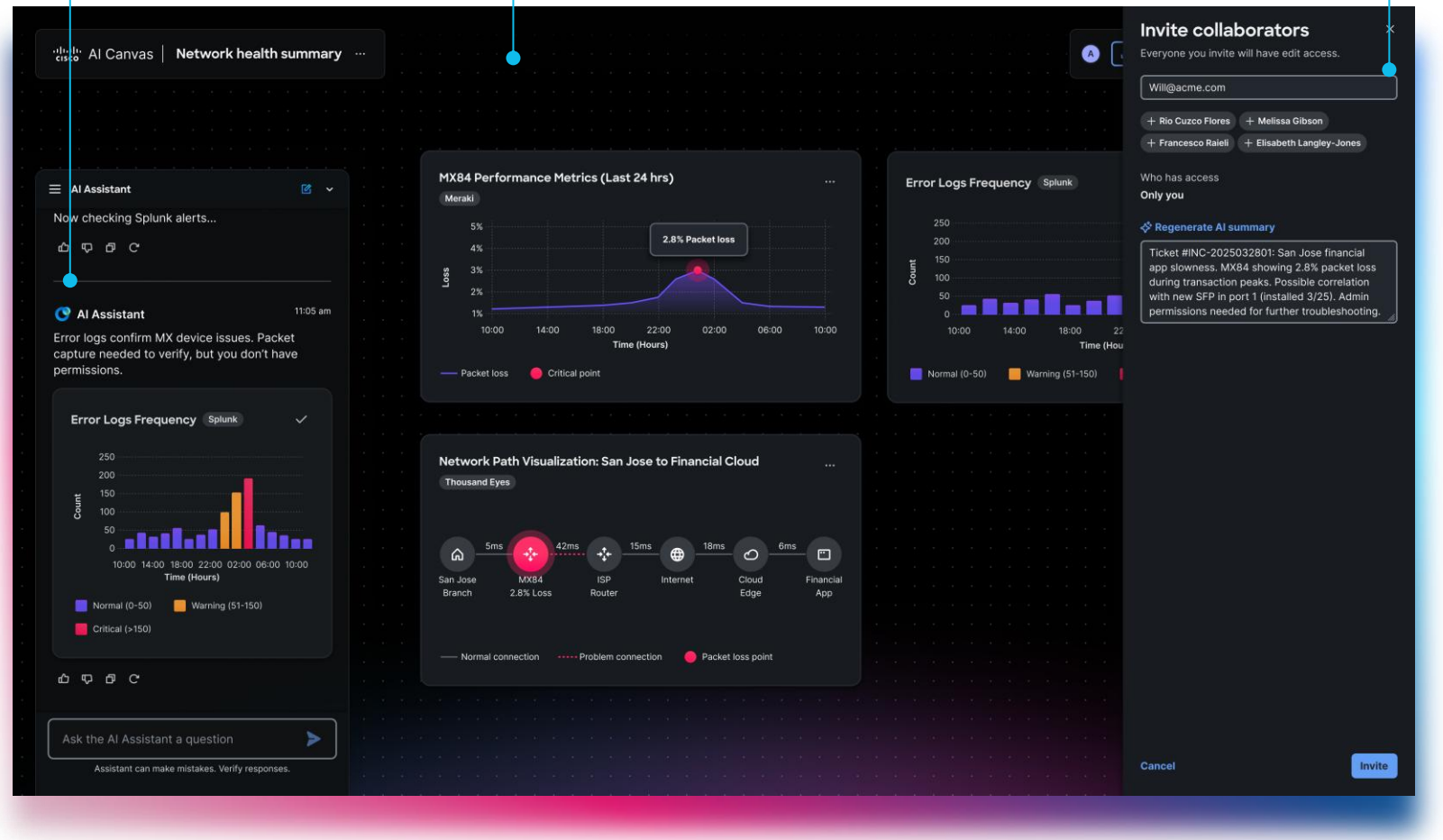
- Acknowledge existing network configuration and provide the best practice network configuration



Cisco AI Canvas

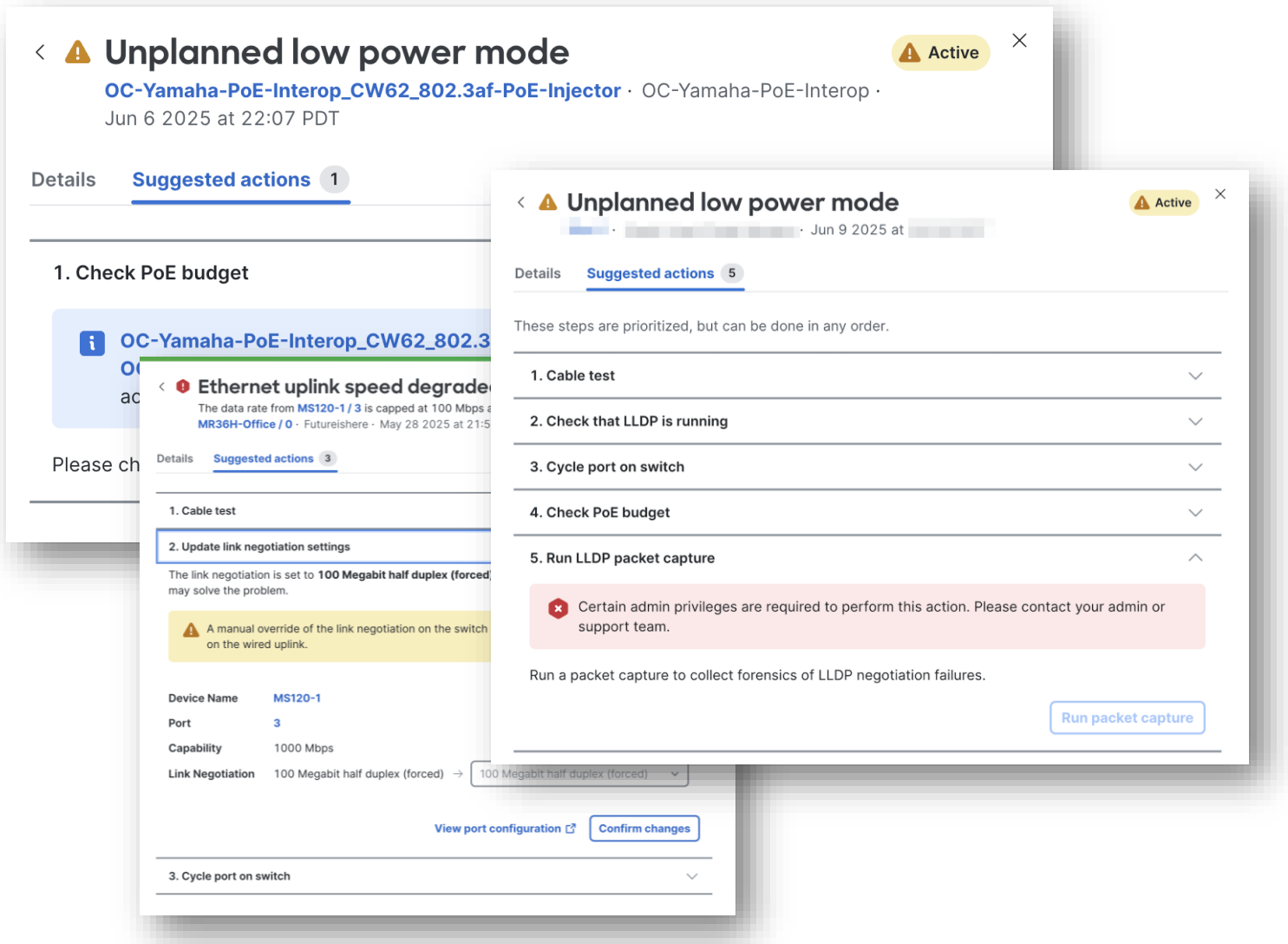
Oct.2025

- Single canvas for cross domain troubleshooting
- Generative UI with reasoning built-in
- Keeps NetOps, SecOps, IT and execs on the same page
- Cross-domain telemetry
- Topology and timeline awareness
- AI-powered insights
- Automated runbooks



Products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis.

Automated Root Cause Analysis (RCA)



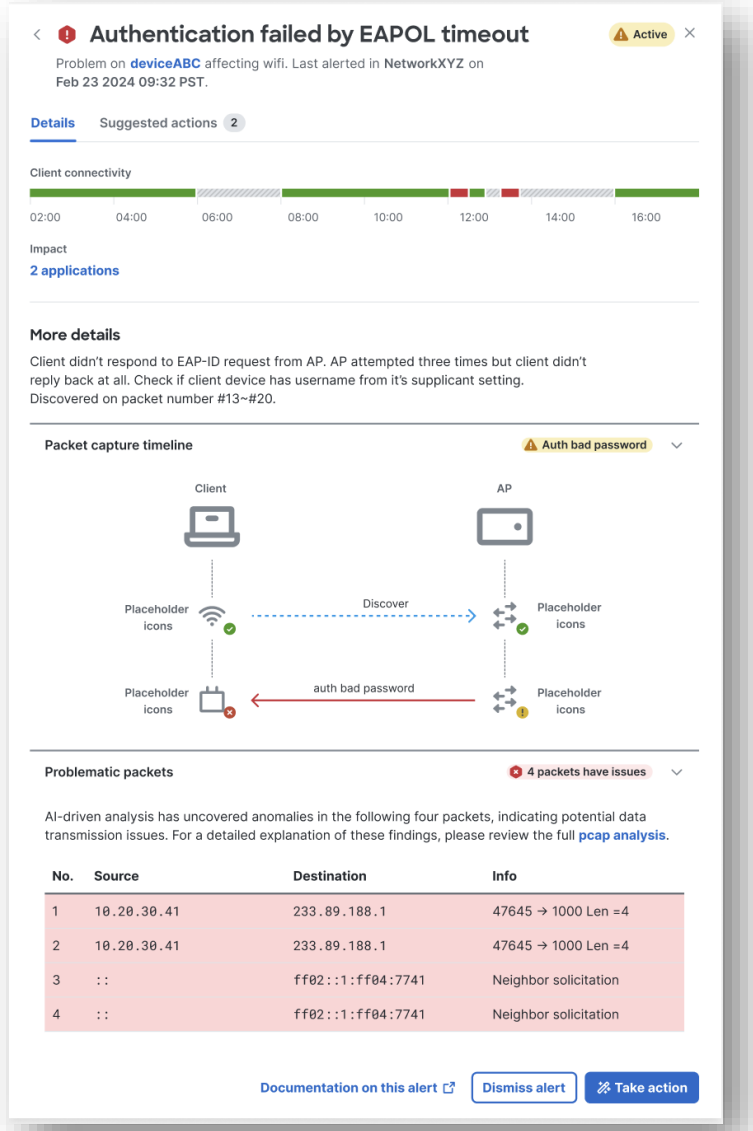
RCA Framework features

- 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

AI Packet CAPture (PACAP) Analysis

MR-ADV

- **AI PCAP analyzer**
  Uses multi-modal AI models using contextualized PCAP model, Client events and configuration data
- **Intelligent capture**
  Automatically seize the moments of client failure and upload PCAP files to AI Cloud
- **AI PCAP model**
  Uses supervised fine-tuning and RLHF to analysis client packet exchanges
- **Generative AI**
  Translate & summarize dozens of PCAP exchanges into human-readable text



Vidcast - Wireless Recom | Meraki Dashboard | Packet Capture - Meraki Dash

n1.meraki.dev.ikarem.io/alice_sim_networ/n/piF_Lcl/manage/clients/k042df3/overview?eventsIncluded=dhcp%2Cdns%2Capplication%2Cauthentication%2Cassociation&t0=17501...

Meraki | Show admin | Demo Networks | Search

Network
alice_sim_network - wireless

Network-wide
Assurance
Wireless
Organization

Find in Menu

This is a Cisco internal organization.

View old version

← Clients

My Phone

Client connectivity

Jun 17 2025 00:04 PDT → Jun 17 2025 05:11 PDT

Association | Authentication | DHCP | DNS | Applications

Current | Offline | Wireless | Jun 17, 2025, 16:23 (UTC -7)

Client connections

Client details

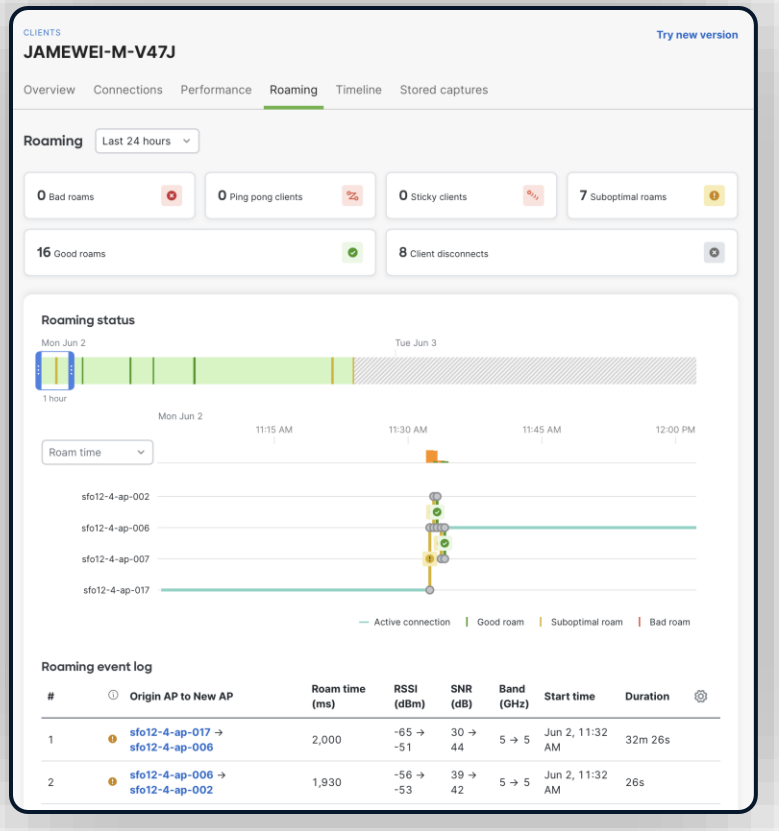
Status	Last seen Jun 17 16:21 View location	IPv4 address	10.4.45.243	Device policy	Normal
SSID	alice_sim_network	IPv6 address	Unknown	Bandwidth	unlimited
Access point	c4:d6:66:62:9b:d0 Topology	MAC address	b8:27:eb:63:11:e7	Layer3 firewall	Unknown
Signal	55db	VLAN ID	Unknown	Layer7 firewall	Unknown
		Port forwarding	None		

English

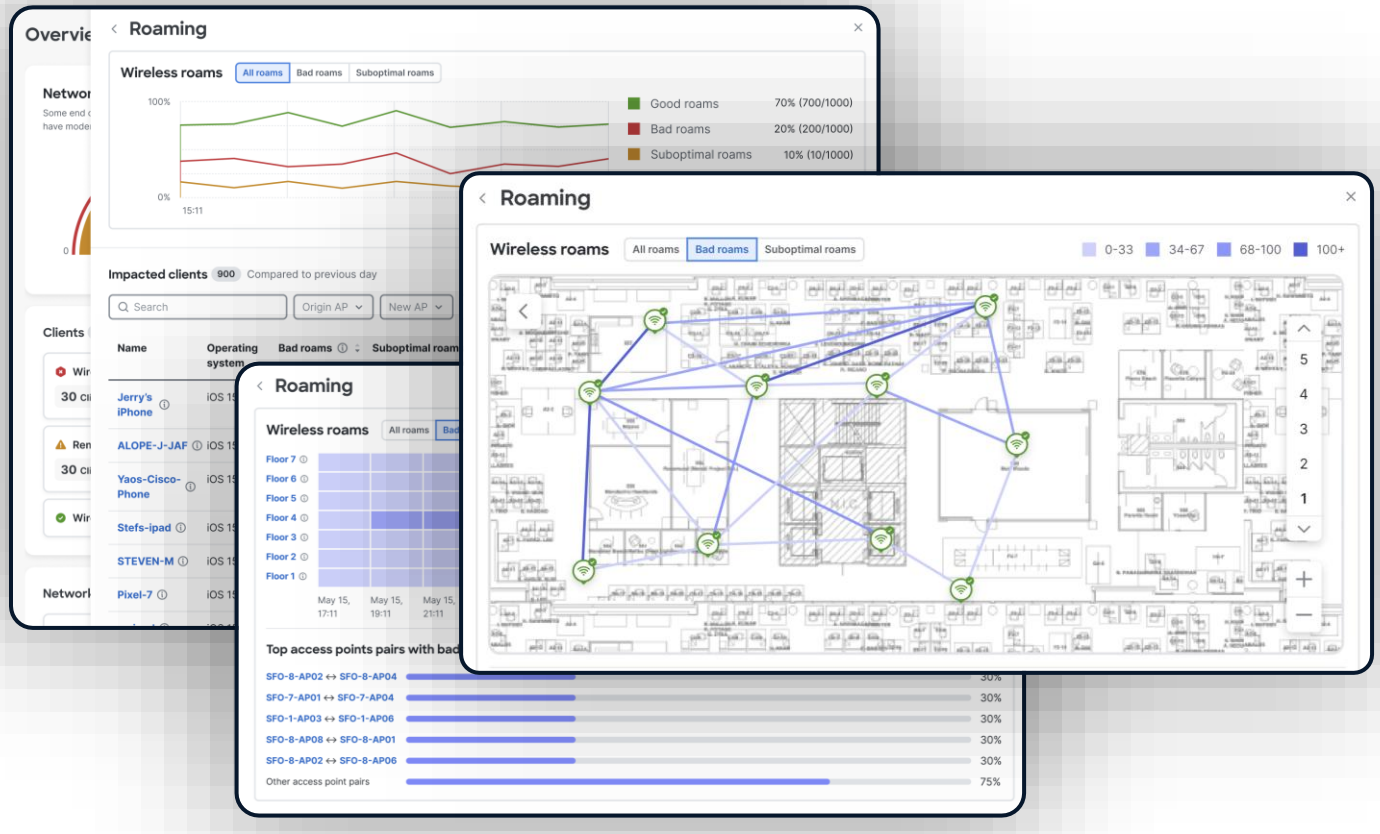
Roaming Analytics

MR-ENT

- Tools for per-device and network-wide troubleshooting



Per-Client Roaming Timeline



Network-wide Roaming Health (coming soon)

Cloud Full stack solution

Early Access – Q4 CY25

Automated network experience monitoring

Integrated Service Assurance — Transform your APs, switches and routers to test network availability and connectivity

End-to-end tests — Client onboarding, connectivity (Wireless, LAN, WAN) and network services tests

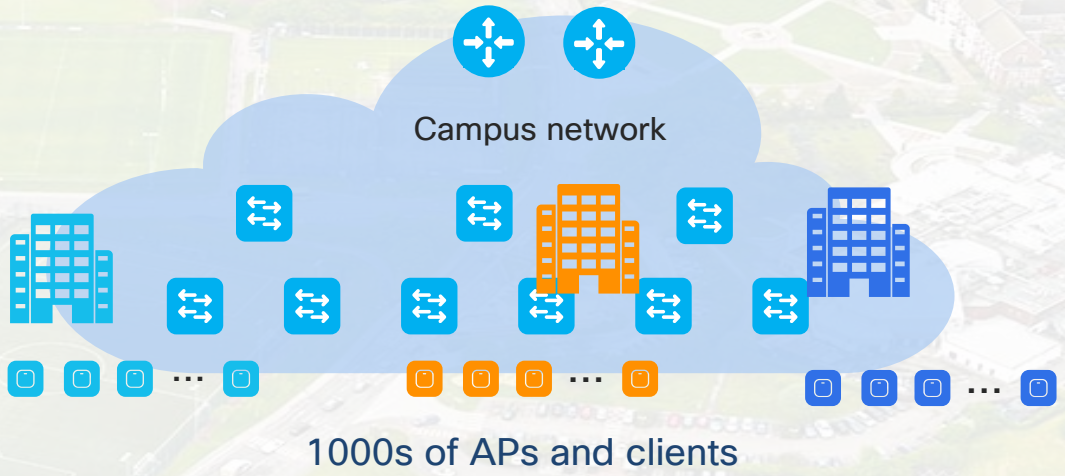
100% coverage — Automated test coverage across your entire network

No additional HW or cable pulls — Supported on existing infrastructure you have deployed

Conclusions

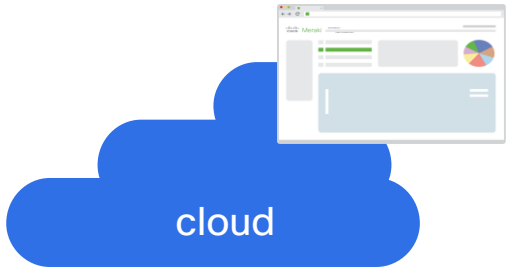
Network Architecture: Cloud Managed Campus

- Follow recommendations for AP placement, RF and WLAN Design
- Distributed vs. centralized: multiple design criteria to determine if adopting a data plane design. Start from the customer requirements (seamless roaming, scale, services needed, wired infra, app requirements).
- With the introduction of Campus Gateway, you now have the option to centralize

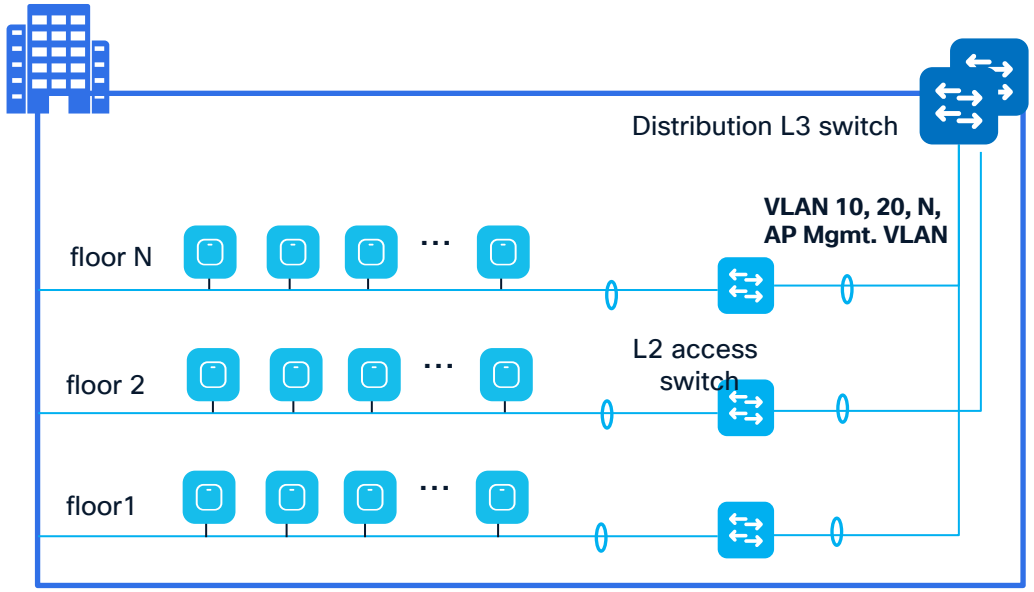


Small/Medium Campus deployment

Scenario 1



On prem



L2 roaming Deployment:

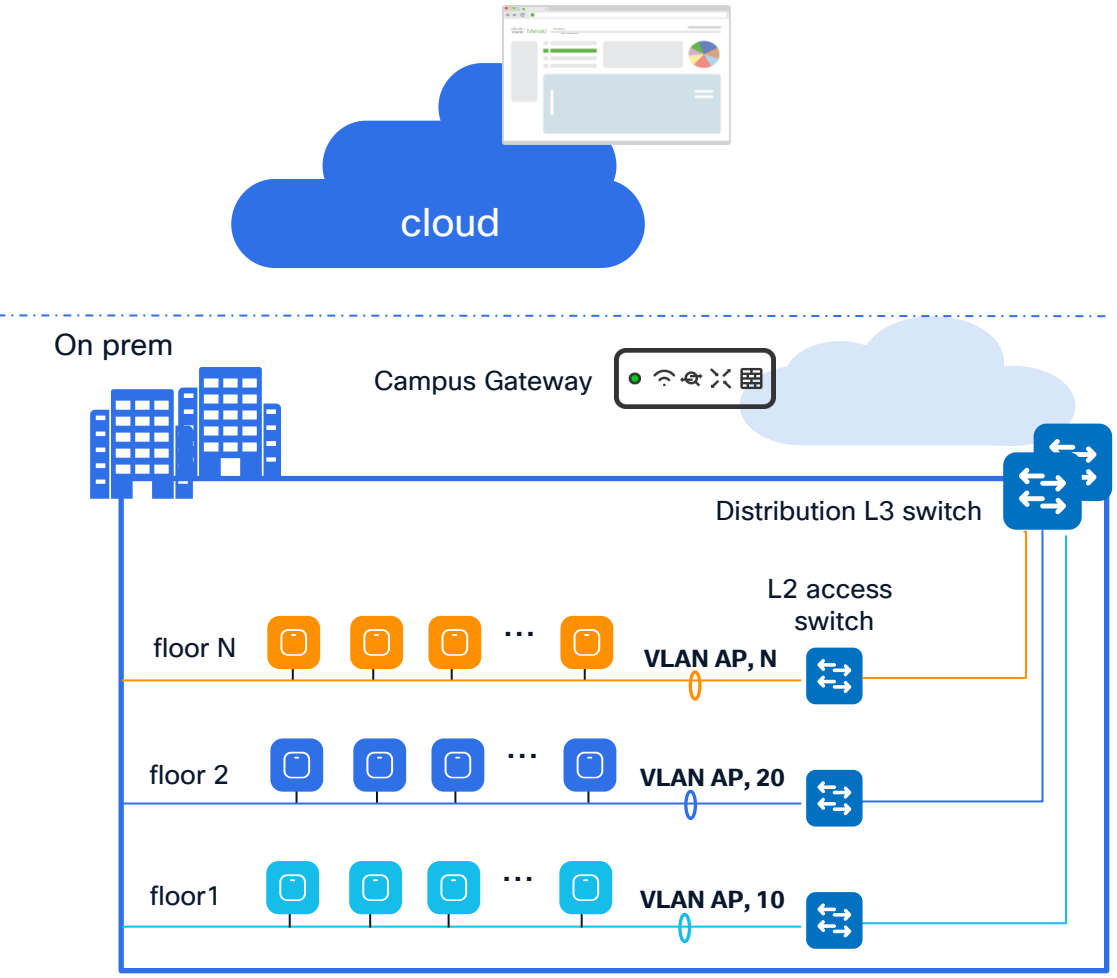
- Roaming domain = building = Meraki Network
- AP per roaming domain < 200/300
- VLAN design = VLANs span the whole building

Design Recommendations:

- SSIDs in bridge mode
- L2 broadcast boundary at the building distribution switch
- AP switchports configured as trunks (common AP management VLAN and client VLANs on all switches)
- Choose subnet mask to accommodate the expected # of devices per VLAN per building (VLAN pooling in R30)
- Use Stack/VSL technology at L3 switch to reduce impact of spanning tree
- Configure regular Layer 2 distributed roaming

Medium/Large Campus deployment

Scenario 2



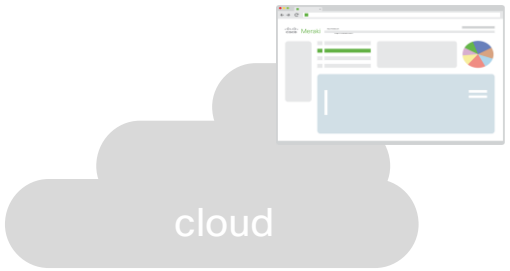
L3 roaming across floors/building Deployment:

- Roaming domain = floors/building/multiple buildings
- AP per roaming domain > 200/300
- VLAN design = **VLANs span only single floor/wiring closet**

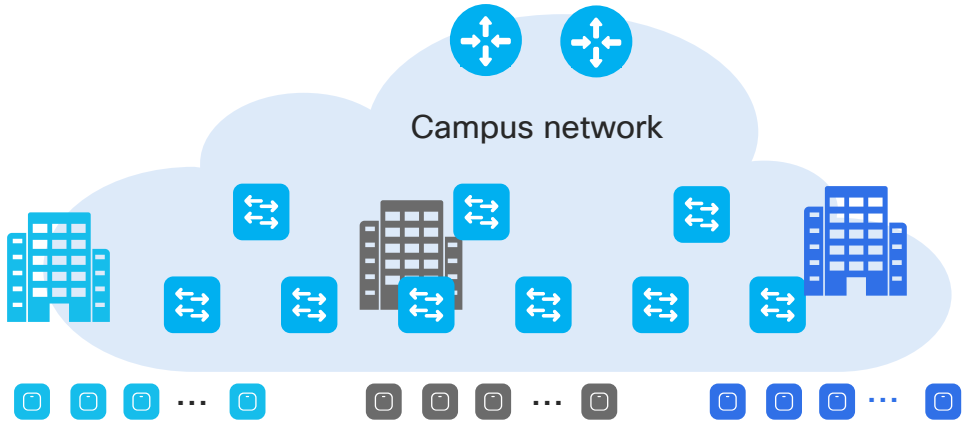
Design Recommendations:

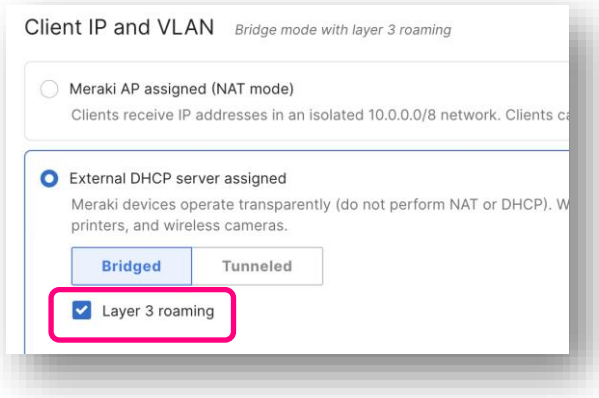
- L2 broadcast boundary at the building distribution switch
- SSIDs in Tunnel mode to Campus Gateway
- AP switchports configured as access port
- Centralized client VLANs
- Choose centralized subnet mask to accommodate the expected # of devices per VLAN per roaming domain
- Connect Campus Gateway to distribution switch or data center switch that can handle the MAC and ARP scale

Large scale deployments – Not recommended

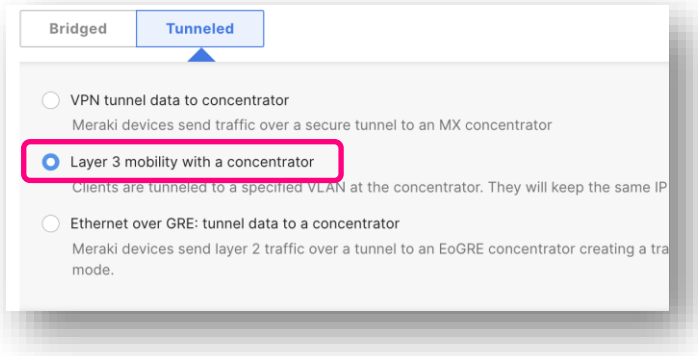


On prem





Distributed L3 Roaming (DL3R)



L3 Mobility with MX concentrator

Both these solutions are NOT recommended for a scale deployments

Complete your session evaluations

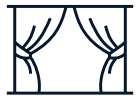
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: siarena@cisco.com

Thank you

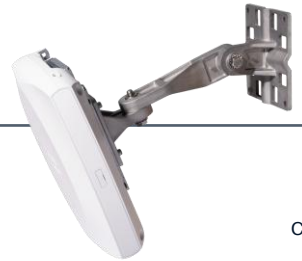

CISCO

The Wi-Fi 7 portfolio

CleanAir® Pro

CW9176I

12 Spatial Streams
4x4: 4 MU-MIMO
across 3 radios, 3 bands
(2.4/5GHz (XOR), 5 GHz, 6GHz)
BLE/IoT radio
Single 10Gbps multigigabit
Ultra Wide Band (UWB)
USB 2.0 – 9W
Accelerometer
Built-in GPS/GNSS, w/ support for ext. antenna
Integrated Omnidirectional Antenna



CleanAir® Pro

CW9176D1

12 Spatial Streams
4x4: 4 MU-MIMO
across 3 radios, 3 bands
(2.4/5GHz (XOR), 5 GHz, 6GHz)
BLE/IoT radio
Single 10Gbps multigigabit
Ultra Wide Band (UWB)
USB 2.0 – 9W
Accelerometer
Built-in GPS/GNSS, w/ support for ext. antenna
Integrated Directional Antenna (70x70)

CleanAir® Pro

CW9178I

16 Spatial Streams
4x4: 4 MU-MIMO
across 4 radios, 3 bands
(2.4 GHz, dual 5GHz, 6GHz)
BLE/IoT radio
Dual 10Gbps multigigabit
Ultra Wide Band (UWB)
USB 2.0 – 9W
Accelerometer
Built-in GPS/GNSS, w/ support for ext. antenna
Integrated Omnidirectional Antenna

Same brackets as always > Reduced Time, Reduced Waste

The Wi-Fi 7 portfolio

CleanAir® **Pro**

CW9172I

6 Spatial Streams
2x2:2 across 3 radios, 3 bands (2.4GHz, 5GHz, 6GHz)
-or-
2x2:2 on 2.4GHz and 4x4:4 on 5GHz
BLE/IoT radio
Single 2.5Gbps multigigabit uplink
USB 2.0 – 4.5W
DC Power Jack
Integrated Omnidirectional Antenna

CleanAir® **Pro**

CW9172H

6 Spatial Streams
2x2:2 across 3 radios, 3 bands (2.4GHz, 5GHz, 6GHz)
BLE/IoT radio
Single 2.5Gbps multigigabit uplink
3x 1Gbps LAN port with 1x POE out
1x Passthrough port
Integrated Omnidirectional Antenna

Same brackets as always.
9172H compatible with Meraki or Catalyst brackets

Wi-Fi 7: New indoor APs

CleanAir® **Pro**

CW9171I

4 Spatial Streams

2x2:2 across 2 radios, 3 bands
(2.4GHz and 5GHz
-or-
2.4GHz and 6GHz)

BLE/IoT and dedicated scan radio

Single 2.5Gbps multigigabit uplink

USB 2.0 – 4.5W

DC Power Jack

Integrated Omnidirectional Antenna

Global Use AP

Same bracket as always, AIR-AP-BRACKET-1 and AIR-AP-BRACKET-2

CleanAir® **Pro**

CW9174I/E

10 Spatial Streams

2x2:2 on 2.4GHz and 4x4:4 on 5GHz and 6GHz
-or-
4x4:4 on 2.4GHz and 5GHz

BLE/IoT and dedicated scan radio

Single 5Gbps multigigabit uplink

USB 2.0 – 9W

DC Power Jack

Integrated Omnidirectional or
DART-8 External Antenna

Global Use AP

Same brackets as always, AIR-AP-BRACKET-1 and AIR-AP-BRACKET-2

CW9174E Antennas and Accessories

CW-ANT-T-O2-D8

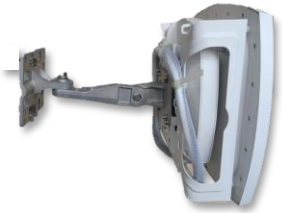
Omnidirectional ceiling mounted antenna with DART8 connector

CW-ANT-T-D2-D8

Directional patch antenna with DART8 connector, CW-MNT-ART2 mount included

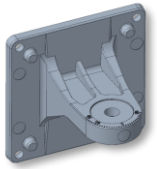
CW-ANT-T-O4-R

Omnidirectional dipole antenna with RP-TNC connector. Requires AIR-CAB002-D8-R=.
Qty: 8 antennas per AP (2.4+5+6 GHz mode), or 4 antennas (2.4+5 GHz mode)



CW-MNT-9

Integrated AP mount. Integrates CW9174E and CW-ANT-T-D2-D8 into one unit



CW-ACC-ADPT1

Adapter to use CW-ANT-T-D2-D8 with C-ANT9103 mount for brown field upgrades

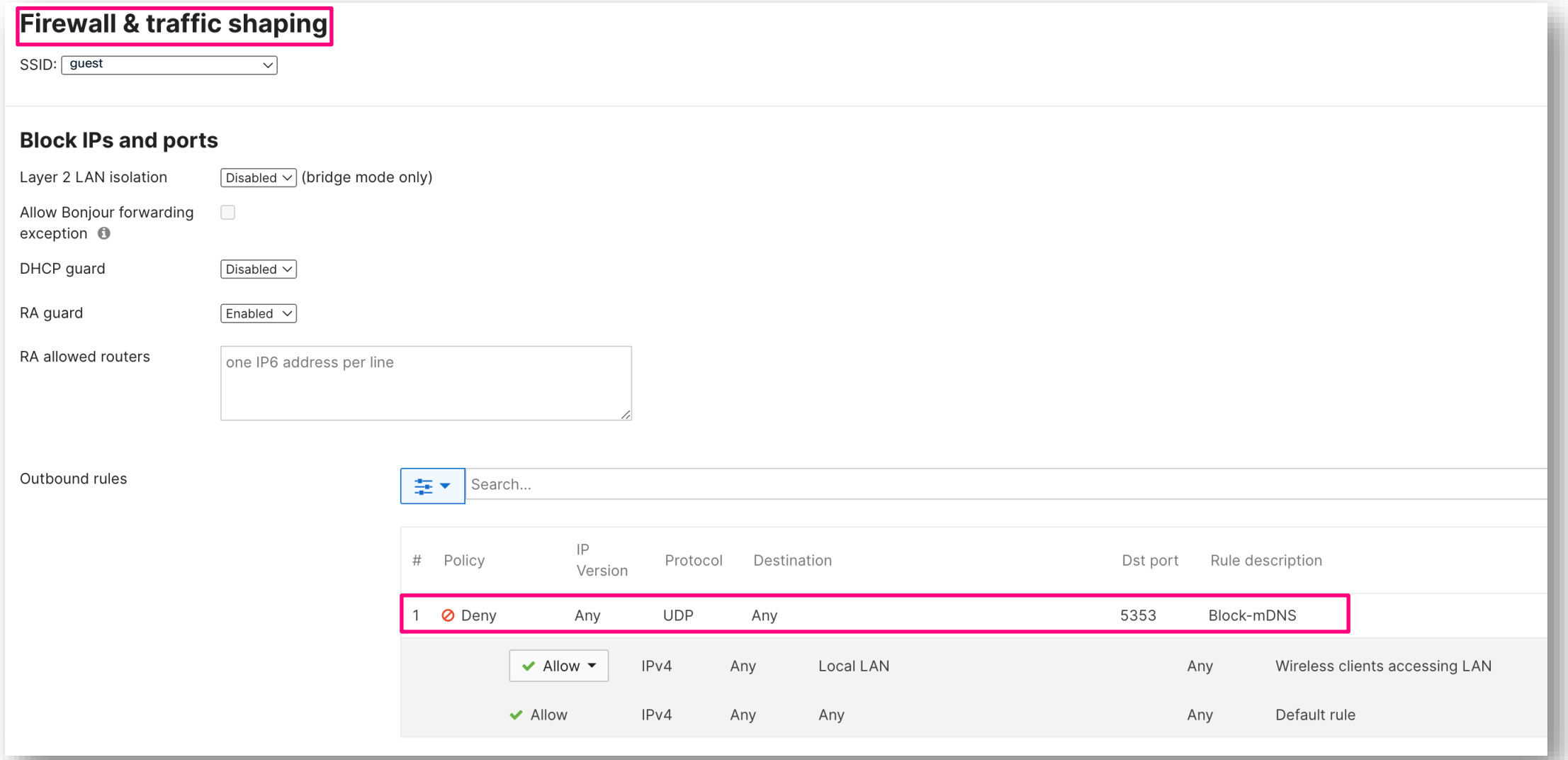
Legacy Antennas Supported

AIR-ANT2524V4C-R/RS
AIR-ANT2544V4M-R/RS
AIR-ANT2566P4W-R/RS
AIR-ANT2566D4M-R/RS
AIR-ANT2513P4M-N/NS
C-ANT9101
C-ANT9102
C-ANT9103
MA-ANT-3-C6
MA-ANT-3-D6
MA-ANT-3-E6
MA-ANT-3-F6

Supports existing DART8 cables and accessories

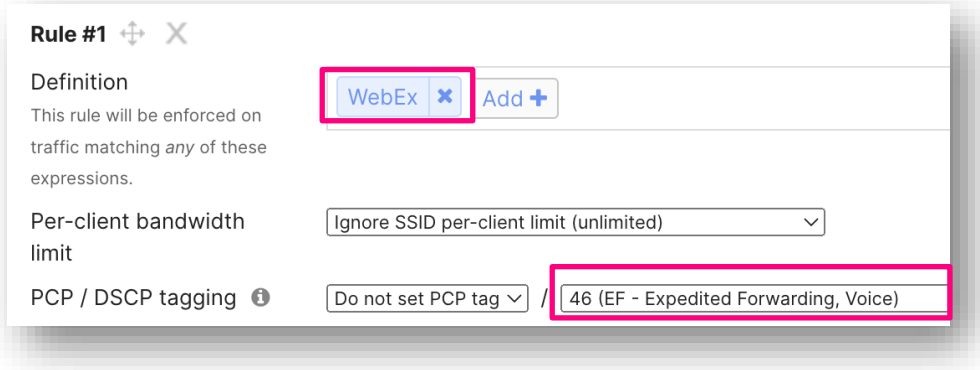
WLAN design

RTP Campus – WLAN Design: No mDNS Policy

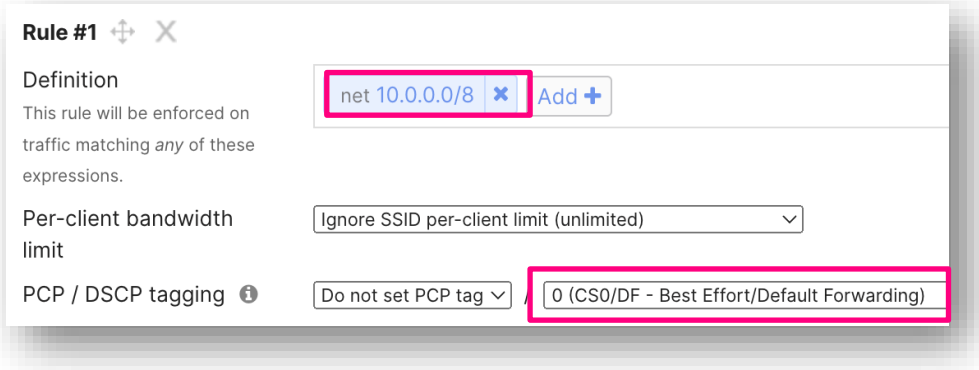


RTP Campus – WLAN Design: QoS policy

Corporate

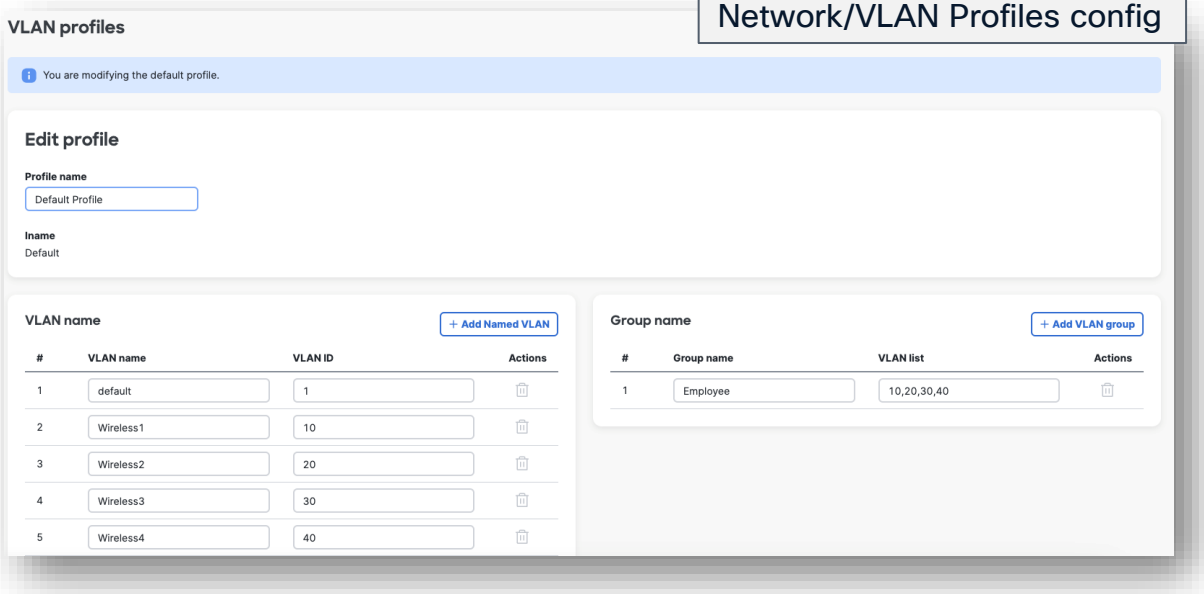


Guest

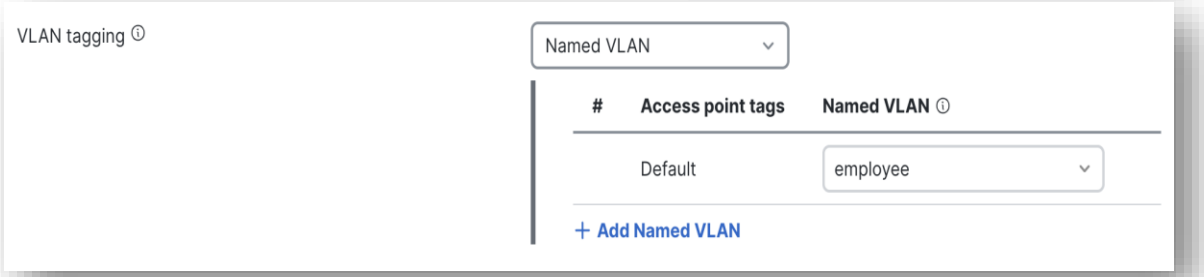


Subnet/VLAN Design considerations

Network/VLAN Profiles config



Wireless/Access Control/SSID

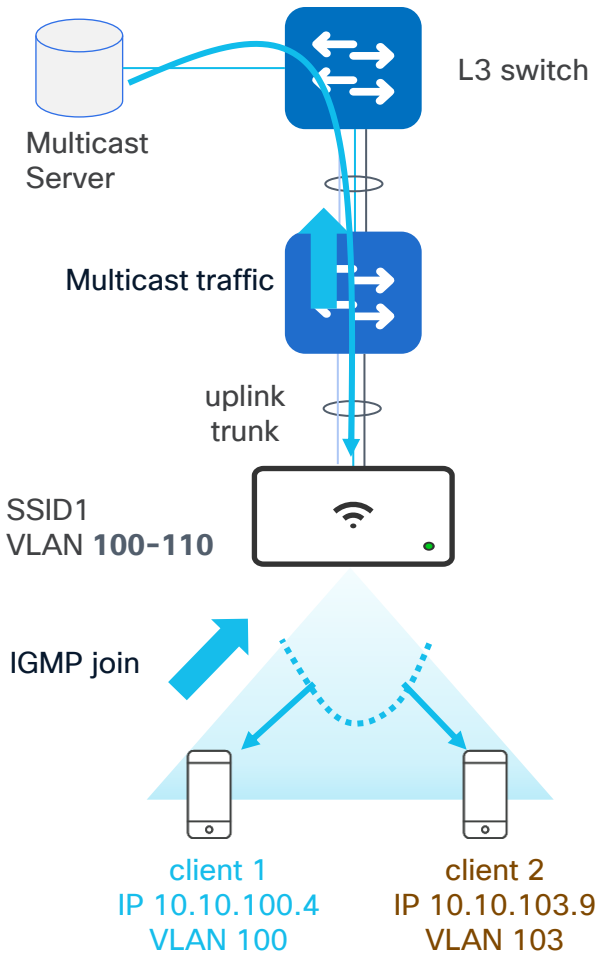


- Problem: You may be forced to use a certain subnet size and hence DHCP scope size (e.g., /24 subnets). Possible reasons:
  - Subnet design and summarization at the distribution level
  - Public IPs: can't really increase/change the subnet size
- Solution: R30 introduces VLAN pooling, this feature allows you to assign multiple VLANs to a single SSID.

- *Please note: VLAN pooling in Dashboard leverages an existing feature called VLAN profiles. The doc says "VLAN profiles can work along with 802.1X, MAB.."*
- *Even if VLAN profiles were created to work with Radius based authentication, VLAN pooling is supported with any security settings, including OPEN, PSK, SAE, Webauth ☺*

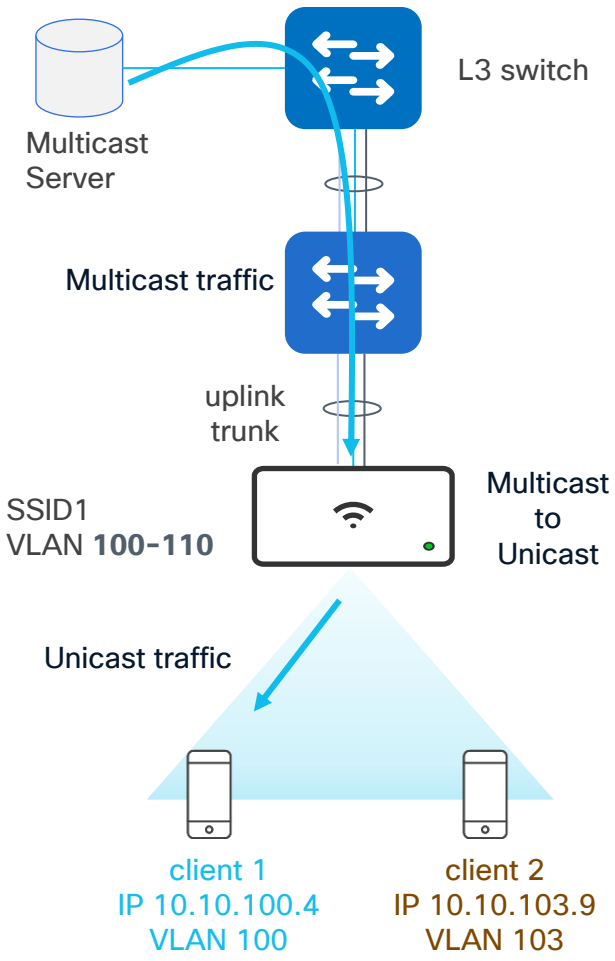
Best Practices

Multicast + AAA VLAN override



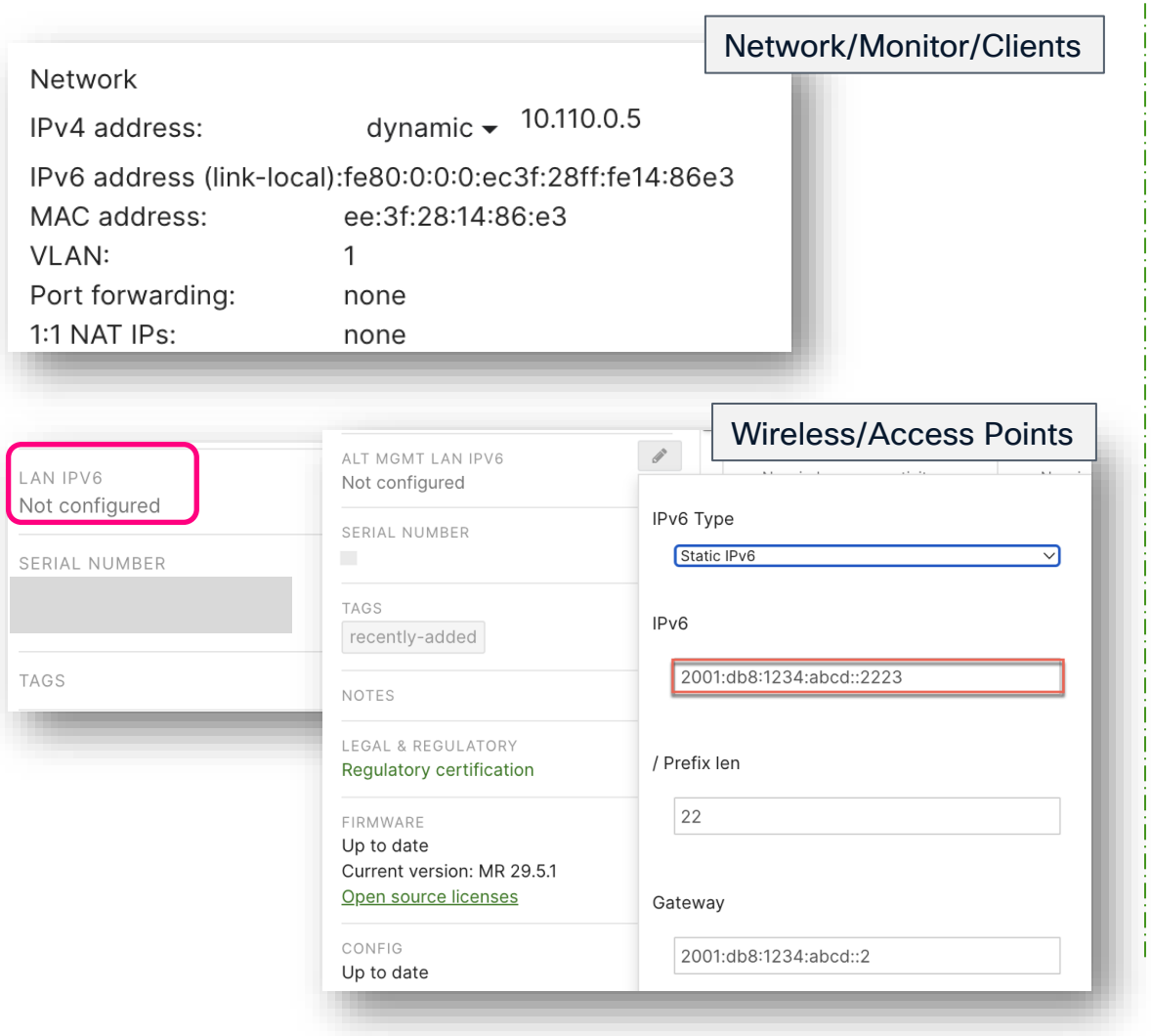
- What (Requirement): Single SSID mapped to multiple client VLANs via AAA policy. IP Multicast separation is required across client VLANs
- Problem: Clients belong to the same SSID. Client 1 requests IP multicast, IGMP query goes on VLAN 100, multicast traffic is received in VLAN 100; in the air, since #1 SSID <> #1 Group Temporal Key (GTK), AP sends it as broadcast and traffic is received by client 2 (on VLAN 103) as well. There is no multicast or broadcast segmentation in air. This applies to IPv4 and IPv6.

Multicast + AAA VLAN override



- What (Requirement): Single SSID mapped to multiple client VLANs via AAA policy. IP Multicast separation is required across client VLANs
- Problem: Clients belong to the same SSID. Client 1 requests IP multicast, IGMP query goes on VLAN 100, multicast traffic is received in VLAN 100; in the air, since #1 SSID <> #1 Group Temporal Key (GTK), AP sends it as broadcast and traffic is received by client 2 (on VLAN 103) as well. There is no multicast or broadcast segmentation in air. This applies to IPv4 and IPv6.
- Solution: Make sure multicast to unicast feature is enabled: Network-wide > General > Wireless Multicast to Unicast Conversion. With this feature, APs “demulticast" traffic over the air, thereby preserving VLAN segmentation. There is a threshold of max 20 clients per multicast group (GV: Group-VLAN), beyond which traffic is sent as multicast.
- Note: From MR29 this is also supported for IPv6 clients
- Note2: multicast IP traffic is not supported on Campus Gateway

IPv6 support



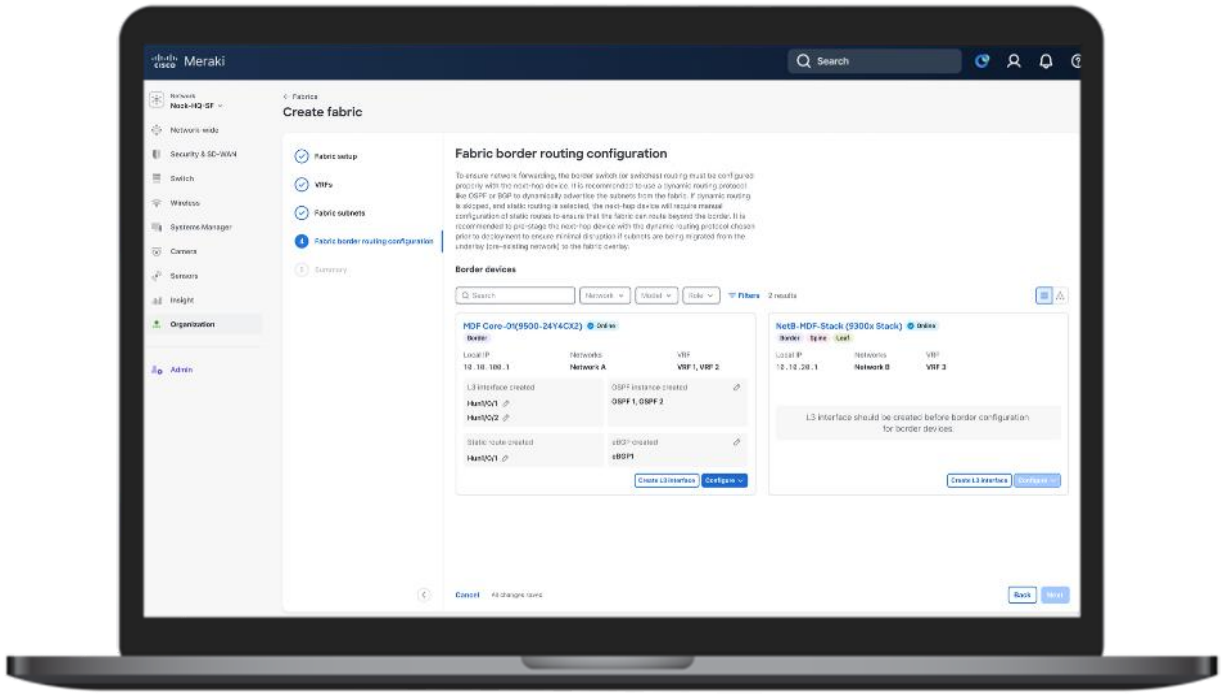
Clients:

- **Additional IPv6 support in R30**: Support for 802.11r/OKC over IPV6 infra (dual-stack was already supported), client IPv6 DL3R over IPv4 infra and WPN fragmentation.

Access Points:

- **Infrastructure IPv6**: AP supports Static and SLAAC (no DHCPv6)
- **Alternate Management Interface** supports for IPv6 in R30

Cisco Cloud-Managed Campus Fabric



Benefit from Cloud Simplicity

Build and manage large sites from an intuitive cloud networking platform

Leverage Existing Investments

Modernize the network while utilizing existing C9K infrastructure

Migrate at Your Own Pace

Incrementally migrate devices and subnets to the cloud over time

Beta: Nov 5, 2025 | Limited Availability: December 2025 (IOS XE 17.18.2)

Cisco Cloud-Managed Campus Fabric

Reduce the number of steps it takes to provision, manage, and troubleshoot sites

Build and enforce segmentation policies that adapt to your network based on the intent of the user

Deploy in a non-disruptive way on top of the devices you already own