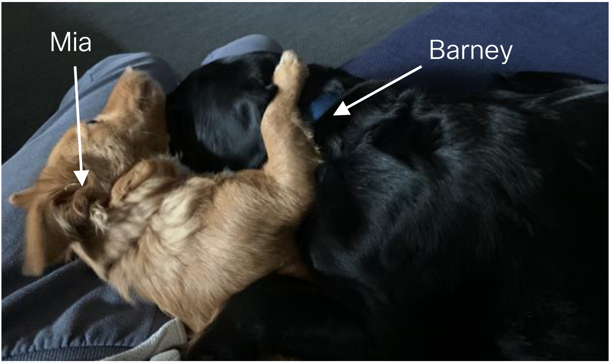
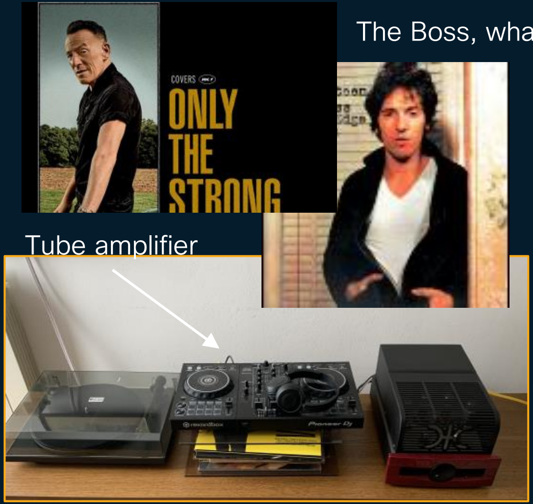
Design your Enterprise Wireless Network with Cisco Meraki

Simone Arena,
Distinguished TME, Cisco Wireless

BRKEWN-2035





The Boss, what else??

Tube amplifier

Le Pergole Torte
Montevertine, 2020

Fiorentina soccer fan

Enterprise Network requirements

A Wireless-Centric View

Mobility, Performance, anything @scale

IT Operation Simplicity, Flexibility

High Availability Resiliency

Assurance, Analytics

Integration with 3rd party systems

End to End Security

Cisco Wireless Management Strategy

On-prem

Customer Managed
Use cases require on-prem delivery.
DIY IT model

Cloud-enabled/hybrid

Need to retain control on prem, cloud Assisted.
Use cloud tools to help run their networks

Cloud first

Prefer cloud-enabled delivery for simplicity.
SaaS IT model

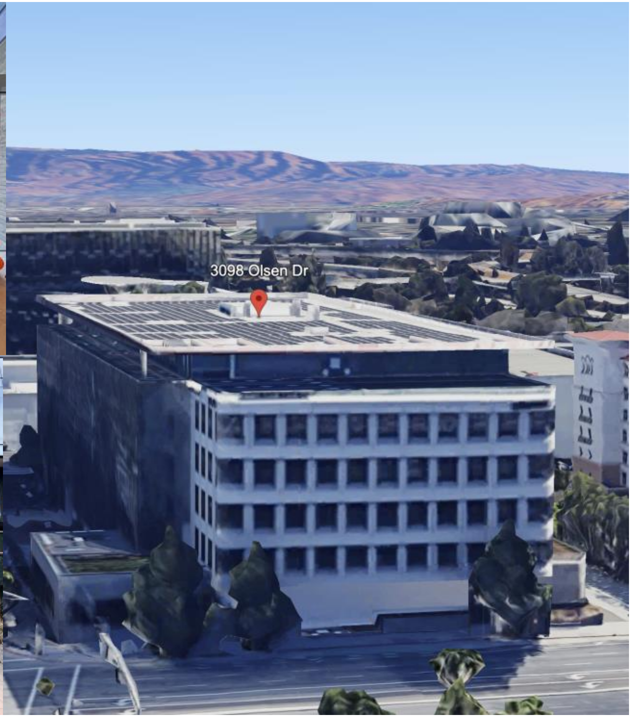
Meeting our customers where they are:
Deliver simplified outcomes to <u>all customers</u>

Agenda

What are we covering:

- Why Cloud Management?
- …and why not?
- Wireless Network Deployment
- Network Architecture & Design
- Best practices

Reference use case: Cisco Building SJC-34



- New Headquarter building in downtown San Jose (Santana Row) – former Splunk
- Six floors. Collaborative Smart Space
- Wireless Network: 200 APs, 400 average with peak of 1500 clients per day
- Two SSIDs: Corporate and Guest
- Wired Network: Catalyst switch infrastructure already in place
- Cisco ISE is used as AAA server

Special Thank you

Chris Tomazic

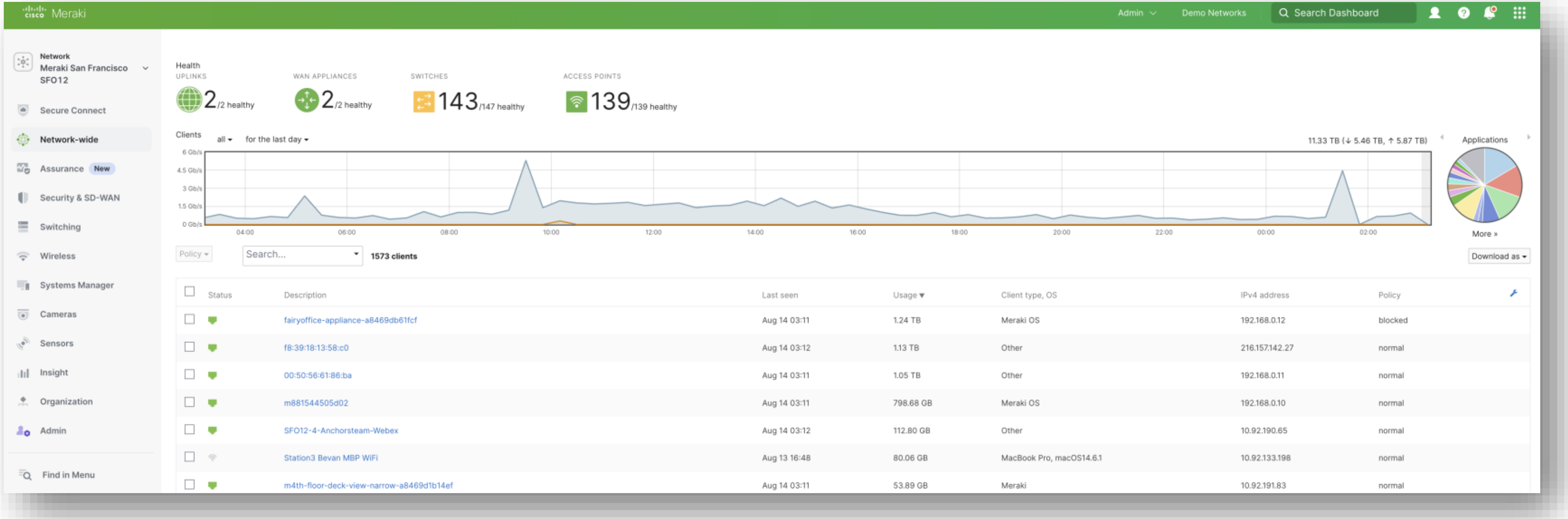
Wireless Tech Lead, Cisco IT

Jason Frazier

Principal Engineer, Cisco IT

Why Cloud Management?

Why Cloud Management? It’s the Dashboard!



Health

UPLINKS 2 /2 healthy

WAN APPLIANCES 2 /2 healthy

SWITCHES 143 /147 healthy

ACCESS POINTS 139 /139 healthy

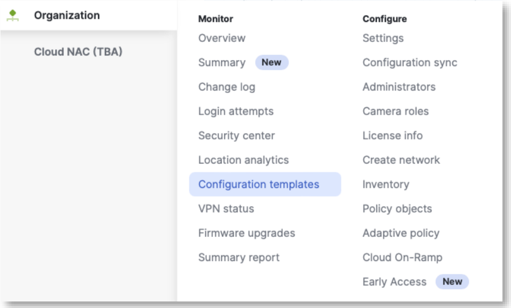
1573 clients

□	Status	Description	Last seen	Usage ▾	Client type, OS	IPv4 address	Policy
□	🟩	fairyoffice-appliance-a8469db61fcf	Aug 14 03:11	1.24 TB	Meraki OS	192.168.0.12	blocked
□	🟩	f8:39:18:13:58:c0	Aug 14 03:12	1.13 TB	Other	216.157.142.27	normal
□	🟩	00:50:56:61:86:ba	Aug 14 03:11	1.05 TB	Other	192.168.0.11	normal
□	🟩	m881544505d02	Aug 14 03:11	798.68 GB	Meraki OS	192.168.0.10	normal
□	🟩	SFO12-4-Anchorsteam-Webex	Aug 14 03:12	112.80 GB	Other	10.92.190.65	normal
□	ᯤ	Station3 Bevan MBP WiFi	Aug 13 16:48	80.06 GB	MacBook Pro, macOS14.6.1	10.92.133.198	normal
□	🟩	m4th-floor-deck-view-narrow-a8469d1b14ef	Aug 14 03:11	53.89 GB	Meraki	10.92.191.83	normal

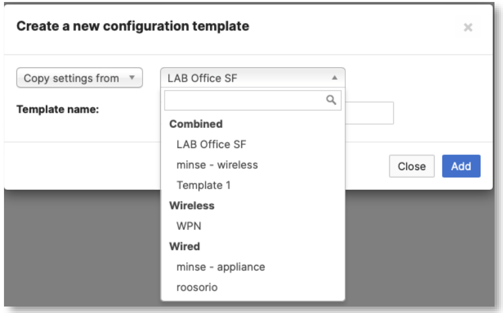
- **Single pane of glass**: Unified visibility and control of the entire network wireless, switching, and security
- **Intuitive and simple: E**liminates costly training or added staff
- **Flexible and scalable**: can access from everywhere, streamlines large networks with tens of thousands of endpoints

Configuration templates for Automation

Easily configure sites across the stack



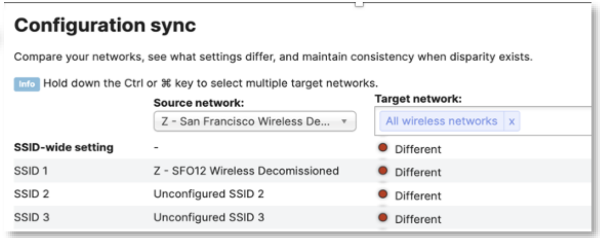
Create the template



Base off “golden” config

- SSIDs (name, enable/disable)
- Some Access control settings
- Radio Settings
- IoT Settings

Local Override



Configuration sync

Compare your networks, see what settings differ, and maintain consistency when disparity exists.

Info Hold down the Ctrl or ⌘ key to select multiple target networks.

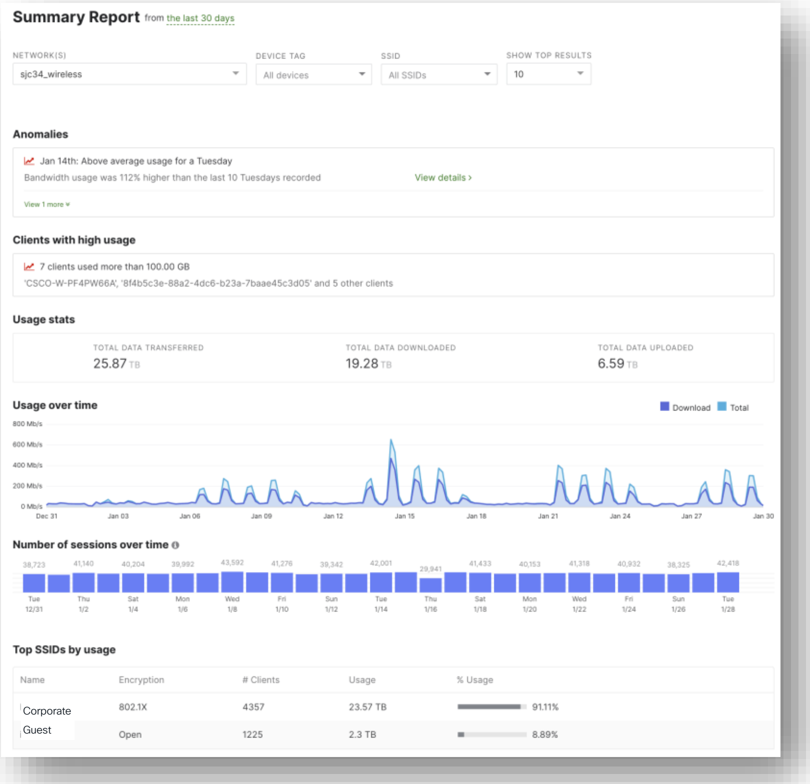
	Source network:	Target network:
	Z - San Francisco Wireless De... ▾	All wireless networks x
SSID-wide setting	-	● Different
SSID 1	Z - SFO12 Wireless Decomissioned	● Different
SSID 2	Unconfigured SSID 2	● Different
SSID 3	Unconfigured SSID 3	● Different

Compare

Network and Device Tags

Network Tags

- Summary reports
- Organization Overview
- Dashboard RBAC
- Camera Roles
- Location Analytics
- Site to Site VPN



Summary Report from the last 30 days

NETWORK(S): sjc34_wireless

DEVICE TAG: All devices

SSID: All SSIDs

SHOW TOP RESULTS: 10

Anomalies

Jan 14th: Above average usage for a Tuesday

Bandwidth usage was 112% higher than the last 10 Tuesdays recorded

Clients with high usage

7 clients used more than 100.00 GB

'CSCO-W-PF4PW66A', '8f4b5c3e-88a2-4dc6-b23a-7baae45c3d05' and 5 other clients

Usage stats

TOTAL DATA TRANSFERRED	TOTAL DATA DOWNLOADED	TOTAL DATA UPLOADED
25.87 TB	19.28 TB	6.59 TB

Usage over time

Number of sessions over time

Top SSIDs by usage

Name	Encryption	# Clients	Usage	% Usage
Corporate	802.1X	4357	23.57 TB	91.11%
Guest	Open	1225	2.3 TB	8.89%

Network and Device Tags

Network Tags

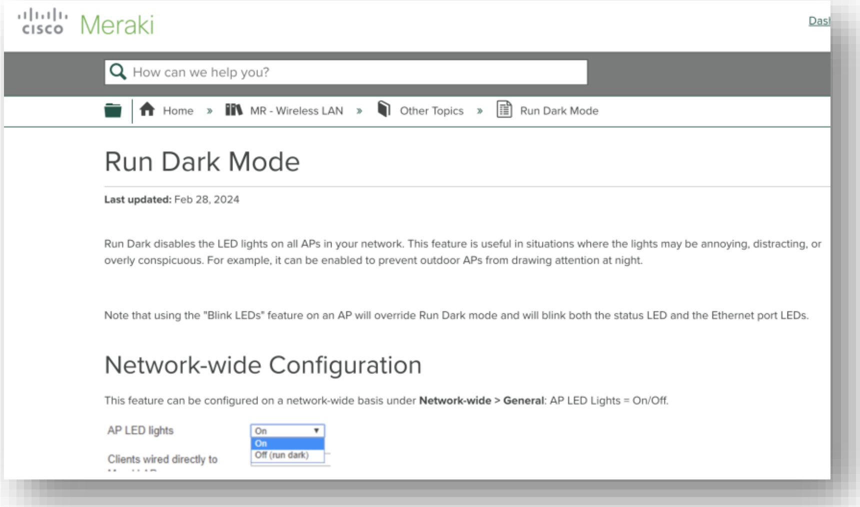
- Summary reports
- Organization Overview
- Dashboard RBAC
- Camera Roles
- Location Analytics
- Site to Site VPN

Device Tags

- SSID Availability
- VLAN Assignment
- Summary reports
- Organization Overview
- Location Analytics
- Filtering mechanism

Device Tag use case

- Meraki has a “dark mode” setting under Network-wide > Config > General: it turns off led (including the ethernet one for the newest APs) on all APs in the Network



Run Dark Mode

Last updated: Feb 28, 2024

Run Dark disables the LED lights on all APs in your network. This feature is useful in situations where the lights may be annoying, distracting, or overly conspicuous. For example, it can be enabled to prevent outdoor APs from drawing attention at night.

Note that using the "Blink LEDs" feature on an AP will override Run Dark mode and will blink both the status LED and the Ethernet port LEDs.

Network-wide Configuration

This feature can be configured on a network-wide basis under **Network-wide** > **General**: AP LED Lights = On/Off.

AP LED lights: On ▾
On
Off (run dark)

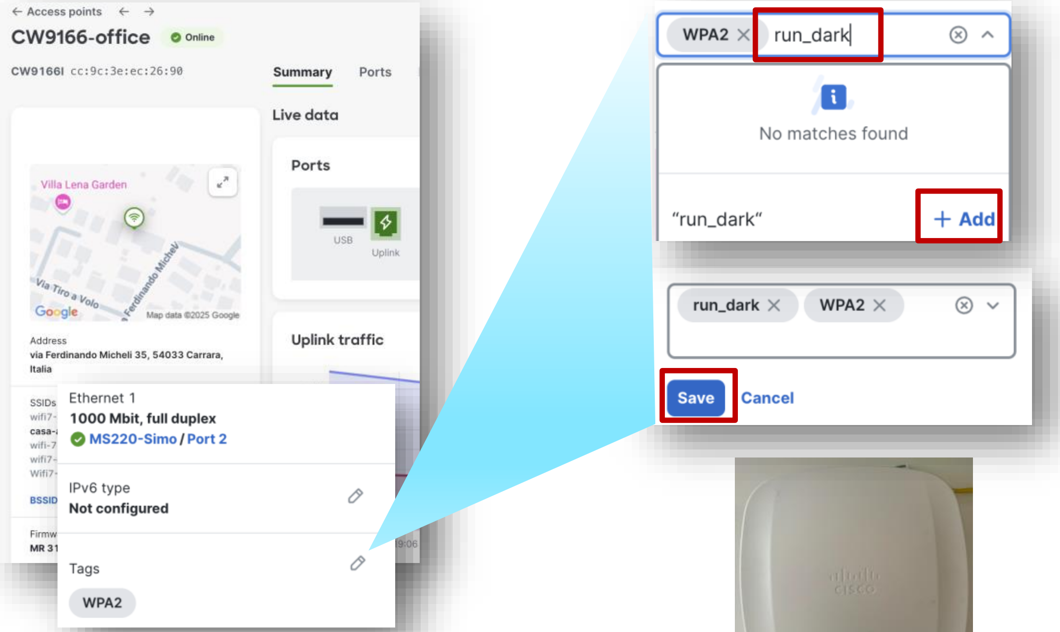
Clients wired directly to

Led is off

- What if you want few APs to have the led off? you can use a device tag

Device Tag use case

- Use the **run_dark** tag. Go to AP page, left column > TAGs section > Click on Edit



← Access points ← →

CW9166-office Online

CW9166I cc:9c:3e:ec:26:90

Summary Ports

Live data

Ports

Uplink traffic

Address
via Ferdinando Micheli 35, 54033 Carrara, Italia

Ethernet 1
1000 Mbit, full duplex
MS220-Simo / Port 2

IPv6 type
Not configured

Tags
WPA2

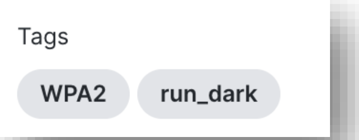
WPA2 ✕ run_dark

No matches found

“run_dark“ + Add

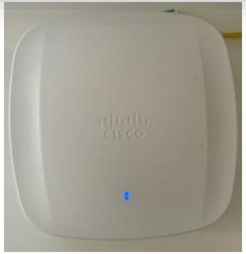
run_dark ✕ WPA2 ✕

Save Cancel

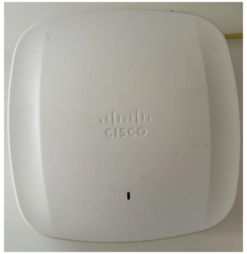


Tags

WPA2 run_dark



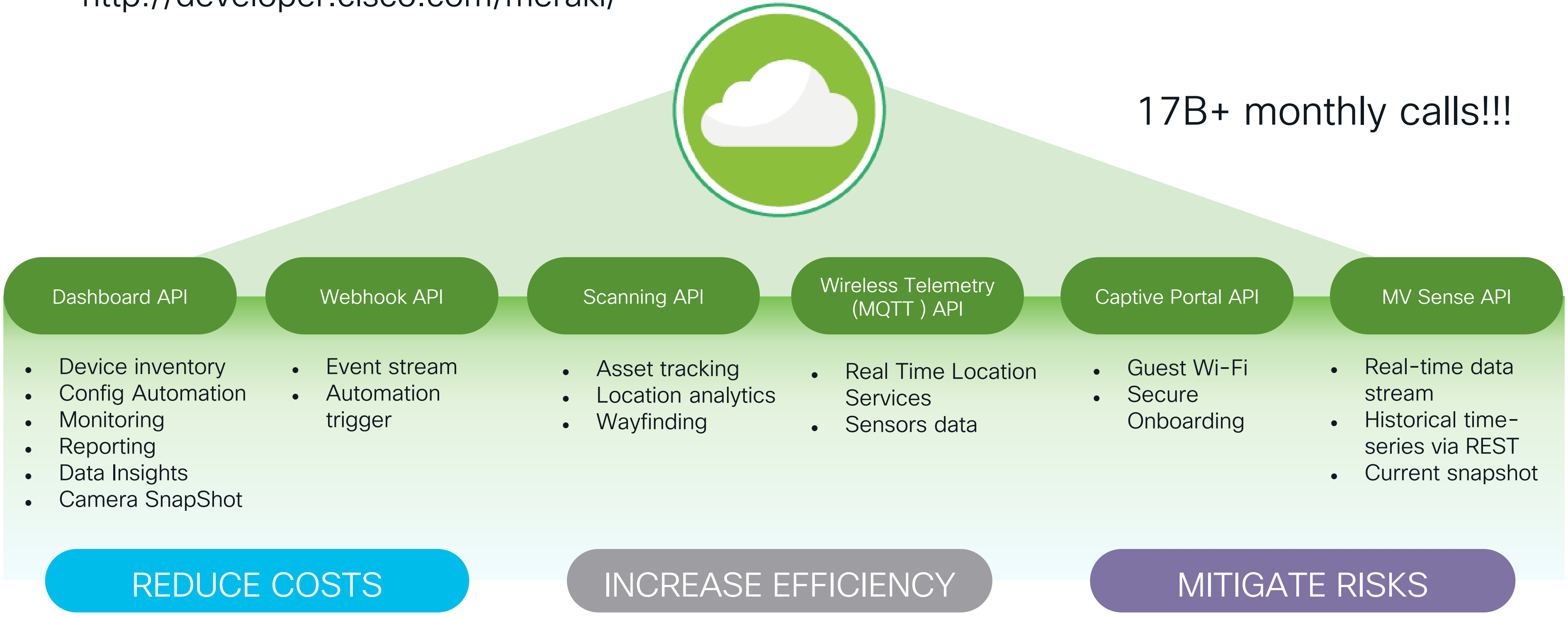
LED goes off



Integration at scale with APIs

http://developer.cisco.com/meraki/

17B+ monthly calls!!!



Dashboard API

- Device inventory
- Config Automation
- Monitoring
- Reporting
- Data Insights
- Camera SnapShot

Webhook API

- Event stream
- Automation trigger

Scanning API

- Asset tracking
- Location analytics
- Wayfinding

Wireless Telemetry (MQTT) API

- Real Time Location Services
- Sensors data

Captive Portal API

- Guest Wi-Fi
- Secure Onboarding

MV Sense API

- Real-time data stream
- Historical time-series via REST
- Current snapshot

REDUCE COSTS

INCREASE EFFICIENCY

MITIGATE RISKS

Why NOT Cloud Management?

Why NOT Cloud Management?

- Does it scale?
- Is it reliable? Would it go down?
- Is it secure? Can I trust it with my data?
- What if I lose the connection to Cloud?
- Do I get the knobs that I need?

Meraki Cloud: Unmatched Scale and Reliability

Unmatched scale to support any network

Largest data lake to power AI/ML intelligent solutions

Programmability at scale for large Enterprise

5.1M+ Customer Networks	16.6M+ Meraki Devices online	192+ Countries
11.4M+ Active APs	652K+ 6E APs deployed	1M+ Roam events from Intel Analytics in 1 day
90M+ Daily end-user devices	90K+ Active API users	17B+ External API monthly calls

Industry's largest-scale cloud networking service

Meraki Cloud: Secure and Highly Available

Secure

24 × 7 automated intrusion detection
& third-party independent validation
More info: https://meraki.cisco.com/trust/

Standards Certified

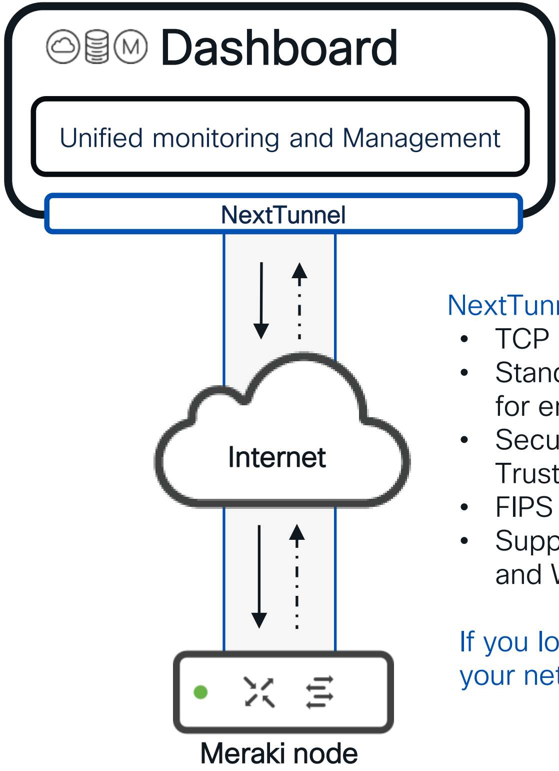
Audited ISO 27001, FIPS CR & FedRAMP
SAS70 type II / SSAE18 type II

Data Privacy & Protection

Follows Cisco MPDA & EU GDPR All data in transit AES256 encrypted

High Availability

99.99% uptime service level agreement
24 × 7 automated failure detection

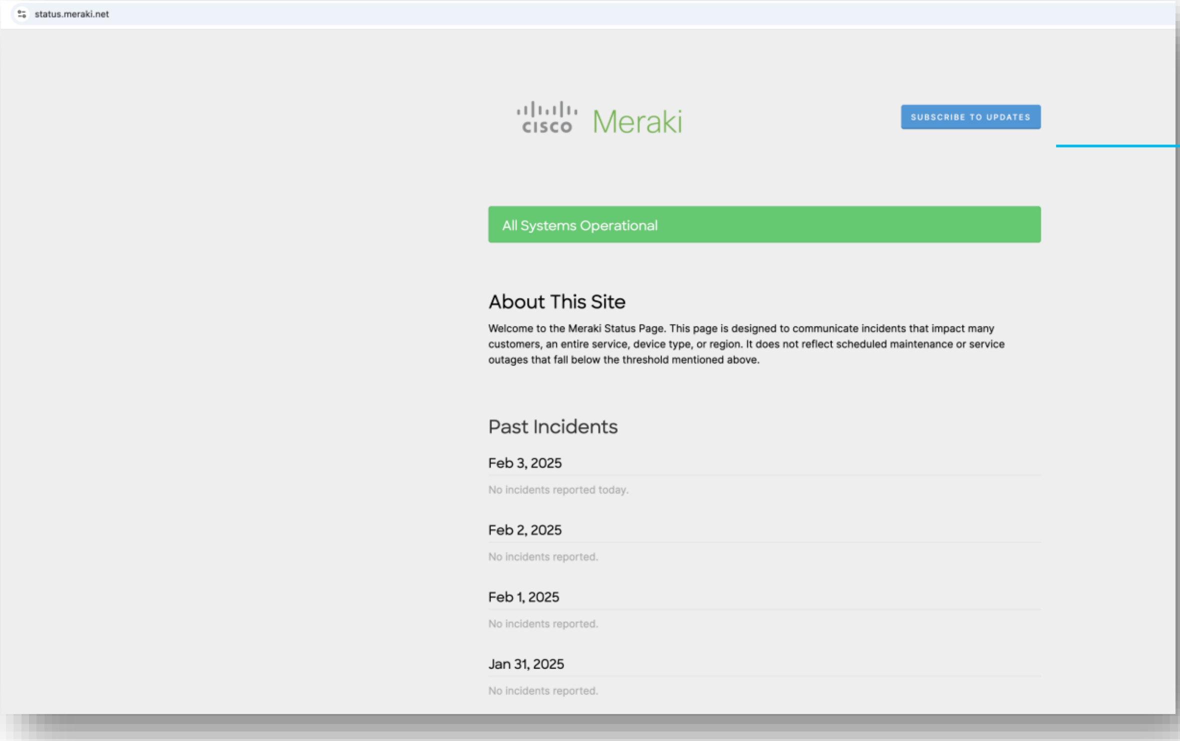


NextTunnel:

- TCP based, port 443
- Standard: TLS 1.2 with AES 256 for encryption
- Secured: Identity based on Cisco Trust Anchor module (TAm)
- FIPS 140-2 compliant
- Support via HTTP proxy with R30 and Wi-Fi 6 MRs and higher

If you lose connection to the Cloud your networks still works!

Meraki Cloud status?



status.meraki.net

All Systems Operational

About This Site

Welcome to the Meraki Status Page. This page is designed to communicate incidents that impact many customers, an entire service, device type, or region. It does not reflect scheduled maintenance or service outages that fall below the threshold mentioned above.

Past Incidents

Feb 3, 2025

No incidents reported today.

Feb 2, 2025

No incidents reported.

Feb 1, 2025

No incidents reported.

Jan 31, 2025

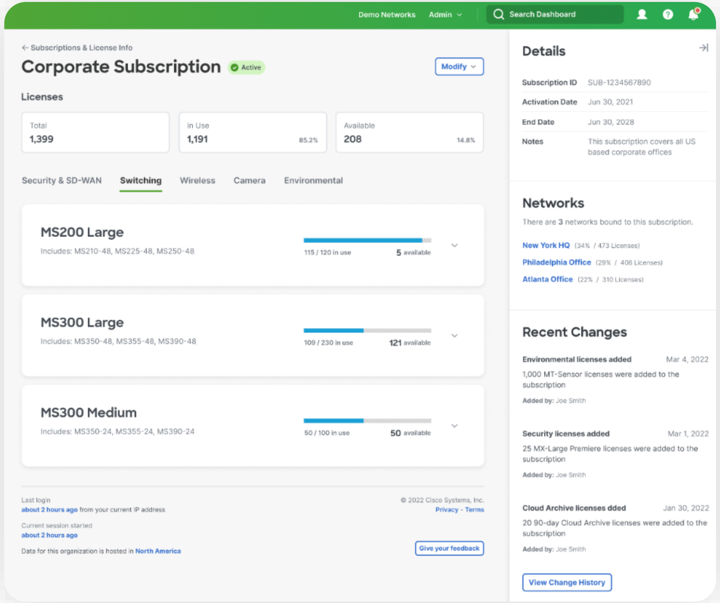
No incidents reported.

You can subscribe

Go to https://status.meraki.net/

Meraki Cloud

You Network still functions if license expires



← Subscriptions & License Info

Corporate Subscription Active

Licenses

Total	In Use	Available
1,399	1,191 85.2%	208 14.8%

Security & SD-WAN | **Switching** | Wireless | Camera | Environmental

MS200 Large
Includes: MS210-48, MS225-48, MS250-48
115 / 120 in use — 5 available

MS300 Large
Includes: MS350-48, MS355-48, MS390-48
109 / 230 in use — 121 available

MS300 Medium
Includes: MS350-24, MS355-24, MS390-24
50 / 100 in use — 50 available

Last login
about 2 hours ago from your current IP address

Current session started
about 2 hours ago

Data for this organization is hosted in North America

© 2022 Cisco Systems, Inc.
Privacy - Terms

Details

Subscription ID	SUB-1234567890
Activation Date	Jun 30, 2021
End Date	Jun 30, 2028
Notes	This subscription covers all US based corporate offices

Networks

There are 3 networks bound to this subscription.

New York HQ (34% / 473 Licenses)
Philadelphia Office (29% / 408 Licenses)
Atlanta Office (22% / 310 Licenses)

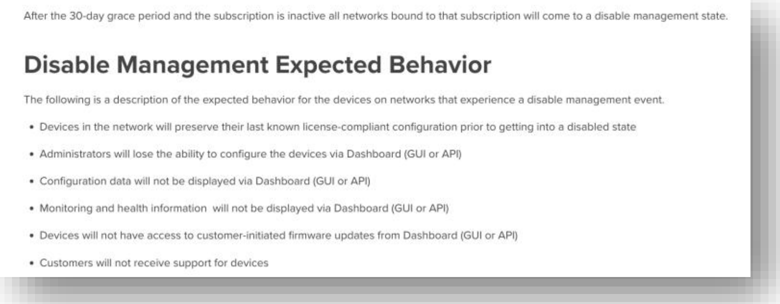
Recent Changes

Environmental licenses added Mar 4, 2022
1,000 MT-Sensor licenses were added to the subscription
Added by: Joe Smith

Security licenses added Mar 1, 2022
25 MX-Large Premiere licenses were added to the subscription
Added by: Joe Smith

Cloud Archive licenses dded Jan 30, 2022
20 90-day Cloud Archive licenses were added to the subscription
Added by: Joe Smith

- Subscription Licensing: Flexible term, flexible start date, different license tiering, per network (not necessarily per org)
- Important: Subscription enforcement will restrict the management of devices; the network still functions if Cloud connection is down



After the 30-day grace period and the subscription is inactive all networks bound to that subscription will come to a disable management state.

Disable Management Expected Behavior

The following is a description of the expected behavior for the devices on networks that experience a disable management event.

- Devices in the network will preserve their last known license-compliant configuration prior to getting into a disabled state
- Administrators will lose the ability to configure the devices via Dashboard (GUI or API)
- Configuration data will not be displayed via Dashboard (GUI or API)
- Monitoring and health information will not be displayed via Dashboard (GUI or API)
- Devices will not have access to customer-initiated firmware updates from Dashboard (GUI or API)
- Customers will not receive support for devices

Overview: https://documentation.meraki.com/General_Administration/Licensing/Meraki_Subscription_Licensing_Overview
Compliance: https://documentation.meraki.com/General_Administration/Licensing/Meraki_Subscription_License_Out_of_Compliance

Meraki Cloud: Network Feature Override (NFO)

Advanced Configuration Options for Enterprises that Need Them

What is it?

Provide additional functionalities that are not available to customers by default

These configurations are gated behind Network Feature Overrides (NFOs)

NFOs can be applied on one network, multiple networks, or organization-wide

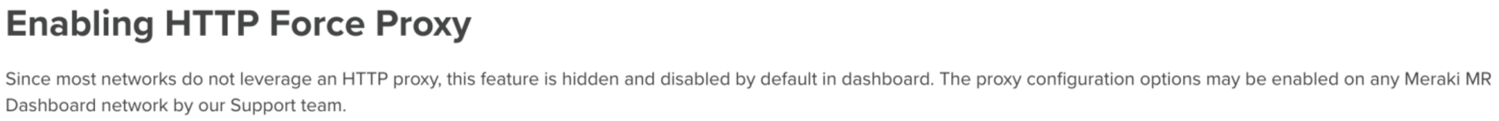
Why?

NFOs are intended to be used by specific types of customers

Use cases that don't make sense for most customer networks

Beta Features use NFO to enable specific services to test and validate

Fully supported by Meraki Support

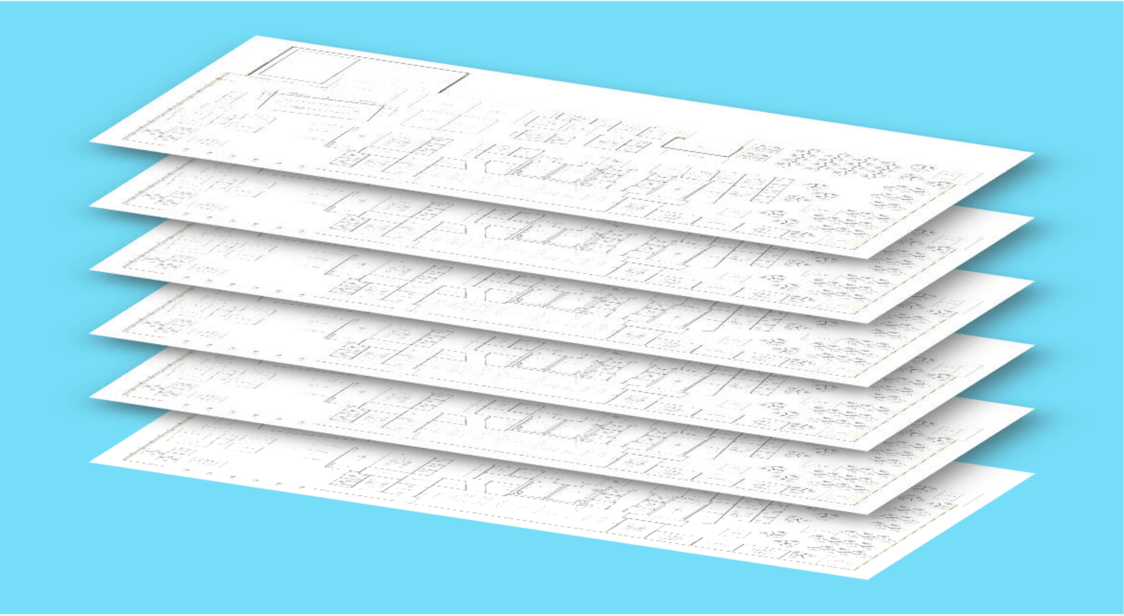


Enabling HTTP Force Proxy

Since most networks do not leverage an HTTP proxy, this feature is hidden and disabled by default in dashboard. The proxy configuration options may be enabled on any Meraki MR Dashboard network by our Support team.

Wireless Deployment

The SJC-34 Building



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

Cisco Catalyst 9166I Access Point

Cisco® Catalyst® 9166I/D

Common Hardware, Tri-Radio with 12 Spatial Streams!

Same model for Cloud and On-prem!

6E

Penta-Radio Architecture

1. 2.4 GHz Serving Radio (Slot 0): 4x4:4SS
2. 5 GHz Serving Radio (Slot 1): 4x4:4SS
3. 6 GHz Serving Radio (Slot 2): 4x4:4SS (XOR)
   5GHz Serving Radio (Slot 2): 4x4:4SS
4. Dedicated AI/ML-Driven Scanning Radio
5. 2.4 GHz IoT Radio

5 Gbps Multigigabit (mGig) PoE Ports

Optional DC Power

Full radio performances with 803.3at! (PoE+)

9166D1 - Directional antenna architecture

- 2.4+5 GHz: 6 dBi gain (70x70 deg), 6 GHz: 8 dBi (60x60)*
- Same X,Y as CW9166I – and only 0.1cm taller!
- Wide support for pan/tilt combinations
- Accelerometer to determine AP tilt

Cisco Catalyst 9166I Access Point

Cisco® Catalyst® 9166I/D

Common Hardware, Tri-Radio with 12 Spatial Streams!

6E

Penta-Radio Architecture

1. 2.4 GHz Serving Radio (Slot 0): 4x4:4SS
2. 5 GHz Serving Radio (Slot 1): 4x4:4SS
3. 6 GHz Serving Radio (Slot 2): 4x4:4SS (XOR)
   5GHz Serving Radio (Slot 2): 4x4:4SS
4. Dedicated AI/ML-Driven Scanning Radio
5. 2.4 GHz IoT Radio

5 Gbps Multigigabit (mGig) PoE Ports

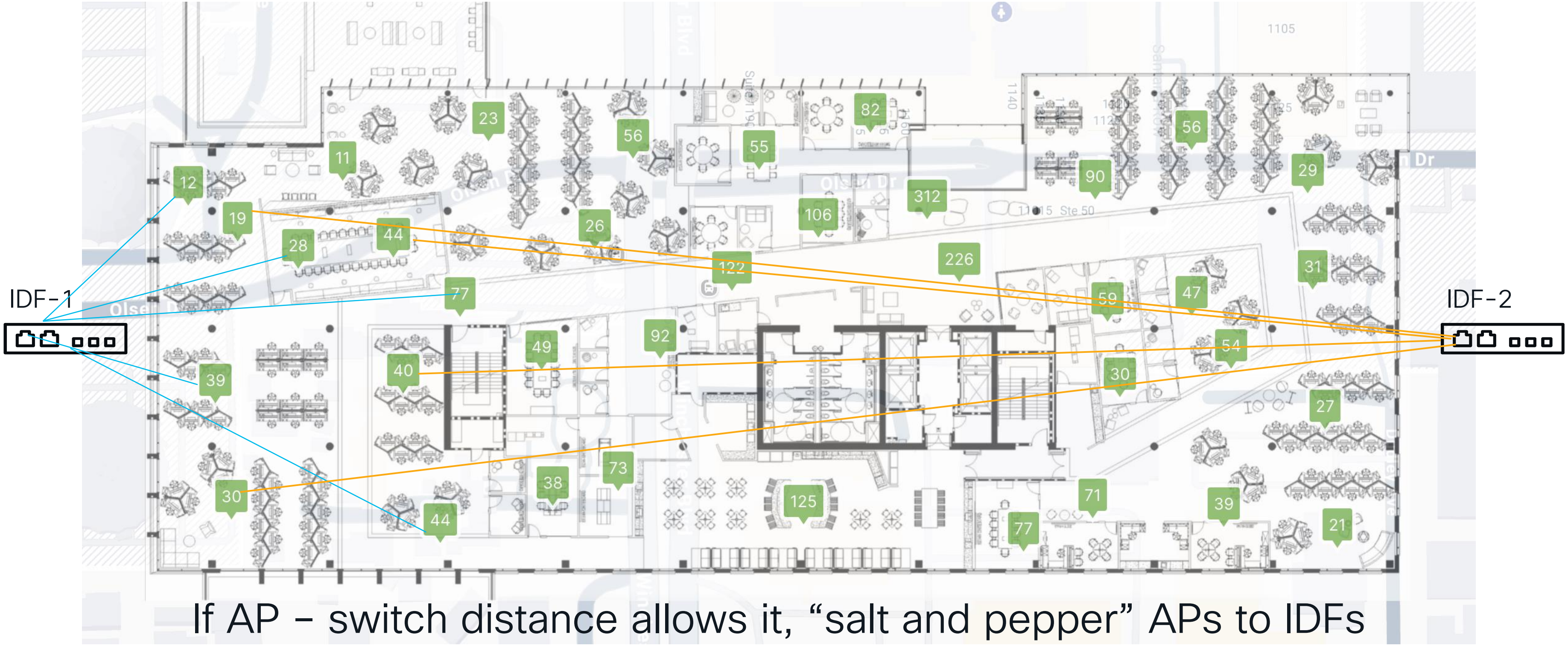
Optional DC Power

Full radio performances with 803.3at! (PoE+)

9166D1 - Directional antenna architecture

- 2.4+5 GHz: 6 dBi gain (70x70 deg), 6 GHz: 8 dBi (60x60)*
- Same X,Y as CW9166I – and only 0.1cm taller!
- Wide support for pan/tilt combinations
- Accelerometer to determine AP tilt

SJC-34: AP placement



If AP – switch distance allows it, "salt and pepper" APs to IDFs

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

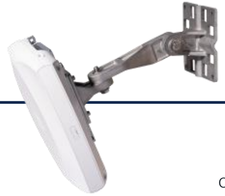
Ultra Wide Band (UWB)

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

NEW

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

NEW

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

Software Management

MR software recommendation

	r30.X Most stable release	r31.X r31.5.1 is now General Availability (GA)
Adoption	8.3M MRs on r30	1M MRs on r31
Why?	Most deployed release	AI- Enhanced RRM Zero Wait DFS 6GHz Transition mode for dot1x SSID Proactive client packet capture

Current recommended releases **r30.7.1and r31.5.1**

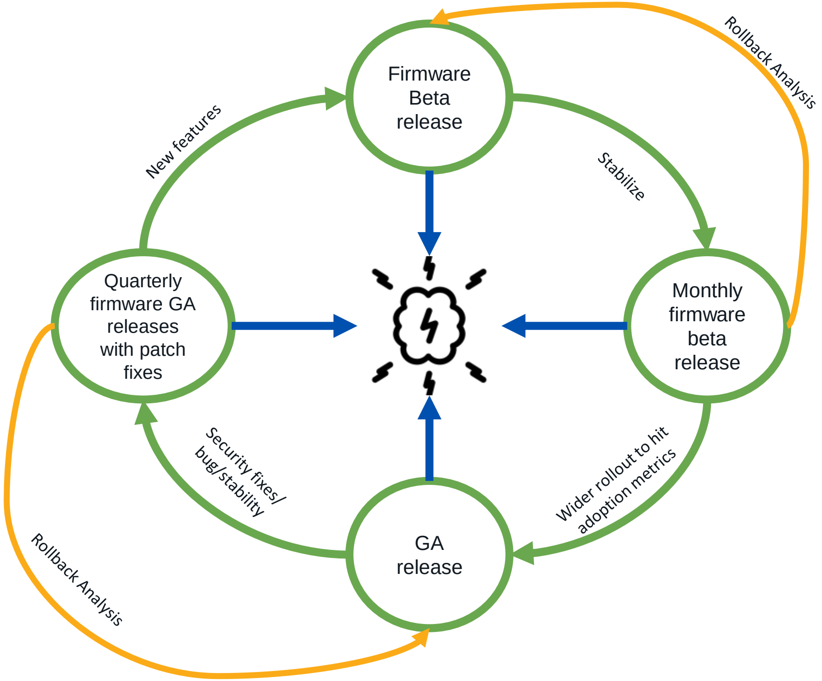
Cloud managed Wireless Firmware Upgrades

Intelligent firmware rollout that constantly monitors firmware globally

Global monitoring for all deployed firmware

Proactive monitoring for software stability

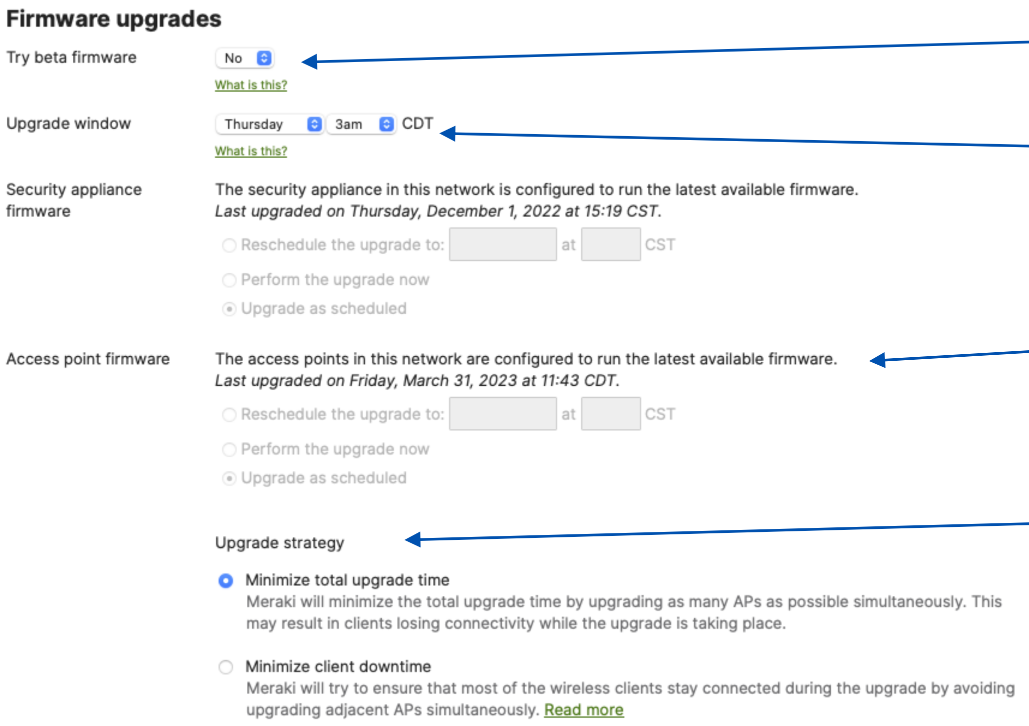
Proactive outreach to resolve issues



Firmware Beta release
Rollback Analysis
New features
Stabilize
Quarterly firmware GA releases with patch fixes
Monthly firmware beta release
Security fixes/ bug/stability
Wider rollout to hit adoption metrics
GA release
Rollback Analysis

Wireless Firmware Upgrades

Flexibility - Software Updates Scheduling per network



Firmware upgrades

Try beta firmware: No
What is this?

Upgrade window: Thursday 3am CDT
What is this?

Security appliance firmware: The security appliance in this network is configured to run the latest available firmware.
Last upgraded on Thursday, December 1, 2022 at 15:19 CST.

○ Reschedule the upgrade to: at CST
○ Perform the upgrade now
● Upgrade as scheduled

Access point firmware: The access points in this network are configured to run the latest available firmware.
Last upgraded on Friday, March 31, 2023 at 11:43 CDT.

○ Reschedule the upgrade to: at CST
○ Perform the upgrade now
● Upgrade as scheduled

Upgrade strategy

● Minimize total upgrade time
Meraki will minimize the total upgrade time by upgrading as many APs as possible simultaneously. This may result in clients losing connectivity while the upgrade is taking place.

○ Minimize client downtime
Meraki will try to ensure that most of the wireless clients stay connected during the upgrade by avoiding upgrading adjacent APs simultaneously. Read more

Beta? – Yes | No

When? – Based on local time

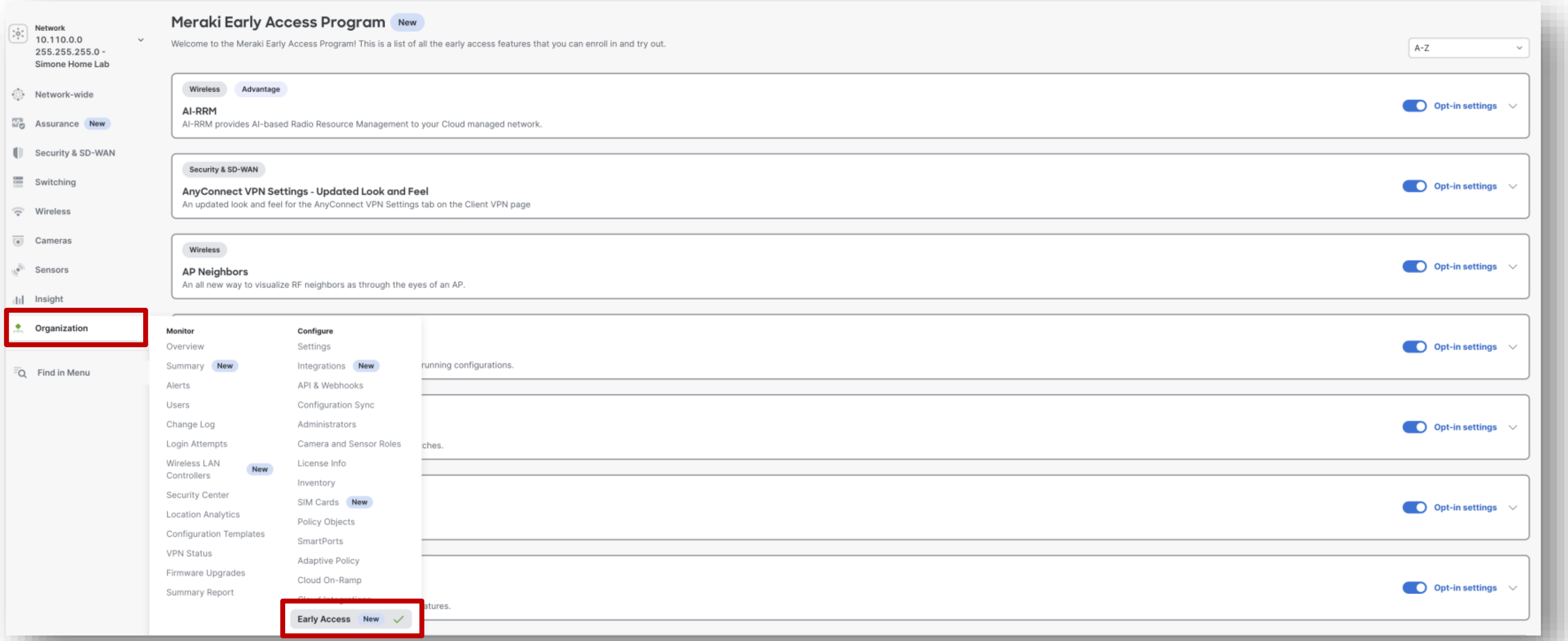
What? – MR, MS, MX

Upgrade Strategy?
Fast or don't disrupt clients

If APs > 80, dashboard will perform a staggered upgrade in addition to the strategy selected to minimize load

Want to try new features?

Opt-in in the Early Access Program



Meraki Early Access Program New

Welcome to the Meraki Early Access Program! This is a list of all the early access features that you can enroll in and try out.

Wireless Advantage
AI-RRM
AI-RRM provides AI-based Radio Resource Management to your Cloud managed network.
Opt-in settings

Security & SD-WAN
AnyConnect VPN Settings - Updated Look and Feel
An updated look and feel for the AnyConnect VPN Settings tab on the Client VPN page
Opt-in settings

Wireless
AP Neighbors
An all new way to visualize RF neighbors as through the eyes of an AP.
Opt-in settings

running configurations.
Opt-in settings

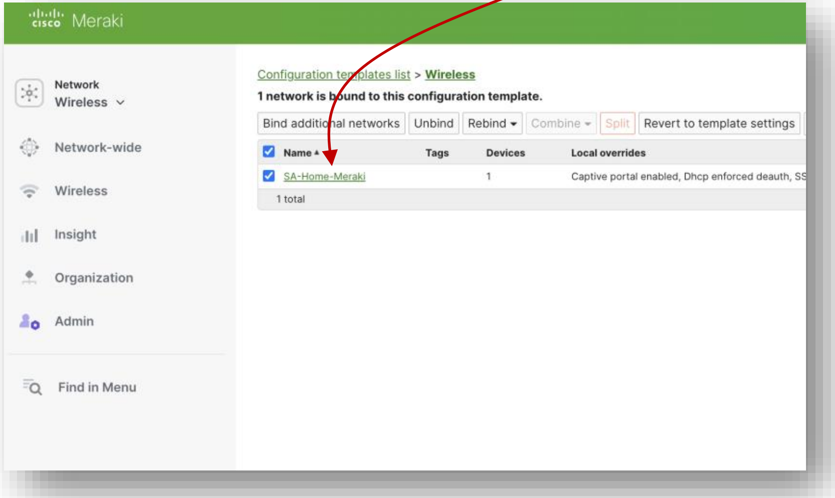
ches.
Opt-in settings

Opt-in settings

atures.
Opt-in settings

Wireless Firmware Upgrades

- If your Network is bound to a template, you cannot upgrade the single Network

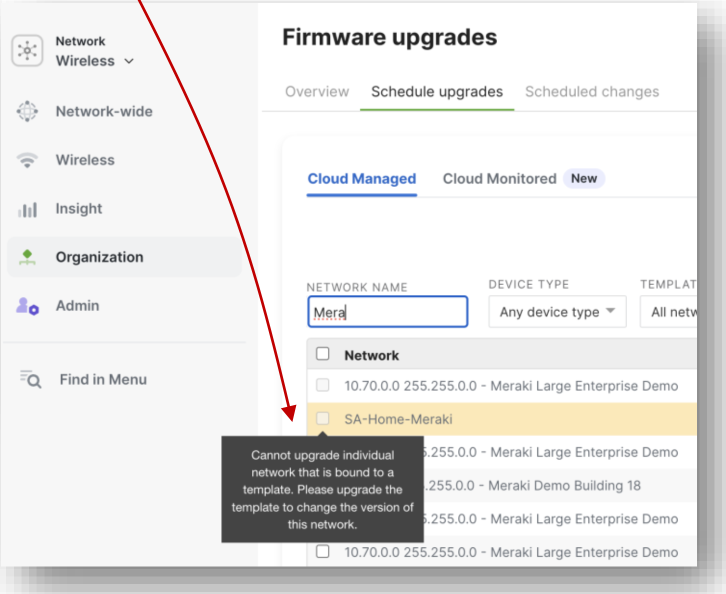


Configuration templates list > Wireless

1 network is bound to this configuration template.

☑ Name	Tags	Devices	Local overrides
☑ SA-Home-Meraki		1	Captive portal enabled, Dhcp enforced deauth, SS

1 total



Firmware upgrades

NETWORK NAME: Mera

DEVICE TYPE: Any device type

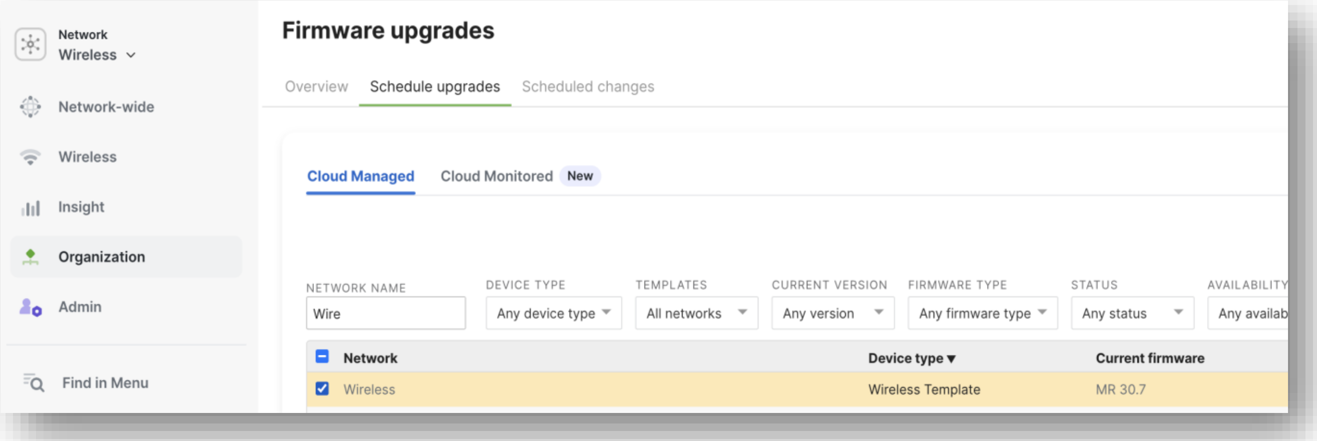
TEMPLAT: All netw

☐ Network
☐ 10.70.0.0 255.255.0.0 - Meraki Large Enterprise Demo
☐ SA-Home-Meraki
.255.0.0 - Meraki Large Enterprise Demo
.255.0.0 - Meraki Demo Building 18
.255.0.0 - Meraki Large Enterprise Demo
☐ 10.70.0.0 255.255.0.0 - Meraki Large Enterprise Demo

Cannot upgrade individual network that is bound to a template. Please upgrade the template to change the version of this network.

Wireless Firmware Upgrades

- If your Network is bound to a template, you cannot upgrade the single Network
- You need to upgrade the template and all the bound Networks



Firmware upgrades

NETWORK NAME	DEVICE TYPE	TEMPLATES	CURRENT VERSION	FIRMWARE TYPE	STATUS	AVAILABILITY
Wire	Any device type	All networks	Any version	Any firmware type	Any status	Any availab

☐ Network	Device type ▾	Current firmware
☑ Wireless	Wireless Template	MR 30.7

WLAN Design

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

Wi-Fi 6E

WPA3/Enhanced Open Mandatory

Protected Management Frame (PMF) Mandatory

6E

7

Wi-Fi 7 add-on

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

WPA3 /OWE mandatory for 11be MCS rates & MLO

* (AKM: 24 & 25), (Cipher: CCMP128 or GCMP 256)

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

What options would you have?

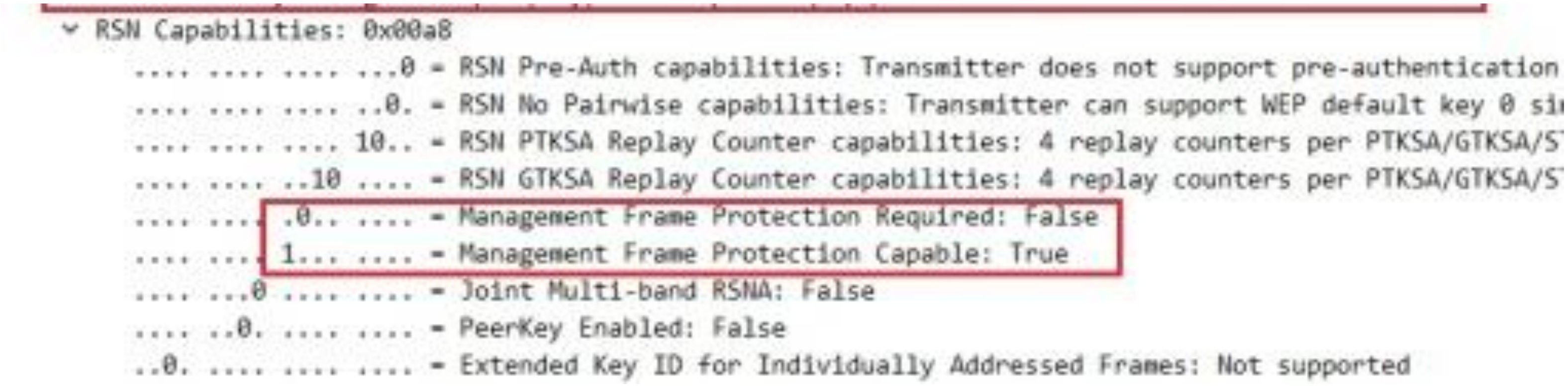
1 ”All-In”: Reconfigure the existing WLAN to WPA3, one SSID for all radio policies (2.4/5/6 GHz) – Most Aggressive

2 “Multiple SSIDs”: Redesign your SSIDs, adding SSID/WLAN with specific security settings – Most Flexible

3 “Transition mode SSID”: Use Transition Mode to support multiple security in different bands - Most Conservative

If you cannot control clients, Transition Mode is recommended

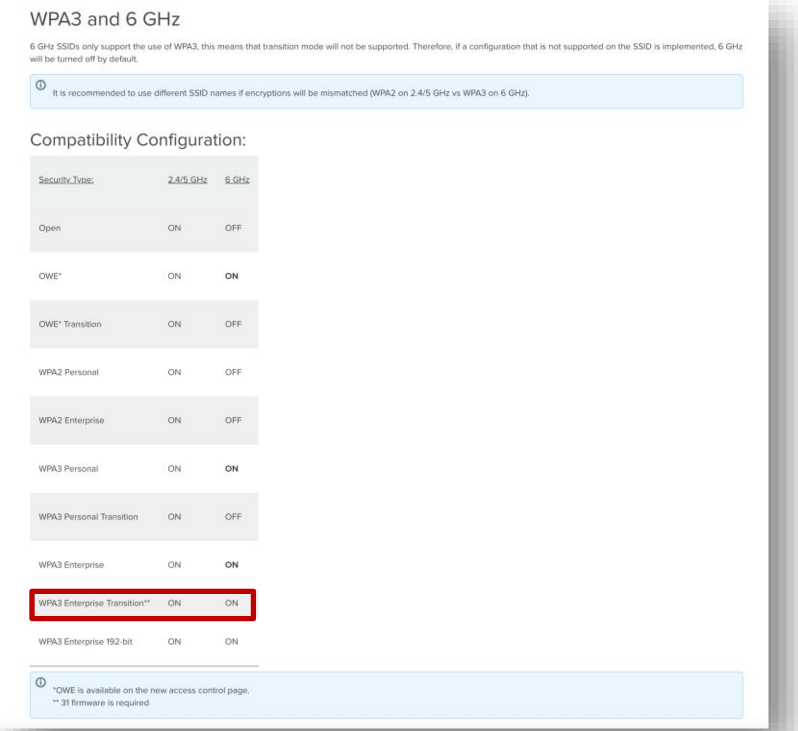
WPA3 Transition mode



```
  RSN Capabilities: 0x00a8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 si
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/S
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/S
      .... .... .0.. .... = Management Frame Protection Required: False
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
```

- 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

Wi-Fi 6GHz security compliance



WPA3 and 6 GHz

6 GHz SSIDs only support the use of WPA3, this means that transition mode will not be supported. Therefore, if a configuration that is not supported on the SSID is implemented, 6 GHz will be turned off by default.

ⓘ It is recommended to use different SSID names if encryptions will be mismatched (WPA2 on 2.4/5 GHz vs WPA3 on 6 GHz).

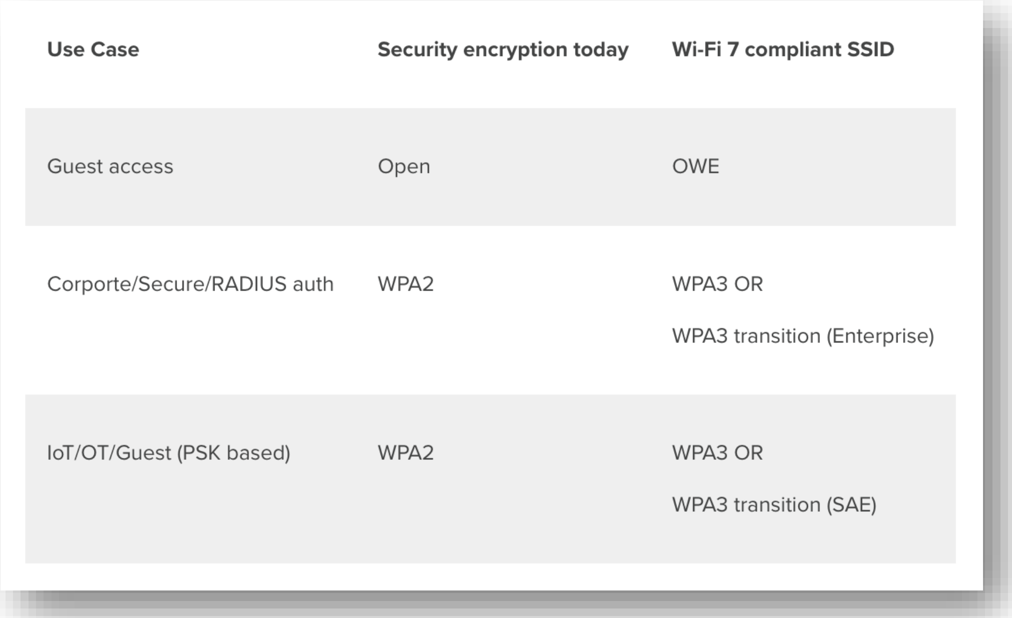
Compatibility Configuration:

Security Type:	2.4/5 GHz	6 GHz
Open	ON	OFF
OWE*	ON	**ON**
OWE* Transition	ON	OFF
WPA2 Personal	ON	OFF
WPA2 Enterprise	ON	OFF
WPA3 Personal	ON	**ON**
WPA3 Personal Transition	ON	OFF
WPA3 Enterprise	ON	**ON**
WPA3 Enterprise Transition**	ON	ON
WPA3 Enterprise 192-bit	ON	ON

ⓘ *OWE is available on the new access control page.
** 31 firmware is required

- 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 on Enterprise starting MR 31.1.1
- WPA3 Personal Transition mode is supported starting MR 31.1.6
- Configuration guide recently updated https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

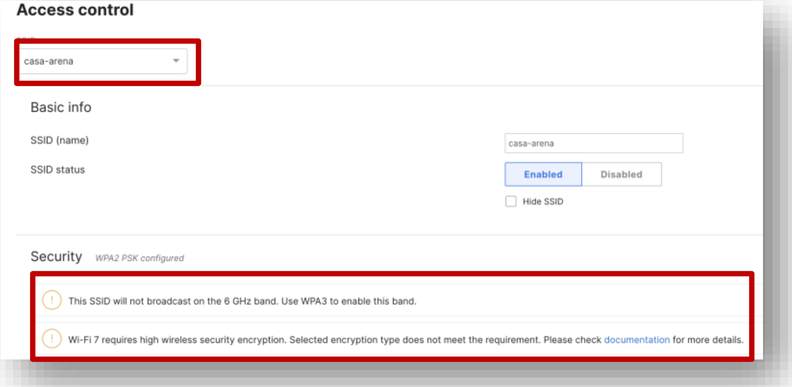
Wi-Fi 7 security compliance



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: Transition mode is not an option for OWE in Wi-Fi 7 standard

Wi-Fi 7 security compliance



Access control

casa-arena

Basic info

SSID (name) casa-arena

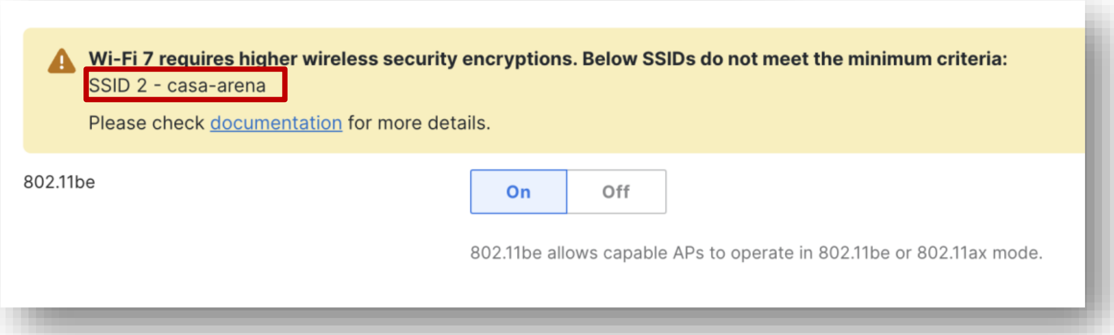
SSID status Enabled Disabled

☐ Hide SSID

Security *WPA2 PSK configured*

This SSID will not broadcast on the 6 GHz band. Use WPA3 to enable this band.

Wi-Fi 7 requires high wireless security encryption. Selected encryption type does not meet the requirement. Please check documentation for more details.



Wi-Fi 7 requires higher wireless security encryptions. Below SSIDs do not meet the minimum criteria:

SSID 2 - casa-arena

Please check documentation for more details.

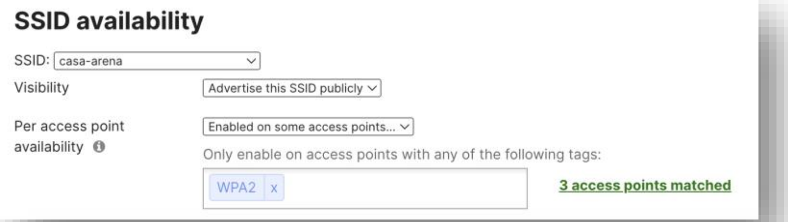
802.11be On Off

802.11be allows capable APs to operate in 802.11be or 802.11ax mode.

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 security compliance: workaround



SSID availability

SSID: casa-arena

Visibility: Advertise this SSID publicly

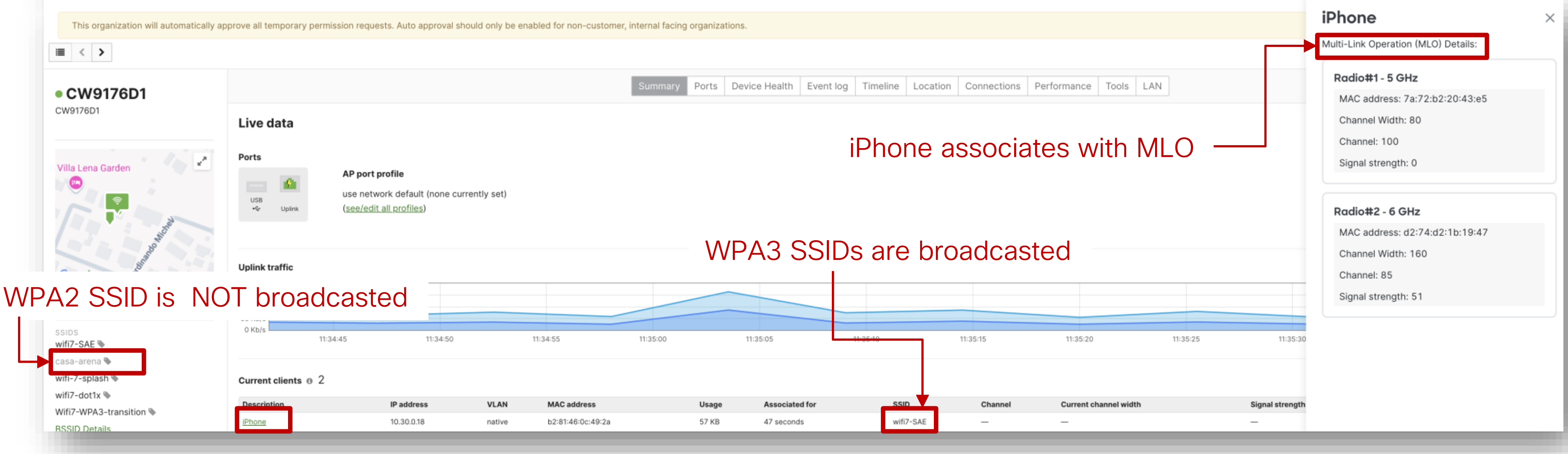
Per access point availability ⓘ: Enabled on some access points...

Only enable on access points with any of the following tags:

WPA2 x

3 access points matched

- Enable WPA2 SSID only on non-Wi-Fi 7 APs
- Wi-Fi 7 SSIDs are now enabled on Wi-Fi 7 APs



This organization will automatically approve all temporary permission requests. Auto approval should only be enabled for non-customer, internal facing organizations.

● CW9176D1

CW9176D1

Live data

Ports

AP port profile

use network default (none currently set)
(see/edit all profiles)

Uplink traffic

SSIDS
wifi7-SAE
casa-arena
wifi-7-splash
wifi7-dot1x
Wifi7-WPA3-transition
BSSID Details

Current clients ⓘ 2

Description	IP address	VLAN	MAC address	Usage	Associated for	SSID	Channel	Current channel width	Signal strength
iPhone	10.30.0.18	native	b2:81:46:0c:49:2a	57 KB	47 seconds	wifi7-SAE	—	—	—

iPhone

Multi-Link Operation (MLO) Details:

Radio#1 - 5 GHz
MAC address: 7a:72:b2:20:43:e5
Channel Width: 80
Channel: 100
Signal strength: 0

Radio#2 - 6 GHz
MAC address: d2:74:d2:1b:19:47
Channel Width: 160
Channel: 85
Signal strength: 51

iPhone associates with MLO

WPA3 SSIDs are broadcasted

WPA2 SSID is NOT broadcasted

SJC-34 WLAN Design: #2 SSIDs

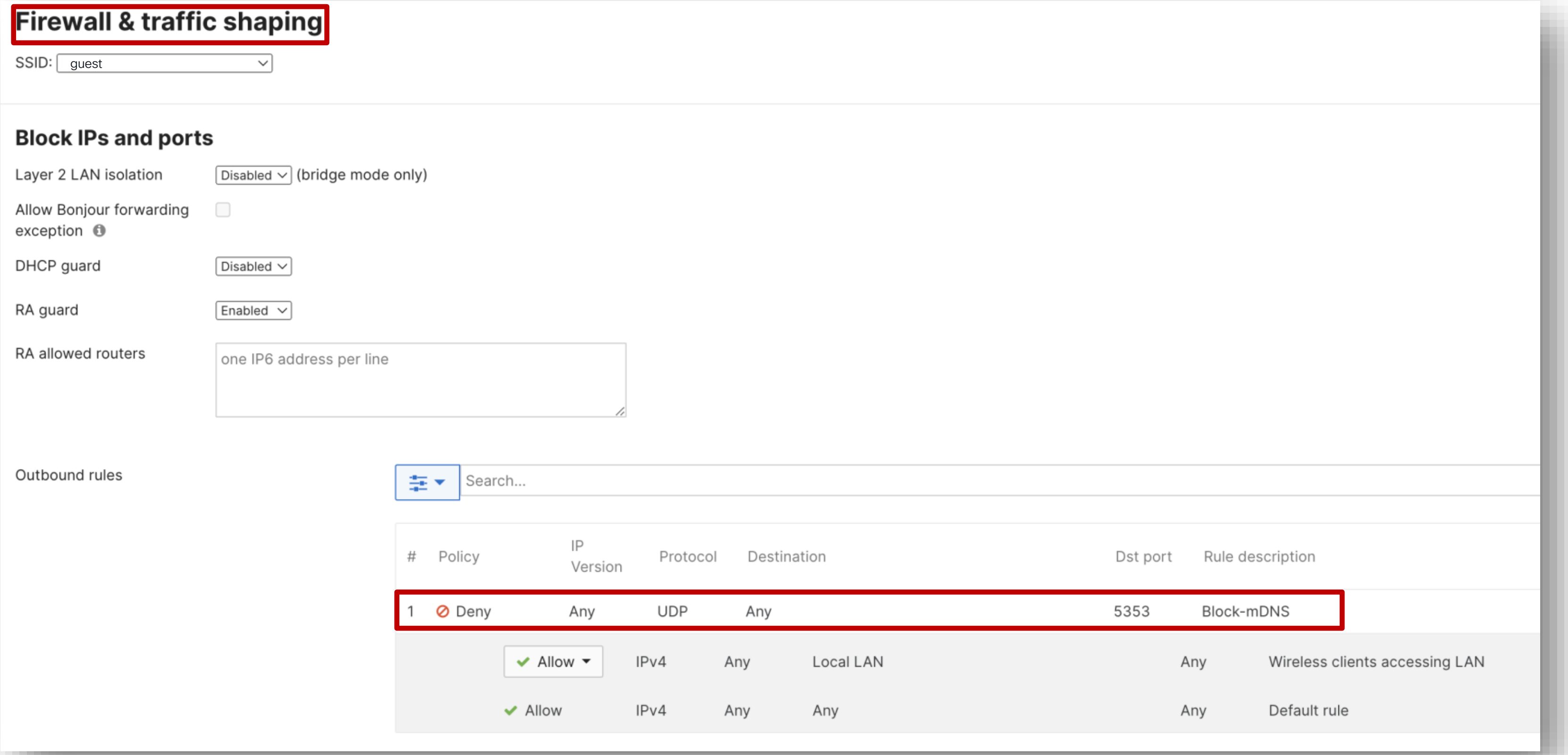
Corporate

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

Guest

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

SJC34 WLAN Design: No mDNS Policy



Firewall & traffic shaping

SSID: guest

Block IPs and ports

Layer 2 LAN isolation	Disabled (bridge mode only)
Allow Bonjour forwarding exception	□
DHCP guard	Disabled
RA guard	Enabled
RA allowed routers	one IP6 address per line

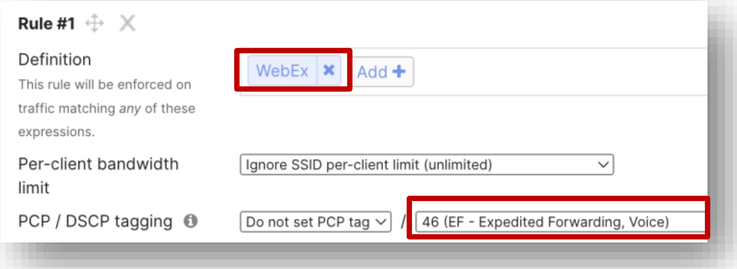
Outbound rules

Search...

#	Policy	IP Version	Protocol	Destination	Dst port	Rule description
1	Deny	Any	UDP	Any	5353	Block-mDNS
	✓ Allow	IPv4	Any	Local LAN	Any	Wireless clients accessing LAN
	✓ Allow	IPv4	Any	Any	Any	Default rule

SJC34 WLAN Design: QoS policy

Corporate



Rule #1

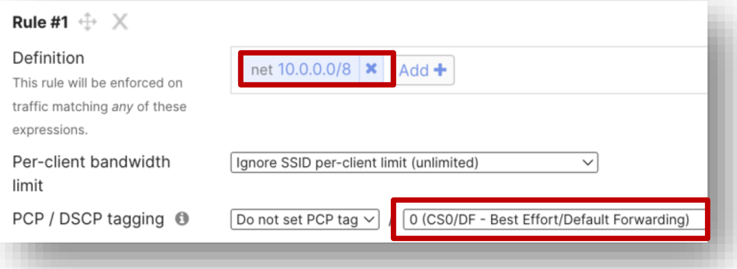
Definition
This rule will be enforced on traffic matching *any* of these expressions.

WebEx ✖ Add ✚

Per-client bandwidth limit: Ignore SSID per-client limit (unlimited)

PCP / DSCP tagging Do not set PCP tag / 46 (EF - Expedited Forwarding, Voice)

Guest



Rule #1

Definition
This rule will be enforced on traffic matching *any* of these expressions.

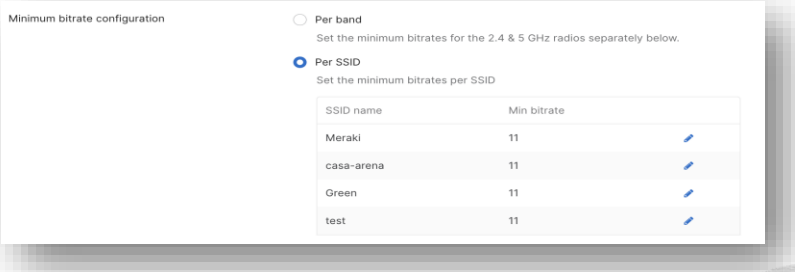
net 10.0.0.0/8 ✖ Add ✚

Per-client bandwidth limit: Ignore SSID per-client limit (unlimited)

PCP / DSCP tagging Do not set PCP tag / 0 (CS0/DF - Best Effort/Default Forwarding)

RF Design

Advanced RF features used



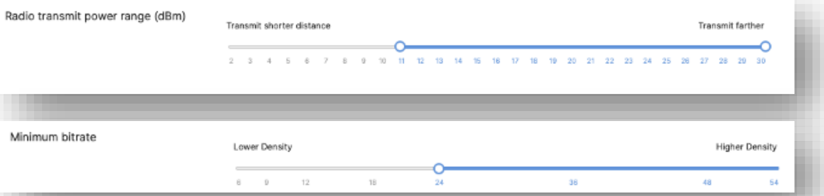
Minimum bitrate configuration

○ Per band
Set the minimum bitrates for the 2.4 & 5 GHz radios separately below.

● Per SSID
Set the minimum bitrates per SSID

SSID name	Min bitrate
Meraki	11
casa-arena	11
Green	11
test	11

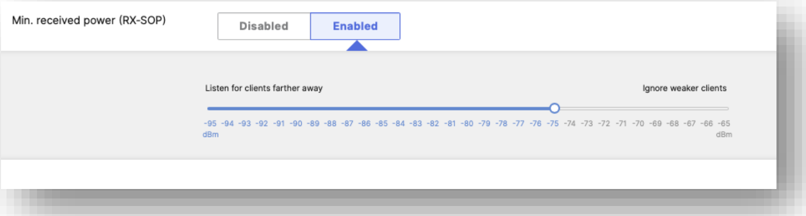
Per band vs per SSID settings



Radio transmit power range (dBm)

Minimum bitrate

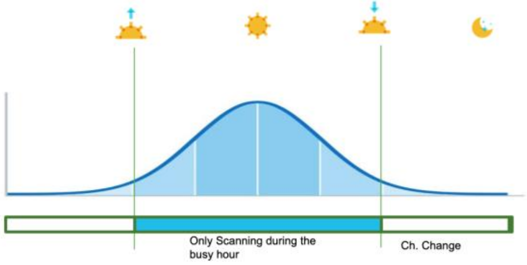
TX Power & Bit rate control



Min. received power (RX-SOP)

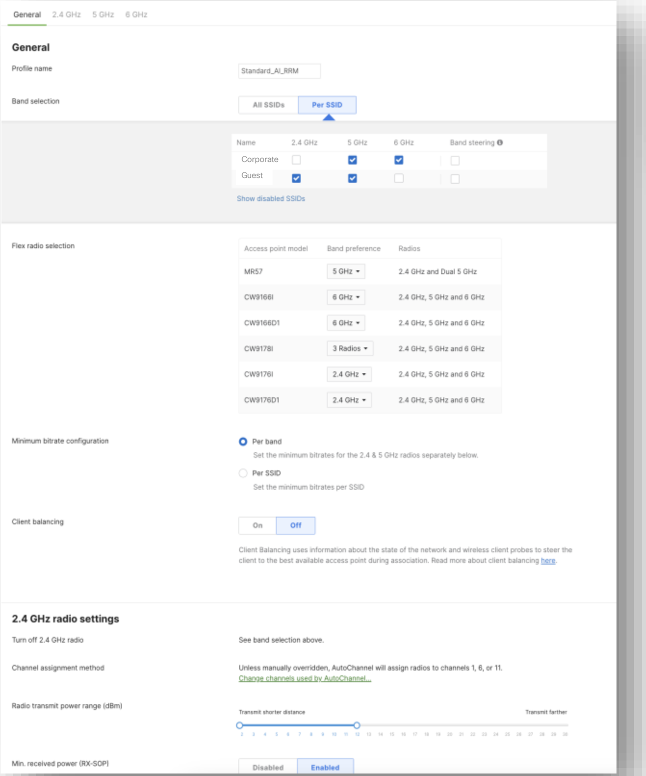
Disabled [✓ Enabled]

Fine tune with RX-SOP



AutoRF > AI Enhanced RRM

SJC-34 RF Profile



General

Profile name: Standard_AI_RRM

Band selection: All SSIDs [✓ Per SSID]

Name	2.4 GHz	5 GHz	6 GHz	Band steering
Corporate	☐	☑	☑	☐
Guest	☑	☑	☐	☐

Show disabled SSIDs

Flex radio selection

Access point model	Band preference	Radios
MR57	5 GHz	2.4 GHz and Dual 5 GHz
CW9166I	6 GHz	2.4 GHz, 5 GHz and 6 GHz
CW9166D1	6 GHz	2.4 GHz, 5 GHz and 6 GHz
CW9178I	3 Radios	2.4 GHz, 5 GHz and 6 GHz
CW9176I	2.4 GHz	2.4 GHz, 5 GHz and 6 GHz
CW9176D1	2.4 GHz	2.4 GHz, 5 GHz and 6 GHz

Minimum bitrate configuration

● Per band
Set the minimum bitrates for the 2.4 & 5 GHz radios separately below.

○ Per SSID
Set the minimum bitrates per SSID

Client balancing: On [✓ Off]

Client Balancing uses information about the state of the network and wireless client probes to steer the client to the best available access point during association. Read more about client balancing here.

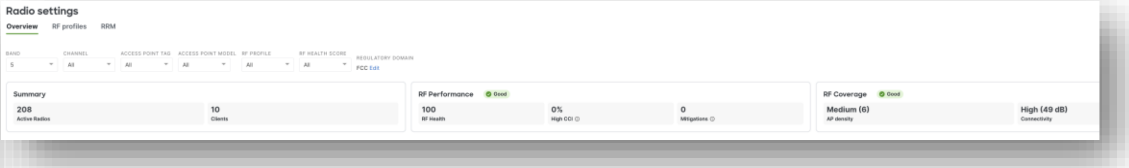
2.4 GHz radio settings

Turn off 2.4 GHz radio: See band selection above.

Channel assignment method: Unless manually overridden, AutoChannel will assign radios to channels 1, 6, or 11.
Change channels used by AutoChannel...

Radio transmit power range (dBm)

Min. received power (RX-SOP): Disabled [✓ Enabled]



Radio settings

BAND: 5
CHANNEL: All
ACCESS POINT TAG: All
ACCESS POINT MODEL: All
RF PROFILE: All
RF HEALTH SCORE: All
REGULATORY DOMAIN: FCC Edit

Summary
208 Active Radios
10 Clients

RF Performance ✓ Good
100 RF Health
0% High CCI ⓘ
0 Mitigations ⓘ

RF Coverage ✓ Good
Medium (6) AP density
High (49 dB) Connectivity

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

R31

AI-Enhanced RRM

AI-Enhanced improves wireless reliability

Trend-Based RRM

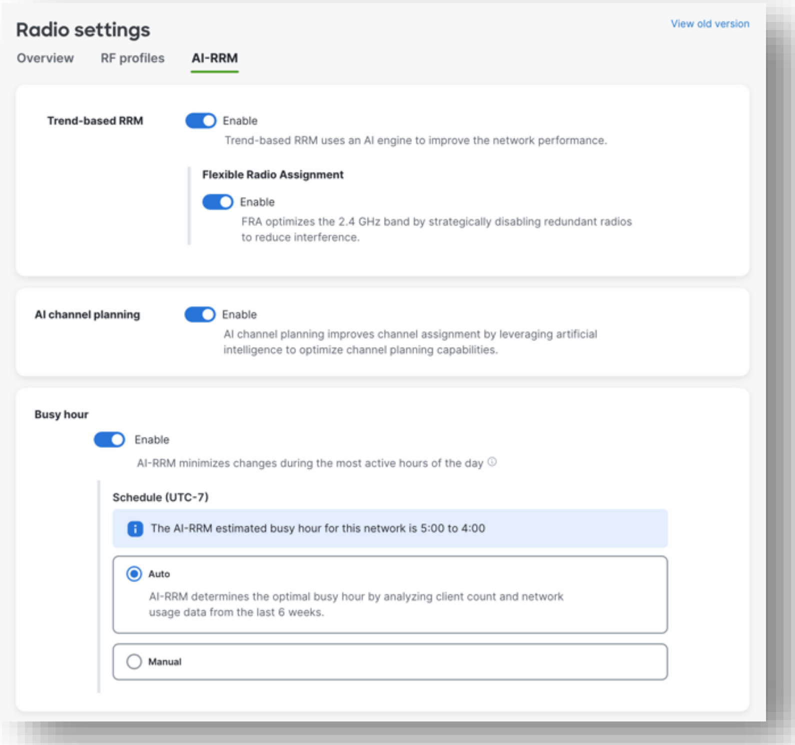
Optimize RF with weeks of historical analysis

Flexible Radio Assignment

Optimize band selection to minimize 2.4 GHz interference

Busy Hour Aware

Minimize disruptive changes during the critical times of day



Radio settings

View old version

Overview | RF profiles | AI-RRM

Trend-based RRM

Enable

Trend-based RRM uses an AI engine to improve the network performance.

Flexible Radio Assignment

Enable

FRA optimizes the 2.4 GHz band by strategically disabling redundant radios to reduce interference.

AI channel planning

Enable

AI channel planning improves channel assignment by leveraging artificial intelligence to optimize channel planning capabilities.

Busy hour

Enable

AI-RRM minimizes changes during the most active hours of the day

Schedule (UTC-7)

The AI-RRM estimated busy hour for this network is 5:00 to 4:00

● Auto

AI-RRM determines the optimal busy hour by analyzing client count and network usage data from the last 6 weeks.

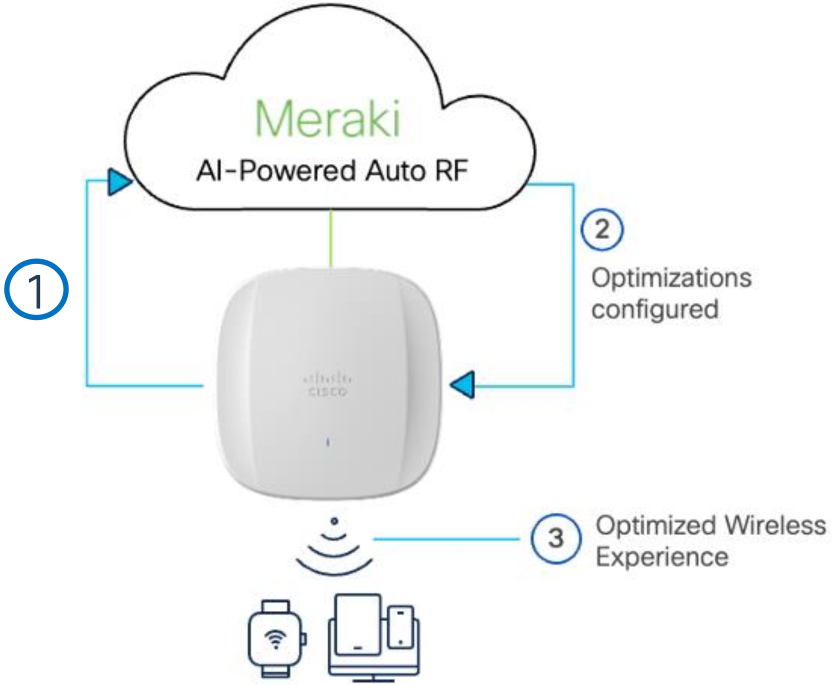
○ Manual

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 vs autoRF*: what you need to know

	autoRF (RRM)	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

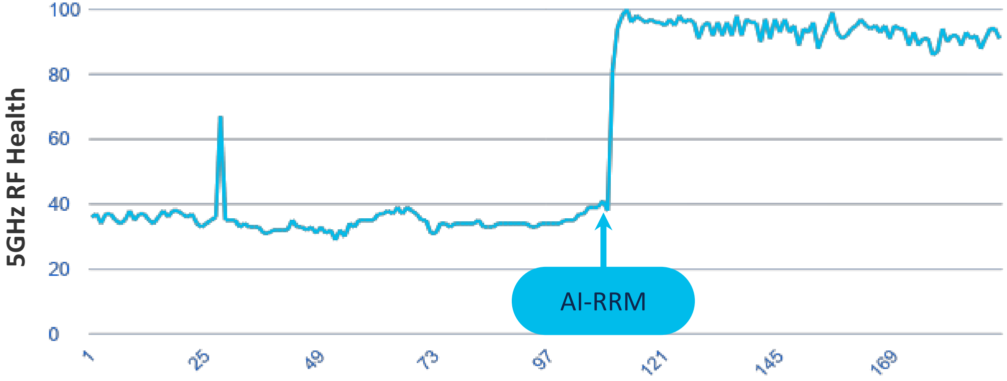
AI-RRM vs autoRF*: what you need to know

	autoRF (RRM)	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

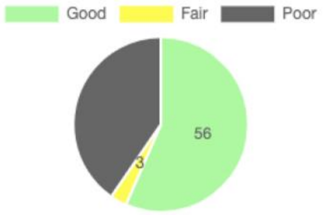
*autoRF is rebranded as RRM

AI-Enhanced RRM in action

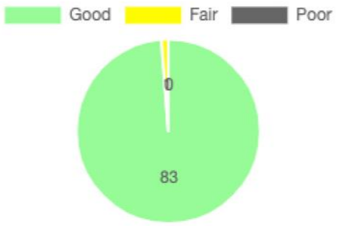
Leading AI Company’s AI-RRM adoption



5GHz RF Health (before Mar 6th)



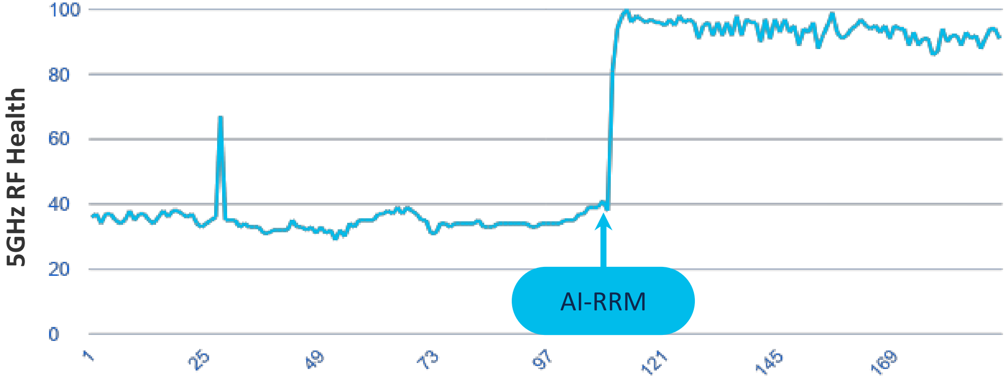
5GHz RF Health (after Mar 6th)



- Wireless RF Health improved drastically after AI-RRM
- Co-Channel Interferences reduction
- Well distributed Wi-Fi channel allocations
- Reduced Channel changes with auto Busy Hour
- Improved Client SNR

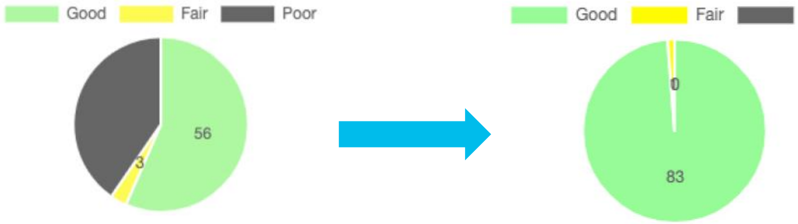
AI-Enhanced RRM in action

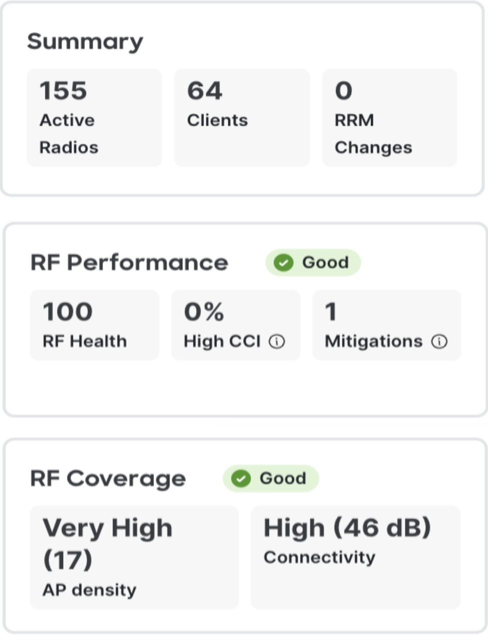
Leading AI Company’s AI-RRM adoption



5GHz RF Health (before Mar 6th)

5GHz RF Health (after Mar 6th)





Summary

155 Active Radios

64 Clients

0 RRM Changes

RF Performance ✓ Good

100 RF Health

0% High CCI ⓘ

1 Mitigations ⓘ

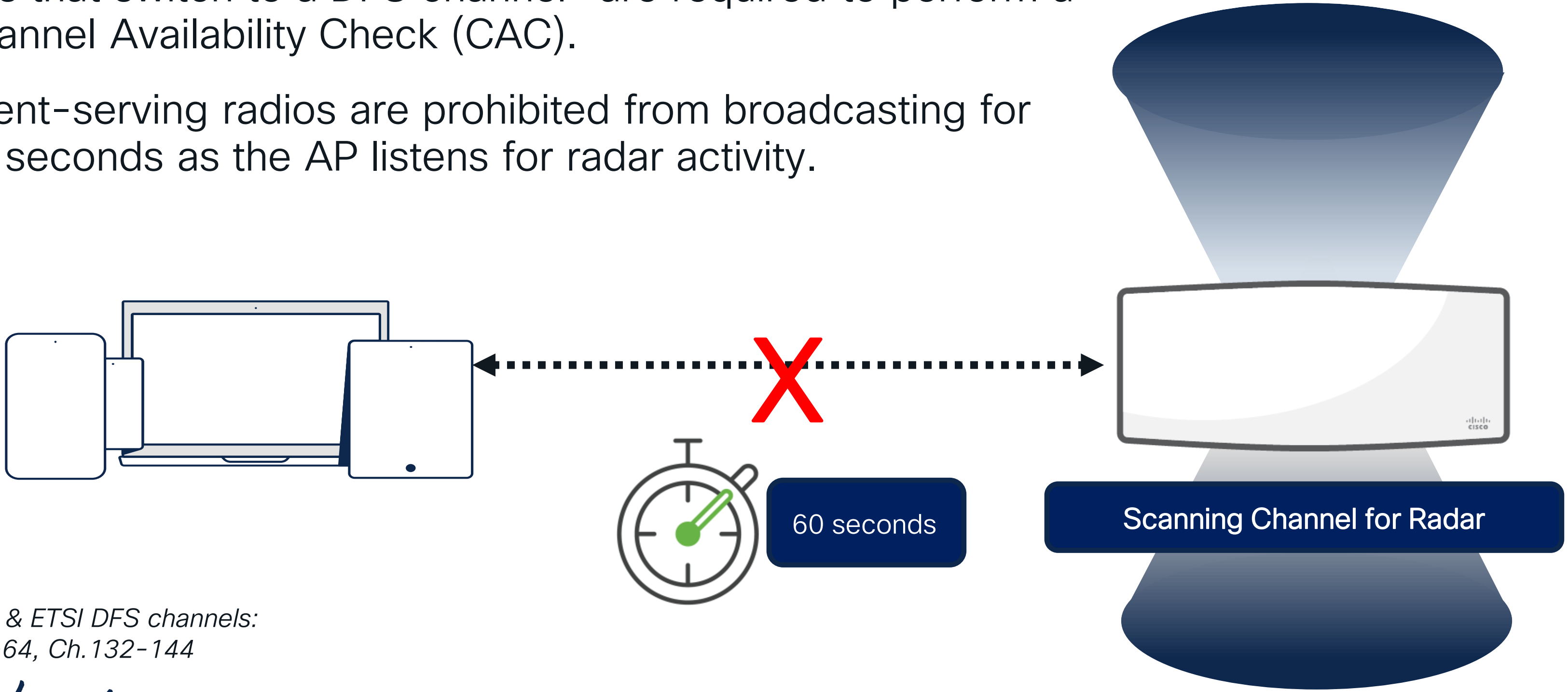
RF Coverage ✓ Good

Very High (17) AP density

High (46 dB) Connectivity

Dealing with DFS Channels

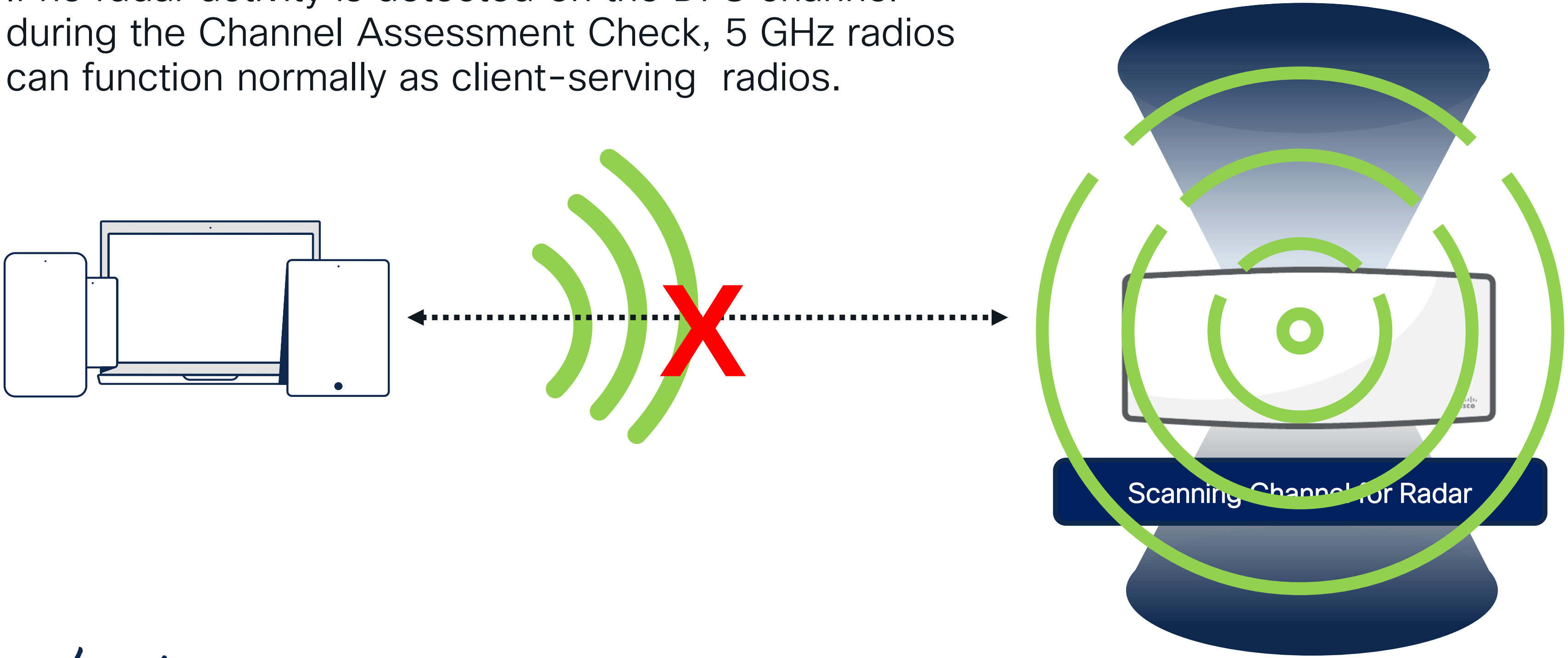
- APs that switch to a DFS channel* are required to perform a Channel Availability Check (CAC).
- Client-serving radios are prohibited from broadcasting for 60 seconds as the AP listens for radar activity.



(*) FCC & ETSI DFS channels:
Ch. 52-64, Ch.132-144

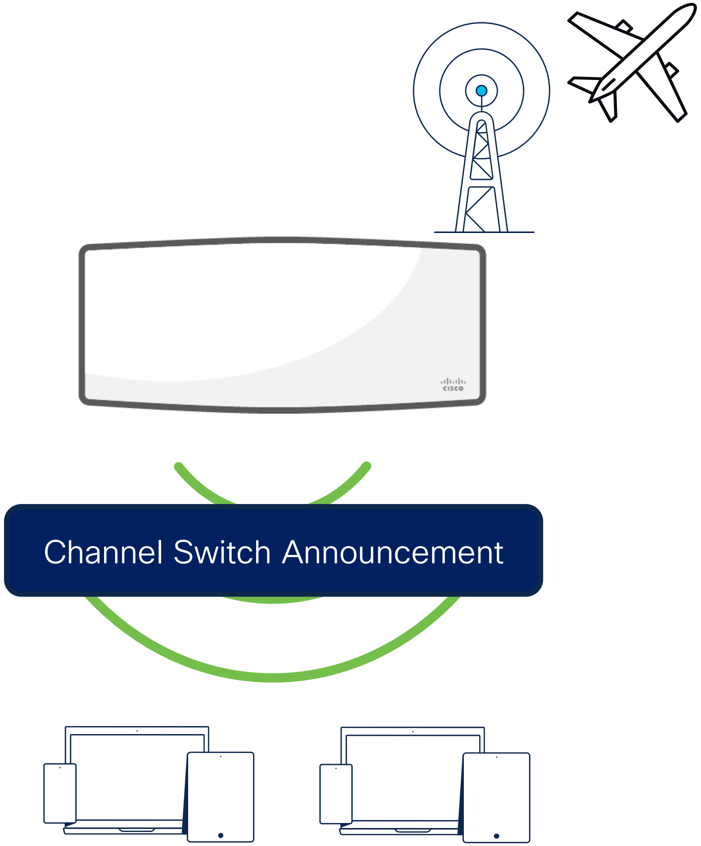
Dealing with DFS Channels

- If no radar activity is detected on the DFS channel during the Channel Assessment Check, 5 GHz radios can function normally as client-serving radios.



Dealing with DFS Channels

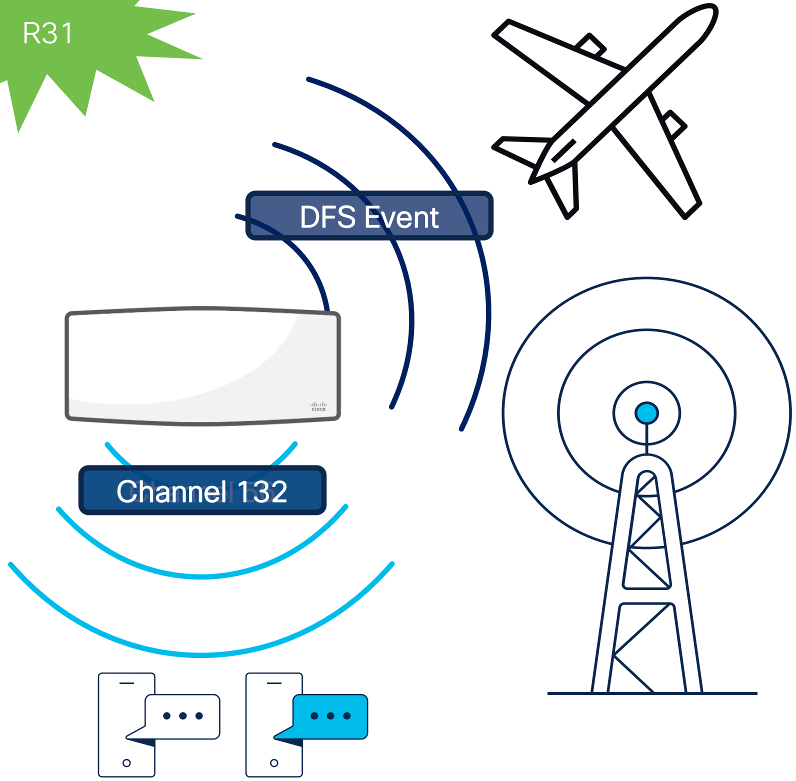
- If AP is already on a DFS channel and a DFS event is detected, the AP's client radio issues a Channel Switch Announcement (CSA) management message.
- Channel Switch Announcement instructs clients to switch to a new channel immediately.
- Problem: In environments with lots of DFS activity, many APs will end up switching to (same) non-DFS channels



Solution: Zero Wait DFS

R31

- Zero wait DFS enables the 5 GHz radios to monitor radar signals on DFS channels while operating on a different channel assignment.
- If a radar event is detected on the current DFS channel, client-serving radios will switch to a new DFS channel and transmit immediately, preserving current client connections.
- Supported on MR55, MR45, MR56, MR46, MR46E, MR86, MR57, CW9166I, CW9166D1, CW9164 and later

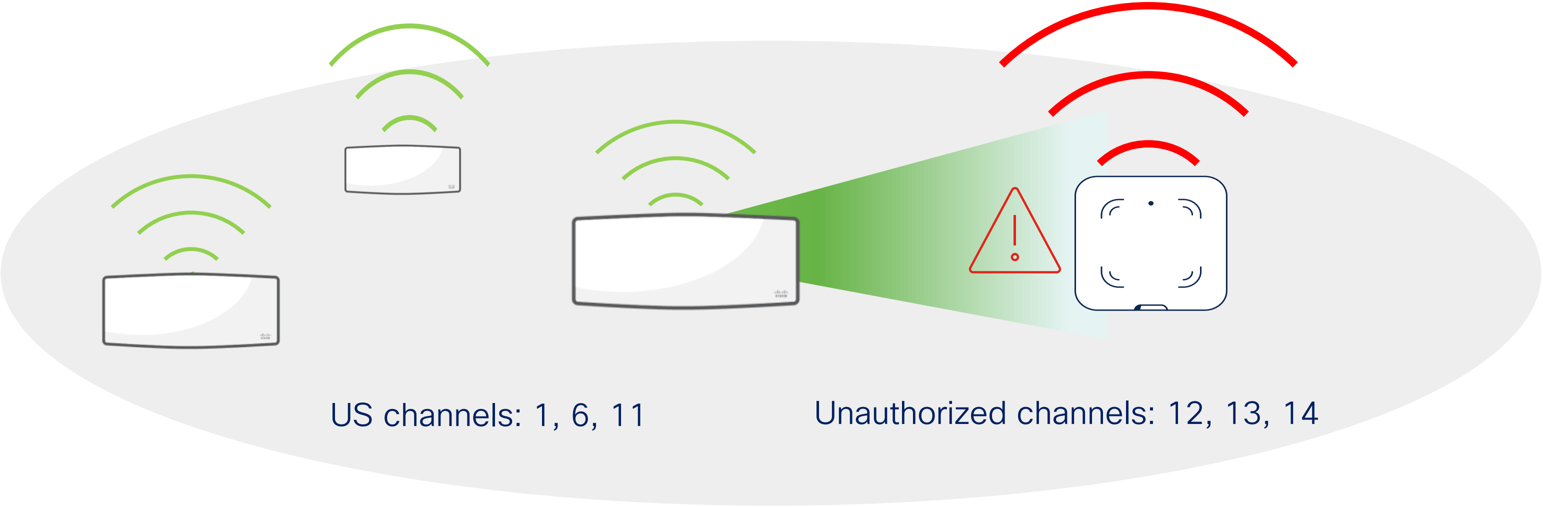


FCC & ETSI DFS channels:
Ch. 52-64, Ch.132-144

Air-Marshal: Enhanced Rogue Detection

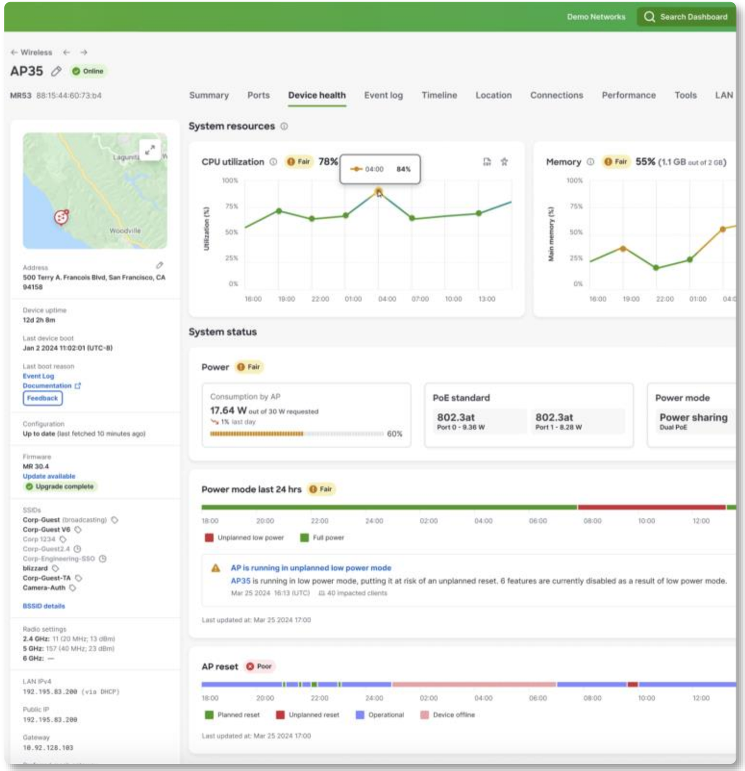
R31

- Air Marshall’s rogue detection support has been extended beyond the channels in the regulatory domain. Dashboard now generates alerts for rogue APs broadcasting on unauthorized 2.4 and 5 GHz radio channels.



RF Monitoring and Troubleshooting

AP Device Health



Address
500 Terry A. Francois Blvd, San Francisco, CA 94158

Device uptime
12d 2h 8m

Last device boot
Jan 2 2024 11:02:01 (UTC-8)

Last boot reason
Event Log
Documentation
Feedback

Configuration
Up to date (last fetched 10 minutes ago)

Firmware
MR 30.4
Update available
Upgrade complete

SSIDs
Corp-Guest (broadcasting)
Corp-Guest V6
Corp 1234
Corp-Guest2.4
Corp-Engineering-SSO
blizzard
Corp-Guest-TA
Camera-Auth

BSSID details

Radio settings
2.4 GHz: 11 (20 MHz; 13 dBm)
5 GHz: 157 (40 MHz; 23 dBm)
6 GHz: —

LAN IPv4
192.195.83.200 (via DHCP)

Public IP
192.195.83.200

Gateway
10.92.128.103

System status

Power Fair

Consumption by AP
17.64 W out of 30 W requested
1% last day
60%

PoE standard
802.3at
Port 0 - 9.36 W
802.3at
Port 1 - 8.28 W

Power mode
Power sharing
Dual PoE

Power mode last 24 hrs Fair

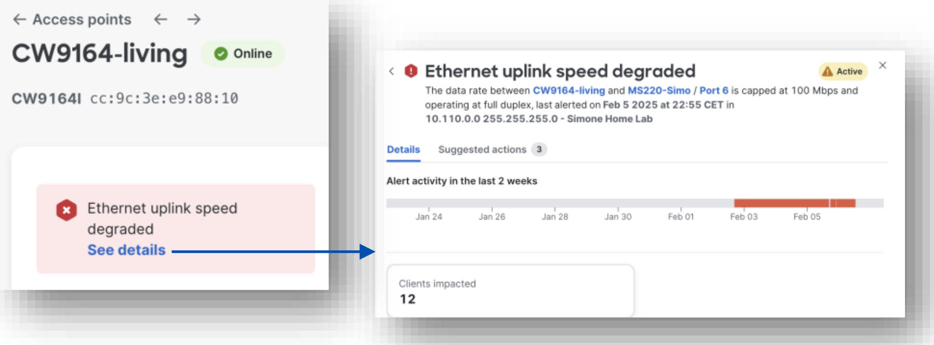
AP is running in unplanned low power mode
AP35 is running in low power mode, putting it at risk of an unplanned reset. 6 features are currently disabled as a result of low power mode.
Mar 25 2024 16:13 (UTC) 40 impacted clients

Last updated at: Mar 25 2024 17:00

AP reset Poor

Last updated at: Mar 25 2024 17:00

- CPU and Memory usage trend
- Contextual AP Uptime trend
- PoE / Power monitoring
- Integrated AP Alert remediation



CW9164-living

CW9164I cc:9c:3e:e9:88:10

Ethernet uplink speed degraded

Ethernet uplink speed degraded

The data rate between CW9164-living and MS220-Simo / Port 6 is capped at 100 Mbps and operating at full duplex, last alerted on Feb 5 2025 at 22:55 CET in 10.110.0.0 255.255.255.0 - Simone Home Lab

Alert activity in the last 2 weeks

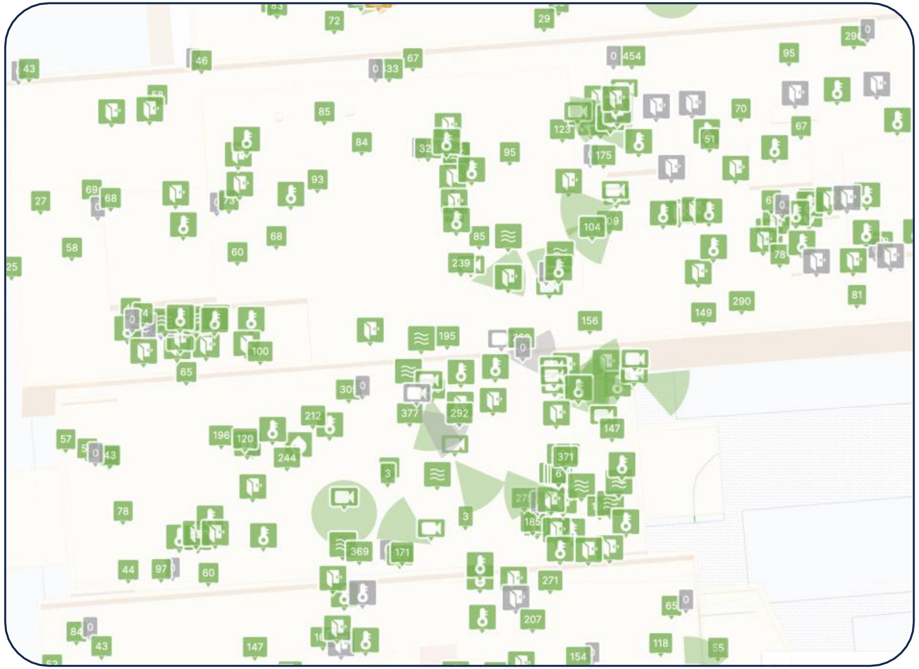
Clients impacted
12

AP Neighbors feature

RF interference is difficult to visualize

It’s difficult to identify the source of interference

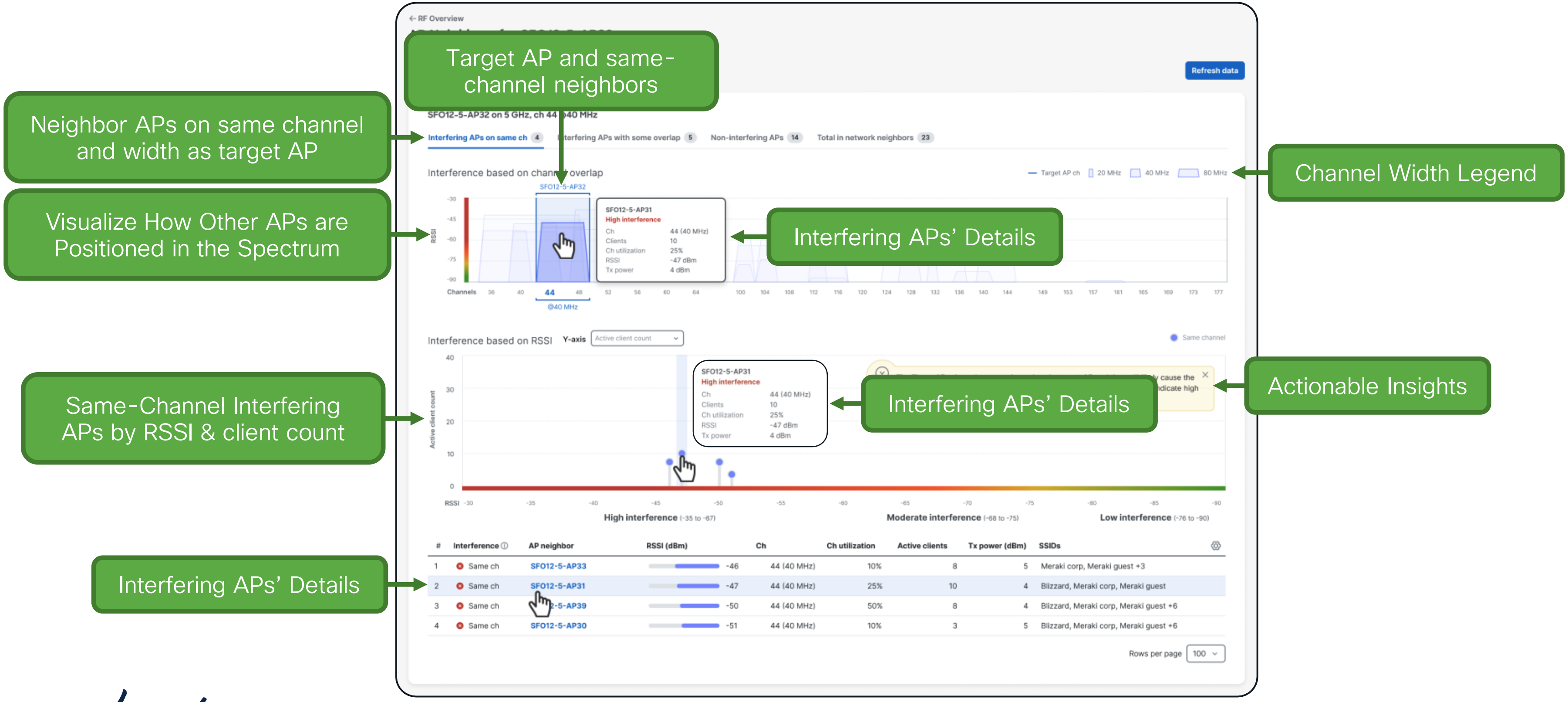
Today’s widgets show impacted APs but not details of the sources



65

AP Neighbors feature

Visualize Same-Channel AP Interference with AP Neighbors



Target AP and same-channel neighbors

Neighbor APs on same channel and width as target AP

Visualize How Other APs are Positioned in the Spectrum

Same-Channel Interfering APs by RSSI & client count

Interfering APs' Details

Channel Width Legend

Interfering APs' Details

Actionable Insights

Interfering APs' Details

← RF Overview

Refresh data

SFO12-5-AP32 on 5 GHz, ch 44 @40 MHz

Interfering APs on same ch 4 | Interfering APs with some overlap 5 | Non-interfering APs 14 | Total in network neighbors 23

Interference based on channel overlap

SFO12-5-AP31
High interference
Ch 44 (40 MHz)
Clients 10
Ch utilization 25%
RSSI -47 dBm
Tx power 4 dBm

Interference based on RSSI Y-axis Active client count

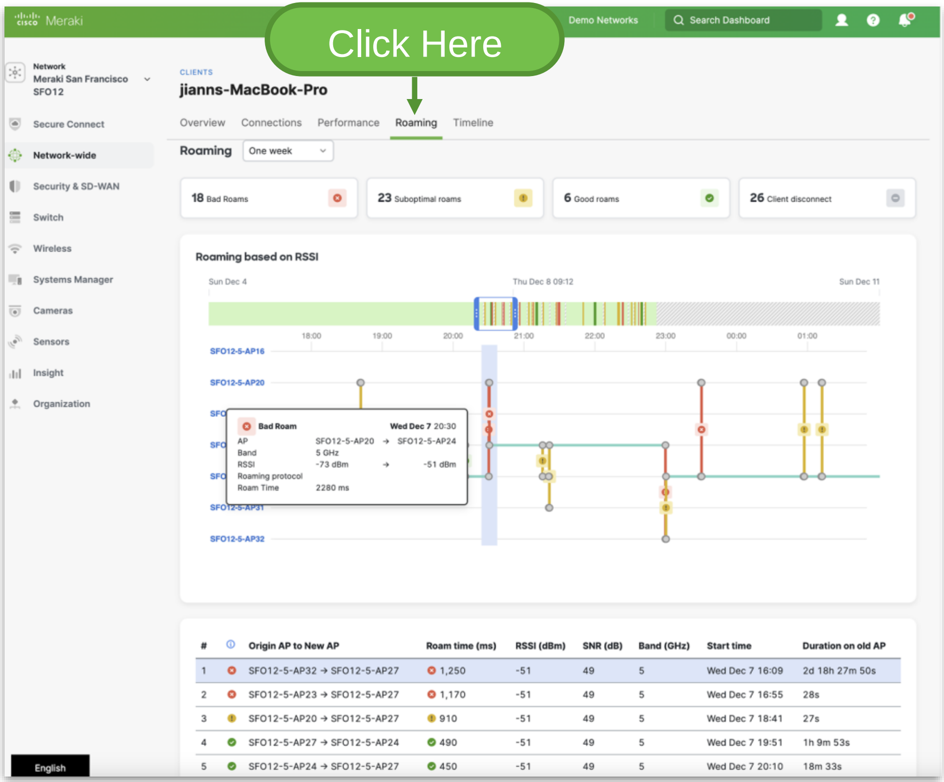
High interference (-35 to -67) Moderate interference (-68 to -75) Low interference (-76 to -90)

SFO12-5-AP31
High interference
Ch 44 (40 MHz)
Clients 10
Ch utilization 25%
RSSI -47 dBm
Tx power 4 dBm

#	Interference	AP neighbor	RSSI (dBm)	Ch	Ch utilization	Active clients	Tx power (dBm)	SSIDs
1	Same ch	SFO12-5-AP33	-46	44 (40 MHz)	10%	8	5	Meraki corp, Meraki guest +3
2	Same ch	SFO12-5-AP31	-47	44 (40 MHz)	25%	10	4	Blizzard, Meraki corp, Meraki guest
3	Same ch	2-5-AP39	-50	44 (40 MHz)	50%	8	4	Blizzard, Meraki corp, Meraki guest +6
4	Same ch	SFO12-5-AP30	-51	44 (40 MHz)	10%	3	5	Blizzard, Meraki corp, Meraki guest +6

Rows per page 100

Client Roaming Analytics



Click Here

jianns-MacBook-Pro

Roaming

18 Bad Roams | 23 Suboptimal roams | 6 Good roams | 26 Client disconnect

Bad Roam — Wed Dec 7 20:30
AP: SFO12-5-AP20 → SFO12-5-AP24
Band: 5 GHz
RSSI: -73 dBm → -51 dBm
Roaming protocol
Roam Time: 2280 ms

#	ⓘ	Origin AP to New AP	Roam time (ms)	RSSI (dBm)	SNR (dB)	Band (GHz)	Start time	Duration on old AP
1	☒	SFO12-5-AP32 → SFO12-5-AP27	☒ 1,250	-51	49	5	Wed Dec 7 16:09	2d 18h 27m 50s
2	☒	SFO12-5-AP23 → SFO12-5-AP27	☒ 1,170	-51	49	5	Wed Dec 7 16:55	28s
3	!	SFO12-5-AP20 → SFO12-5-AP27	! 910	-51	49	5	Wed Dec 7 18:41	27s
4	✓	SFO12-5-AP27 → SFO12-5-AP24	✓ 490	-51	49	5	Wed Dec 7 19:51	1h 9m 53s
5	✓	SFO12-5-AP24 → SFO12-5-AP27	✓ 450	-51	49	5	Wed Dec 7 20:10	18m 33s

Intuitive client roaming visualization with detailed events for triage simplification.

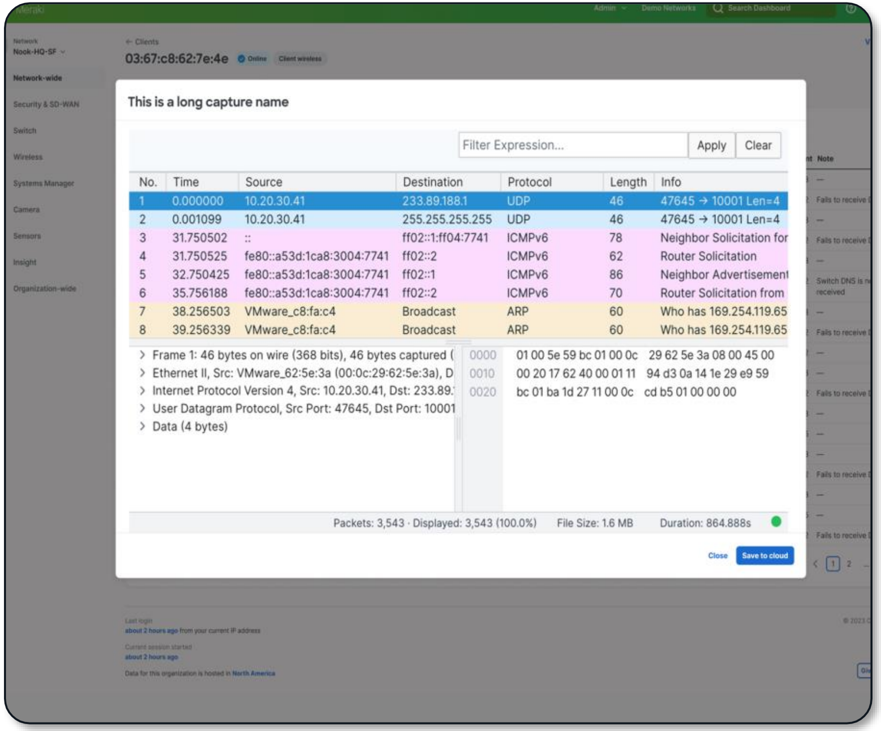
Roaming Event Tiers: Bad, Suboptimal, Good, Ping-Pong, Disconnected.

Visualization supports a 1-hour to 2 min view.

Pro-Active Cloud Packet Capture

R31

- Automated Packet Capture upon client connection or roaming failure
- Native Packet Analyzer integration
- Easy cloud access of historical PCAP files
- Supported in both MS Switch & MR APs



03:67:c8:62:7e:4e

This is a long capture name

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.20.30.41	233.89.188.1	UDP	46	47645 → 10001 Len=4
2	0.001099	10.20.30.41	255.255.255.255	UDP	46	47645 → 10001 Len=4
3	31.750502	::	ff02::1:ff04:7741	ICMPv6	78	Neighbor Solicitation for
4	31.750525	fe80::a53d:1ca8:3004:7741	ff02::2	ICMPv6	62	Router Solicitation
5	32.750425	fe80::a53d:1ca8:3004:7741	ff02::1	ICMPv6	86	Neighbor Advertisement
6	35.756188	fe80::a53d:1ca8:3004:7741	ff02::2	ICMPv6	70	Router Solicitation from
7	38.256503	VMware_c8:fa:c4	Broadcast	ARP	60	Who has 169.254.119.65
8	39.256339	VMware_c8:fa:c4	Broadcast	ARP	60	Who has 169.254.119.65

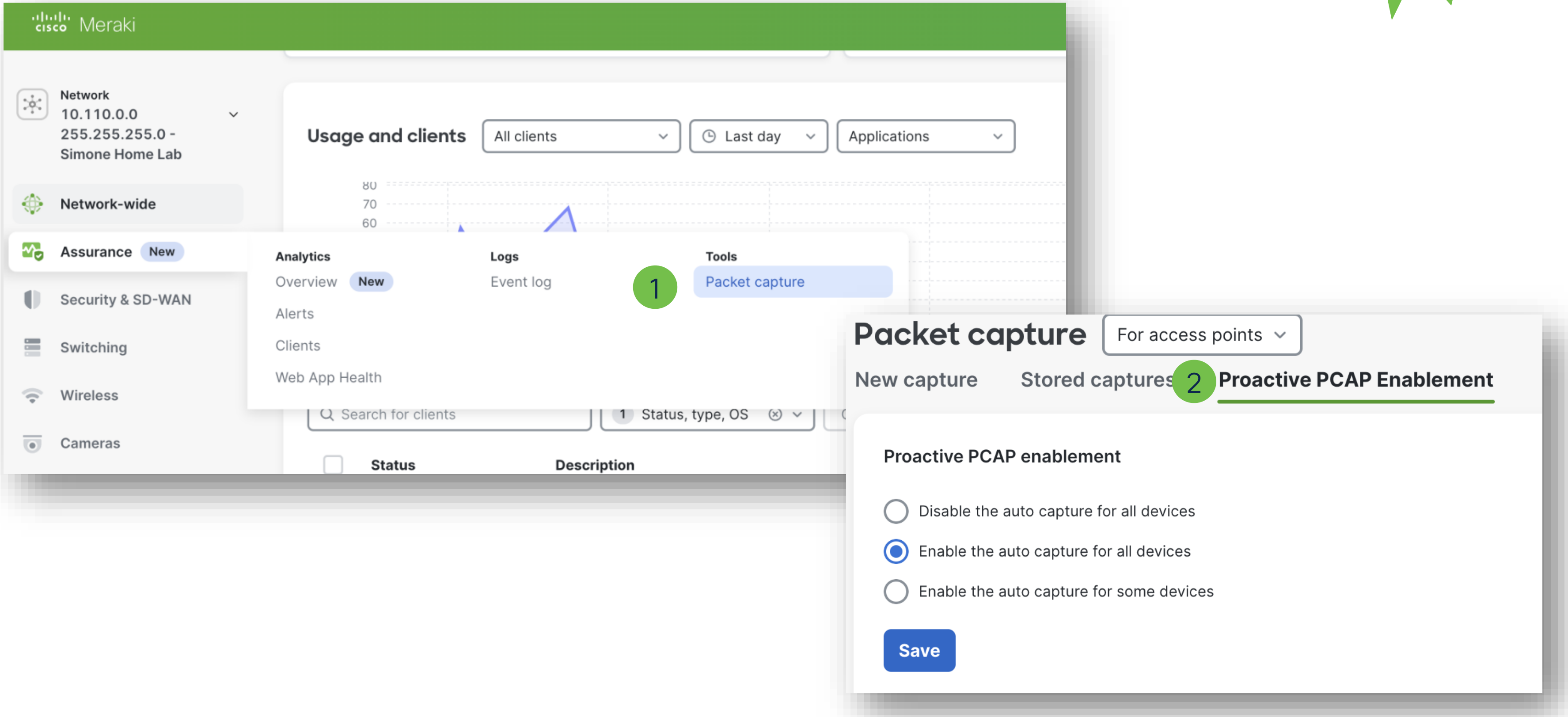
```
> Frame 1: 46 bytes on wire (368 bits), 46 bytes captured (
> Ethernet II, Src: VMware_62:5e:3a (00:0c:29:62:5e:3a), D
> Internet Protocol Version 4, Src: 10.20.30.41, Dst: 233.89.
> User Datagram Protocol, Src Port: 47645, Dst Port: 10001
> Data (4 bytes)
```

```
0000   01 00 5e 59 bc 01 00 0c   29 62 5e 3a 08 00 45 00
0010   00 20 17 62 40 00 01 11   94 d3 0a 14 1e 29 e9 59
0020   bc 01 ba 1d 27 11 00 0c   cd b5 01 00 00 00
```

Packets: 3,543 · Displayed: 3,543 (100.0%)   File Size: 1.6 MB   Duration: 864.888s

Pro-Active Cloud Packet Capture

R31



Packet capture

Proactive PCAP enablement

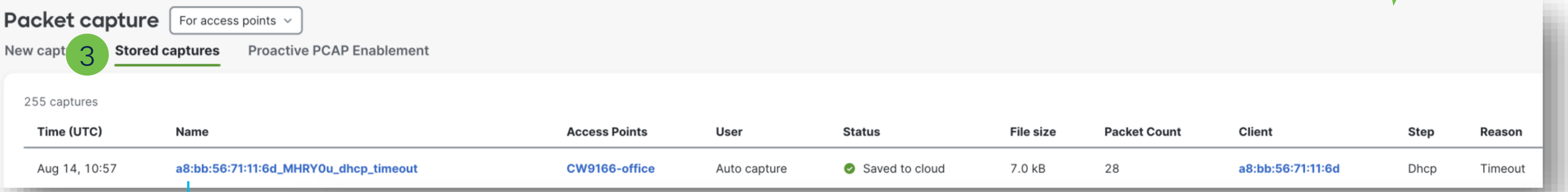
○ Disable the auto capture for all devices

● Enable the auto capture for all devices

○ Enable the auto capture for some devices

Pro-Active Cloud Packet Capture

R31



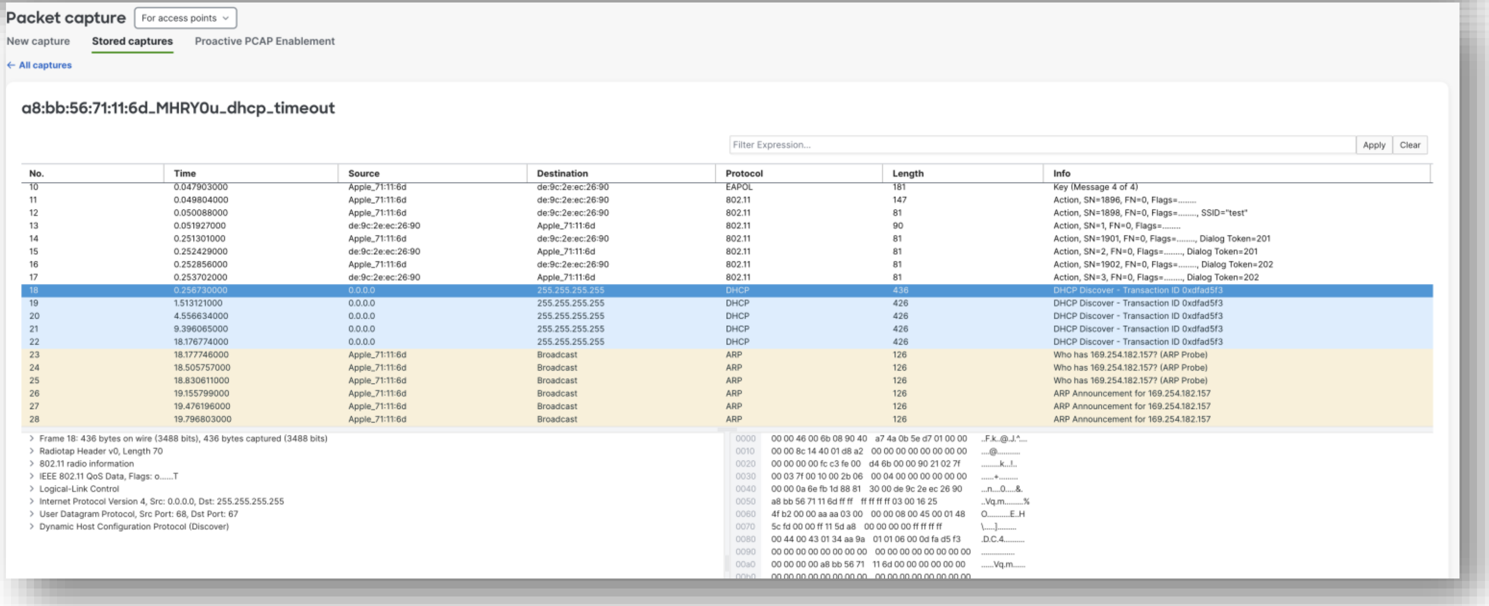
Packet capture

For access points ⌄

New capt 3 **Stored captures** Proactive PCAP Enablement

255 captures

Time (UTC)	Name	Access Points	User	Status	File size	Packet Count	Client	Step	Reason
Aug 14, 10:57	a8:bb:56:71:11:6d_MHRY0u_dhcp_timeout	CW9166-office	Auto capture	✓ Saved to cloud	7.0 kB	28	a8:bb:56:71:11:6d	Dhcp	Timeout



Packet capture

For access points ⌄

New capture **Stored captures** Proactive PCAP Enablement

← All captures

a8:bb:56:71:11:6d_MHRY0u_dhcp_timeout

Filter Expression... Apply Clear

No.	Time	Source	Destination	Protocol	Length	Info
10	0.047903000	Apple_71:11:6d	de:9c:2e:ec:26:90	EAPOL	181	Key (Message 4 of 4)
11	0.049804000	Apple_71:11:6d	de:9c:2e:ec:26:90	802.11	147	Action, SN=1896, FN=0, Flags=........
12	0.050088000	Apple_71:11:6d	de:9c:2e:ec:26:90	802.11	81	Action, SN=1898, FN=0, Flags=........, SSID="test"
13	0.051927000	de:9c:2e:ec:26:90	Apple_71:11:6d	802.11	90	Action, SN=1, FN=0, Flags=........
14	0.251301000	Apple_71:11:6d	de:9c:2e:ec:26:90	802.11	81	Action, SN=1901, FN=0, Flags=........, Dialog Token=201
15	0.252429000	de:9c:2e:ec:26:90	Apple_71:11:6d	802.11	81	Action, SN=2, FN=0, Flags=........, Dialog Token=201
16	0.252856000	Apple_71:11:6d	de:9c:2e:ec:26:90	802.11	81	Action, SN=1902, FN=0, Flags=........, Dialog Token=202
17	0.253702000	de:9c:2e:ec:26:90	Apple_71:11:6d	802.11	81	Action, SN=3, FN=0, Flags=........, Dialog Token=202
18	0.256730000	0.0.0.0	255.255.255.255	DHCP	436	DHCP Discover - Transaction ID 0xdfad5f3
19	1.513121000	0.0.0.0	255.255.255.255	DHCP	426	DHCP Discover - Transaction ID 0xdfad5f3
20	4.556634000	0.0.0.0	255.255.255.255	DHCP	426	DHCP Discover - Transaction ID 0xdfad5f3
21	9.396065000	0.0.0.0	255.255.255.255	DHCP	426	DHCP Discover - Transaction ID 0xdfad5f3
22	18.176774000	0.0.0.0	255.255.255.255	DHCP	426	DHCP Discover - Transaction ID 0xdfad5f3
23	18.177746000	Apple_71:11:6d	Broadcast	ARP	126	Who has 169.254.182.157? (ARP Probe)
24	18.505757000	Apple_71:11:6d	Broadcast	ARP	126	Who has 169.254.182.157? (ARP Probe)
25	18.830611000	Apple_71:11:6d	Broadcast	ARP	126	Who has 169.254.182.157? (ARP Probe)
26	19.155799000	Apple_71:11:6d	Broadcast	ARP	126	ARP Announcement for 169.254.182.157
27	19.476196000	Apple_71:11:6d	Broadcast	ARP	126	ARP Announcement for 169.254.182.157
28	19.796803000	Apple_71:11:6d	Broadcast	ARP	126	ARP Announcement for 169.254.182.157

```
> Frame 18: 436 bytes on wire (3488 bits), 436 bytes captured (3488 bits)
> Radiotap Header v0, Length 70
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: o......T
> Logical-Link Control
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

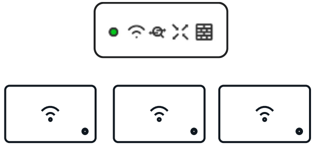
```
0000  00 00 46 00 6b 08 90 40   a7 4a 0b 5e d7 01 00 00   ..F.k..@.J.^....
0010  00 00 8c 14 40 01 d8 a2   00 00 00 00 00 00 00 00   ....@...........
0020  00 00 00 00 fc c3 fe 00   d4 6b 00 00 90 21 02 7f   .........k...!..
0030  00 03 7f 00 10 00 2b 06   00 04 00 00 00 00 00 00   ......+.........
0040  00 00 0a 6e fb 1d 88 81   30 00 de 9c 2e ec 26 90   ...n....0.....&.
0050  a8 bb 56 71 11 6d ff ff   ff ff ff ff 03 00 16 25   ..Vq.m.........%
0060  4f b2 00 00 aa aa 03 00   00 00 08 00 45 00 01 48   O...........E..H
0070  5c fd 00 00 ff 11 5d a8   00 00 00 00 ff ff ff ff   \.....]........
0080  00 44 00 43 01 34 aa 9a   01 01 06 00 0d fa d5 f3   .D.C.4..........
0090  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00a0  00 00 00 00 a8 bb 56 71   11 6d 00 00 00 00 00 00   ......Vq.m......
00b0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
```

Network Architecture

Network Architecture > Customer deployments

Large, Medium Campus

> Centralized Data Plane architecture

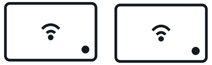


km^2/mi^2

E.g., University Campus

Distribute Enterprise: Branch, Small Campus

> Distributed Data Plane architecture

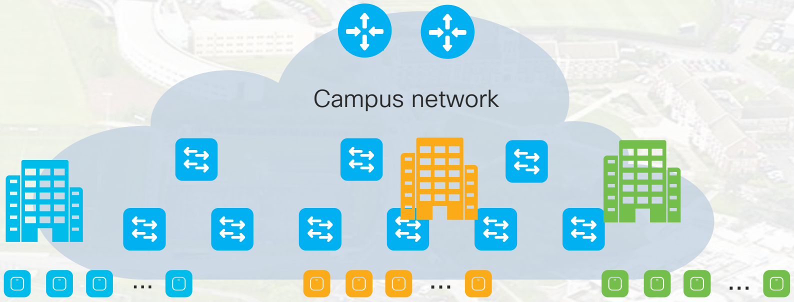


m^2/ft^2

e.g., Retail

Network Architecture: Large Campus with Meraki

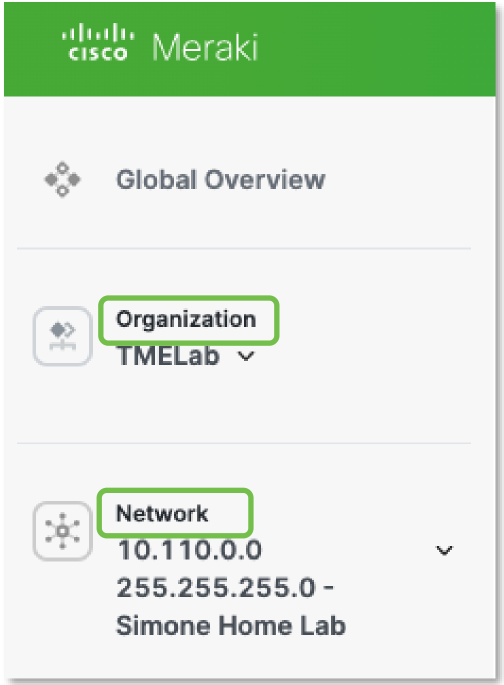
“Distributed Data Plane architecture” > Can we do it?



1000s of APs and clients

Before we answer this question..

Meraki Organization and Meraki Network



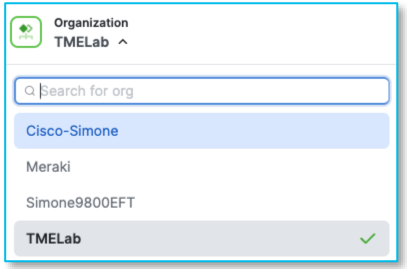
Global Overview

Organization
TMELab

Network
10.110.0.0 255.255.255.0 - Simone Home Lab

Organization: A collection of networks that are all part of a single organizational entity

Recommended 25k nodes* due to Dashboard performance



Organization
TMELab

Search for org

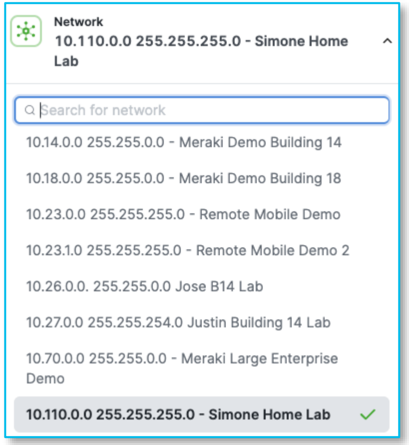
- Cisco-Simone
- Meraki
- Simone9800EFT
- TMELab ✓

Need more scale?

Configure multiple Orgs
Multi org view
Example:
CompanyA-East org
CompanyA-West org

Network: Set of Meraki devices, their configurations, statistics, and other Services. It is the administrative domain

Recommended 1,000 nodes due to Dashboard performance



Network
10.110.0.0 255.255.255.0 - Simone Home Lab

Search for network

- 10.14.0.0 255.255.0.0 - Meraki Demo Building 14
- 10.18.0.0 255.255.0.0 - Meraki Demo Building 18
- 10.23.0.0 255.255.255.0 - Remote Mobile Demo
- 10.23.1.0 255.255.255.0 - Remote Mobile Demo 2
- 10.26.0.0. 255.255.0.0 Jose B14 Lab
- 10.27.0.0 255.255.254.0 Justin Building 14 Lab
- 10.70.0.0 255.255.0.0 - Meraki Large Enterprise Demo
- 10.110.0.0 255.255.255.0 - Simone Home Lab ✓

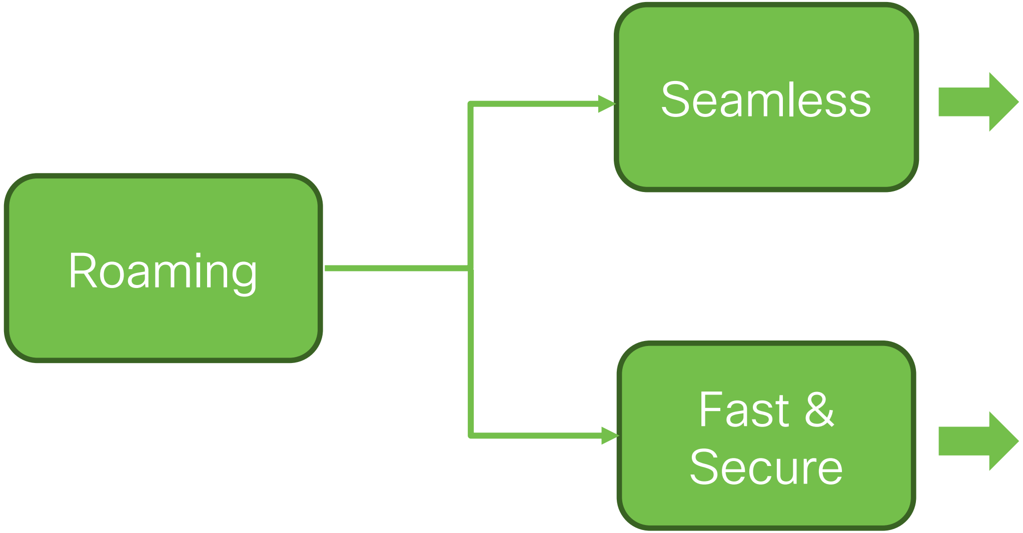
Network maps to a geo or logical location (site, group of buildings, building, etc.)

For Wireless, it defines scope of SSIDs and policies (including RF profiles)

It is the Services domain

*Node: any Meraki devices (MR, MS, MX, MV, MT, etc.)

Roaming refresher

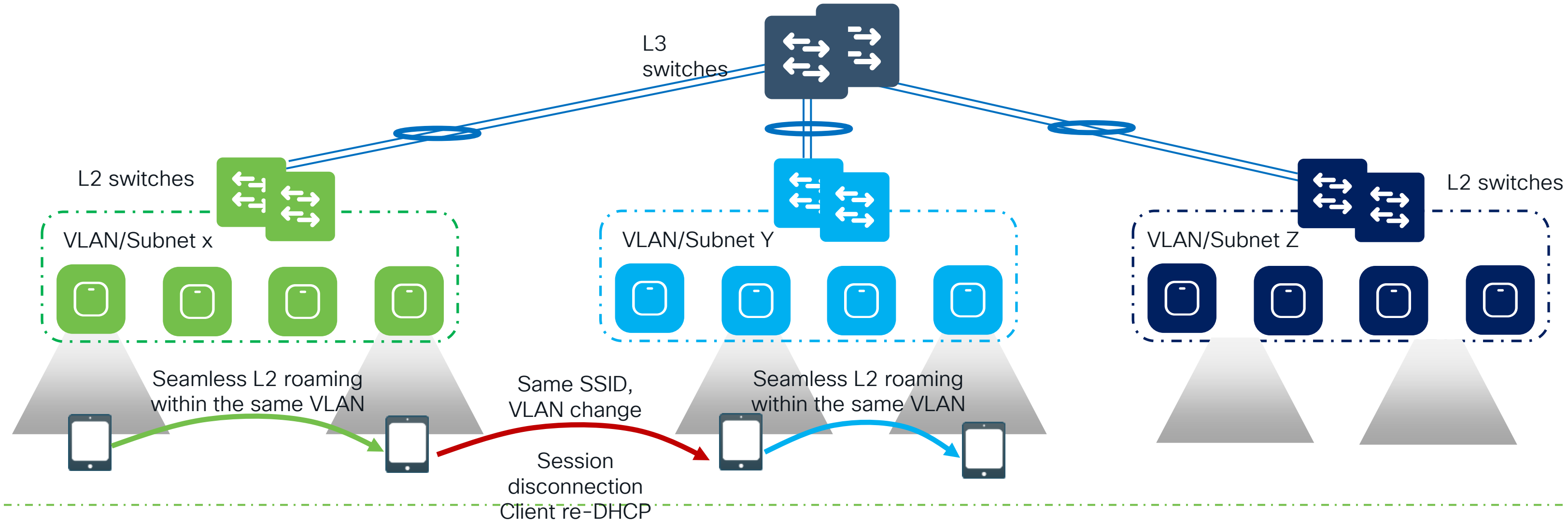


Seamless roaming = Keeping information consitent (IP & policy) as client roams between APs

Keeping **roaming secure** with a **delay of few 10s of ms.**

No need to re-auth with AAA at every roam
Requires some form of **key caching protocol** > 802.11r (or OKC).
Optimized roaming with support of 802.11k/v

How important is seamless roaming?

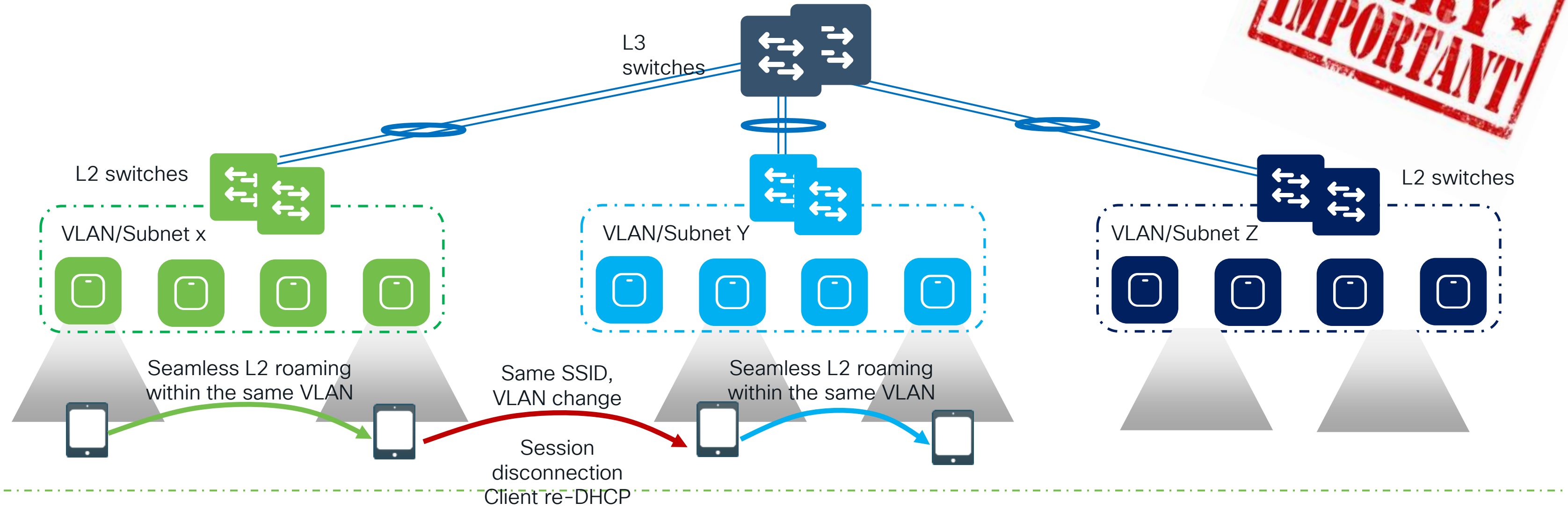

L3 switches
L2 switches
VLAN/Subnet x
VLAN/Subnet Y
L2 switches
VLAN/Subnet Z
Seamless L2 roaming within the same VLAN
Same SSID, VLAN change
Session disconnection Client re-DHCP
Seamless L2 roaming within the same VLAN

What if there is a VLAN change? session breaks. How bad it breaks, it depends on the client OS:

- Even with a full re-auth on roaming, some **client OS may consider same subnet and do not check DHCP**
- Windows does a DHCP inform and GW detection, but **no OS will go through the whole DHCP discovery** process
- Other client OSes will not do anything and DHCP will simply time out (**30 sec session break**)
- If roaming fails and client receives a de-auth, then the client will do a full DHCP discovery (still 4/5 sec)

How important is seamless roaming?

VERY IMPORTANT

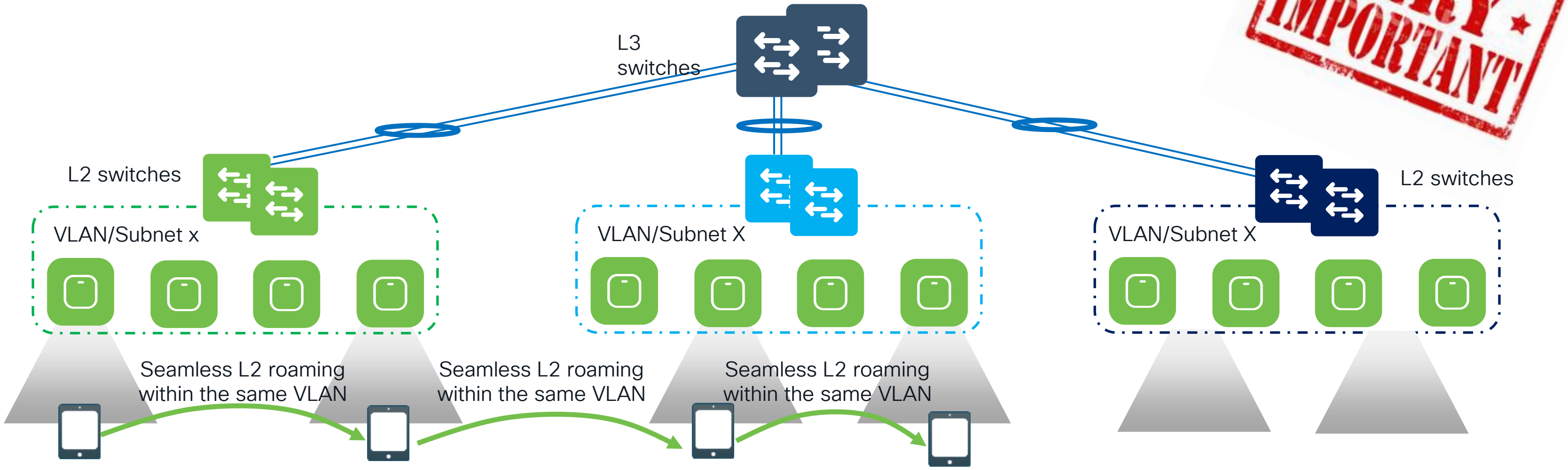


What else you should consider?

- Impact on the Applications: would they recover?
- VPN tunnel: would it need to be re-established
- Pressure on DHCP server in case of a mass roam
- etc.

How important is seamless roaming?

VERY IMPORTANT


L3 switches
L2 switches
VLAN/Subnet x
VLAN/Subnet X
VLAN/Subnet X
L2 switches
Seamless L2 roaming within the same VLAN
Seamless L2 roaming within the same VLAN
Seamless L2 roaming within the same VLAN

What else you should consider?

- Impact on the Applications: would they recover?
- VPN tunnel: would it need to be re-established
- Pressure on DHCP server in case of a mass roam
- etc.

What do you need for Seamless Roaming?
you need the same VLAN/L2 broadcast domain

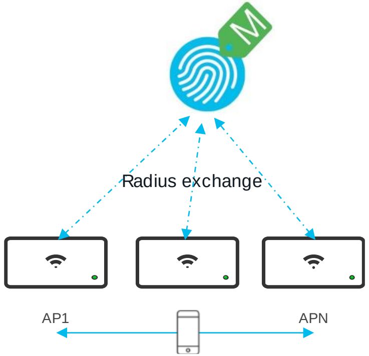
How important is fast secure roaming?

It depends…

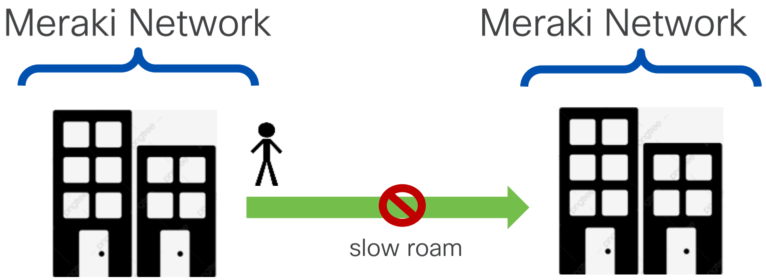
- **Really important for latency sensitive applications**: voice is very common, but also manufacturing applications, VR/AR, etc. Primary verticals: Healthcare, Manufacturing, Enterprise, etc.

- **Is Fast Roaming always important? No**. Some applications leverages buffers that provide consistent experience over periodic network interruptions or delays (Netflix). Others like FB and YouTube use QUIC that is pretty robust as well to interruptions or latency

- **Fast roaming also helps reducing the load and pressure on AAA** servers, as the full authentication exchange with AAA happens only once, the first time the client connects (only accounting might be sent during roaming) > impotant in high client scale deployments



Meraki Network: What you need to know?



Meraki Network = **Fast-roaming domain**
Crossing Meraki Network boundaries requires re-auth regardless of client VLAN

- Roaming in a Meraki Network:

	L2 roaming (same VLAN)	DL3R* (different VLANs)
Same SSID	• Client re-auth (slow roam) • Seamless (same IP)	• Client re-auth (slow roam) • Seamless (same IP)
802.11r (or OKC)	• Fast roaming • Seamless (same IP)	• Fast roaming (not supported) • Seamless (same IP)**

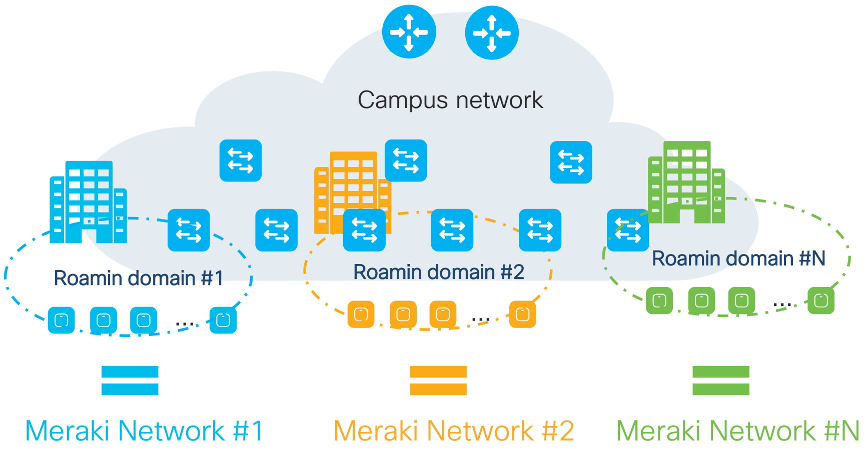
(*) DL3R = Distributed Layer 3 roaming
(**) DL3R + 802.11r not officially supported because not tested at scale

- Scale at Meraki Network
  - MAX Meraki devices (including MRs): 1k (soft limit)
  - MAX RF profiles: 50
  - Max 1500 MRs per RF profile
  - MAX SSIDs: 15
  - MAX clients: 50,000 (soft limit, dashboard performance)

Network Design

Network Design

How to deal with a “Distributed Data Plane” solution?



Design recommendations:

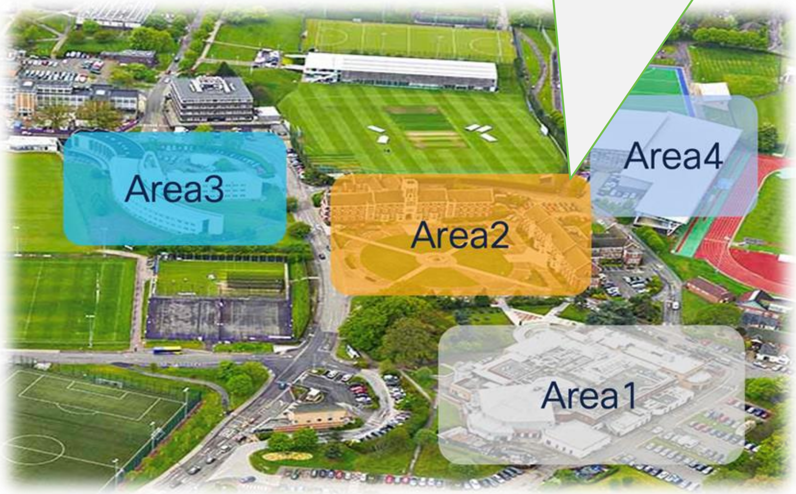
- Understand the customer requirements specifically around seamless and fast roaming
- Design around seamless roaming domains
- Map Meraki Networks to roaming domains
- Gather scale numbers (APs, clients, auth/s, etc.)
- Properly design and size VLANs and Layer 2 broadcast domains
- Apply wired & wireless configuration best practices

Understand the customer requirements

Design leveraging clear RF boundaries to minimizes client session breaks

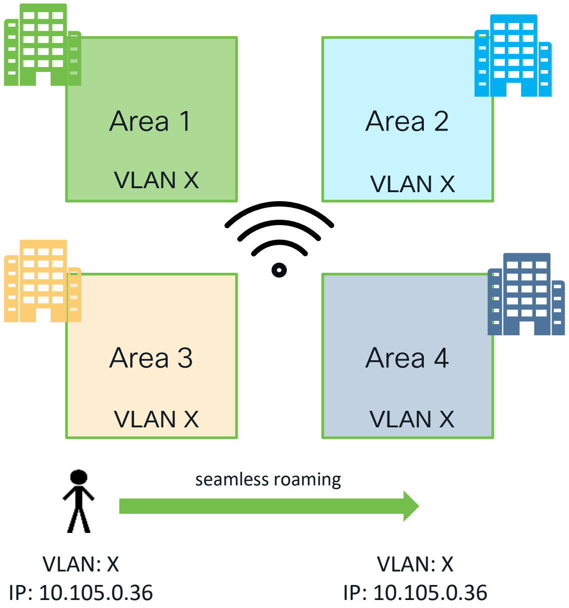
- Familiarize yourself with the Campus areas
- Identify seamless roaming domains: RF continuity, same SSID, same L2 broadcast domain (VLAN)
- Roaming domain can be a floor, a building, group floors the building, groups of buildings, etc.
- Examples:
  - Geographical areas: Look for sections of the campus that can be logically carved out. North, West, East, South Campus is named like that for a reason.
  - Outdoor Wireless: Try to group outdoor wireless areas within the buildings they're attached
  - Auditoriums/sport venues: Areas with large # of clients, best to create a dedicated network for them

Tip: Campus maps reflect operational workflows. Ask yourself how these are mapped to SSID & VLANs currently



Understand the customer requirements

Design leveraging clear RF boundaries to minimizes client session breaks



- **Requirements**: Continuous RF coverage & seamless roaming across areas > design to have the same VLAN, same subnet
- Consider RF leakage between floors > becomes a seamless roaming domain even if not physically moving between floors

Design considerations:

- Seamless roaming would mean spanning the same VLAN across multiple L2 switches, across multiple wiring closet and possibly across multiple building
- 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 number of clients, the DHCP scope design, etc.
- Need to apply the access network design best practices and recommendations

Bottom line: seamless roaming domain = L2 broadcast domain;
How big can you make a seamless roaming domain? It depends ☺

Seamless roaming domain: How big is too big?

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**

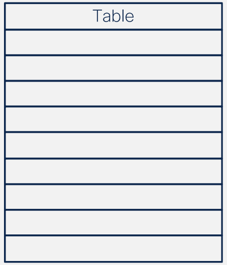
(IPv4 Unicast, IPv6 Link Local, IPv6 Unique Local, IPv6 Global Unicast)

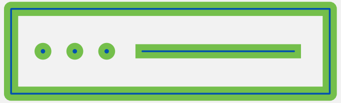
Windows 11: up to 16 IPv6 IP addresses (!!)

Seamless roaming domain: How big is too big?

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**

Seamless roaming domain: How big is too big?

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

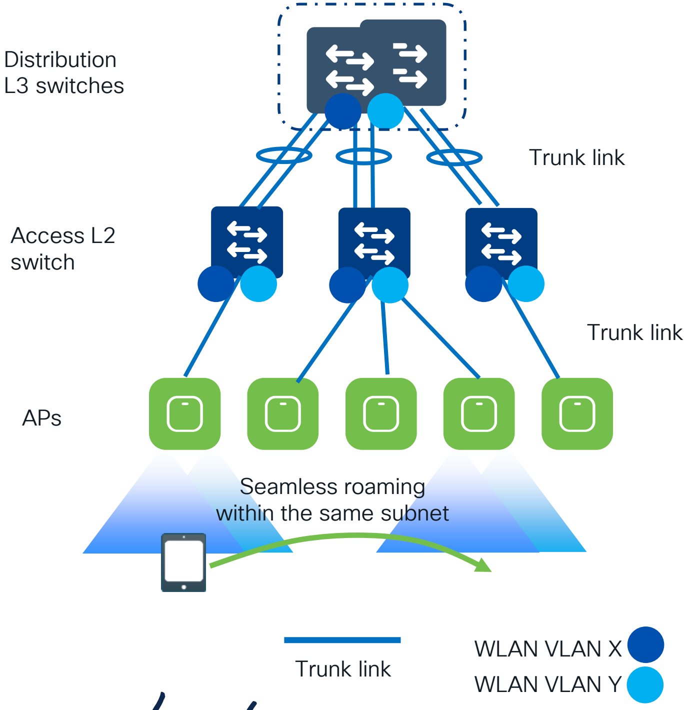
Layer 3 switch = Catalyst 9300 (or MS equivalent)

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**

Access Network Design

Switching network considerations

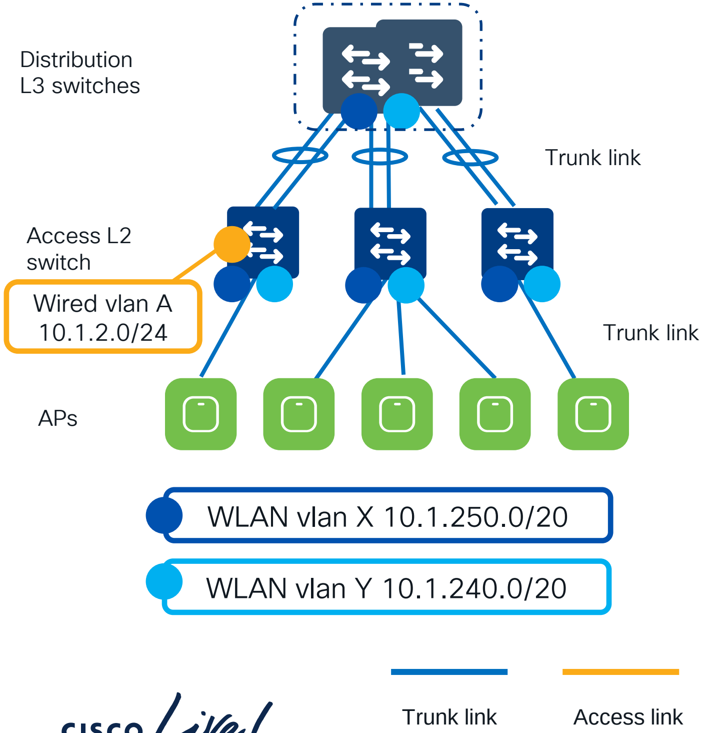


Single logical switch at Distribution Layer:

- Configure StackWise Virtual or Virtual Stacking at the distribution layer switches to have redundancy but no deliberate L2 loops
- Uplinks must be configured as trunks and EtherChannel
- Only the required VLANs should be allowed on trunks to distribution layer switches

Access Network Design

Switching network considerations

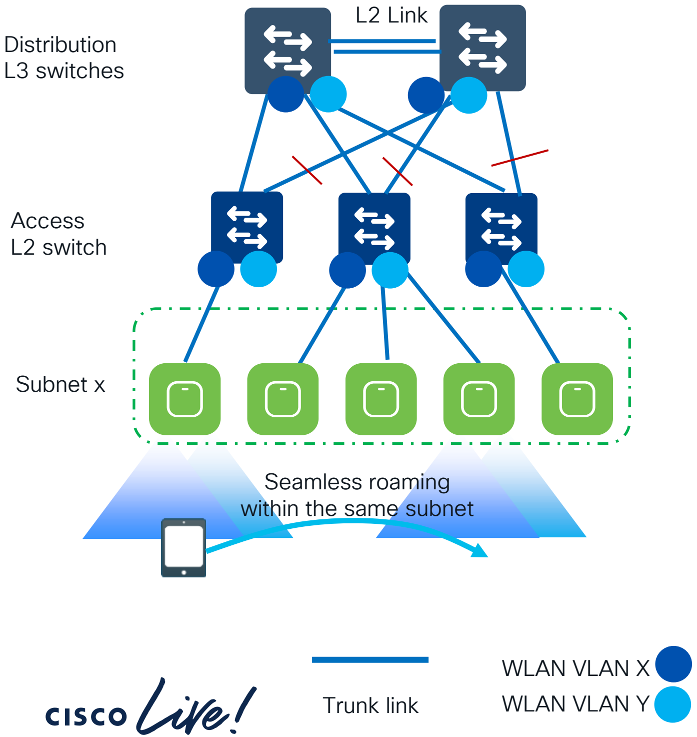


Single logical switch at Distribution Layer:

- Configure StackWise Virtual or Virtual Stacking at the distribution layer switches to have redundancy but no deliberate L2 loops
- Uplinks must be configured as trunks and EtherChannel
- Only the required VLANs should be allowed on trunks to distribution layer switches
- VLANs associated with wired clients should be confined to a single switch. VLANs for wireless clients should span across the access switches in the roaming domain

Access Network Design

Switching network considerations

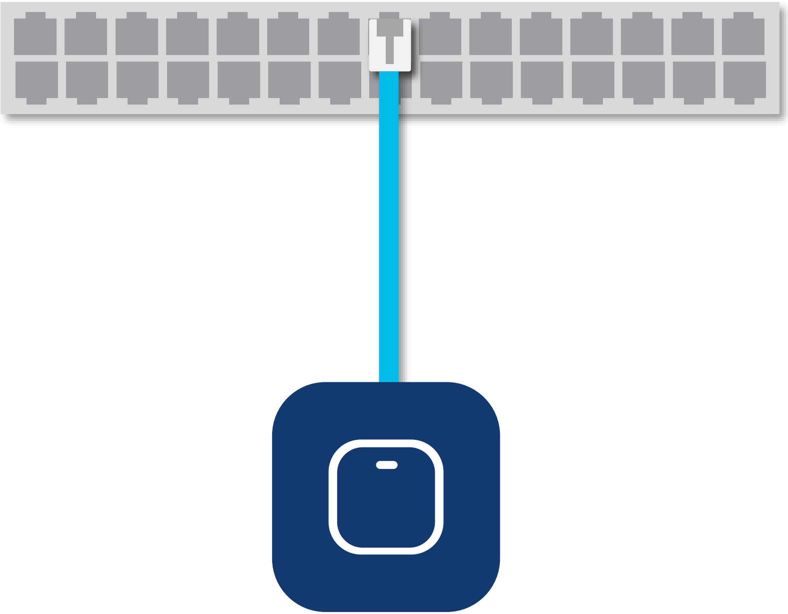


Individual switches at Distribution Layer:

- Configure HSRP to provide first-hop redundancy
- STP Root and HSRP primary should be configured to be on the same switch
- Uplinks will be configured as trunks and EtherChannel. RootGuard on downlinks and LoopGuard on uplinks
- Only the required VLANs should be allowed on trunks to distribution layer.
- VLANs associated with wired clients should be confined to a single switch. VLANs for wireless clients should span across the access switches in the roaming domain

Access Network Design

Switchport settings



Enable LLDP for correct PoE Power Negotiation (AP name is shown as well)

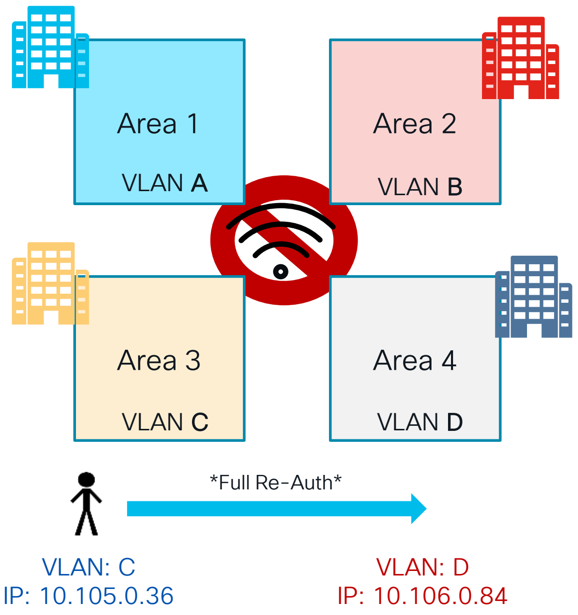
mGIG and 802.3at (PoE+) recommended

Configure 802.1q, STP Portfast Trunk BPDU guard and Root Guard

Configure to trust DSCP from APs (“mls qos trust dscp” on catalyst switch)

Understand the customer requirements

Design leveraging clear RF boundaries to minimizes client session breaks



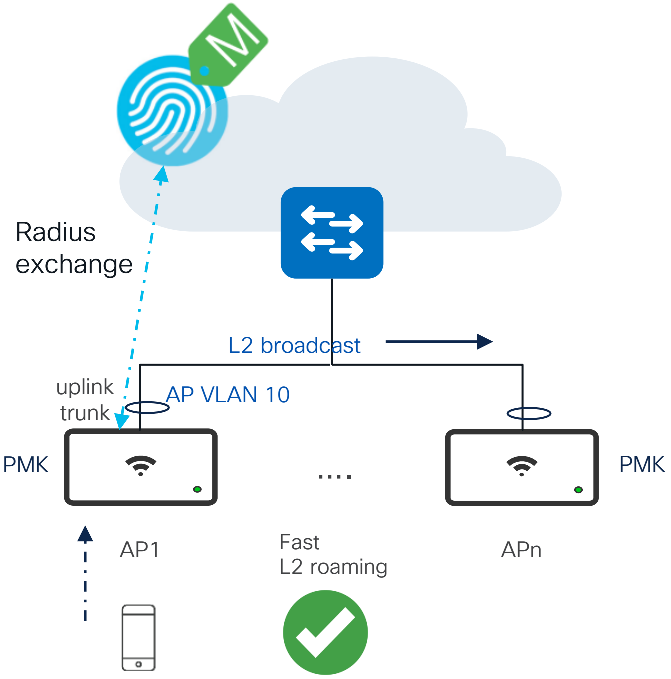
Requirement: No RF coverage between areas. Crossing RF coverage boundaries requires a full client re-auth and client's IP address change…and that's OK!

Design considerations:

- Use a different VLAN/broadcast domain for each area (i.e., area is group of buildings, separated by a street from other areas)
- Reducing the broadcast domain is a very good design idea
- Lower impact of traffic like broadcast, unknown unicast and multicast (BUM)
- Reduced fault and security domain (TCAM/ARP attacks, broadcast storms, etc.)
- Simplified management: use VLAN to easily locate clients

MRs: What happens behind the scenes...

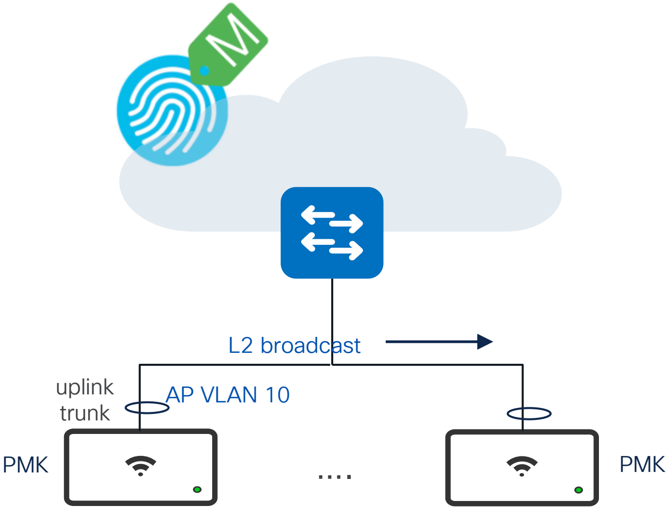
What information is shared between MRs?



Broadcast sent on AP VLAN:

- Fast Roaming (PMK tracker): Pair Master Key (PMK) info is shared across all MRs in the same VLAN for L2 roaming. Other info shared to allow seamless roaming:
  - Client Session Timeout, Group Policy name
  - Starting R30: VLAN ID is shared
  - Starting R31: both VLAN name and VLAN ID info is shared
    - This means that AAA VLAN override + fast roaming is supported starting these releases. This applies to both OKC and 802.11r
  - Starting R31: client SGT information is supported

What information is shared between MRs?

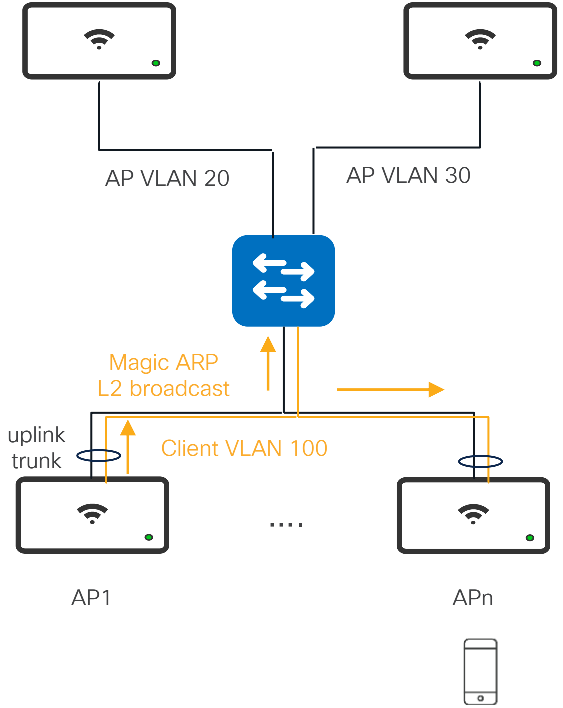


MRs need to be on the same Management VLAN

Broadcast sent on AP VLAN:

- Fast Roaming (PMK tracker): Pair Master Key (PMK) info is shared across all MRs in the same VLAN for L2 roaming. Other info shared to allow seamless roaming:
  - Client Session Timeout, Group Policy name
  - Starting R30: VLAN ID is shared
  - Starting R31: both VLAN name and VLAN ID info is shared
    - This means that AAA VLAN override + fast roaming is supported starting these releases. This applies to both OKC and 802.11r
  - Starting R31: client SGT information is supported
- Client Balancing: State of the wireless network (AP load and client signal info) for better load balancing. Not recommended for large deployments

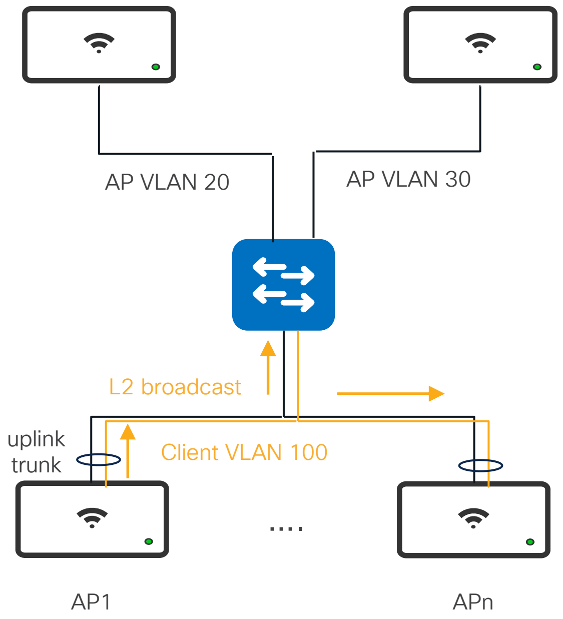
What information is shared between MRs?



Broadcast sent on Client VLANs

- Magic ARPs: a flavor of gratuitous ARP used to clear the state on client roams and update the wired infra.
- Upon roaming, AP1 (roam-to AP) crafts an ARP frame spoofing the client's MAC with a source IP of 0.0.0.0 and target IP 6.x.x.x address. Switch receives it and MAC table is updated
- APn (roam-from AP) upon receiving this packet cleans up the client state
- What if magic ARP is lost? APn will not know that client roamed to another AP and will respond to ARP queries on behalf of the client. Possible MAC flapping seen on the switch
- What could caused Magic ARP to be dropped? Device tracking policy on the switch that checks client MAC and IP and enforces the binding - part of Cisco Switch Integrated Security Feature (SISF) features

What information is shared between MRs?



Other Broadcast sent on Client VLANs

- Broadcast domain mapping: Layer 2 broadcast probes over the uplink to discover broadcast boundaries on each client VLAN <> each AP gathers subnet/VLAN ID mapping. This is needed ONLY is using DL3R*
- Mesh Discovery: For automatic wired mesh discovery and to prevent mesh routing loops
- Client broadcast/multicast: any legit client broadcast/multicast traffic, unless not filtered.
- Note: MRs have inbuilt mechanism to suppress or reduce the impact of client broadcast and multicast (like ARP proxy, rate limiting, multicast to unicast conversion, etc. more info here: https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/Broadcast_Suppression_and_Control_Technologies_for_MR_Access_Points

**DL3R = Distributed L3 Roaming*

What information is shared between MRs?

- MR leverages different types of broadcast on the LAN.
- It’s useful to know this info for troubleshooting:

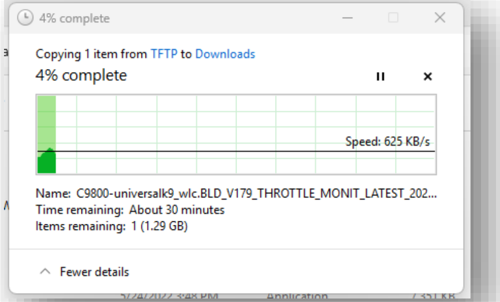
Feature	UDP port
PMK tracker	23541
client load balancing	61111
Dstore (DL3R)	9538
Latency tracker	61112
Opportunistic PCap	30001, 30002

DL3R = Distributed L3 Roaming

What information is NOT shared between MRs?

Client AVC policy info

- The AVC policy (DSCP marking, traffic rate limiting, etc.) exists both on the roam-from and on roamed-to AP. But the client flow state itself is not transferred upon roaming (as of today)
  - The result is that the flow might get the policy applied on the AP it initially associate, but then the policy is no longer applied after roaming:



4% complete

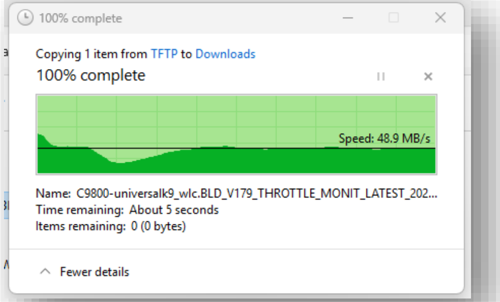
Copying 1 item from TFTP to Downloads

4% complete

Name: C9800-universalk9_wlc.BLD_V179_THROTTLE_MONIT_LATEST_202...
Time remaining: About 30 minutes
Items remaining: 1 (1.29 GB)

Roam-from AP: policy (rate limit) is applied

client roams



100% complete

Copying 1 item from TFTP to Downloads

100% complete

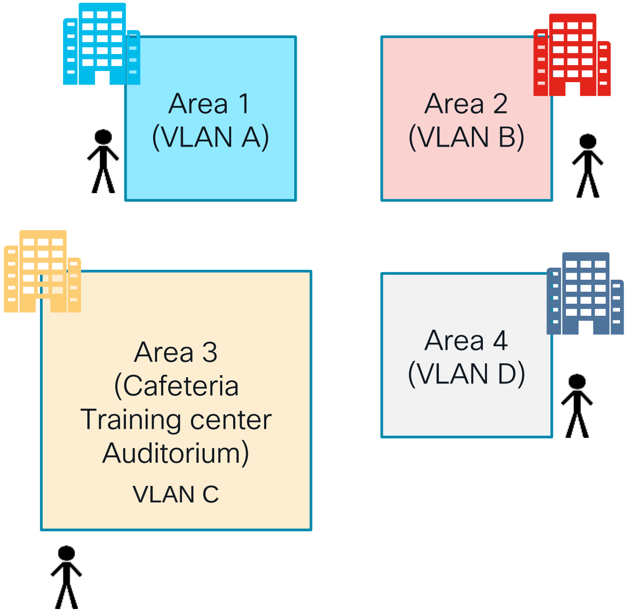
Name: C9800-universalk9_wlc.BLD_V179_THROTTLE_MONIT_LATEST_202...
Time remaining: About 5 seconds
Items remaining: 0 (0 bytes)

Roam-to AP: policy is no longer applied

- Is it a problem? it depends...For this to happen the application cannot be recognized (e.g., encrypted), so that the roam-to AP cannot classify it and apply the policy. Also, most browser pages and applications are made of multiple sessions so any new flow started on the roam-to AP will be correctly classified

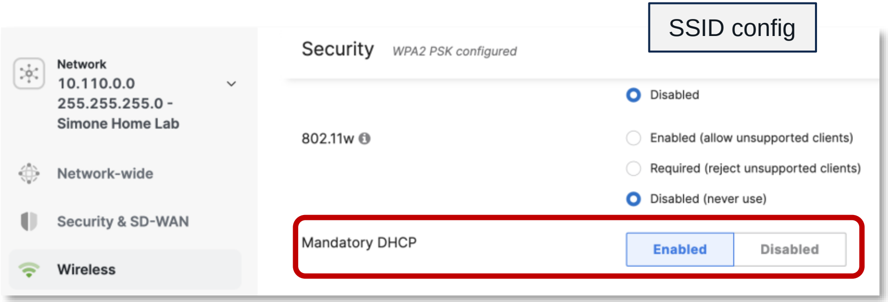
Design Best Practices

DHCP Scope and Lease design considerations



- Size your DHCP scope considering all the possible devices that could join that area to prevent DHCP scope starvation: stationary but also roaming devices from other areas
- 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



SSID config

Security *WPA2 PSK configured*

802.11w
- ● Disabled
- ○ Enabled (allow unsupported clients)
- ○ Required (reject unsupported clients)
- ● Disabled (never use)

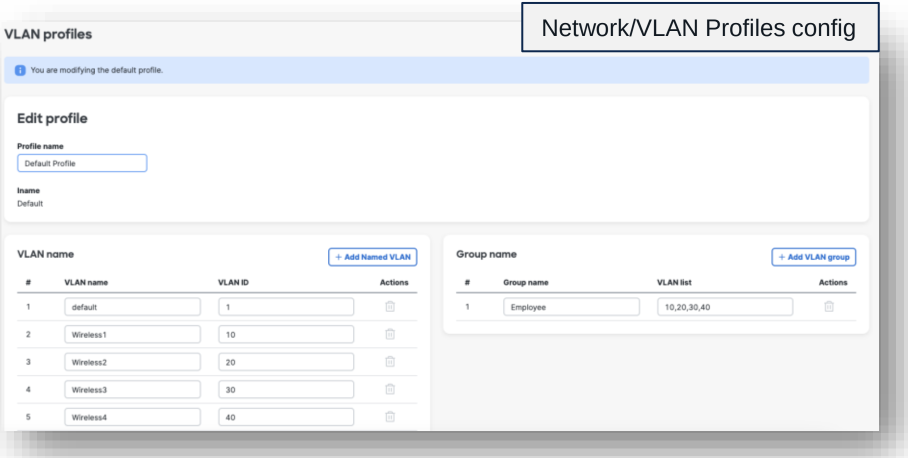
Mandatory DHCP: [✓ Enabled] Disabled

- 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: Mandatory DHCP breaks IPv6 today. Fix is already in place, will be available in r31.2 (May)

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

Subnet/VLAN Design considerations



Network/VLAN Profiles config

VLAN profiles

You are modifying the default profile.

Edit profile

Profile name: Default Profile

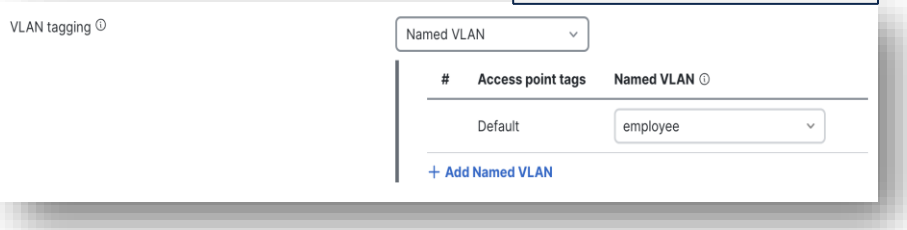
Iname: Default

VLAN name — + Add Named VLAN

#	VLAN name	VLAN ID	Actions
1	default	1	🗑
2	Wireless1	10	🗑
3	Wireless2	20	🗑
4	Wireless3	30	🗑
5	Wireless4	40	🗑

Group name — + Add VLAN group

#	Group name	VLAN list	Actions
1	Employee	10,20,30,40	🗑



Wireless/Access Control/SSID

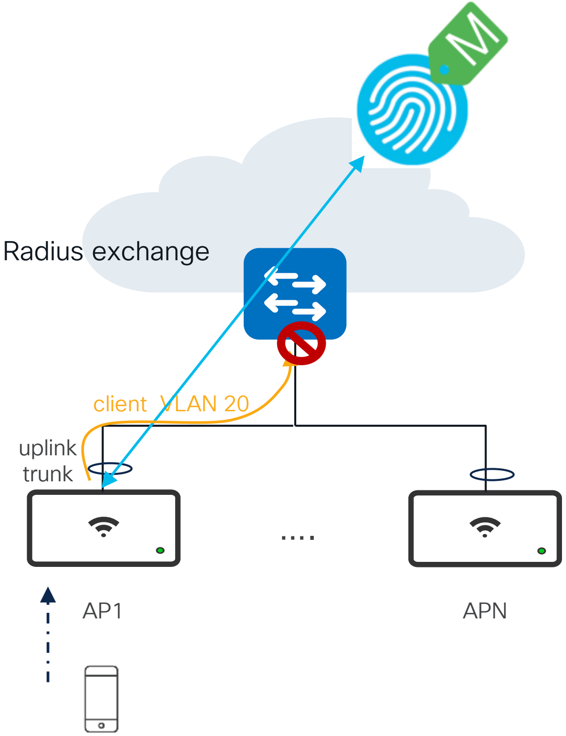
VLAN tagging ⓘ: Named VLAN

#	Access point tags	Named VLAN ⓘ
	Default	employee

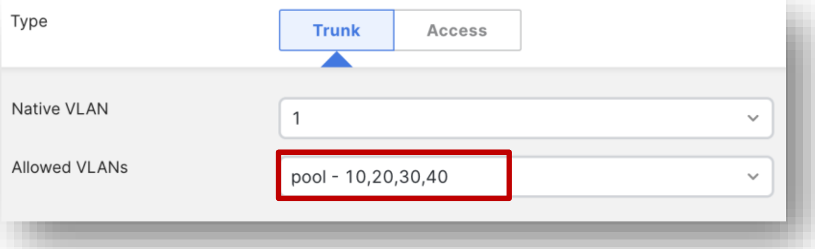
+ Add Named VLAN

- **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 documentation 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 ☺

AAA VLAN override - Recommendation



- Client associates and authenticates to the network via 802.1x or MAB
- AAA returns the client VLAN
- MR bridges the client traffic on uplink trunk connection to the switch and tags the VLAN
- There is no check on the MR if that VLAN is "allowed". It's up to the switch to decide if that vlan is valid or not.
- Recommendation: Configure the allowed VLANs on the switch side. An example from Dashboard and MS switch:

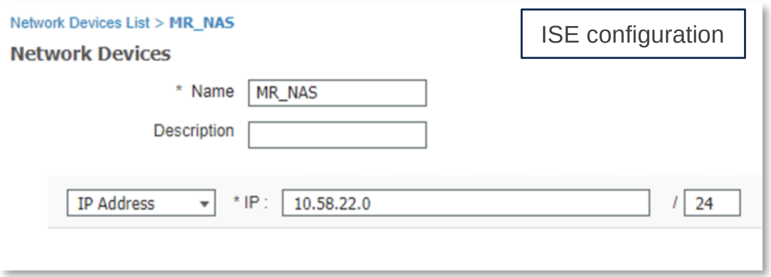


Type: Trunk | Access

Native VLAN: 1

Allowed VLANs: pool - 10,20,30,40

Security design considerations



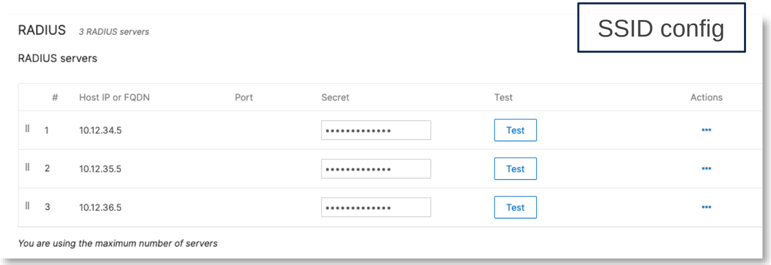
ISE configuration

Network Devices List > MR_NAS

Network Devices

* Name	MR_NAS
Description	
IP Address ▾	* IP : 10.58.22.0 / 24

- Each MR talks to AAA server for 802.1x authentication and must be configured as Network Access Server (NAS); to avoid entering each MR'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

RADIUS *3 RADIUS servers*

RADIUS servers

#	Host IP or FQDN	Port	Secret	Test	Actions
1	10.12.34.5		•••••••••••••	Test	•••
2	10.12.35.5		•••••••••••••	Test	•••
3	10.12.36.5		•••••••••••••	Test	•••

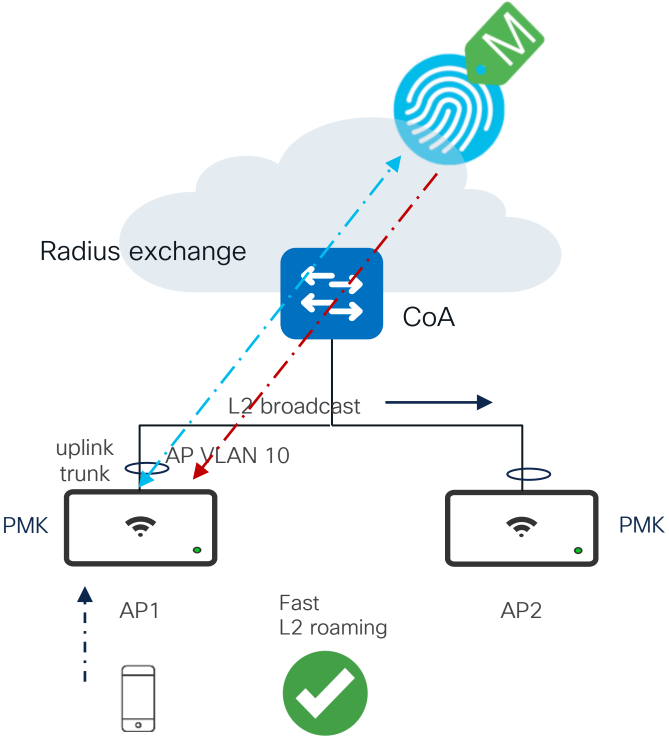
You are using the maximum number of servers

- 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.

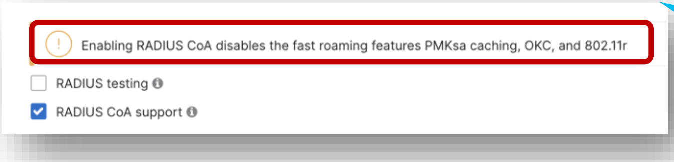
Session timeout

- 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

Security design considerations



- 802.11r/OKC + CoA is NOT supported today
- Dashboard will tell you:



! Enabling RADIUS CoA disables the fast roaming features PMKsa caching, OKC, and 802.11r

□ RADIUS testing

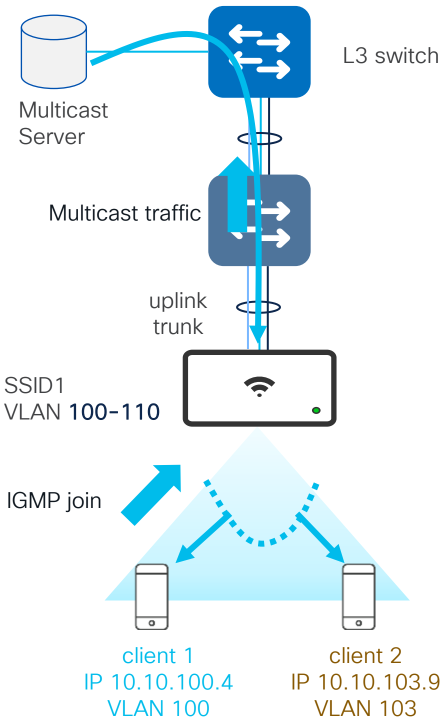
☑ RADIUS CoA support

Fixed in r32.1

Why?

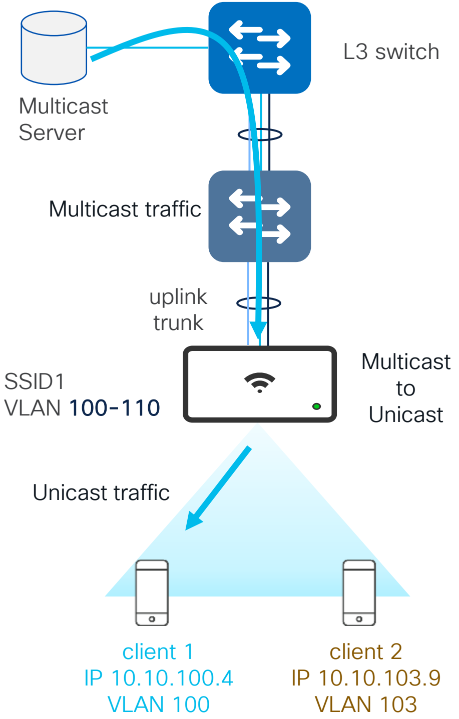
- Client authenticates to an SSID with 802.11r/OKC
- The Network Access Server (NAS) is the first MR that client authenticates with (AP1 in this case)
- The client roams with 802.11r; NAS is not updated
- After the client roamed, AAA issues a CoA: the CoA is delivered to the original AP1, but the client is gone

Multicast + AAA VLAN override



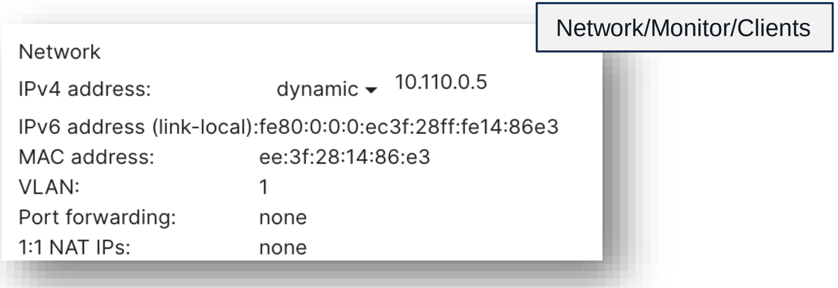
- What (Requirement): Single SSID mapped to multiple client VLANs via AAA policy. IP Multicast separation is required across client VLANs
- Problem: Clients belong to the same SSID. Client 1 requests IP multicast, IGMP query goes on VLAN 100, multicast traffic is received in VLAN 100; in the air, since #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, MRs “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

IPv6 support



Network/Monitor/Clients

Network

IPv4 address: dynamic ▾ 10.110.0.5

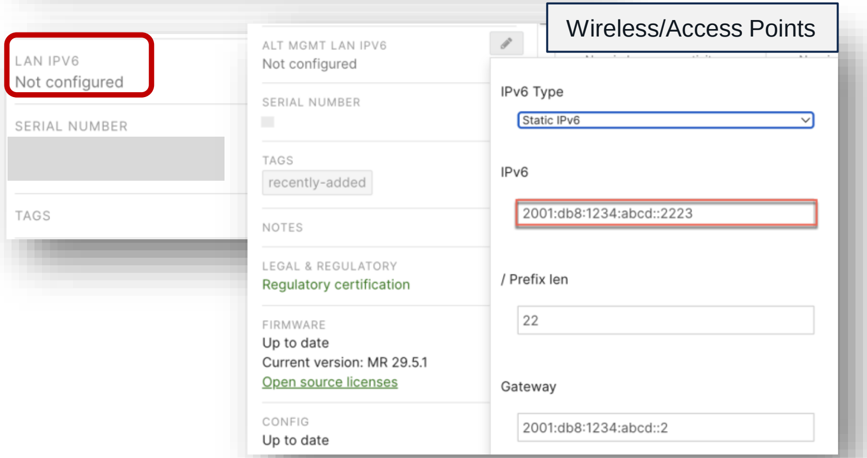
IPv6 address (link-local):fe80:0:0:0:ec3f:28ff:fe14:86e3

MAC address: ee:3f:28:14:86:e3

VLAN: 1

Port forwarding: none

1:1 NAT IPs: none



Wireless/Access Points

LAN IPV6
Not configured

SERIAL NUMBER

TAGS

ALT MGMT LAN IPV6
Not configured

SERIAL NUMBER

TAGS
recently-added

NOTES

LEGAL & REGULATORY
Regulatory certification

FIRMWARE
Up to date
Current version: MR 29.5.1
Open source licenses

CONFIG
Up to date

IPv6 Type: Static IPv6

IPv6: 2001:db8:1234:abcd::2223

/ Prefix len: 22

Gateway: 2001:db8:1234:abcd::2

Clients:

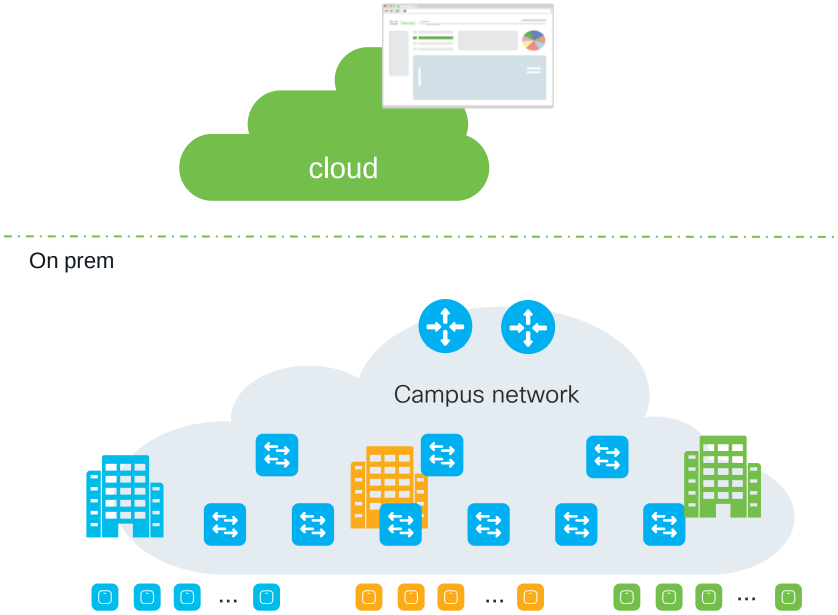
- **Additional IPv6 support in R30**: Support for 802.11r/OKC over IPV6 infra (dual-stack was already supported), client IPv6 DL3R over IPv4 infra and WPN fragmentation.

Access Points:

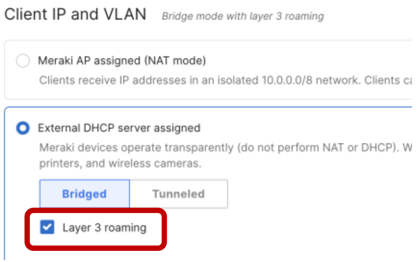
- **Infrastructure IPv6**: MR supports Static and SLAAC (no DHCPv6)
- **Alternate Management Interface** supports for IPv6 in R30

Large scale deployments… a summary

Large scale deployments – Not recommended



- L3 distributed Roaming (L3DR)



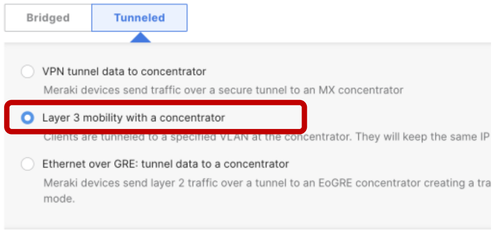
Client IP and VLAN *Bridge mode with layer 3 roaming*

○ Meraki AP assigned (NAT mode)
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients ca

● External DHCP server assigned
Meraki devices operate transparently (do not perform NAT or DHCP). W
printers, and wireless cameras.

☑ Layer 3 roaming

- L3 mobility MX as concentrator



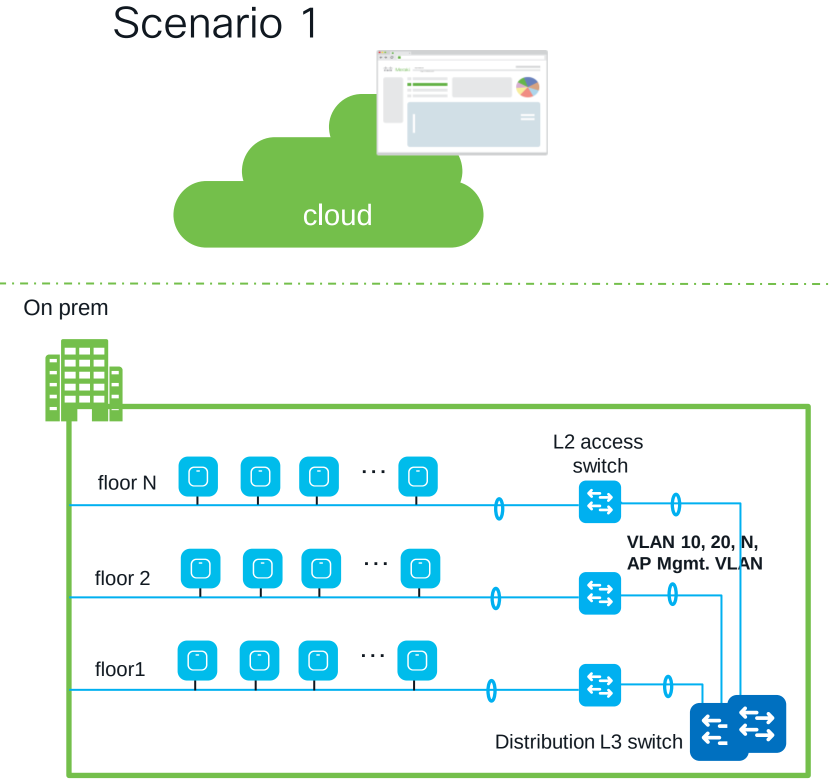
○ VPN tunnel data to concentrator
Meraki devices send traffic over a secure tunnel to an MX concentrator

● Layer 3 mobility with a concentrator
Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP

○ Ethernet over GRE: tunnel data to a concentrator
Meraki devices send layer 2 traffic over a tunnel to an EoGRE concentrator creating a tra
mode.

Both these solutions are not recommended for a large campus deployments

Large scale wireless deployment



L2 roaming Deployment:

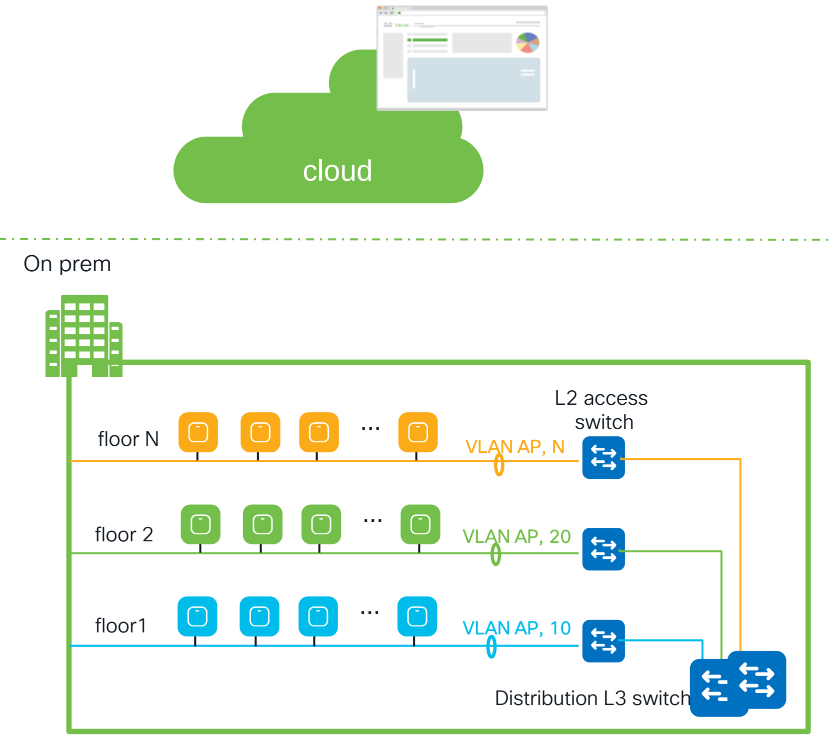
- Roaming domain = building = Meraki Network
- AP per roaming domain < 200/300
- VLAN design = VLANs span the whole building

Design Recommendations:

- 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
- Meraki supports this design today

Large scale wireless deployment

Scenario 2



L3 roaming across floors Deployment:

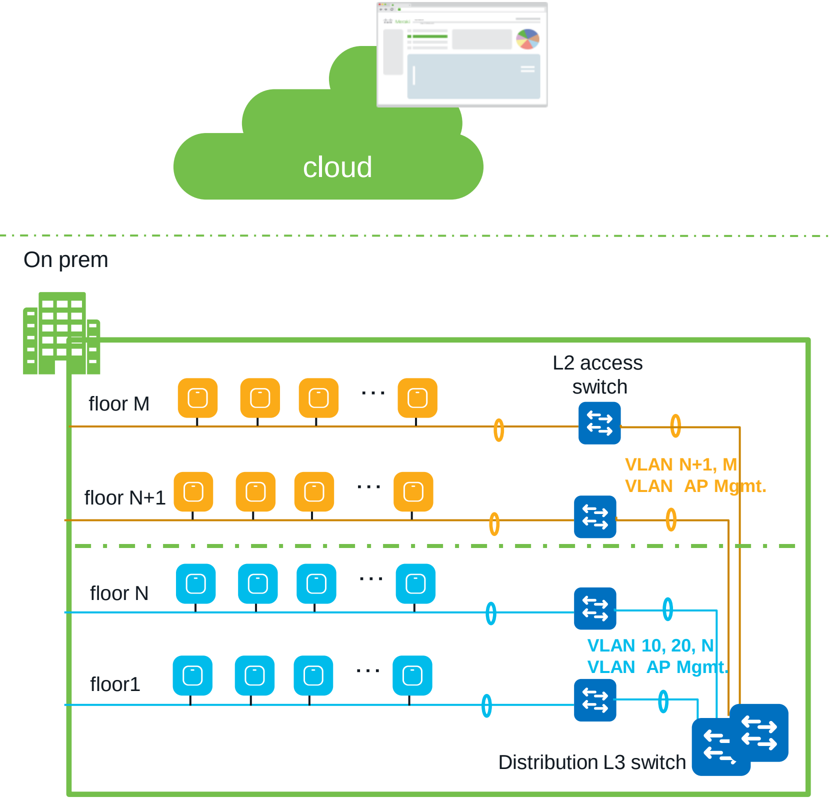
- Roaming domain = building = Meraki Network
- AP per roaming domain < 200/300
- VLAN design = VLANs span only single floor/wiring closet

Design Recommendations:

- L2 broadcast boundary at the building distribution switch
- Different client and AP VLANs at each floor
- AP switchports configured as trunks (one AP management VLAN and client VLANs for each floor
- Choose subnet mask to accommodate the expected # of devices per VLAN per floor (VLAN pooling in R30)
- Use Stack/VSL technology at L3 switch to reduce impact of spanning tree loops
- Consider distributed L3 roaming (DL3R) to cover seamless roaming between floors (possible for RF leakage across floors)
- Supported with caveats (802.11r is not supported with DL3R)

Large scale wireless deployment

Scenario 3



Mixed L2/L3 roaming Deployment:

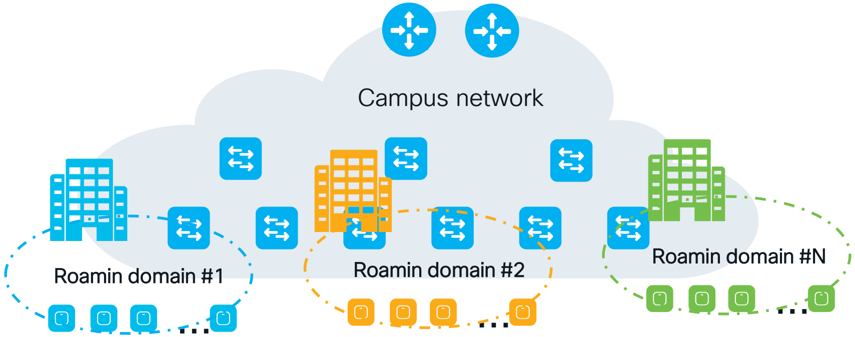
- Roaming domain = Tall building = Meraki Network
- AP per roaming domain > 200
- VLAN design = VLANs span a group of floors/area

Design Recommendations:

- L2 broadcast boundary at the building distribution switch
- Different client and AP VLANs for group of floors
- AP switchports configured as trunks (one AP management VLAN and different client VLANs for each area)
- Choose subnet mask to accommodate the expected # of devices per VLAN, per area (VLAN pooling in R30)
- Use Stack/VSL technology at L3 switch to reduce impact of spanning tree
- Configure L2 roaming within each area and consider distributed L3 roaming (DL3R) to cover roaming between areas
- Supported with caveats (802.11r is not tested at scale with DL3R)

Conclusion

Cisco Meraki Wireless: Ready for Enterprise



1000s of APs and clients

Meraki is ready for Enterprise

- You can have a large wireless deployments with 1000s of Access Points and 10k clients with Meraki today
- You can support seamless and fast roaming
- This may apply to University campuses, large Enterprise deployments, etc.

How to make it work?

- Gather and understand the customer requirements
- Familiarize yourself with the customer deployment to understand if and where seamless/fast roaming is needed
- Design around seamless roaming domains
- Properly design and size VLANs and broadcast domains
- Follow L2 wired access design and security best practices
- And, of course...apply best practices!

Cisco Wireless = Architecture flexibility

IT operations / Architecture	On-prem Managed	Cloud Management
Centralized	✓	Campus Gateway
Distributed	✓	✓

Webex App

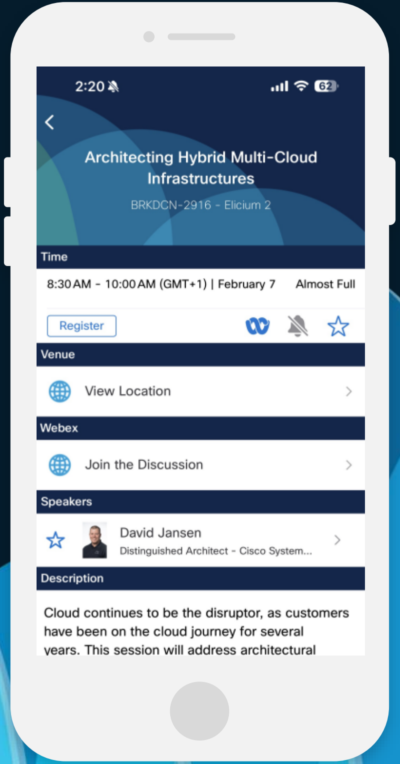
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.



2:20

Architecting Hybrid Multi-Cloud Infrastructures

BRKDCN-2916 - Elicium 2

Time

8:30 AM - 10:00 AM (GMT+1) | February 7 Almost Full

Register

Venue

View Location

Webex

Join the Discussion

Speakers

David Jansen
Distinguished Architect - Cisco System...

Description

Cloud continues to be the disruptor, as customers have been on the cloud journey for several years. This session will address architectural

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

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 ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: siarena@cisco.com

Thank you

cisco Live!

GO BEYOND