
cisco Live!
Let's go

The bridge to possible

Cisco Meraki Wireless: Ready for Enterprise

Subtitle goes here

Simone Arena, Distinguished TME, Cisco Wireless

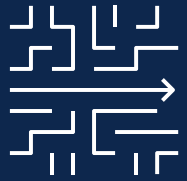
cisco Live!

BRKEWN-2035

Enterprise Network

A Wireless-Centric View

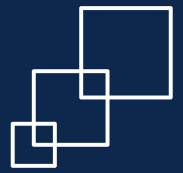
Mobility, Performance, anything @scale



IT Operation Simplicity, Flexibility

High Availability

Assurance, Analytics



Integration with 3rd party systems

End to End Security

Cisco Wireless Management Strategy

On-prem

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 **all customers**

Agenda

- Cloud Management
- Meraki Enterprise class features
- Network Architecture & Design
- Best practices
- Conclusions

Cloud Management

Reduce Enterprise IT Operations Complexity

Radically faster deployment, management and troubleshooting

Configuration and monitoring from a **single pane of glass**

Automation with APIs to dramatically improve outcomes and experiences

Assurance and **Analytics** simplifies network operations and troubleshooting

Meraki Cloud: Unmatched Scale and Reliability

Unmatched scale to support any network

- 4.7M+ Customer Networks
- 15M+ Meraki Devices online
- 192+ Countries

Largest data lake to power AI/ML intelligent solutions

- ~10M Active APs
- 225K+ 6E APs deployed
- 850K+ Roam events from Intel Analytics in 1 day

Programmability at scale for large Enterprise

- 350M+ Daily end-user devices
- 3.4M+ Active API users
- 10B+ External API monthly calls

Born in the cloud, growing daily, and trusted everywhere

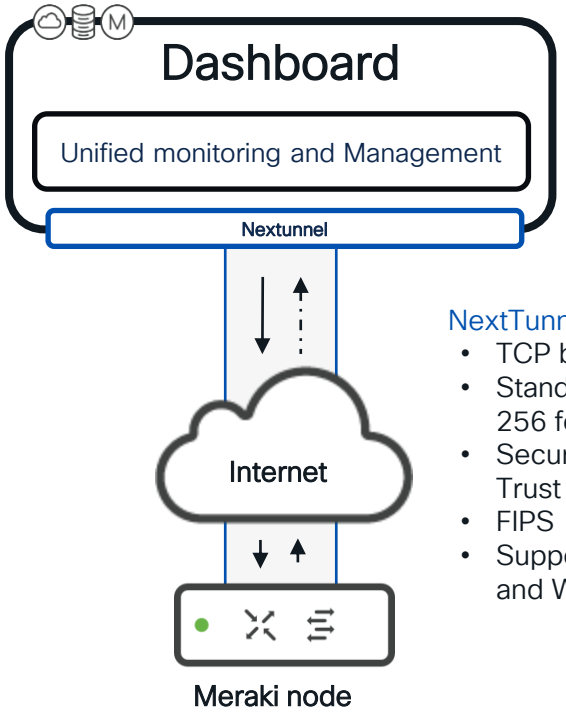
Secure and Highly Available Cloud

Secure
24×7 automated intrusion detection
& third-party independent validation

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

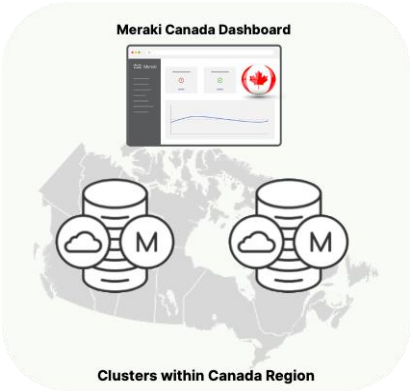


NextTunnel:
- TCP based, port 443
- Standard protocol: TLS 1.2 with AES 256 for encryption
- Secured: Identity based on Cisco Trust Anchor module (TAm)
- FIPS 140-2 compliant
- Support via HTTP proxy with R30 and Wi-Fi 6 MRs and higher

More info: https://meraki.cisco.com/trust/

Meraki Dashboard available Globally

- Cisco owned DCs in Americas/EMEA/APJC
- Also running some footprint in AWS Cloud
- GDPR complaint



- Geo Cloud to help customers address data residency needs
- Clusters reside in public clouds for the region
- Available in China and Canada (AWS) and growing

LARGE ENTERPRISES

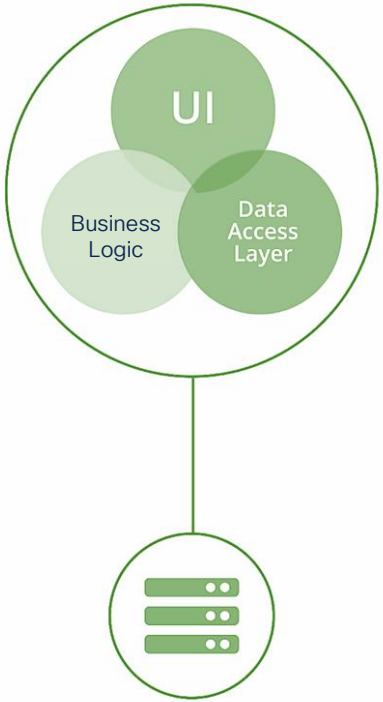
Security & Compliance

- Direct Connect for dedicated access to Meraki dashboard
- Meraki Dashboard traffic transported over dedicated circuits, not public internet links
- Control over performance and additional security
- *Under consideration*

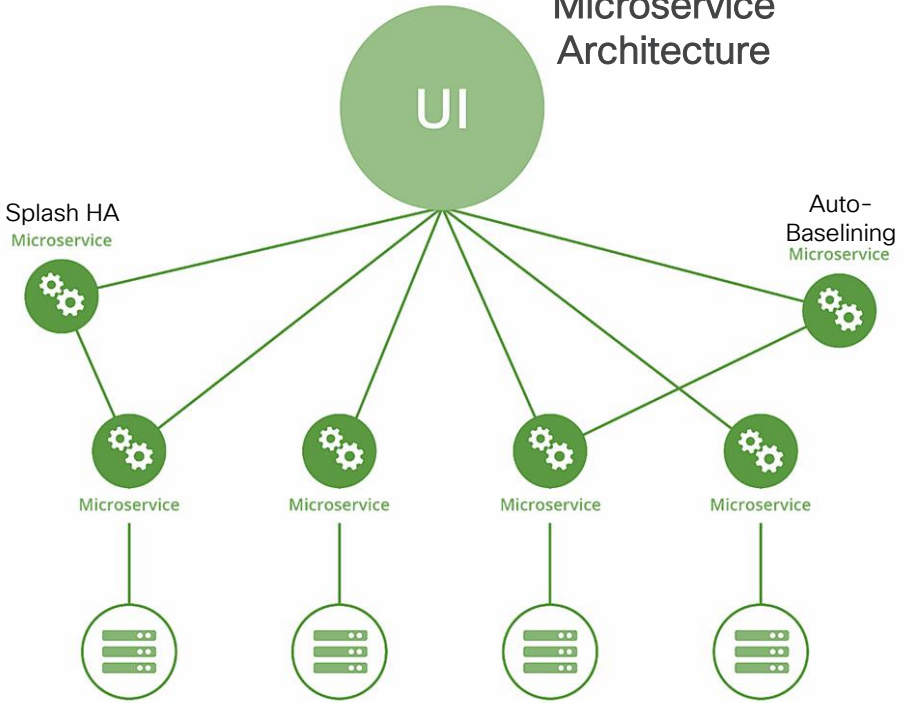
Cloud Architecture

Highly distributed to support global customers

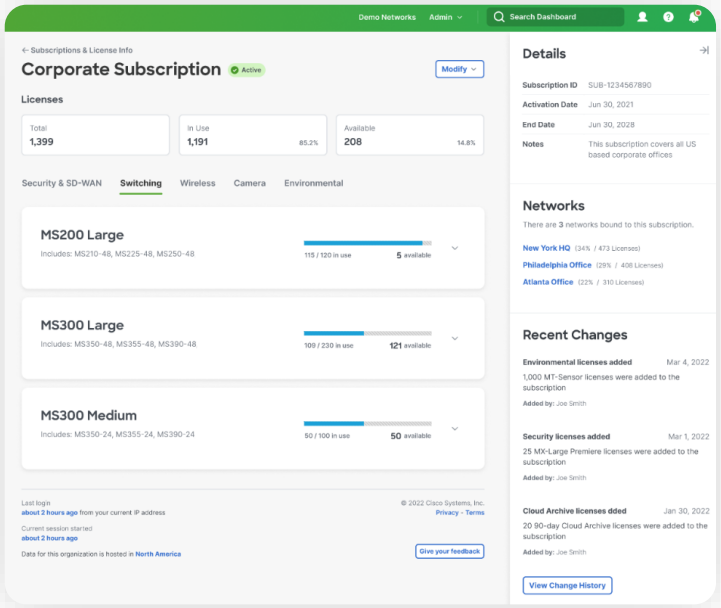
Shard Architecture



Microservice Architecture



Meraki Subscription Licensing



- Super flexible: Flexible term, Flexible start date, different license tiering, per network (not org)
- Important: Subscription enforcement will restrict the management of devices, the network still functions

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

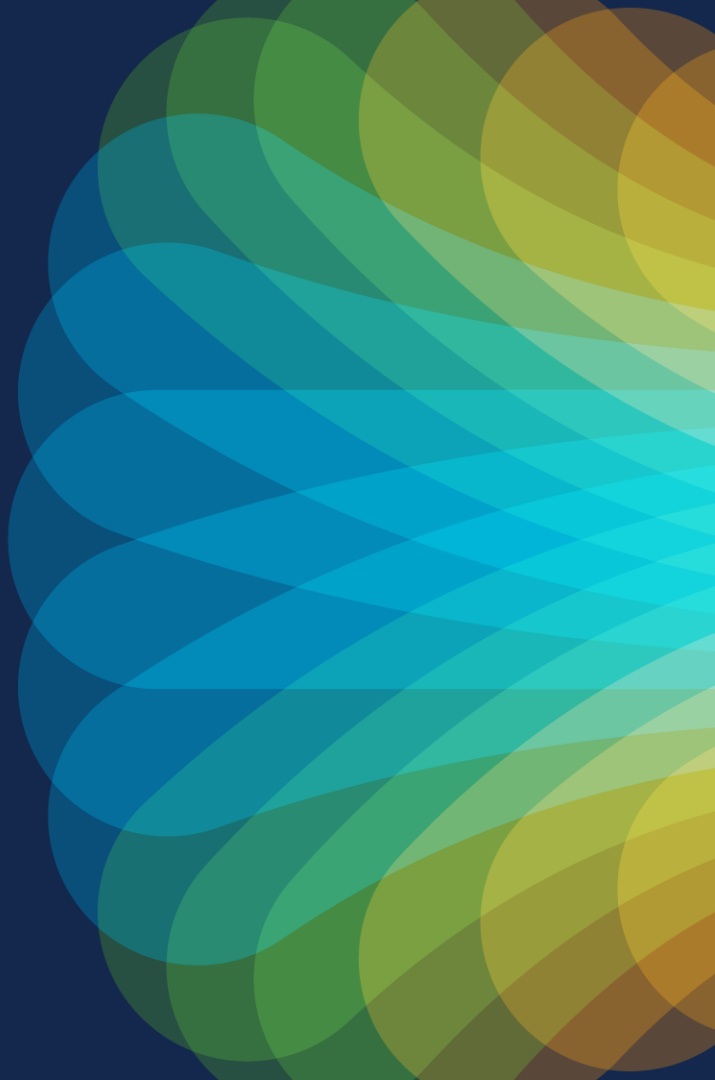
The following is a description of the expected behavior for the devices on networks that experience a disable management event.

- 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

Cloud Management: Easy and Flexible Configuration



Simple Onboarding and Access

- Order can have a single or multiple device/license
- Power up devices and they pull config from dashboard
- Plug and Play eases deployment considerably

RBAC included with Meraki Dashboard

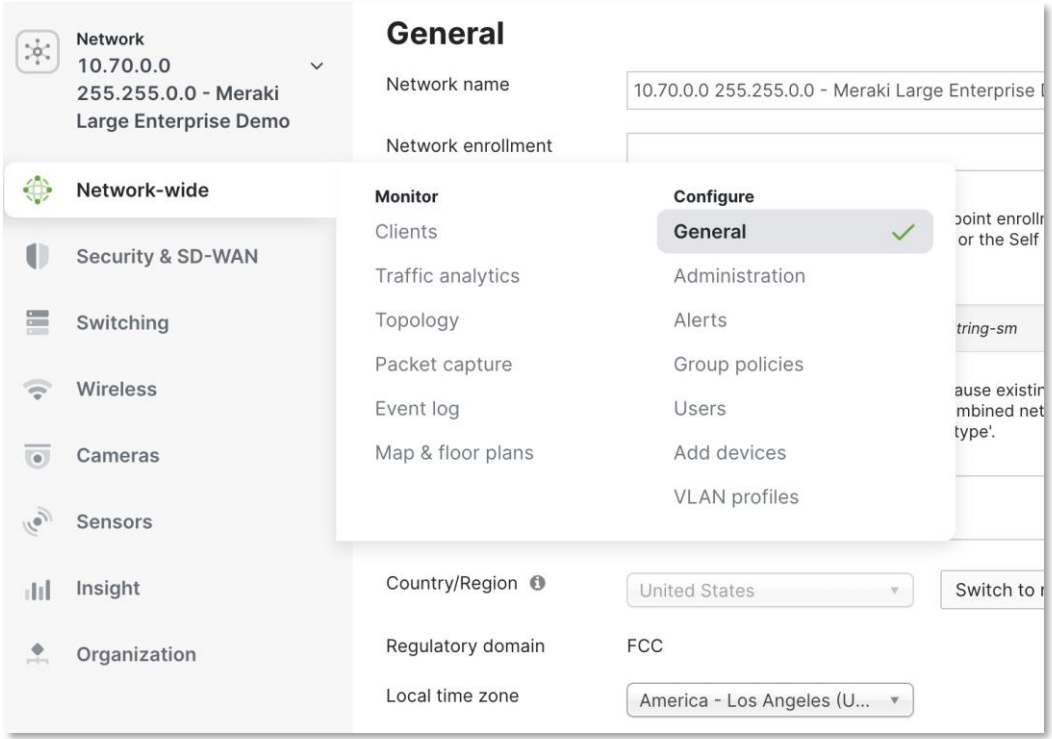
Full Admin	Read Only Admin	Guest Ambassador	Monitor Only Admin
Organization & Network	Organization & Network	Network Only	Network Only

SAML Single Sign-On >
https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Configuring_SAML_Single_Sign-on_for_Dashboard

More details on Dashboard administration >
https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions

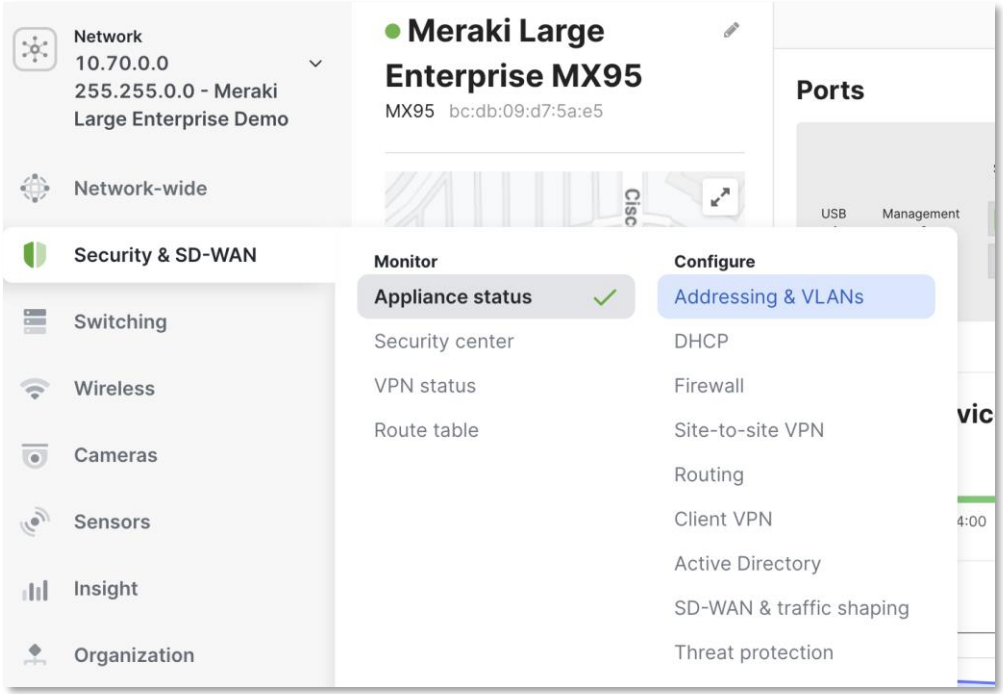
Configuration made easy with Cloud!!!

- Never get lost in the configuration again!
- Start at the top and work your way down
- Network Config



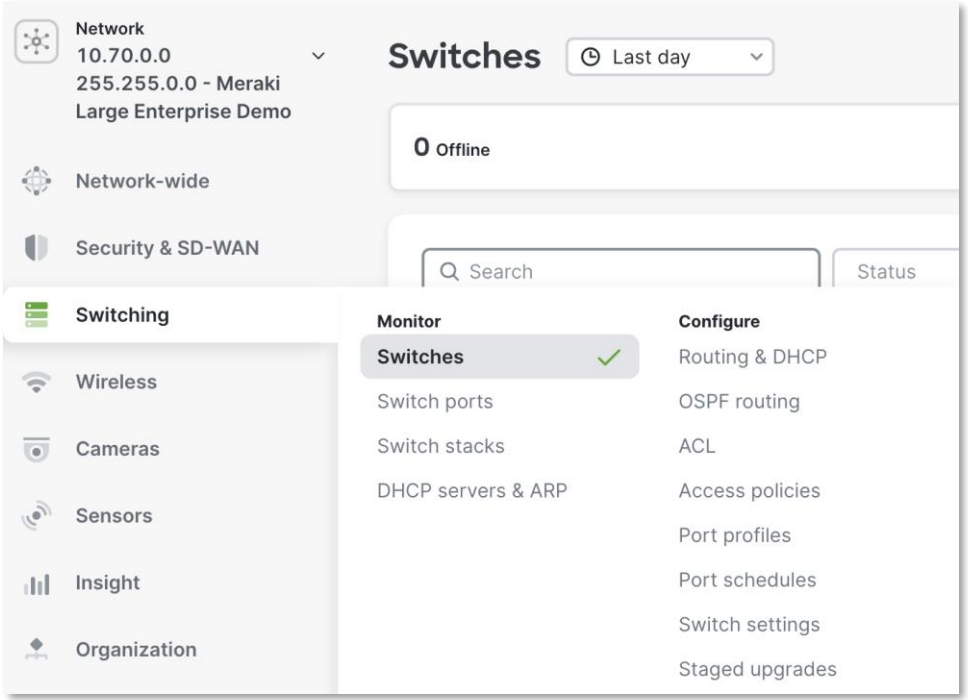
Configuration made easy with Cloud!!!

- Never get lost in the configuration again!
- Start at the top and work your way down
- Network Config
- MX Config



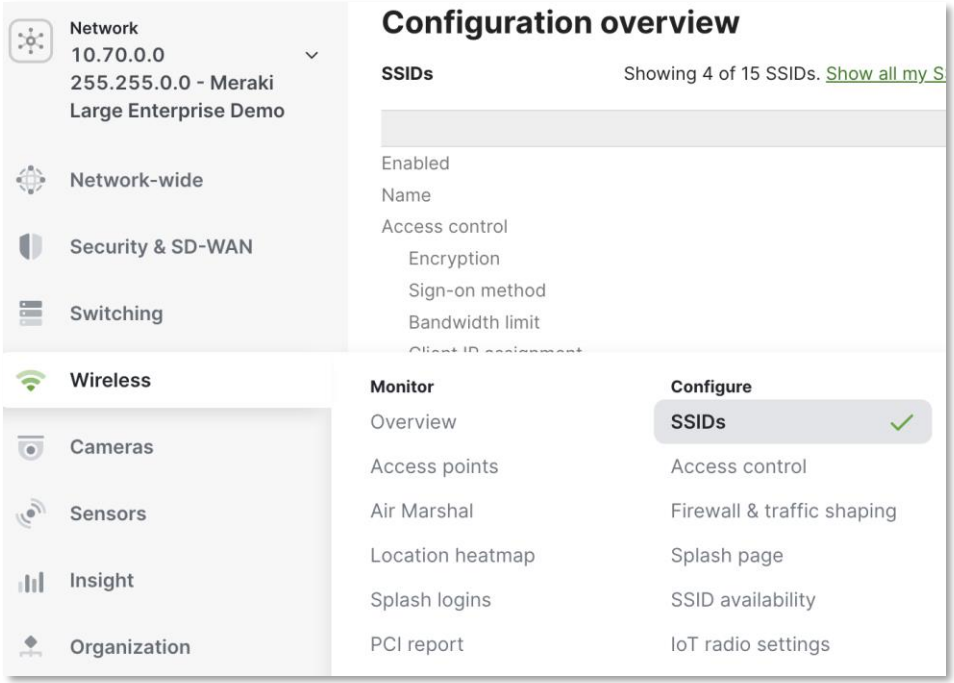
Configuration made easy with Cloud!!!

- Never get lost in the configuration again!
- Start at the top and work your way down
- Network Config
- MX Config
- Switch Config



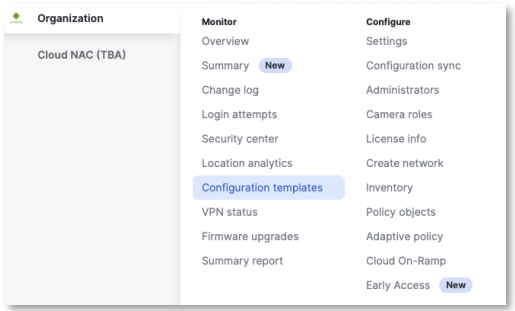
Configuration made easy with Cloud!!!

- Never get lost in the configuration again!
- Start at the top and work your way down
- Network Config
- MX Config
- Switch Config
- Wireless Config

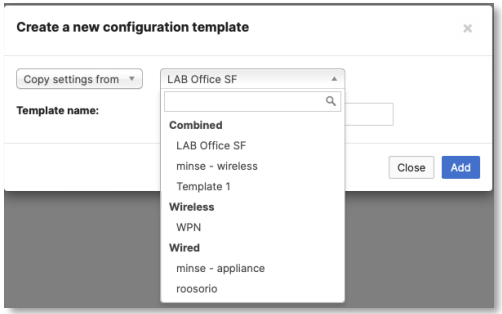


Configuration templates for Automation

Easily configure sites across the stack



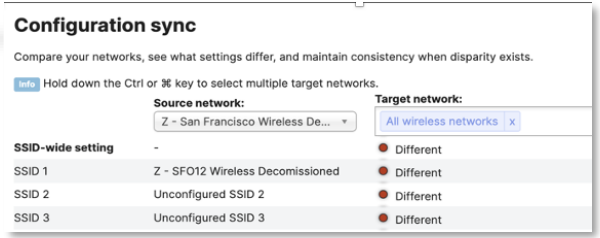
Create the template



Base off “golden” config

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

Local Override



Compare

Using tags to for additional Flexibility

Network Tags

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

Device Tags

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

Integration at scale with APIs

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

Dashboard API	Webhook API	Scanning API	Wireless Telemetry (MQTT) API	Captive Portal API	MV Sense API
• Device inventory • Config Automation • Monitoring • Reporting • Data Insights • Camera SnapShot	• Event stream • Automation trigger	• Asset tracking • Location analytics • Wayfinding	• Real Time Location Services • Sensors data	• Guest Wi-Fi • Secure Onboarding	• Real-time (4Hz) data stream • Historical time-series via REST • Current snapshot

REDUCE COSTS

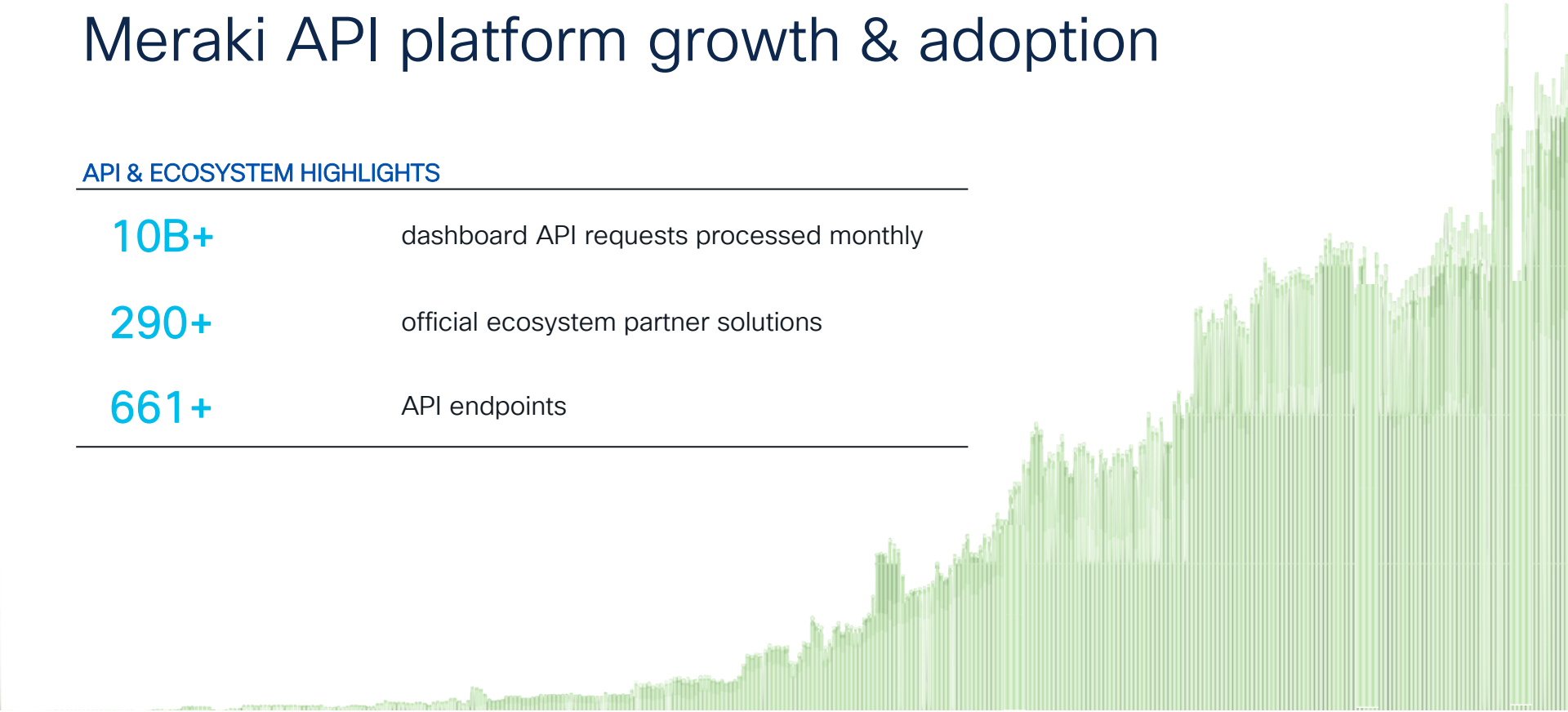
INCREASE EFFICIENCY

MITIGATE RISKS

Meraki API platform growth & adoption

API & ECOSYSTEM HIGHLIGHTS

10B+	dashboard API requests processed monthly
290+	official ecosystem partner solutions
661+	API endpoints



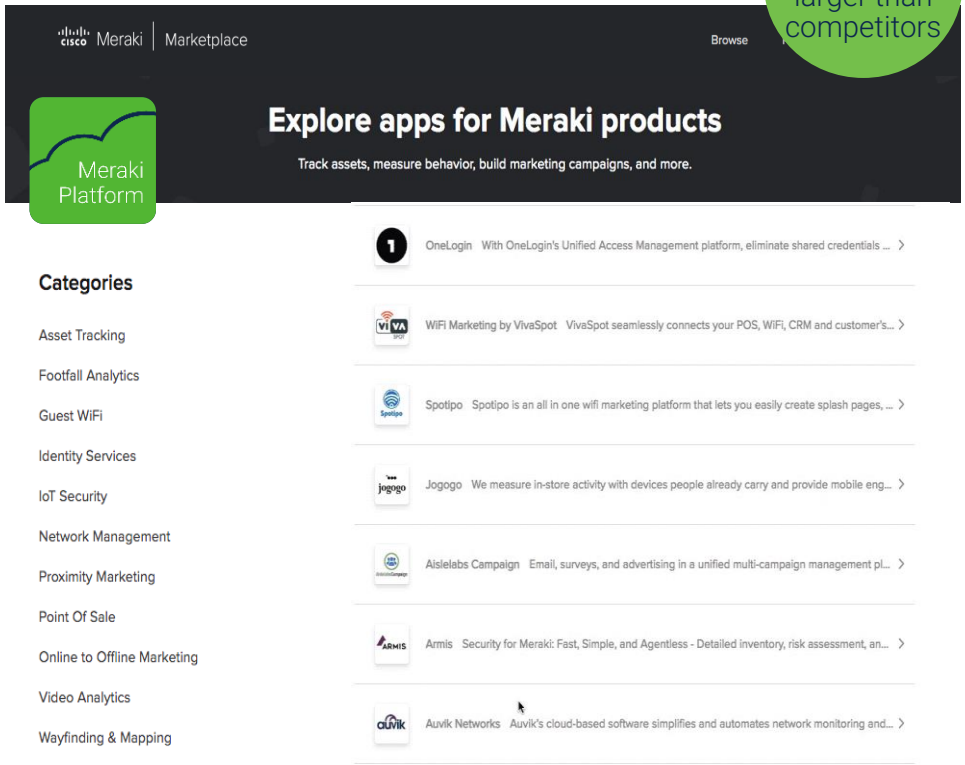
The power of the Meraki Marketplace

3x larger than competitors

150+
Communities Partners

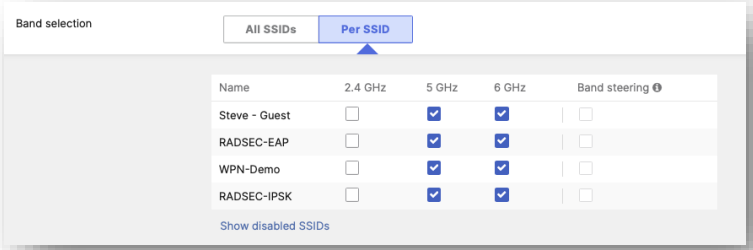
24+
Categories

290+
Ecosystem apps



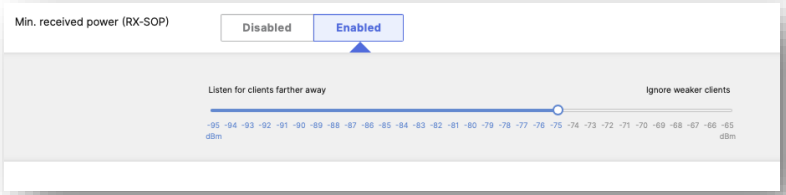
Enterprise Features

Advanced RF Management

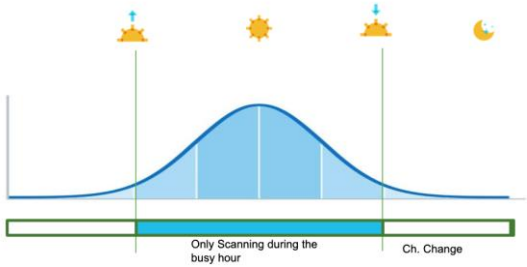


Per band vs per SSID settings

TX Power & Bit rate control



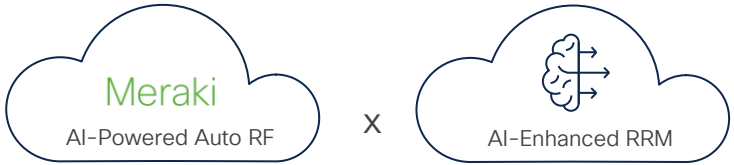
Fine tune with RX-SOP



AI powered AutoRF

Enterprise Class RF Management

How do we provide a consistent RF outcome without regard to platform?



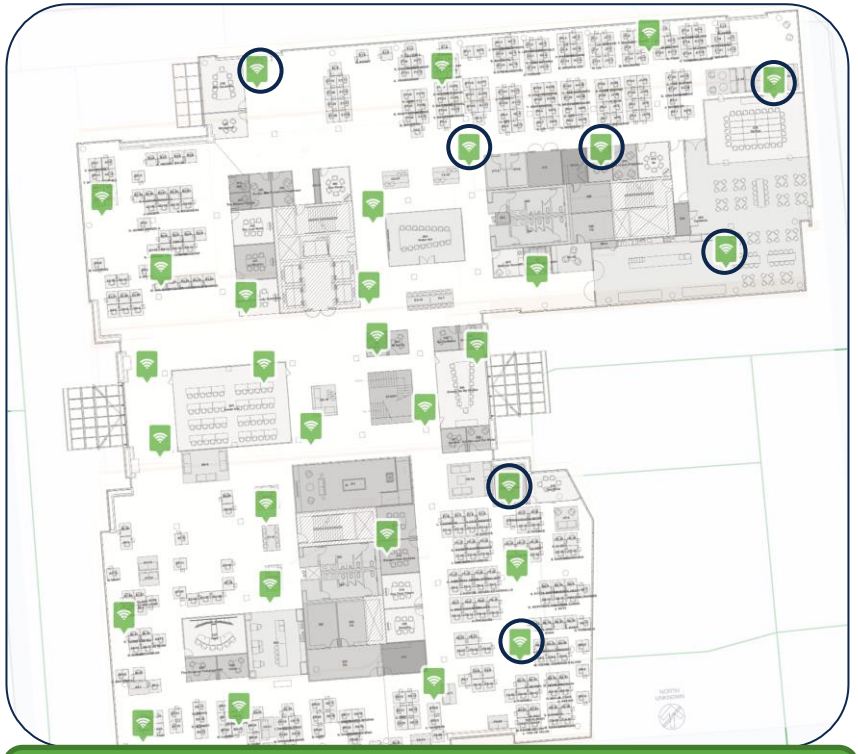
Integration with AI-Enhanced RRM

- Inherit advanced RRM features with less development cycles.
- Best in class solutions available regardless of architecture choice
- Brings benefit to 192k+ customers and ~10M APs immediately.

AI Channel Planning

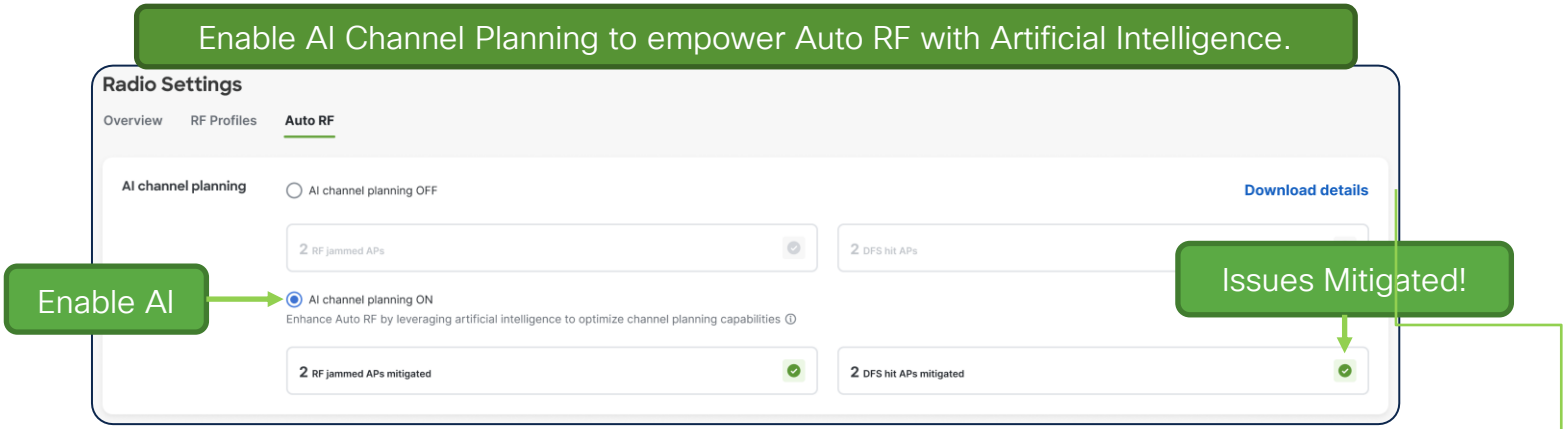
Reduce Client Disruptions by 50%

Powered by
AI-Enhanced RRM



AI learns your wireless with 6+ weeks of data to prioritize channels with the best wireless experience.

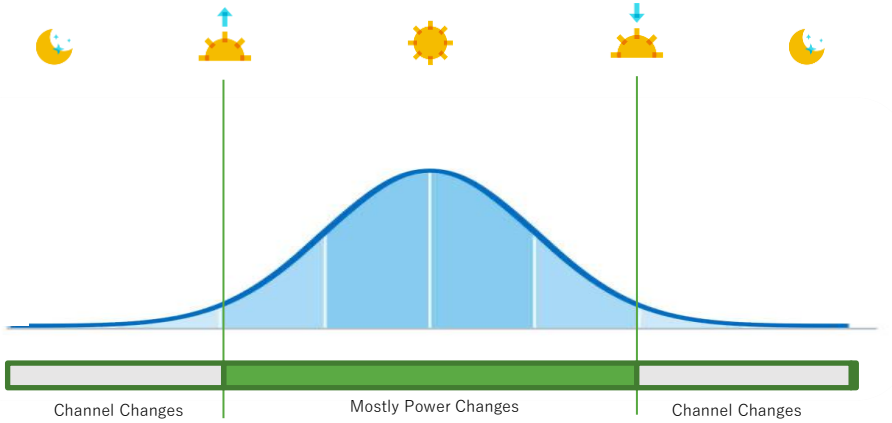
AI Channel Planning: How to enable?



AP Name	Issue	Band (GHz)	Channel	AI Channel Planning Mitigation	Start Time	End Time
AP1	<None, Frequent DFS Hit, RF Jammed>	<2.4, 5, 6>	<Channel>	<Channel Avoided, Channel Monitored, Feature Disabled>	<Start Time>	<End Time>
AP1	RF Jammed	6	104	Channel Avoided	3/23/23 - 12:45 PM	3/25/23 - 12:45 PM
AP1	Frequent DFS Hit	5	108	Channel Monitored	3/23/23 - 5:45 PM	4/23/23 - 5:45 PM
AP2	RF Jammed	6	100	Channel Avoided	3/23/23 - 5:45 PM	3/27/23 - 5:45 PM
AP3	RF Jammed	6	100	Feature Disabled	N/A	N/A

Busy Hours

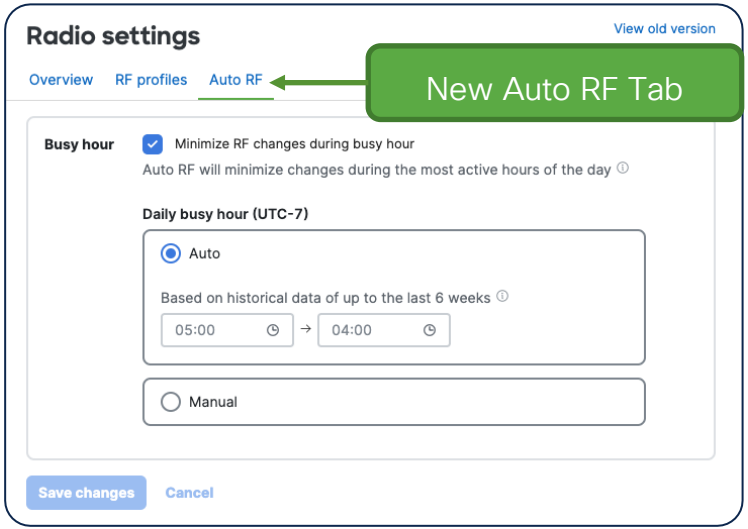
Minimize Client Disruption by reducing channel changes



Promotes seamless connectivity for users by minimizing channel and width changes during peak hours.

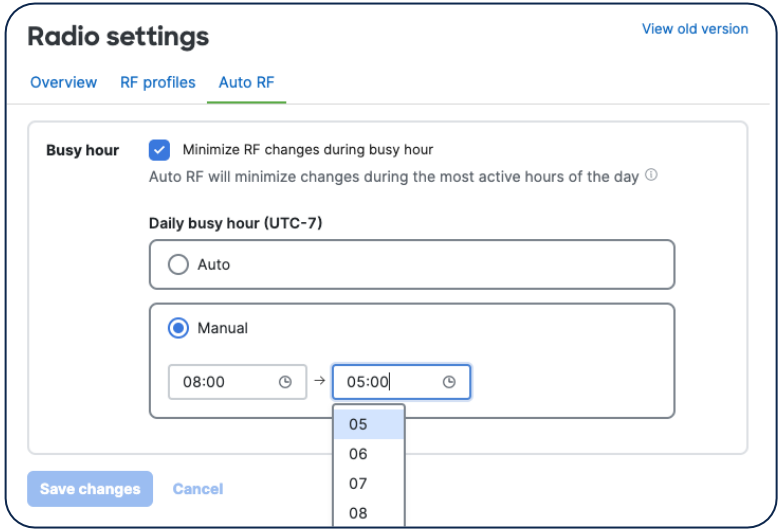
Powered by
AI-Enhanced RRM

Busy Hours: What are the options for enabling?



Have AI decide for you...

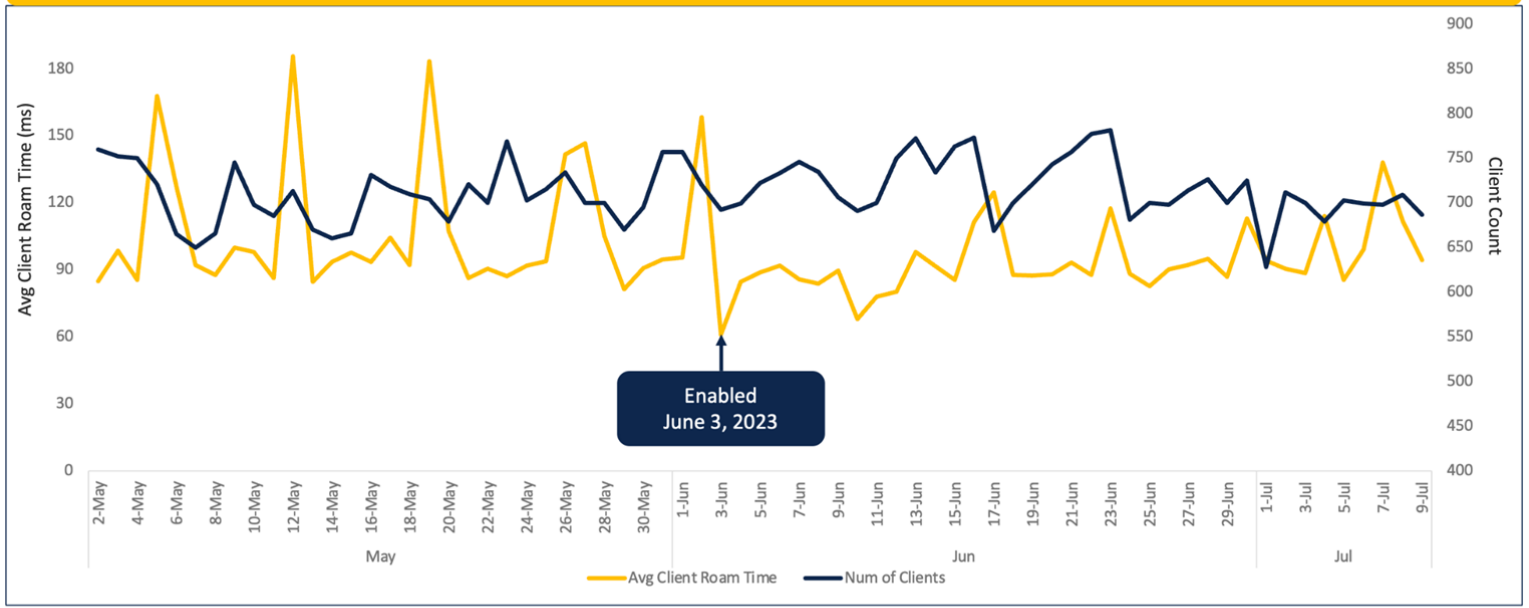
Derived from 6 weeks of client count & traffic data



...or configure time range manually!

Customer's client Roaming Time decreased after Auto RF's Busy Hour and AI Channel Planning was Enabled

Average client roaming time gradually decreased 50%, from 210 ms to around 100 ms!



The client count remained consistent, meaning Busy Hour and AI Channel Planning improved the wireless!

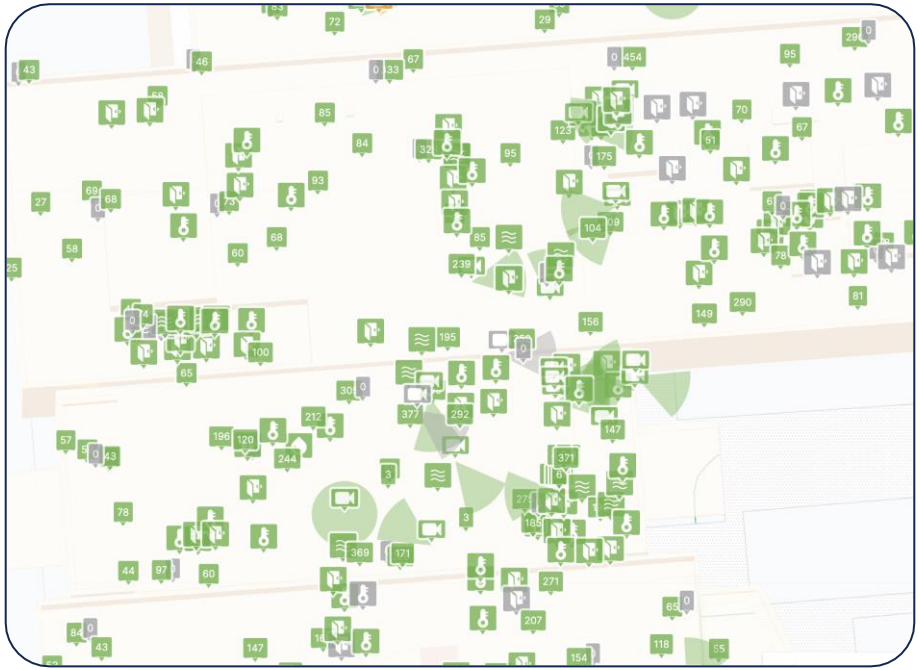
Enterprise class RF made simple

AP Neighbors feature

RF interference is difficult to visualize

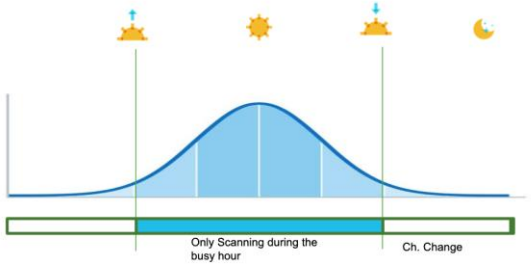
It’s difficult to identify the source of interference

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

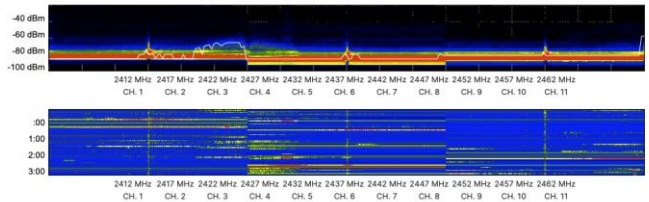


Demo time!

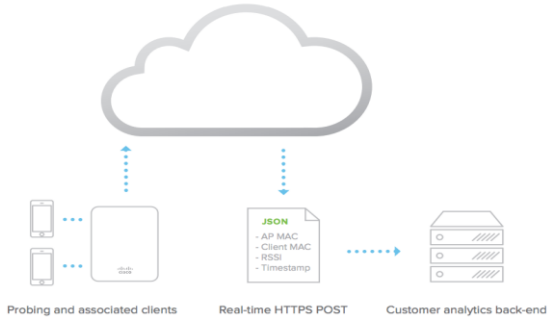
Scanning Radio for AIOps/SecOps/NetOps



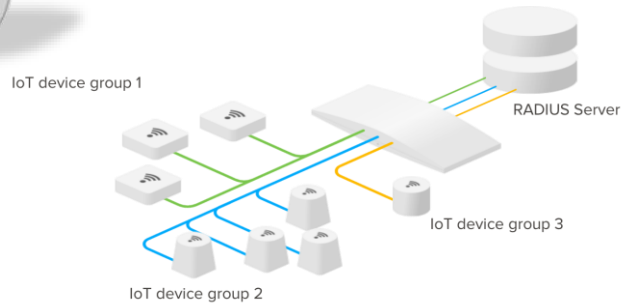
AI powered AutoRF



Spectrum Monitoring



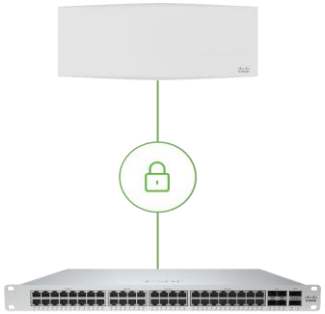
Location Analytics

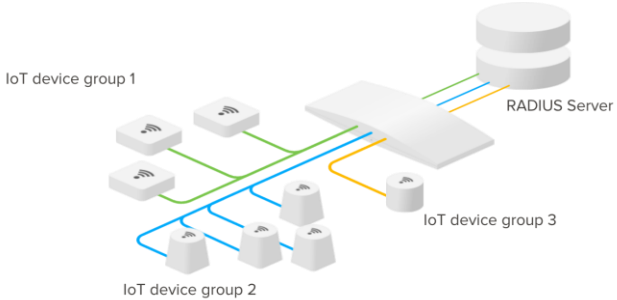


wIDS/wIPS

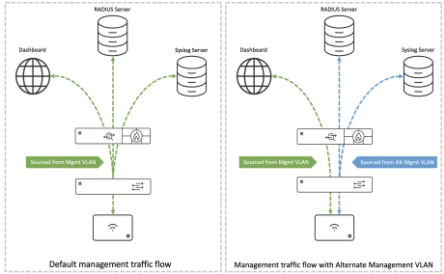
Wireless Security

Adaptive Policy
(TrustSec)

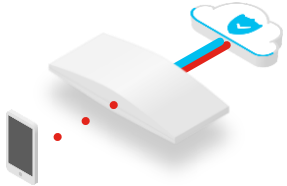




Identity PSK (w and w/o RADIUS)
Wi-Fi Personal Network (WPN)

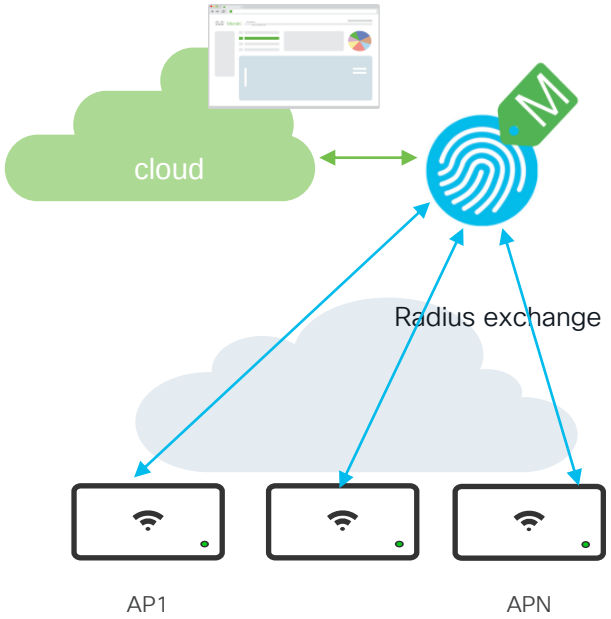


Alternate Management Interface (AMI)

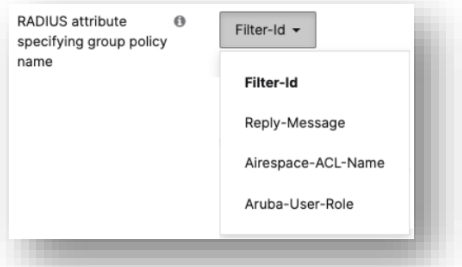


Group Policy + AVC =
Granular control with flexibility

Wireless Security > ISE integration



- L3/L7 Policy assignment via group policy + ISE
- Dynamic VLAN assignment via RADIUS Standard 64/65/81 & Airespace-interface-name VSA



- ISE CWA for guest provisioning
- Device Profile and Posturing
- Note: each AP is a Network Access Server (NAS) client unlike WLC that acts as NAS for all APs

Client Analytics: bringing the client view

Cisco is the *only* company with the size and power to partner with client vendors

Clients send exclusive messages to Cisco APs

What is this client?

- Form factor (phone/tablet/laptop) – Helps learn behavior
- HW (what chipset), SW (what drivers, what OS)
- Spot bugs / specific behavior overrides

How does the client see the RF?

- APs' RSSI, neighbor APs signal, Retries, problems

Why did it leave?

- 802.11 has 'standard' reasons
- what if you click another SSID in your client OS?
- User reasons, upper layer reasons, deeper 802.11 reasons

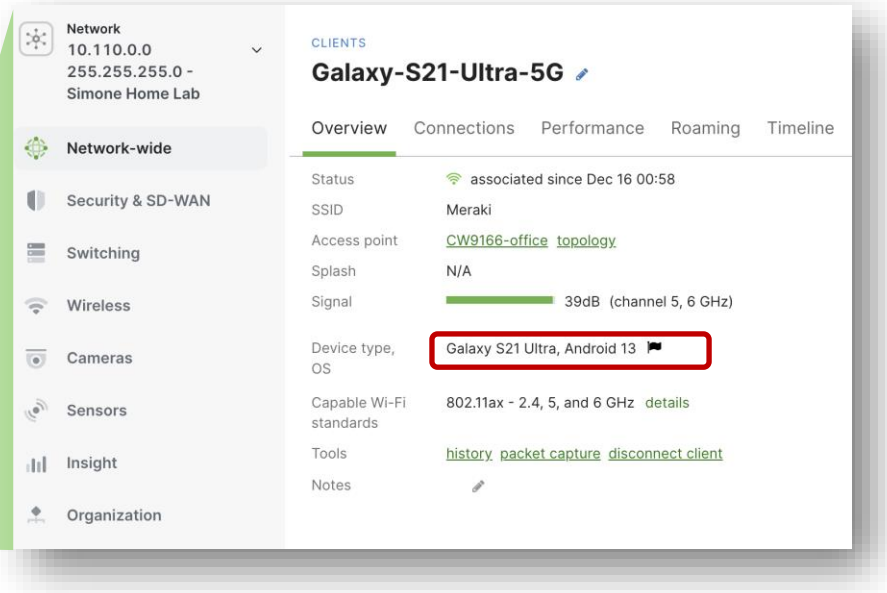
Next: let's exchange further

- Bring the 'view from the ceiling' to the client
- Clients roam faster, find the best cell, optimize its traffic

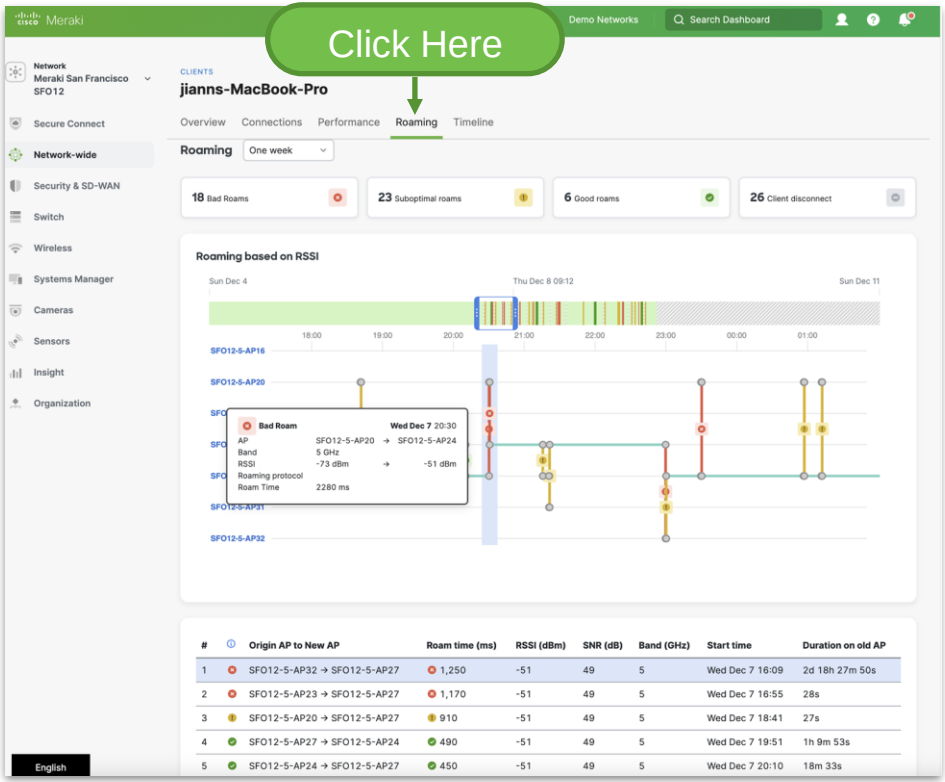
Client Analytics: bringing the client view

Intel, Apple, Samsung Analytics

	Meraki
Intel Connectivity Analytics	MR29
Apple Analytics	MR27
Samsung Analytics	MR29 Client profiling



Client Analytics: Roaming Analytics



#	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

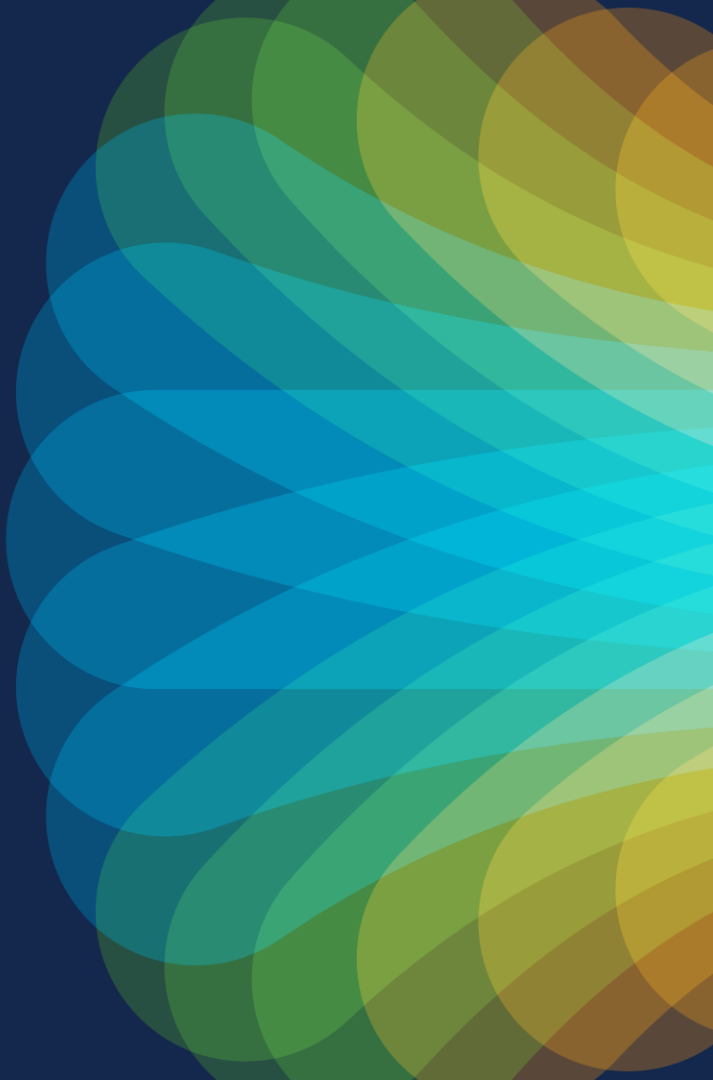
Intuitive client roaming visualization with detailed events for triage simplification.

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

Visualization supports a 1-hour to 2 min view.

Demo time!

Hidden Features



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

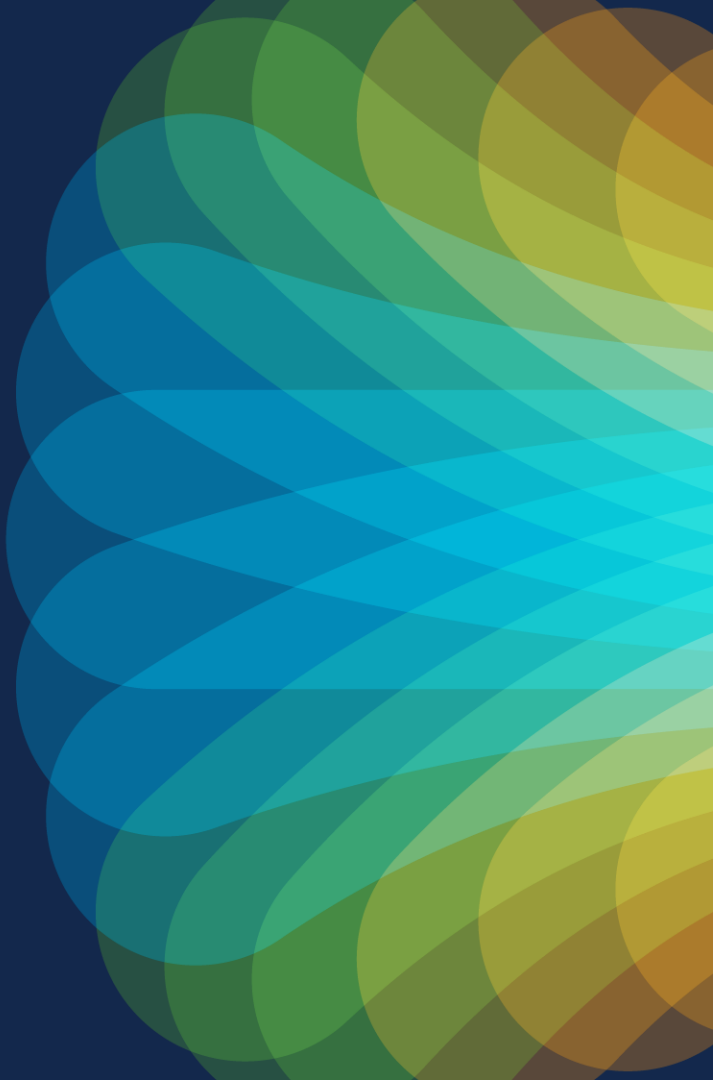
Beta Features use NFO to enable specific services to test and validate

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.

Software updates



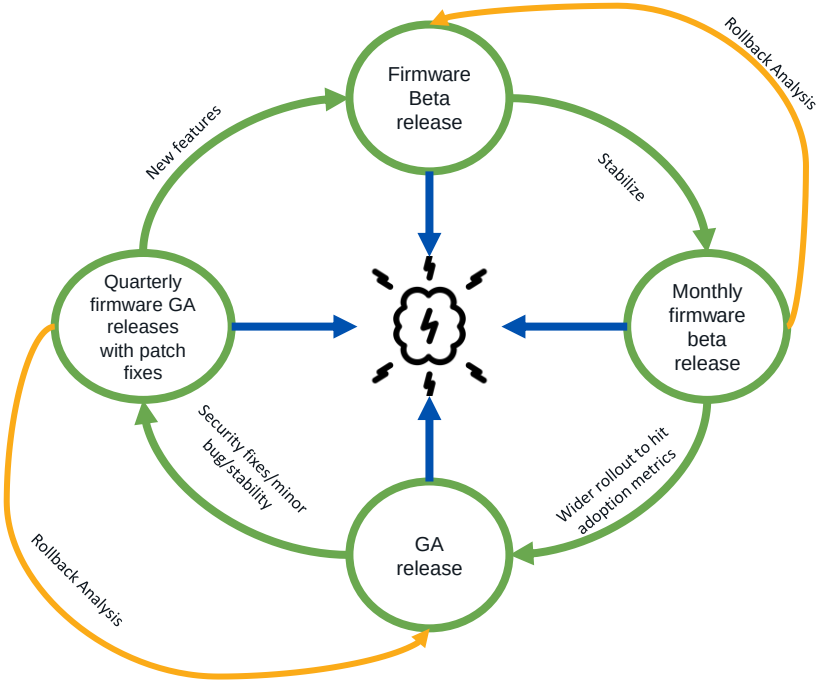
Wireless Firmware Upgrades

Intelligent firmware rollout that constantly monitors firmware globally

Global monitoring for all deployed firmware

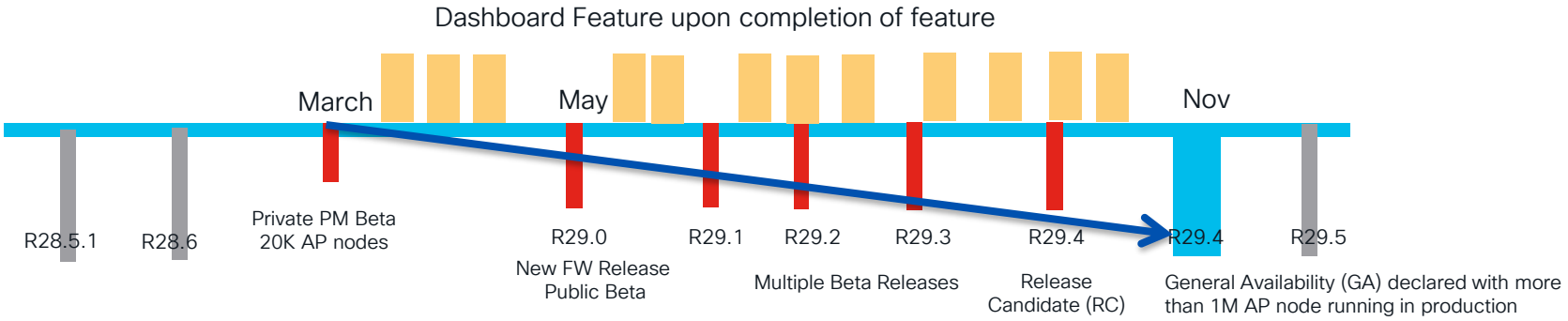
Proactive monitoring for product stability

Proactive outreach to resolve issues



Wireless Firmware Upgrades

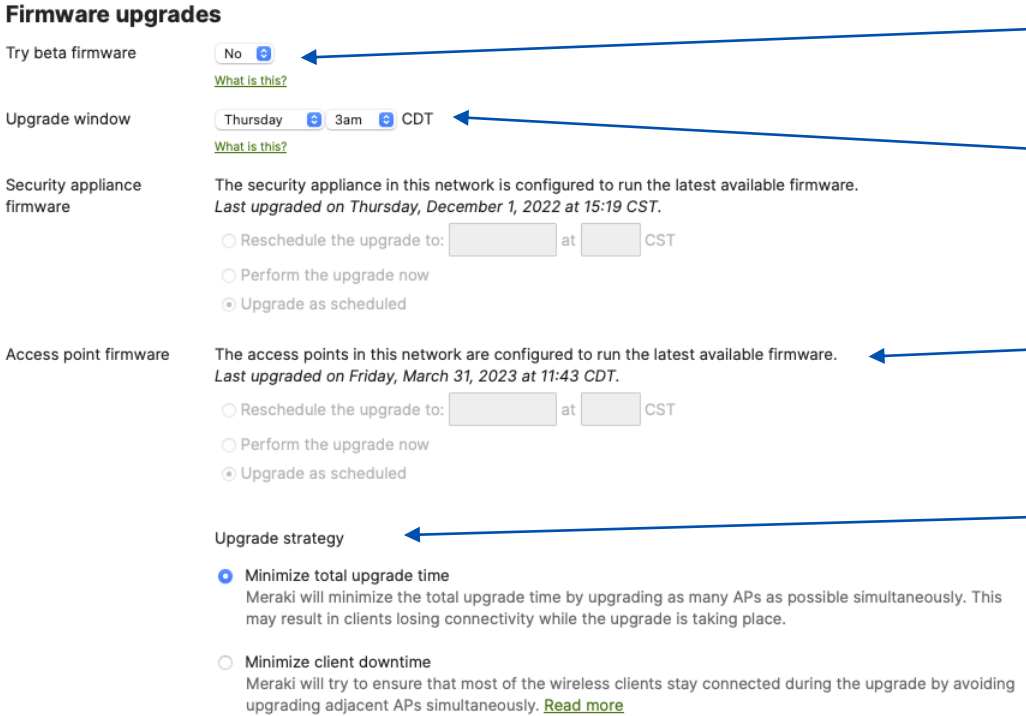
Flexibility – Software Release cycles



- Meraki Feature and Services delivery is done two ways:
  - Firmware-based feature updates with major release every year
  - Dashboard-based feature that can happens at any time due to cloud delivery
  - UI for features may be decoupled if needed for firmware features
- Note: Full Meraki support is available with any public Beta releases

Wireless Firmware Upgrades

Flexibility – Software Updates Scheduling per network



Beta? – Yes | No

When? – Based on local time

What? – MR, MS, MX

Strategy? – Fast or don't disrupt clients

MR software adoption and recommendation

MR29.X *(GA)*

Released in June 2022

6.27M

nodes on r29

1.25%

rollback rate

<0.7%

avg. watchdog rate

MR30.X *(latest GA)*

MR30-5 GA in November 2023

1.7M

nodes on r30

1.85%

rollback rate

<1%

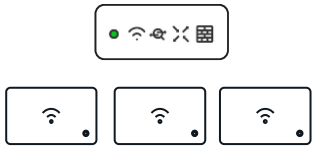
avg. watchdog rate

Current recommended releases **R29-7-1and R30-5**

Network Architecture

Network Architecture > Customer deployments

Large, Medium Campus
> Centralized data plane Deployment



km^2

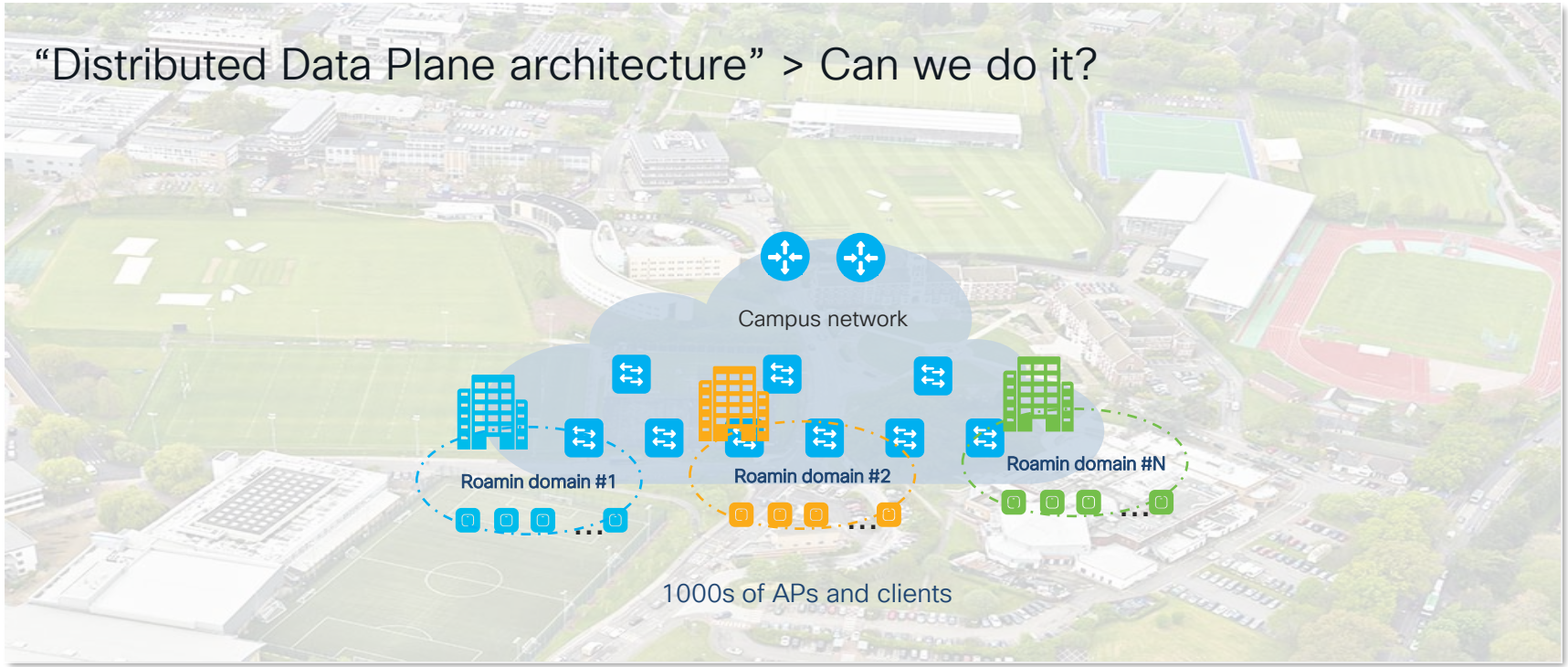
E.g., University Campus

Distribute Enterprise: Branch, Small Campus
> Distributed data plane Deployment

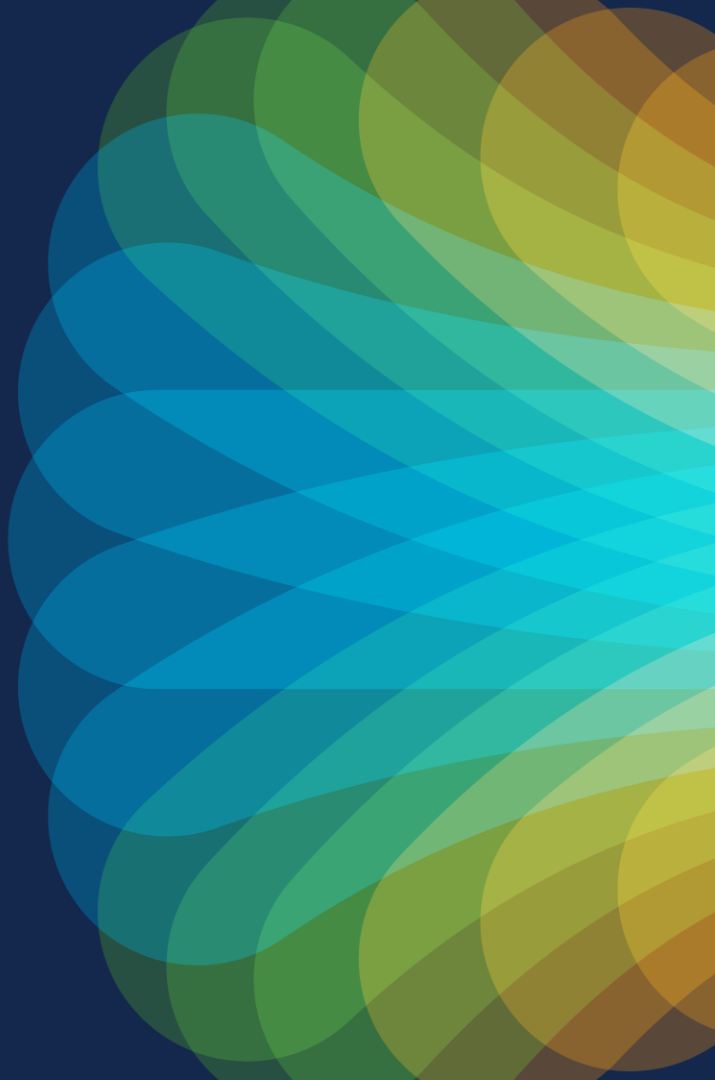
m^2

e.g., Retail

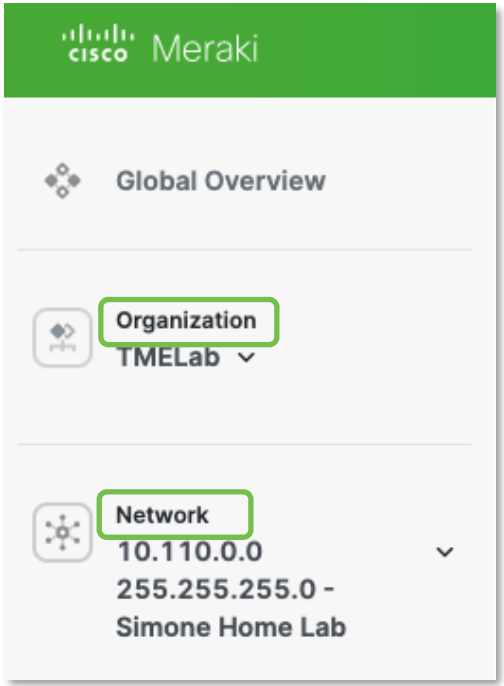
Network Architecture: Large Campus with Meraki



Before we begin..



Meraki Organization and Meraki Network



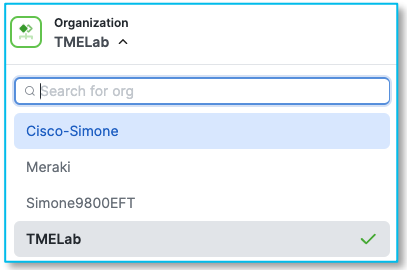
Organization: A collection of networks that are all part of a single organizational entity

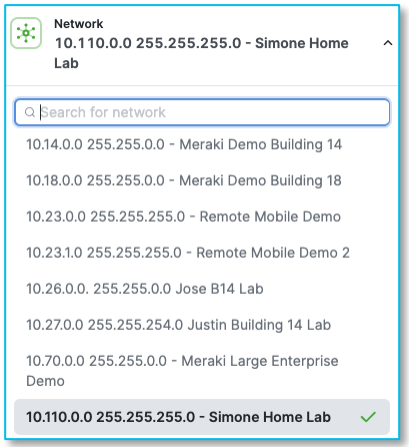
Recommended 25k nodes* due to Dashboard performance

Network: Set of Meraki devices, their configurations, statistics, and other info. Usually mapped to a geo location.

Recommended 1,000 nodes due to Dashboard performance

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





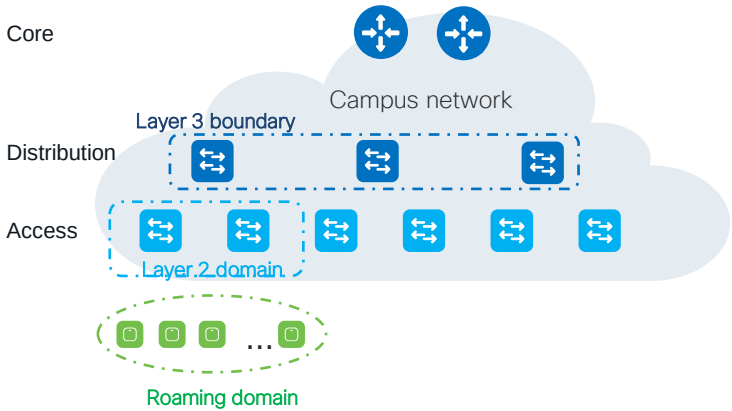
Need more scale?

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

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

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

Network Design Terminology refresher



L3 boundary:

- Limit of the broadcast domain
- Maps to a Layer 3 interface on the distribution switch
- Connects multiple L2 domains

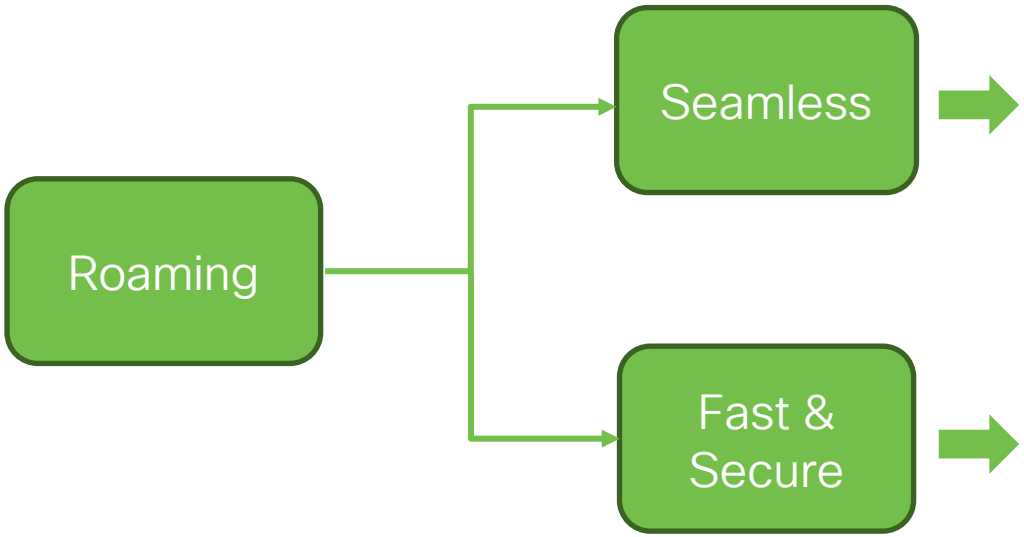
L2 domain:

- Layer 2 access network
- Single broadcast domain
- 1:1 mapping with a VLAN
- Can span multiple access L2 switches

Roaming domain:

- RF continuity domain
- Same SSID

Roaming refresher

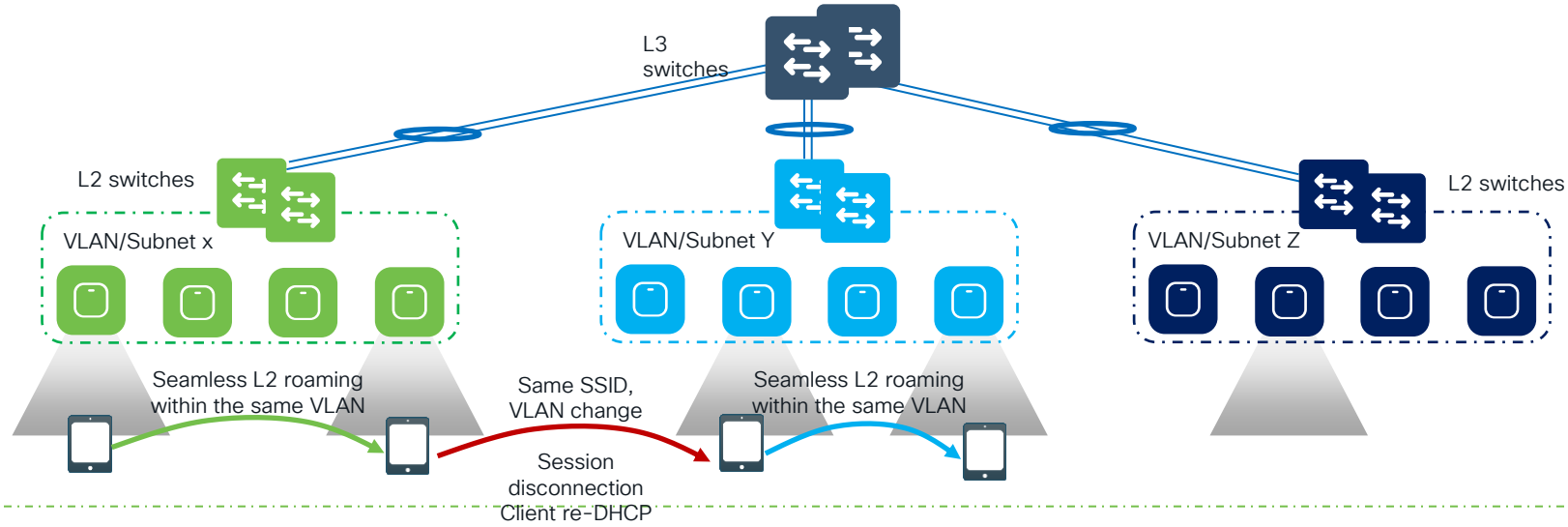


Seamless roaming = Keeping stateful information consitent (VLAN/IP/policy) as client roams between APs

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

Requires some form of **key caching** > 802.11r (or OKC). Optimized roaming with support of 802.11k/v

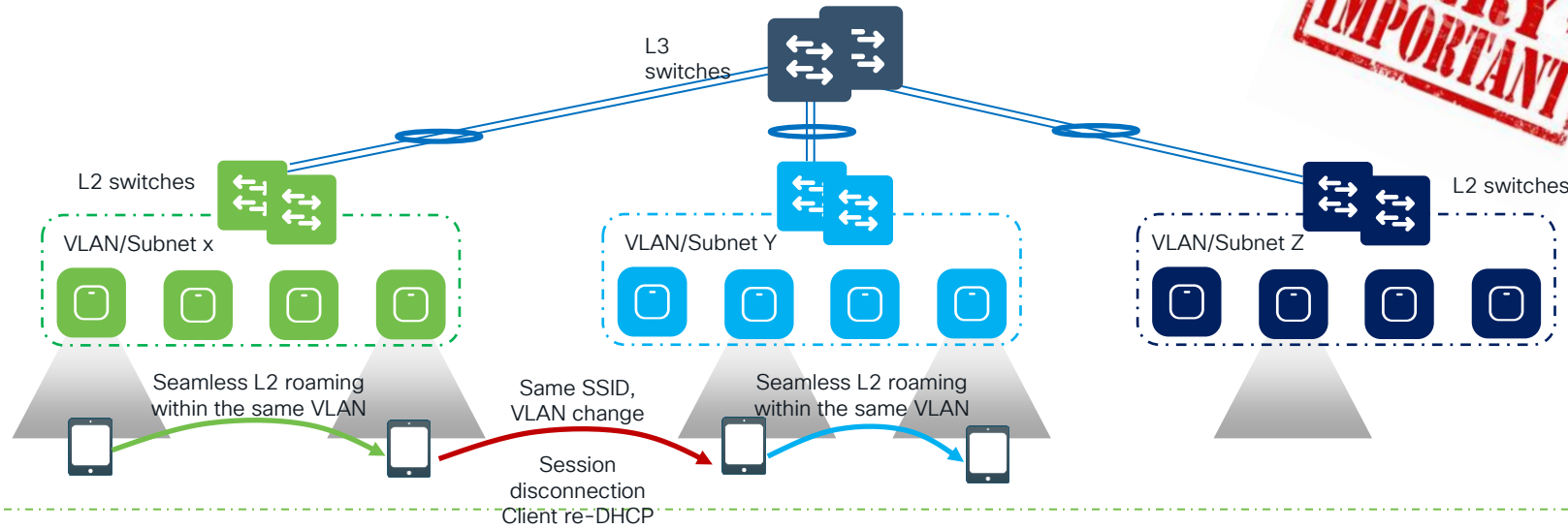
How important is seamless roaming?



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)

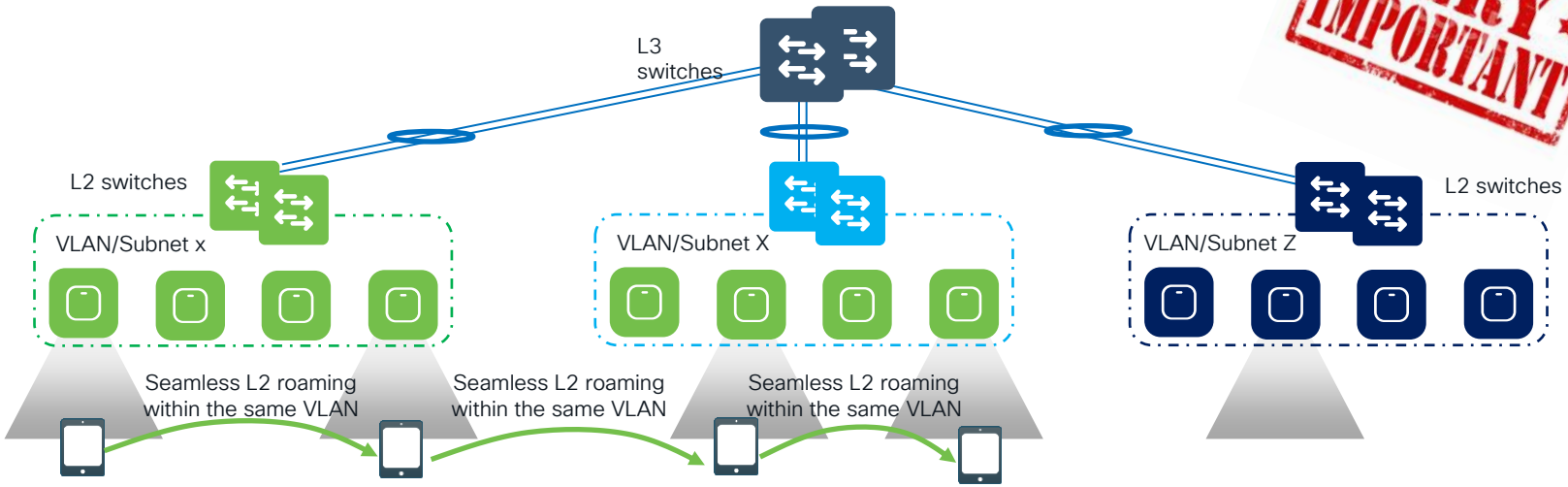
How important is seamless roaming?



What else you should consider?

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

How important is seamless roaming?



What else you should consider?

- Impact on the application: would it recover?
- VPN would 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

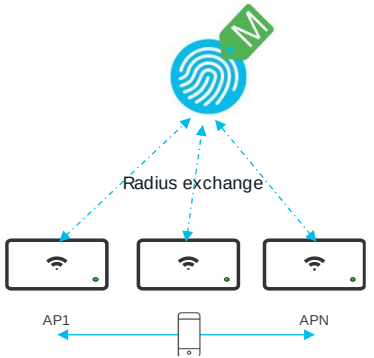
How important is fast secure roaming?

It depends...

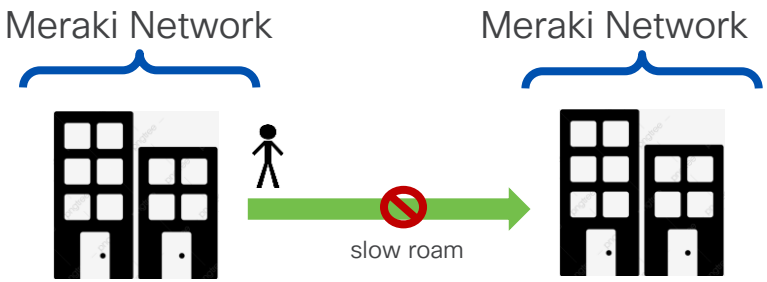
- **Really important for latency sensitive applications**: voice is very common, but also manufacturing applications, VR/AR, etc. Primary verticals: Healthcare, Manufacturing, Enterprise, etc.

- **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

- **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



Meraki Network: What you need to know?



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

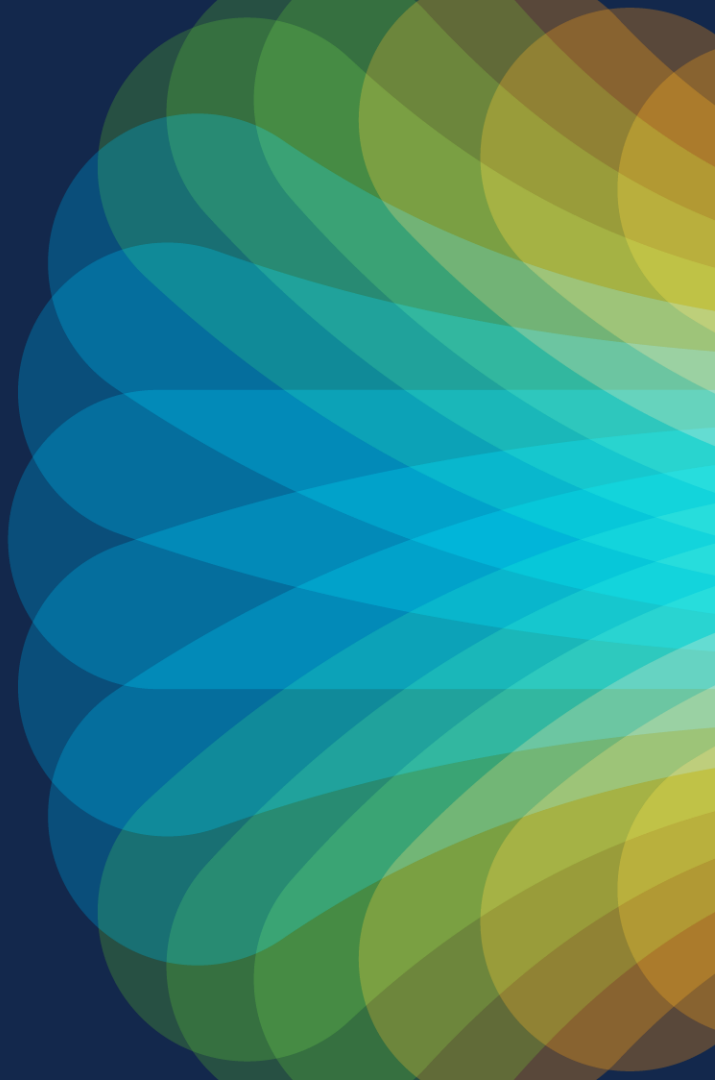
- Roaming in a Meraki Network:

	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 • Seamless (same IP)**

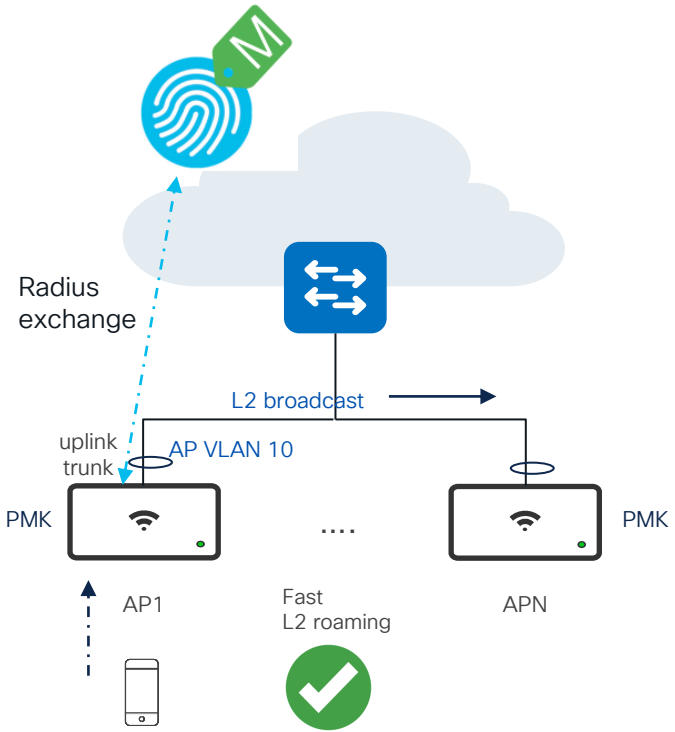
- Scale at Meraki Network
  - MAX Meraki devices (including MRs): 1k (soft limit)
  - MAX RF profiles: 50
  - Max 1500 MRs per RF profile
  - MAX SSIDs: 15
  - MAX clients: 50,000 (soft limit, dashboard performance)
- Rogues: MRs in different Meraki Networks see and report each other as rogues

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

MRs: what happens behind the scenes...



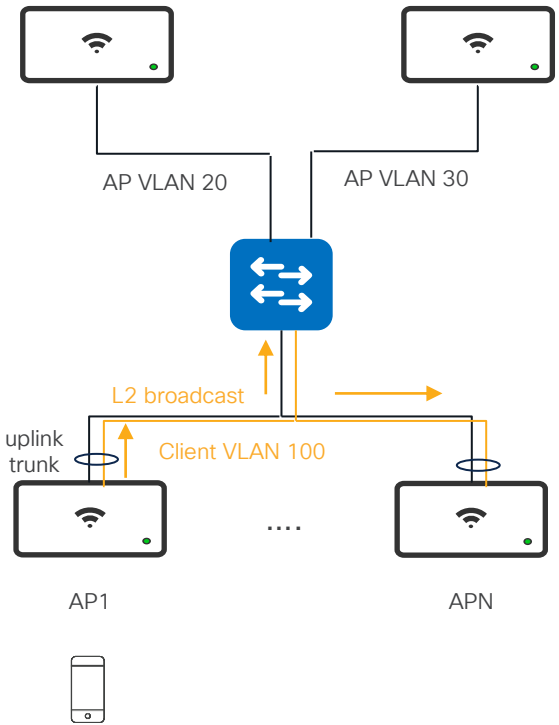
What information is shared between MRs?



Broadcast sent on AP VLAN:

- Fast Roaming: Pair Master Key (PMK) info is shared across all MRs in the same VLAN for L2 roaming. UDP based broadcast (Sport 35213 and Dport 23541)
  - What other info is shared across MRs within the client record to allow seamless roaming?
    - Session timeout, Group name
    - In R30, VLAN ID is supported
    - In R31, both VLAN name and VLAN ID are supported
    - This means that AAA VLAN override + fast roaming is supported starting these releases. This applies to both OKC and 802.11r roaming.
- Client Balancing: State of the wireless network (AP load and client signal info) for better load balancing. UDP based broadcast (UDP port 61111)

What information is shared between MRs?



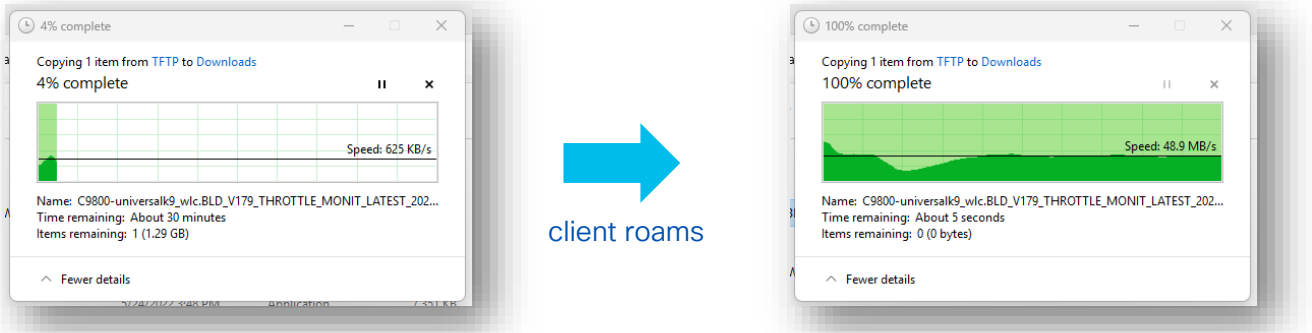
Broadcast sent on Client VLANs

- Magic ARPs: a flavor of gratuitous ARP used to update the wired infra and clear state on client roams. AP crafts an ARP frame spoofing the client's MAC with a 6.x.x.x IP address for uniquely identifying the AP sending the ARP
- 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)

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:



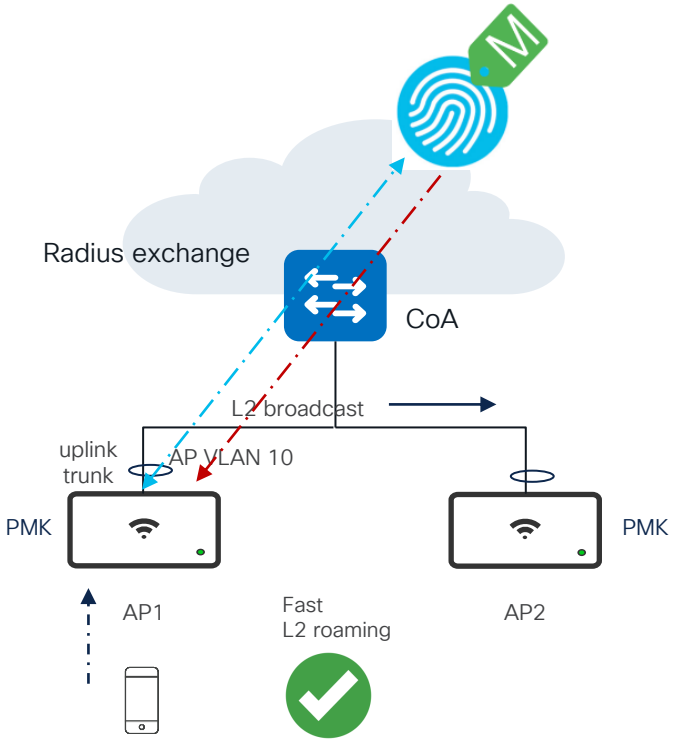
Roam-from AP: policy (rate limit) is applied

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

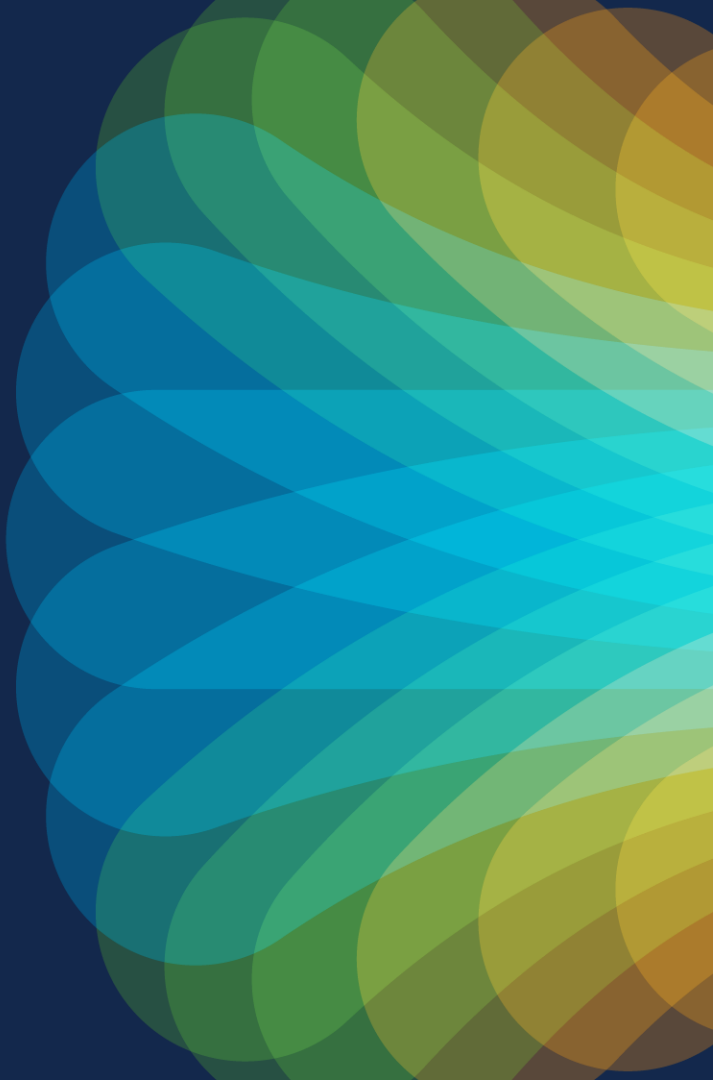
What information is NOT shared between MRs?

Client session ID



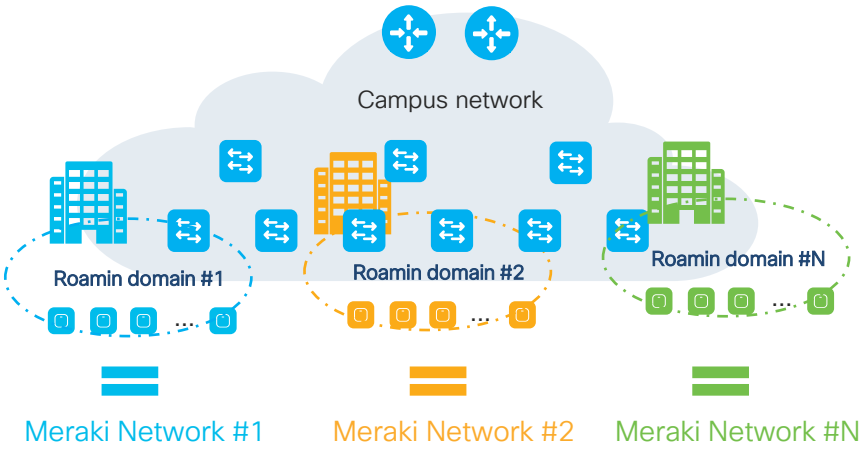
- Client associates and authenticates to an SSID with 802.11r/OKC
- The NAS is the MR (AP1 in this case)
- The client roams with 802.11; this is a fast roam and AP2 doesn't talk to Radius
- After the client roamed, AAA issues a CoA: the CoA is delivered to the original AP1, but the client is gone
- Result: CoA + 802.11r/OKC is NOT supported.
- If you enable CoA on the SSID, make sure you disable 802.11r (OKC is disabled by default)

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

Familiarize yourself with the Campus areas

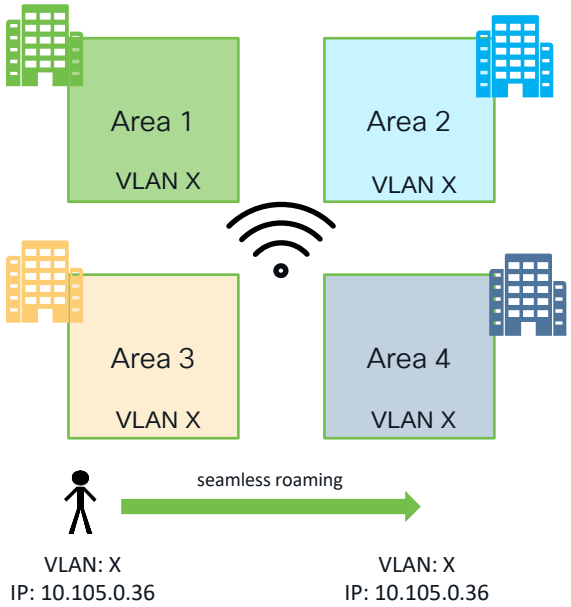
Design leveraging clear RF boundaries to minimizes client session breaks

- 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

Familiarize yourself with the Campus areas

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 for all areas
- 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: L2 roaming domain = broadcast domain; How big can you make it? It depends ☺

Seamless roaming domain: How big is too big?

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?

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?

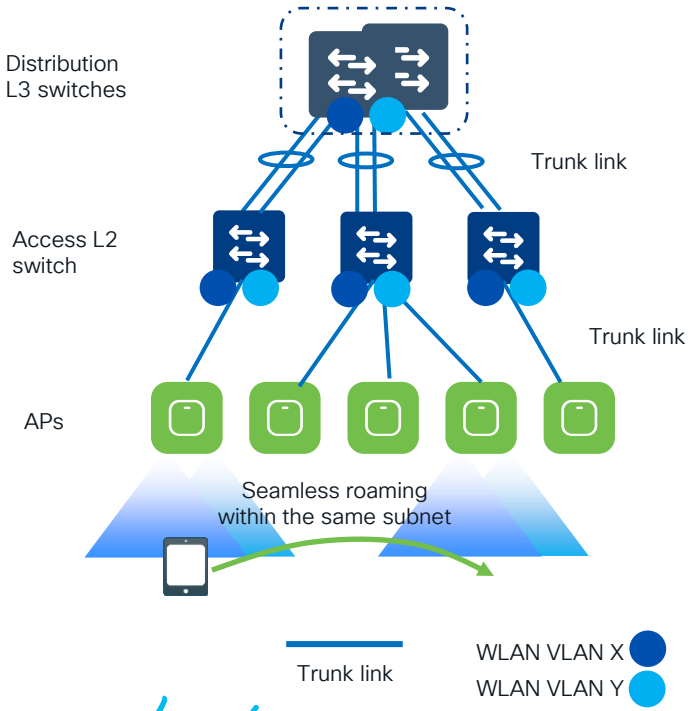
Layer 3 switch = Catalyst 9300 (or MS equivalent)

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 MAC entries is 32k/4 = 8k
- If we assume 40 clients per AP > 8,000/40 = **max 200 APs L2 roaming domain**

Access Network Design

Considerations to size a roaming domain

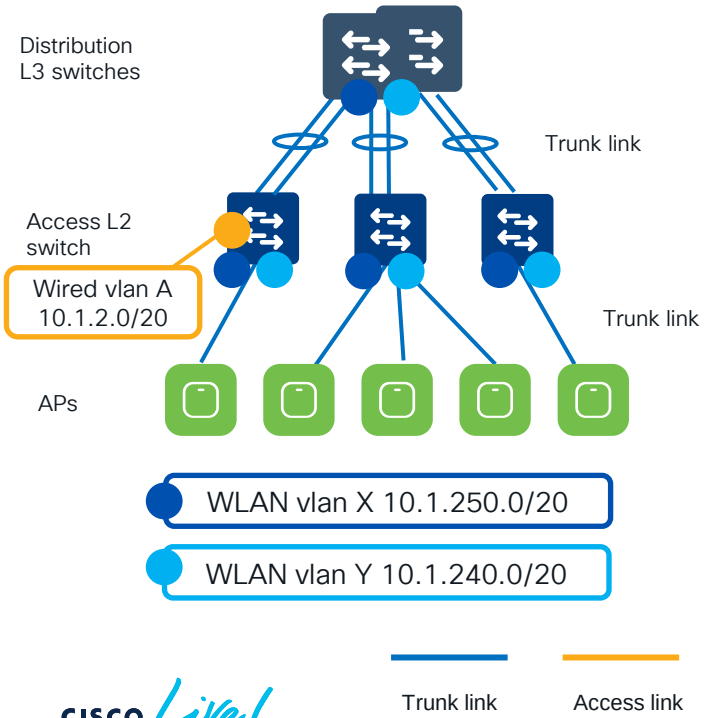


Single logical switch at Distribution Layer:

- 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

Considerations to size a roaming domain

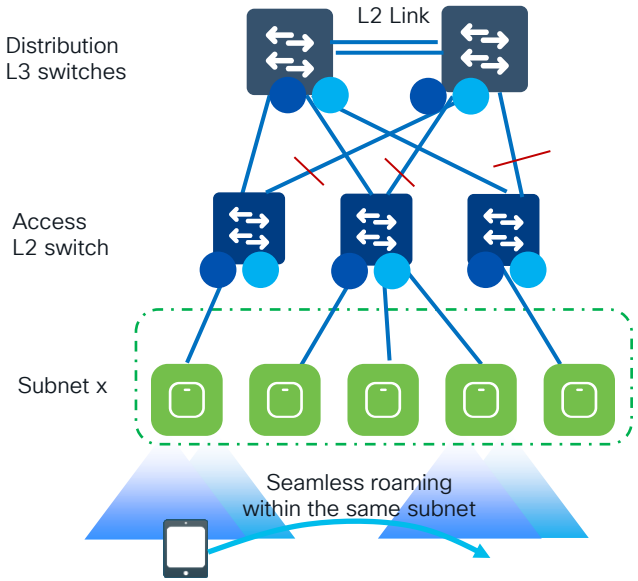


Single logical switch at Distribution Layer:

- 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
- For the ports connected to APs:
  - Configured ports as 802.1q trunks
  - Configure Spanning Tree Portfast Trunk
  - Configure BPDU guard and Root Guard

Access Network Design

Considerations to size a roaming domain

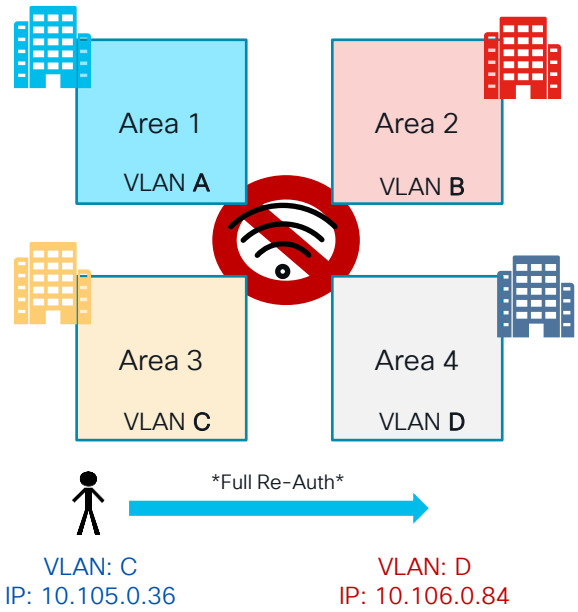


Individual switches at Distribution Layer:

- 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
- For the ports connected to APs:
  - Configured ports as trunks.
  - Configure SPT Portfast Trunk
  - Configure BPDU guard and Root Guard

Familiarize yourself with the Campus areas

Design leveraging clear RF boundaries to minimizes client session breaks



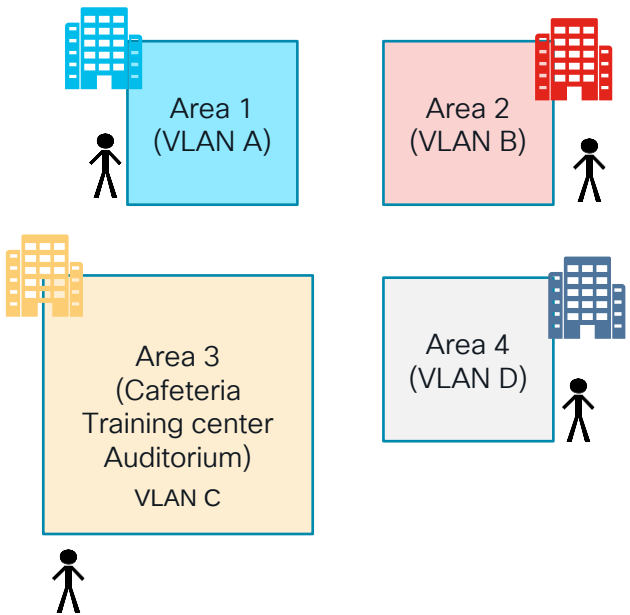
Requirement: No RF coverage between areas. Crossing RF coverage boundaries requires a full client re-auth > and client to change the IP address and that's OK!

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 just a very good design idea
- It lowers the impact of traffic like broadcast, unknown unicast and multicast (BUM)
- Reduces the fault and security domain (TCAM/ARP attacks, broadcast storms, etc.)
- Simplify management: can use VLAN/subnet to easily locate clients

Best Practices

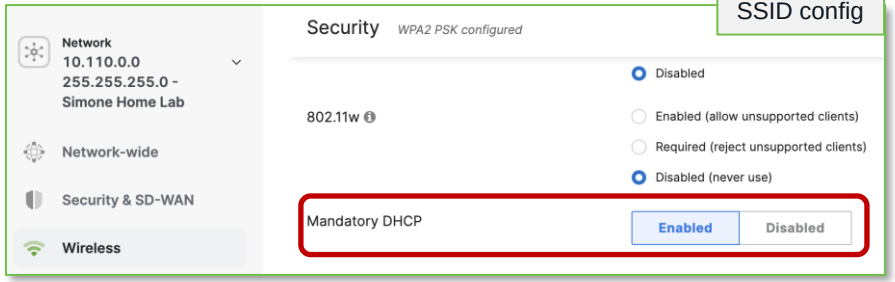
DHCP Scope Design



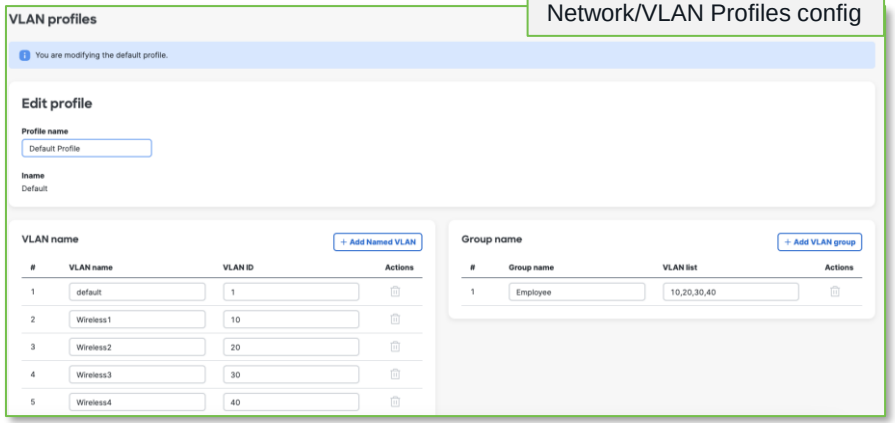
- Size your DHCP scope considering all the possible devices that could join that area to prevent DHCP scope starvation: stationary but also roaming devices from other
  - High density areas (e.g., Auditoriums) need larger scopes (/21 or /20) with shorter lease times
- DHCP Lease is very important to 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 8 hours for Universities
  - Set it to 1 hour for Retailers
  - Set it to 12 hours for normal office deployments
  - Set it very low (e.g., 30 mins) for security reasons (reduced unauthorized time) but there is an impact on the DHCP server and APPs). Also consider Random MAC > keep DHCP lease lower to avoid starvation

DHCP Scope Design

SSID config



Network/VLAN Profiles config

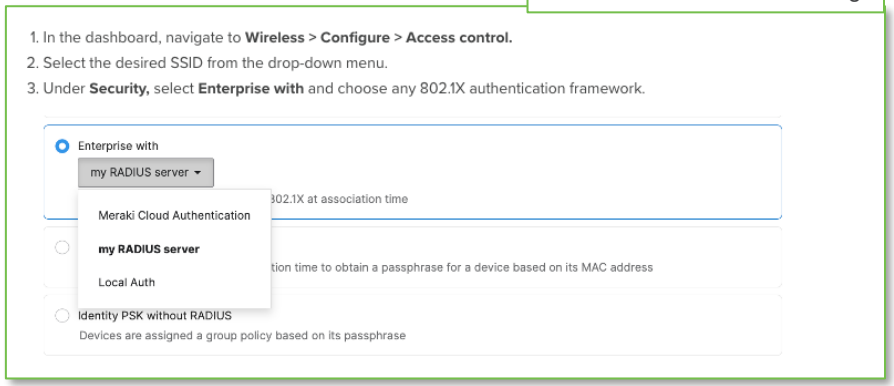


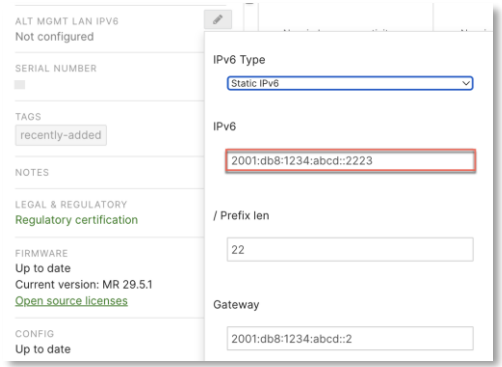
- Set DHCP Mandatory on your SSID access policy, if you don't need Static IP assignment.
  - DHCP Mandatory is a good security practice as system learns and records IP to MAC binding for each client
  - DHCP Mandatory automatically turns on Dynamic ARP inspection (DAI) and IP Source Guard which help 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
  - Note: as of today, fast roaming is not supported
- Subnet design: 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

  In this case, consider VLAN pooling: allows you to assign multiple VLANs to a single SSID. Supported starting from R30 code

VLAN pooling and IPv6

Network/VLAN Profiles config

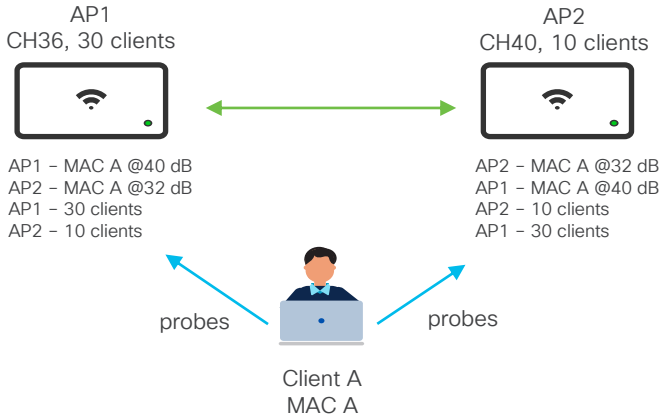




- R30 introduces VLAN pooling, this feature allows you to assign multiple VLANs to a single SSID.
- Please note: VLAN pooling in Dashboard leverages an existing feature called VLAN profiles. The documentation says “VLAN profiles can work along with 802.1X, MAB..”
- Even if VLAN profiles were created to work with Radius based authentication, VLAN pooling is supported with any security settings, including OPEN, PSK, SAE, Webauth ☺

- Additional Client IPv6 in R30: Support for 802.11r/OKC over IPV6 infra (dual-stack was already supported), DL3R over IPv4 infra and WPN fragmentation.
- Infrastructure IPv6: MR supports Static and SLAAC (no DHCPv6)
- Alternate Management Interface supports for IPv6 in R30

Client (Load) Balancing

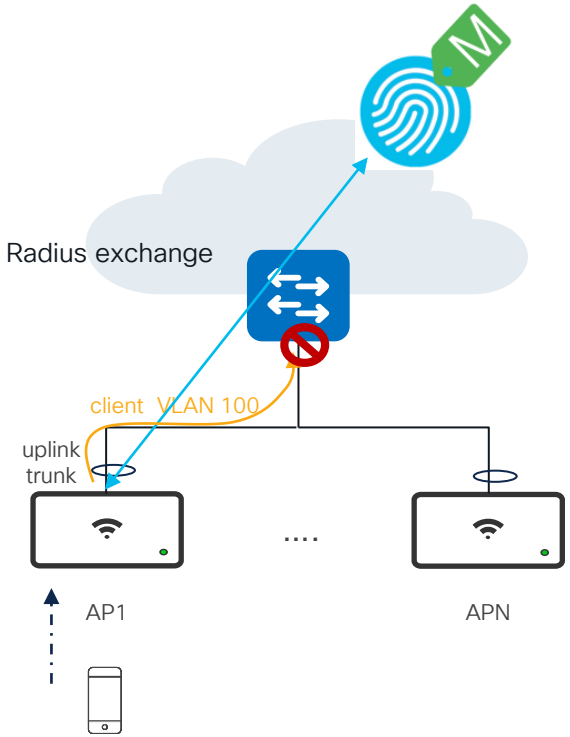


10597 166.523399	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
10598 166.523401	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
10599 166.538127	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
10600 166.538130	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
10637 167.526331	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
10638 167.526339	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
10639 167.536819	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
10640 167.536822	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
14400 227.965360	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
14401 227.965363	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
14508 228.969047	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
14509 228.969052	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
14510 228.980722	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
14511 228.980725	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
18318 289.725782	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
18319 289.725788	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
18377 290.714548	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
18378 290.714552	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111
18379 290.725002	192.168.222.14	255.255.255.255	UDP	155	Source port: 61111 Destination port: 61111
18380 290.725005	192.168.222.14	255.255.255.255	UDP	108	Source port: 61111 Destination port: 61111

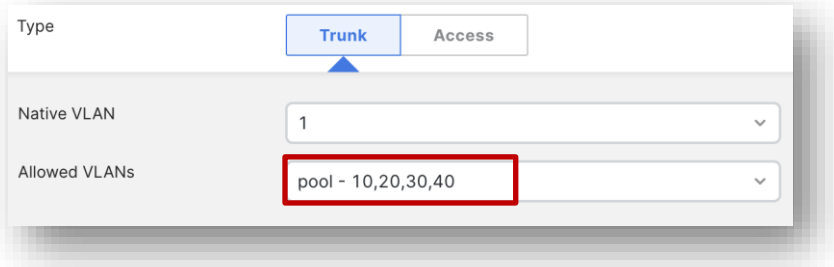
- What: Client balancing uses information about the state of the wireless network (AP and clients) to steer the client to the best available access point
- How: Two methods supported:
  - Passive: At client association, based on probes and association rejection
  - Active: At client association but also post association and only for 802.11v-capable clients using BSS-TM frames (MR 29 or higher).

  Client Balancing information is shared between APs using L2 broadcast messages on UDP port 61111
- Recommendation: For high density deployments Client Balancing should be turned off as the amount of processing due to probes could overwhelm the network.
- Client Balancing is turned off by default for newly created Meraki Networks

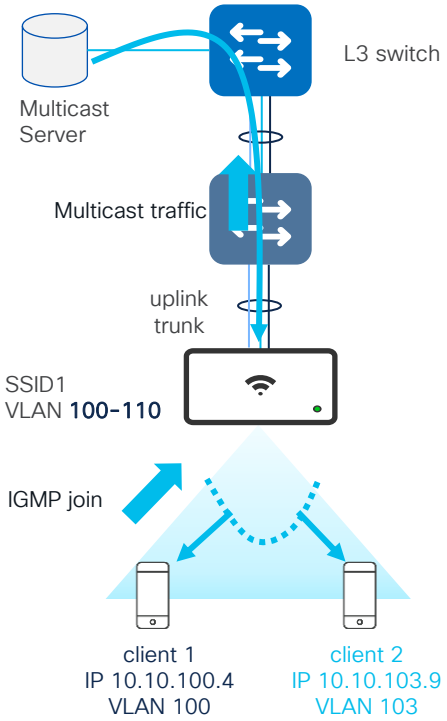
AAA VLAN override



- 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:

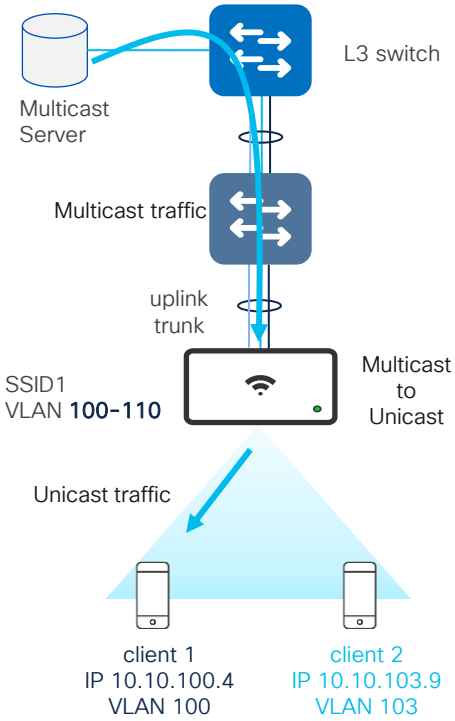


Multicast + AAA VLAN override



- What (Requirement): Single SSID mapped to multiple client VLANs via AAA policy. IP Multicast separation is required across client VLANs
- How: 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.

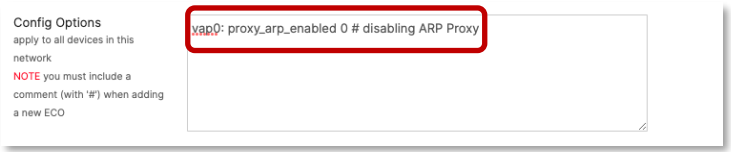
Multicast + AAA VLAN override



- What (Requirement): Single SSID mapped to multiple client VLANs via AAA policy. IP Multicast separation is required across client VLANs
- How: 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.
- Recommendation: 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

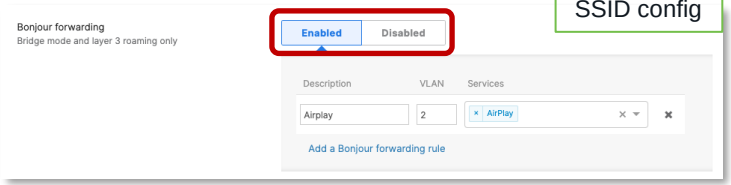
Multicast/broadcast handling

Admin only Network config



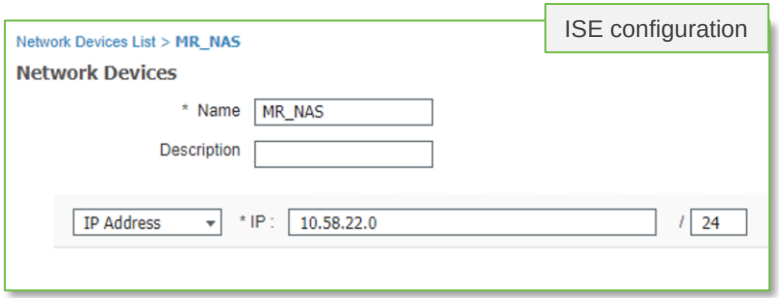
- ARP proxy is enabled by default on MRs and cannot be disabled. MR replies to ARP requests on behalf of the client preventing broadcast traffic in the air
  - Need to disable ARP proxy for passive client's support? This can be done via Meraki Support per SSID

SSID config

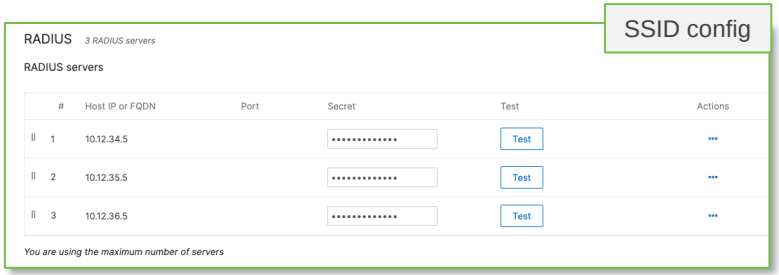


- mDNS/Bonjour is supported and allow services to work across multiple VLANs. You can choose specific services as well to enable Bonjour forwarding for a limited subset of services, e.g. only for AirPlay. MR 30.X firmware allows Bonjour to function even when the Layer 2 isolation is enabled on the same SSID. Location specific filters are not supported.

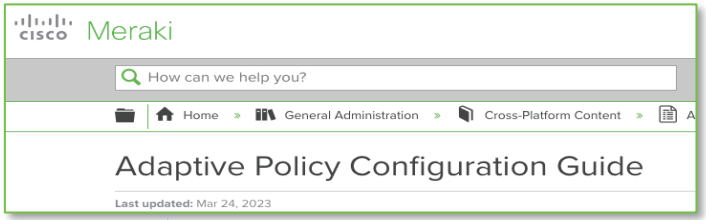
Security Considerations



- 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

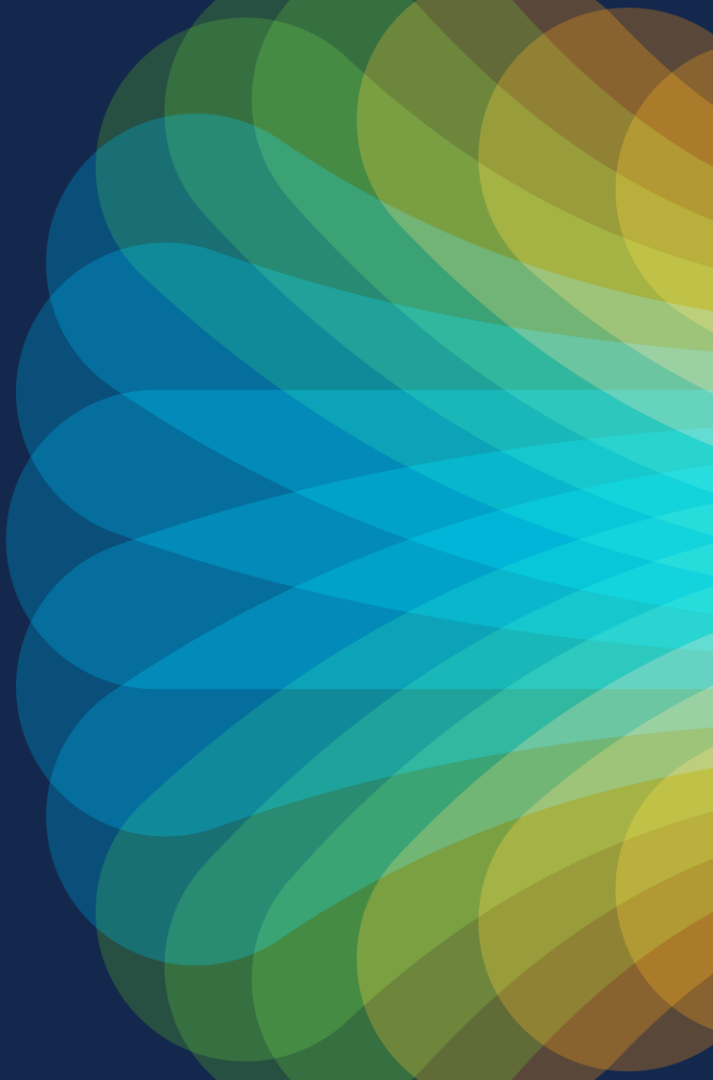


- Meraki has a limit of max #3 AAA servers per SSID. Usually this is not a constrain. For large, high-density deployments, you might consider placing a load balancer in front of the AAA servers. Configure source based sticky load balance, to make sure that each client session always talk to the same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

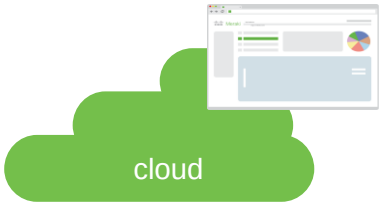


- Cisco Group Based Policy is supported on Meraki. It's called Adoptive Policy. Note: only inline tagging is supported (no SXP). Please refer to this doc for CMD device support: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/policy-platform-capability-matrix.pdf

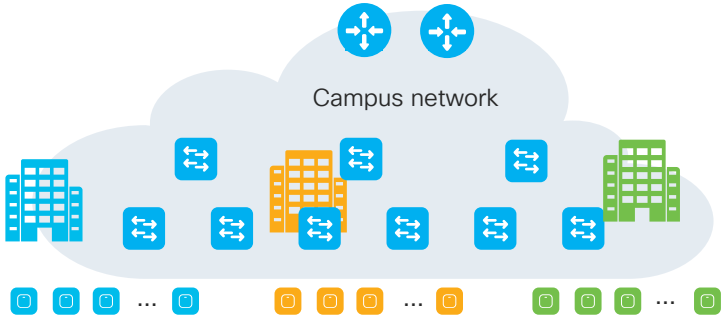
Large scale deployments



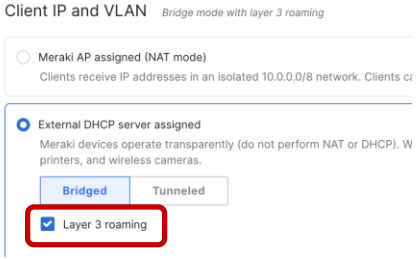
Large scale deployments – Not recommended



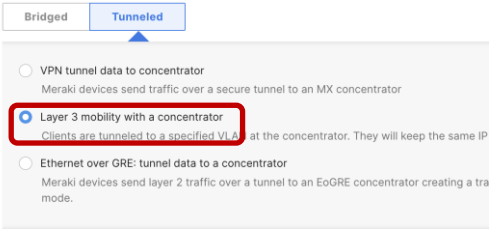
On prem



- L3 distributed Roaming (L3DR)



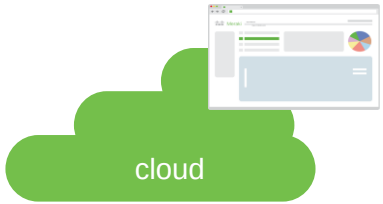
- L3 mobility MX as concentrator



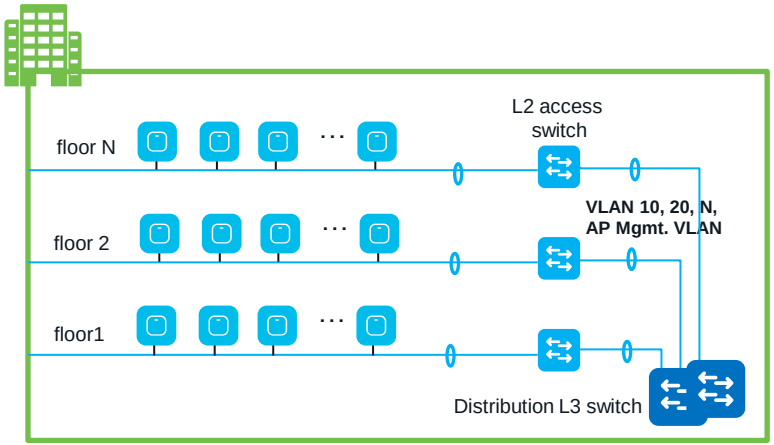
Both these solutions are not recommended for a large campus deployment

Large scale wireless deployment

Scenario 1



On prem



L2 roaming deployment:

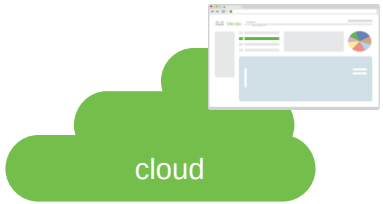
- Roaming domain = building
- AP per roaming domain < 200
- VLAN design = VLANs span the whole building

Design Recommendations:

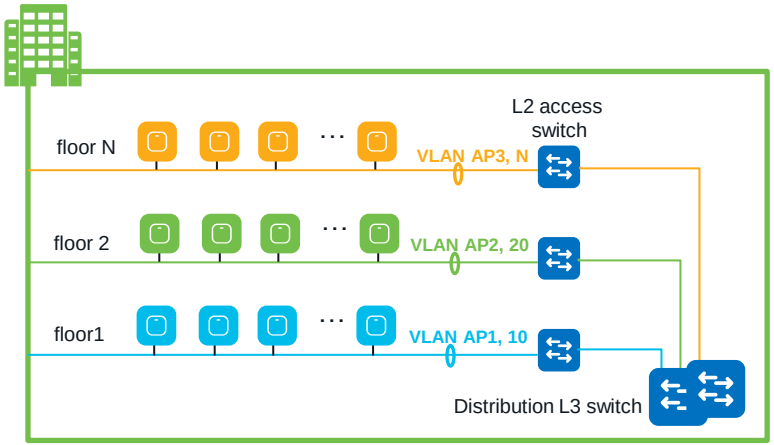
- L2 broadcast boundary at the building distribution switch
- Configure regular Layer 2 distributed roaming
- AP switchports configured as trunks (common AP management VLAN and client VLANs on all switches)
- Choose subnet mask to accommodate the expected # of devices per VLAN per building (VLAN pooling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

Large scale wireless deployment

Scenario 2



On prem



L3 roaming across floors Deployment:

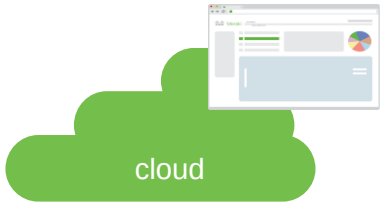
- Roaming domain = building
- AP per roaming domain < 200
- VLAN design = VLANs span only single floor/wiring closet

Design Recommendations:

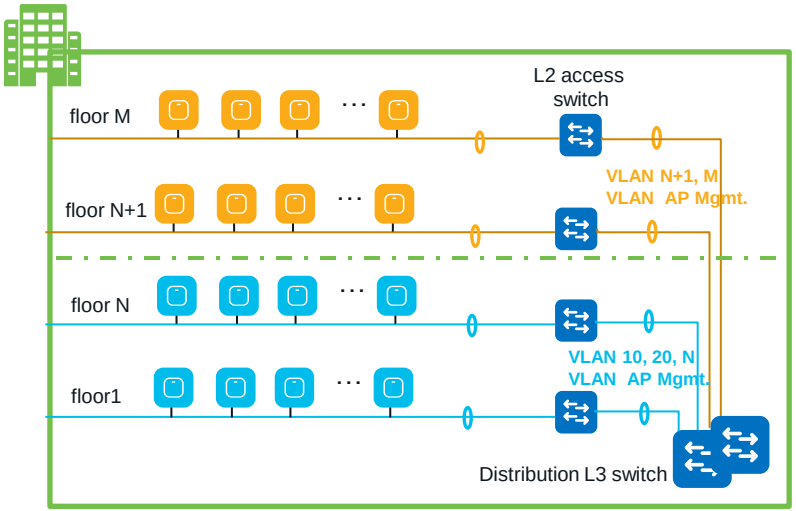
- L2 broadcast boundary at the building distribution switch
- Different client and AP VLANs at each floor
- AP switchports configured as trunks (one AP management VLAN and client VLANs for each floor
- Choose subnet mask to accommodate the expected # of devices per VLAN per floor (VLAN pooling in R30)
- Use Stack/VSL technology at L3 switch to reduce impact of spanning tree
- Configure 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



On prem



Mixed L2/L3 roaming Deployment:

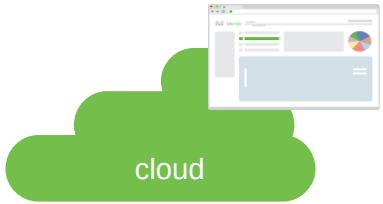
- Roaming domain = building
- AP per roaming domain > 200
- VLAN design = VLANs span a group of floors/area

Design Recommendations:

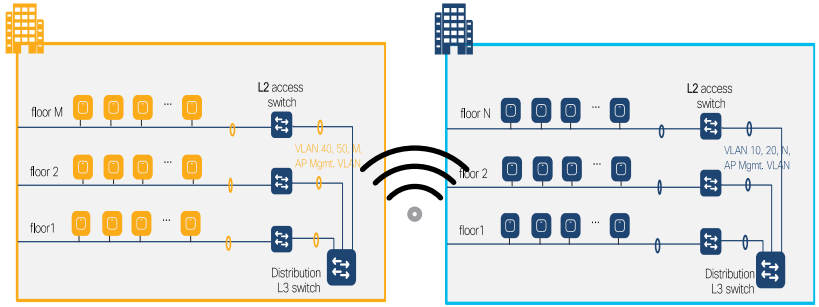
- L2 broadcast boundary at the building distribution switch
- Different client and AP VLANs for group of floors
- AP switchports configured as trunks (one AP management VLAN and different client VLANs for each area)
- Choose subnet mask to accommodate the expected # of devices per VLAN, per area (VLAN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

Large scale wireless deployment

Scenario 4



On prem



outdoor coverage or RF leaking between buildings

L3 roaming across buildings Deployment:

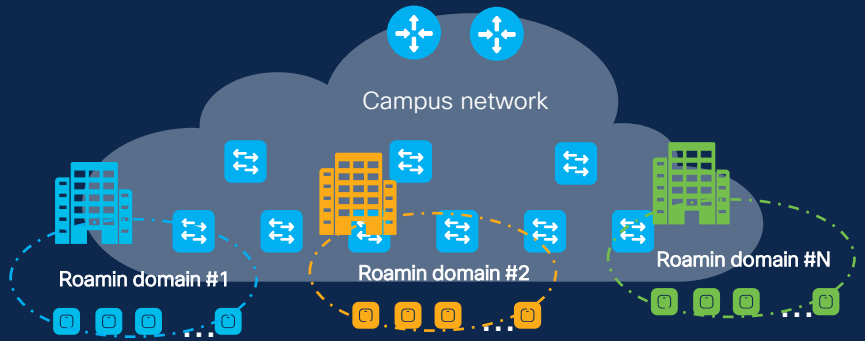
- Roaming domain = multiple buildings
- AP per roaming domain > 200
- VLAN design = VLANs span a single building

Design Recommendations:

- L2 broadcast boundary at each building distribution switch
- AP switchports configured as trunks (common AP management VLAN and client VLANs on all switches in each building)
- 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 L2 roaming within each building and distributed L3 roaming (DL3R) to cover roaming between buildings.
- Supported with caveats (802.11r is not tested at scale with DL3R)

Conclusion

Cisco Meraki Wireless: Ready for Enterprise



1000s of APs and clients

Is Meraki ready for Enterprise?

- Yes! 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!

Meeting our customers where they are

On-prem

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

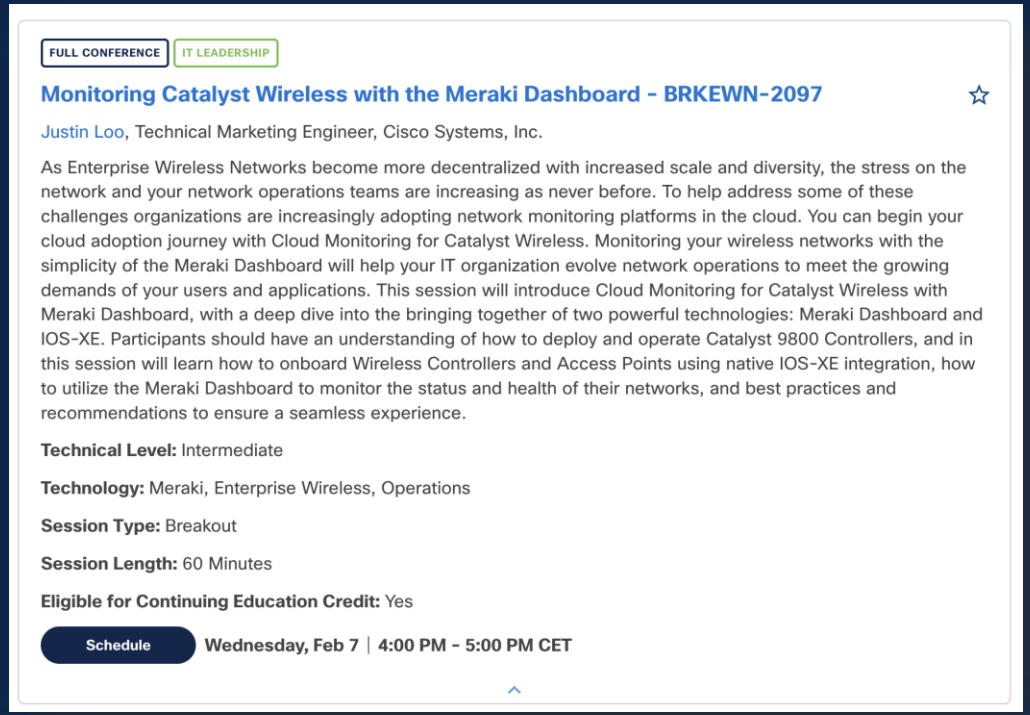
Cloud first

Prefer cloud-enabled delivery for simplicity. SaaS IT model

Cisco Wireless Mission: Deliver simplified outcomes to **all customers**

Cisco Wireless = Architecture flexibility

Cloud Monitoring for Catalyst Wireless



- If you want to start your journey to cloud…
- Protect your on-prem investment in Catalyst wireless and star enjoying the benefits of Cloud management like Scalability and Flexibility


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go

AP Neighbors feature

Roaming Analytics feature