The bridge to possible

# Designing the Right Enterprise Wireless Architecture for Challenging Environments

(On-Premises, Cloud, and Hybrid)

Alan Dumdei TSA
LinkedIn: aldumdei

BRKEWN-2054

#CiscoLive

# Cisco Webex App

## Questions?

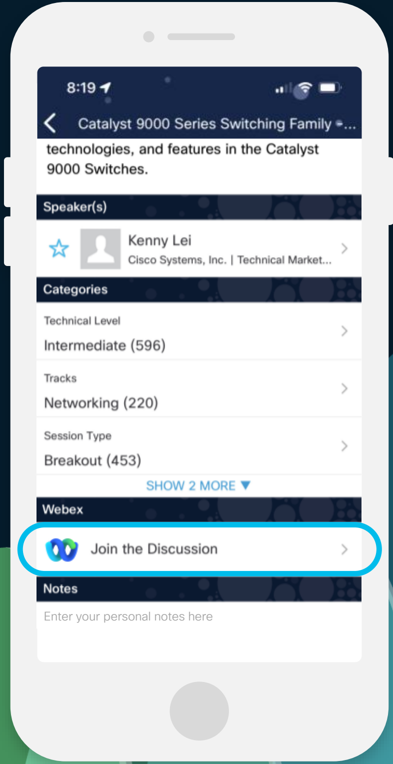
Use Cisco Webex App to chat
with the speaker after the session

## How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKENW-2054



8:19

Catalyst 9000 Series Switching Family -...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

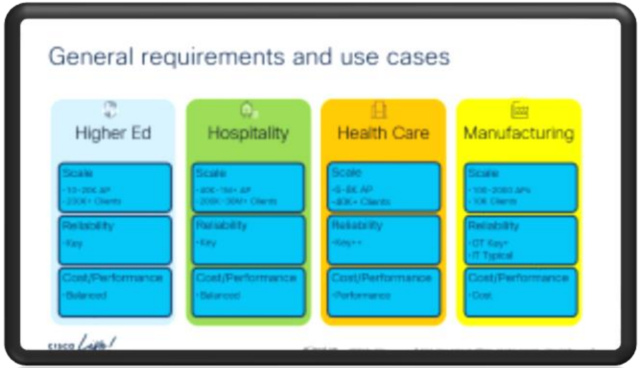
Notes

Enter your personal notes here

# Agenda

- Understanding of some of the challenges of complex wireless environments.
- Be able to relate these challenges and solutions to your network.
- Arm you with:
  - Mapping Vertical, use cases, and architectures.
  - Solutions and work arounds
  - Things to watch out for
  - Tools to help you in your wireless deployment

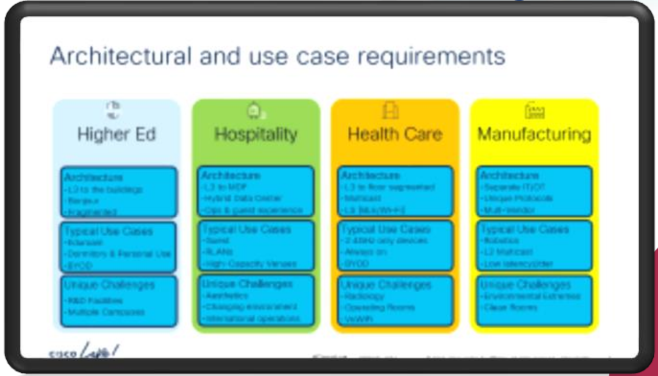
# General Design



General requirements and use cases

| Higher Ed | Hospitality | Health Care | Manufacturing |
|---|---|---|---|
| Scale<br>-10-20K AP<br>-200K+ Clients | Scale<br>-40K-1M+ AP<br>-200K-30M+ Clients | Scale<br>-5-8K AP<br>-80K+ Clients | Scale<br>-100-2000 APs<br>-10K Clients |
| Reliability<br>-Key | Reliability<br>-Key | Reliability<br>-Key++ | Reliability<br>-OT Key+<br>-IT Typical |
| Cost/Performance<br>-Balanced | Cost/Performance<br>-Balanced | Cost/Performance<br>-Performance | Cost/Performance<br>-Cost |

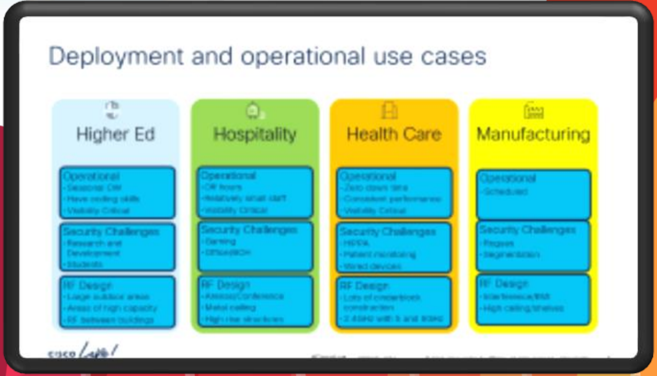
# Architectural Design



Architectural and use case requirements

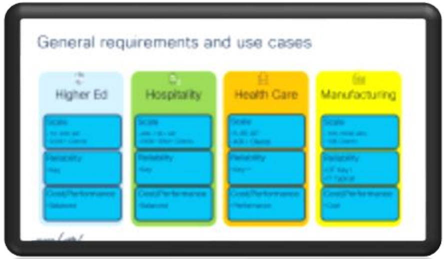
| Higher Ed | Hospitality | Health Care | Manufacturing |
|---|---|---|---|
| Architecture<br>-L2 to the buildings<br>-[illegible]<br>-Fragmented | Architecture<br>-L3 to MDF<br>-Hybrid Data Center<br>-Ops & guest experience | Architecture<br>-L3 to floor segmented<br>-Multicast<br>-L3 [illegible] | Architecture<br>-Separate IT/OT<br>-Unique Protocols<br>-Multi-Vendor |
| Typical Use Cases<br>-Eduroam<br>-Dormitory & Personal Use<br>-BYOD | Typical Use Cases<br>-Guest<br>-RLANs<br>-High Capacity Venues | Typical Use Cases<br>-2.4GHz only devices<br>-Always on<br>-BYOD | Typical Use Cases<br>-Robotics<br>-L2 Multicast<br>-Low latency/order |
| Unique Challenges<br>-R&D Facilities<br>-Multiple Campuses | Unique Challenges<br>-Aesthetics<br>-Changing environment<br>-International operations | Unique Challenges<br>-Radiology<br>-Operating Rooms<br>-VoWifi | Unique Challenges<br>-Environmental Extremes<br>-Clean Rooms |

# Deployment



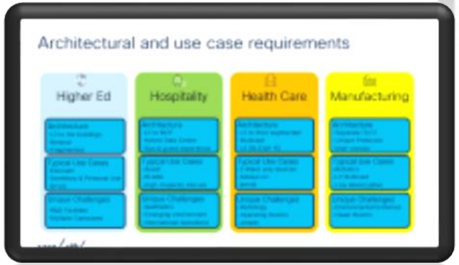
Deployment and operational use cases

| Higher Ed | Hospitality | Health Care | Manufacturing |
|---|---|---|---|
| Operational<br>-Seasonal [illegible]<br>-Have coding skills<br>-Visibility Critical | Operational<br>-Off hours<br>-Relatively small staff<br>-Visibility Critical | Operational<br>-Zero down time<br>-Consistent performance<br>-Visibility Critical | Operational<br>-Scheduled |
| Security Challenges<br>-Research and Development<br>-Students | Security Challenges<br>-Gaming<br>-[illegible] | Security Challenges<br>-HIPAA<br>-Patient monitoring<br>-Wired devices | Security Challenges<br>-Rogues<br>-Segmentation |
| RF Design<br>-Large outdoor areas<br>-Areas of high capacity<br>-RF between buildings | RF Design<br>-Arenas/Conference<br>-Metal ceiling<br>-High rise structures | RF Design<br>-Lots of concrete/brick construction<br>-2.4GHz with 5 and 6GHz | RF Design<br>-Interference/EMI<br>-High ceiling/shelves |



General requirements and use cases

Higher Ed | Hospitality | Health Care | Manufacturing



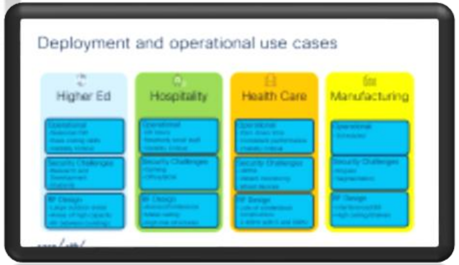
Architectural and use case requirements

Higher Ed | Hospitality | Health Care | Manufacturing

## Design

- Design Constructs
- Architectures
- HA
- Multicast

Cloud
On Prem
Hybrid



Deployment and operational use cases

Higher Ed | Hospitality | Health Care | Manufacturing

## Deploy

- iPSK/UDN/WPN
- RF Design
- Security
- WNCd

# General requirements and use cases

## Higher Ed

### Scale

- 10-20K AP
- 200K+ Clients

### Reliability

- Key

### Cost/Performance

- Balanced

## Hospitality

### Scale

- 40K-1M+ AP
- 200K-30M+ Clients

### Reliability

- Key

### Cost/Performance

- Balanced

## Health Care

### Scale

- 6-8K AP
- 40K+ Clients

### Reliability

- Key++

### Cost/Performance

- Performance

## Manufacturing

### Scale

- 100-2000 APs
- 10K Clients

### Reliability

- OT Key+
- IT Typical

### Cost/Performance

- Cost

# Architectural and use case requirements

## Higher Ed

### Architecture
- L3 to the buildings
- Bonjour
- Fragmented

### Typical Use Cases
- Eduroam
- Dormitory & Personal Use
- BYOD

### Unique Challenges
- R&D Facilities
- Multiple Campuses

## Hospitality

### Architecture
- L3 to MDF
- Hybrid Data Center
- Ops & guest experience

### Typical Use Cases
- Guest
- RLANs
- High-Capacity Venues

### Unique Challenges
- Aesthetics
- Changing environment
- International operations

## Health Care

### Architecture
- L3 to floor segmented
- Multicast
- LS (BLE/Wi-Fi)

### Typical Use Cases
- 2.4GHz only devices
- Always on
- BYOD

### Unique Challenges
- Radiology
- Operating Rooms
- VoWiFi

## Manufacturing

### Architecture
- Separate IT/OT
- Unique Protocols
- Mult-Vendor

### Typical Use Cases
- Robotics
- L2 Multicast
- Low latency/jitter

### Unique Challenges
- Environmental Extremes
- Clean Rooms

# Deployment and operational use cases

## Higher Ed

Operational
- Seasonal CW
- Have coding skills
- Visibility Critical

Security Challenges
- Research and Development
- Students

RF Design
- Large outdoor areas
- Areas of high capacity
- RF between buildings

## Hospitality

Operational
- Off hours
- Relatively small staff
- Visibility Critical

Security Challenges
- Gaming
- Office/BOH

RF Design
- Arenas/Conference
- Metal ceiling
- High rise structures

## Health Care

Operational
- Zero down time
- Consistent performance
- Visibility Critical

Security Challenges
- HIPPA
- Patient monitoring
- Wired devices

RF Design
- Lots of cinderblock construction
- 2.4GHz with 5 and 6GHz

## Manufacturing

Operational
- Scheduled

Security Challenges
- Rogues
- Segmentation

RF Design
- Interference/EMI
- High ceiling/shelves

# Design Constructs

# Wired considerations for wireless architectures

## Switching

- L3/L2/Trunk challenges
  - Switching/Routing
  - Roaming
- PoE

## Segmentation

- VLAN
- VRF
- SGT
- Fabric

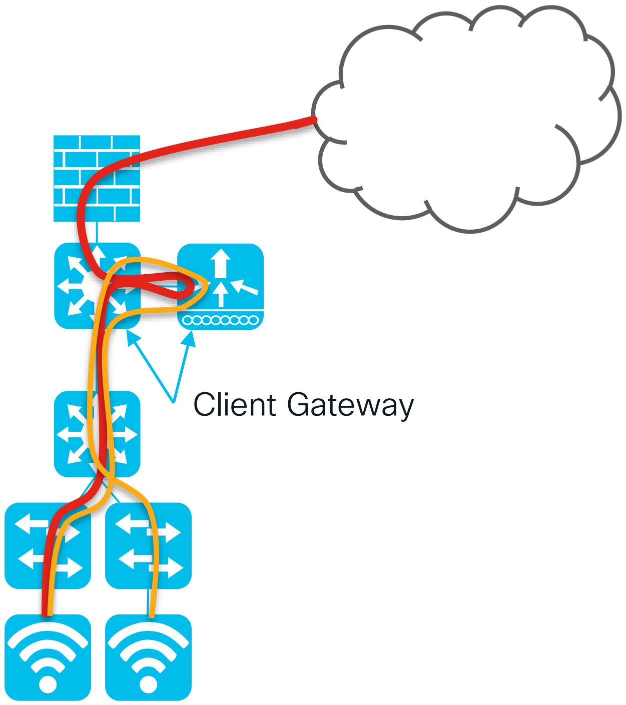
## Gateway Requirements

- CAM Table
- Throughput
- IP helper

## Cloud Considerations

- Private vs Public
- Must be FlexConnect LS
- Manageability

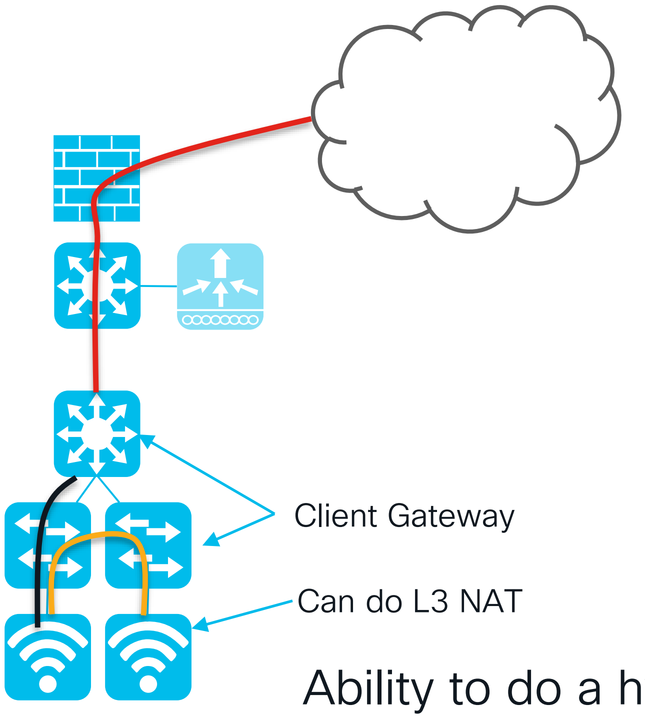
# Some Basics – Central Switching



Central Switching/Tunnel

- Data plane terminates in the WLC
- Central authentication
- Central key management
- Central RRM
- Central Policy/ACLs

# Some Basics – Locally Switched



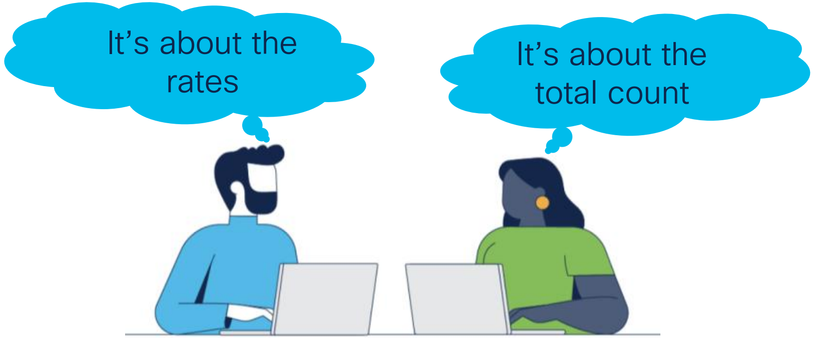
Local Switching/L2

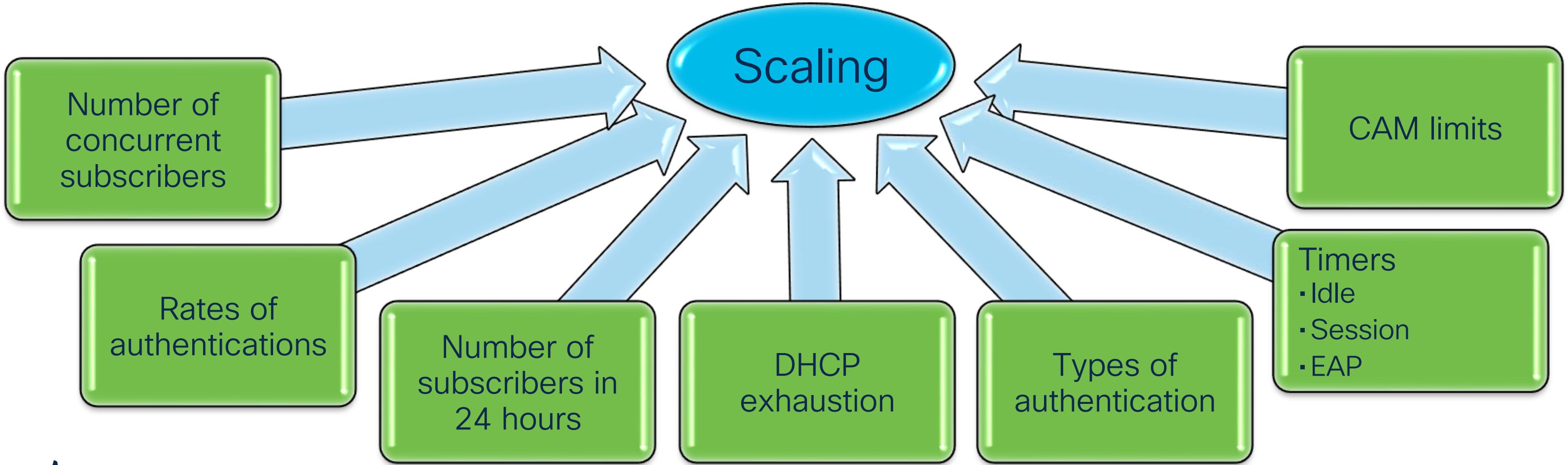
- Data plane terminates in access switch
- Local or Central authentication
- Central key management for FLEX
- Peer-to-Peer Key management for Meraki
- Central RRM (controller or cloud)
- Local Policy/ACLs

Ability to do a hybrid approach with some SSIDs local and some centrally switched

# Think scale!

Wait not that kind of scale!


It's about the rates
It's about the total count


Scaling
Number of concurrent subscribers
Rates of authentications
Number of subscribers in 24 hours
DHCP exhaustion
Types of authentication
Timers
- Idle
- Session
- EAP
CAM limits

# AAA Scale for Wireless

Number of Servers =T/R

Number of Servers =F*T/R

Consider multiple auths per client

**R** = TPS/Server, **T** = Average client device auth in peak period
**F** = ratio of auths to clients (some client devices may auth more than once in busy window or clients have multiple devices)

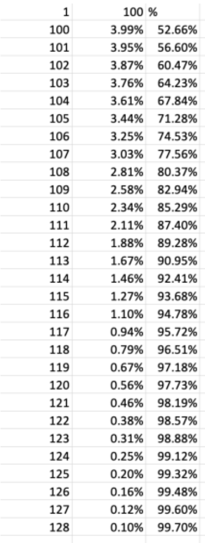
Things to consider:

- Mobile endpoints reauth much more frequent, assume 10 time per hour
- TPS is a peak number not an average
- These numbers apply to both authenticator and server

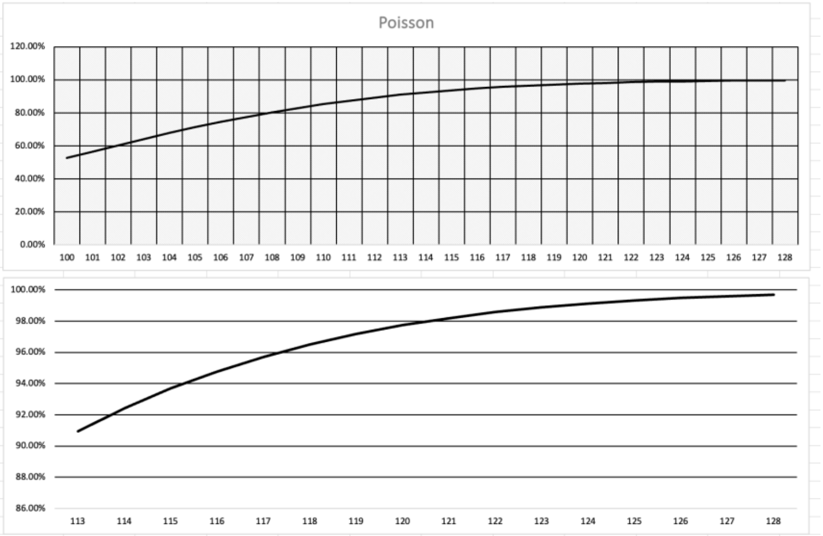
# ...and then there is queuing theory!

- Poisson distribution accepted method for queuing calculations
- This accounts for not all transactions are queued sequentially
- Example, if you wanted 99% success in peak busy hour P=1.26

P= Peak to average based on Poisson Theorem



| 1 | 100 | % |
|---|---|---|
| 100 | 3.99% | 52.66% |
| 101 | 3.95% | 56.60% |
| 102 | 3.87% | 60.47% |
| 103 | 3.76% | 64.23% |
| 104 | 3.61% | 67.84% |
| 105 | 3.44% | 71.28% |
| 106 | 3.25% | 74.53% |
| 107 | 3.03% | 77.56% |
| 108 | 2.81% | 80.37% |
| 109 | 2.58% | 82.94% |
| 110 | 2.34% | 85.29% |
| 111 | 2.11% | 87.40% |
| 112 | 1.88% | 89.28% |
| 113 | 1.67% | 90.95% |
| 114 | 1.46% | 92.41% |
| 115 | 1.27% | 93.68% |
| 116 | 1.10% | 94.78% |
| 117 | 0.94% | 95.72% |
| 118 | 0.79% | 96.51% |
| 119 | 0.67% | 97.18% |
| 120 | 0.56% | 97.73% |
| 121 | 0.46% | 98.19% |
| 122 | 0.38% | 98.57% |
| 123 | 0.31% | 98.88% |
| 124 | 0.25% | 99.12% |
| 125 | 0.20% | 99.32% |
| 126 | 0.16% | 99.48% |
| 127 | 0.12% | 99.60% |
| 128 | 0.10% | 99.70% |



TPS Required = F*P*T

Number of Servers =F*P*T/R

# TPS Example

Peak busy period = 5 minutes
Clients/busy period = 50000
T = 50000/(5*60) = 167 auth/second
F = 1.2 (20% of the clients will auth 2x in the 5-minute window)
P = 1.3 (Increase by 30% to go from average to peak for 99th %)

Peak TPS required = T*F*P = 260 TPS (Plus Redundancy)

ISE Scale numbers (remember looks at **RADIUS Authentication Rates** for TPS)
https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html

# Timers, Timeout, Age Out...

| Affecting | Timer | Range | Default Catalyst | Default Meraki | Best Practice | | Notes |
|---|---|---|---|---|---|---|---|
| EAPOL | EAPOL-Key timeout | 200-5000 (ms) | 1000 | 500 | 400-1000 | | 400ms is mostly OK, only be careful on slow client devices |
| | EAPOL-Key retries | 0-4 (x) | 2 | 4 | 2 | | Best practice is 0 for security reasons but test to be sure it is ok. |
| | EAPOL Group-Key Request | 120-86400 (sec) | 3600 | 500 | 3600 | | Clients must answer this...Standard is 30 seconds default is 10. Must be greater than Idle timeout |
| | Identity Request Timeout | 0-120 (sec) | 30 | 5 | 30 | | 30-60 is good for OTP/smart card. Otherwise lower values are better |
| | Identity request retries | 0-20 (x) | 2 | 5 | 2 | | |
| | dot1x request timeout | 0-120 (sec) | 30 | | 30 | | |
| | dot1x request retries | 0-20 (x) | 2 | | 2 | | |
| | | | | | | | |
| Client | Session timeout | 300 - 86400 (sec) | 1800 | | 28800 | | if user configures any value between 0 (included) and 300 seconds, the session timeout is set automatically to 86400 seconds (24 hours), which is the maximum supported value. Also WEB_AUTH_REQUIRED and POSTURE_REQUIRED time out in 10 minutes regardless. Note, only non-dot1x can go below 300 |
| | Exclusion Timeout | | 180 | | 60 | | This is really just to prevent DOS to AAA for bad acting clients so best to change under the WLAN |
| | Idle timeout | | 300 | 35* | 300-3600 | | High density closer to 300, lower density closer to 600 (prevent Client exhaution) |
| | Idle Threshold | | 0 | | | | |
| | | | | | | | |

* Not configurable

# Timers, Timeout, Age Out…

| Affecting | Timer | Range | Default Catalyst | Default Meraki | Best Practice | | Notes |
|---|---|---|---|---|---|---|---|
| Radius | Retransmit count | 0 - 100 (x) | 3 | 3 | | | Can be set on server or global |
| | Timeout | 0-1000 (s) | 5 | 1 | 5-10 | | Can be set on server or global |
| | Dead Time | 1-1440 (s) | 3 | | 5 | | How long server stays marked as dead before trying again (can set up a probe to test before using dead server) |
| | Dead Criteria Time | 1-120 (s) | 10 | | 5 | | |
| | Dead Critera Tries | 1-100 (s) | 10 | | 3 | | |
| | | | | | | | |
| DHCP | IP Learn timeout | 120 (s) | 120 | | | | Fixed |
| | | | | | | | |
| IP | ARP Timeout | 14400 (s) | 14400 | | | | |
| | MAC address-table aging-time | 10-1000000 (s) | 300 | | | | |
| | CDP Hold Time | | | | | | |
| | CDP Timer | 5-254 (s) | | | | | |
| | | | | | | | |
| | Sleeping Client Timeout | 60-35791 | 720m | | | | Disabled for Passive Clients.  The timeout is in minutes and is typically configured to suite the Web auth network requirements. |
| | | | | | | | |
| RF | Band Select Cycle Threshold | 1-1000 (ms) | 200 (ms) | | | | Works with Cycle Count (1-10) |
| | Age Out Supression | 10-200 (s) | 20 (s) | | | | |
| | Age Out Dual Band | 10-300 (s) | 60 (s) | | | | |

# Understanding Wireless Scale (as it is today)

## Catalyst

WLC scales up to 6000 AP, 64K clients each

A Mobility Group can include up to 24 WLCs of any type

L2 roaming across 144K APs and 1536K clients

A single WLC can support up to 72 controllers in a mobility list (multiple groups)

128 Telemetry Subscriptions

## Meraki

Network scales to 1000 APs and 50K (75K with NFO) clients

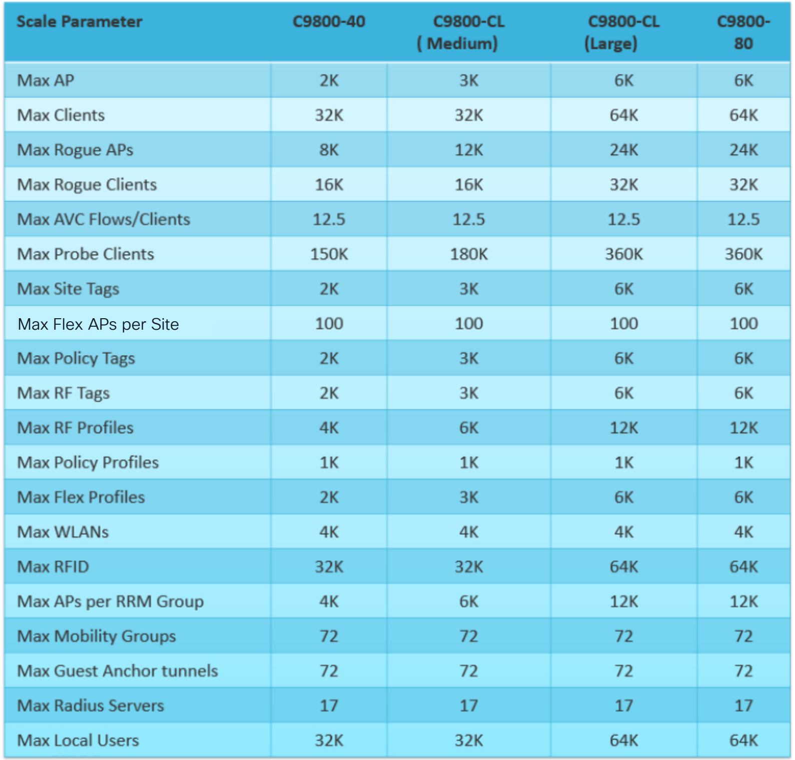
Organization scales to 25000 devices (APs) and 20K Networks

Organizations can be formed on logical or geographic demarcation (ex different countries with different regulatory requirements)

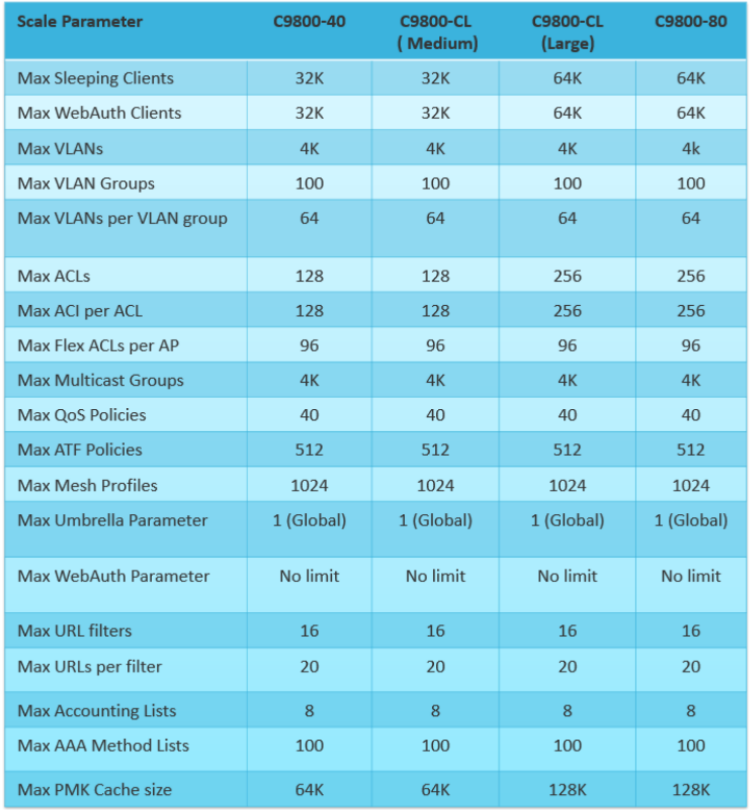
10 API Calls per second per Organization

Note: Scaling beyond 80% of max is not typically recommended

# C9800 Scale Numbers

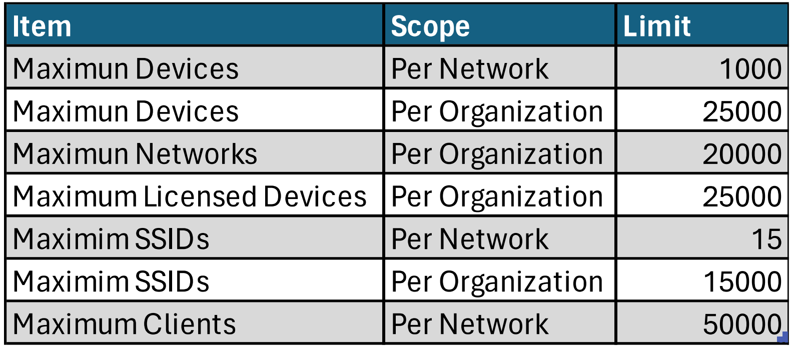


| Scale Parameter | C9800-40 | C9800-CL ( Medium) | C9800-CL (Large) | C9800-80 |
|---|---|---|---|---|
| Max AP | 2K | 3K | 6K | 6K |
| Max Clients | 32K | 32K | 64K | 64K |
| Max Rogue APs | 8K | 12K | 24K | 24K |
| Max Rogue Clients | 16K | 16K | 32K | 32K |
| Max AVC Flows/Clients | 12.5 | 12.5 | 12.5 | 12.5 |
| Max Probe Clients | 150K | 180K | 360K | 360K |
| Max Site Tags | 2K | 3K | 6K | 6K |
| Max Flex APs per Site | 100 | 100 | 100 | 100 |
| Max Policy Tags | 2K | 3K | 6K | 6K |
| Max RF Tags | 2K | 3K | 6K | 6K |
| Max RF Profiles | 4K | 6K | 12K | 12K |
| Max Policy Profiles | 1K | 1K | 1K | 1K |
| Max Flex Profiles | 2K | 3K | 6K | 6K |
| Max WLANs | 4K | 4K | 4K | 4K |
| Max RFID | 32K | 32K | 64K | 64K |
| Max APs per RRM Group | 4K | 6K | 12K | 12K |
| Max Mobility Groups | 72 | 72 | 72 | 72 |
| Max Guest Anchor tunnels | 72 | 72 | 72 | 72 |
| Max Radius Servers | 17 | 17 | 17 | 17 |
| Max Local Users | 32K | 32K | 64K | 64K |

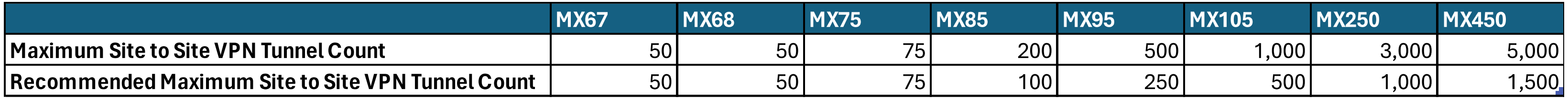


| Scale Parameter | C9800-40 | C9800-CL ( Medium) | C9800-CL (Large) | C9800-80 |
|---|---|---|---|---|
| Max Sleeping Clients | 32K | 32K | 64K | 64K |
| Max WebAuth Clients | 32K | 32K | 64K | 64K |
| Max VLANs | 4K | 4K | 4K | 4k |
| Max VLAN Groups | 100 | 100 | 100 | 100 |
| Max VLANs per VLAN group | 64 | 64 | 64 | 64 |
| Max ACLs | 128 | 128 | 256 | 256 |
| Max ACl per ACL | 128 | 128 | 256 | 256 |
| Max Flex ACLs per AP | 96 | 96 | 96 | 96 |
| Max Multicast Groups | 4K | 4K | 4K | 4K |
| Max QoS Policies | 40 | 40 | 40 | 40 |
| Max ATF Policies | 512 | 512 | 512 | 512 |
| Max Mesh Profiles | 1024 | 1024 | 1024 | 1024 |
| Max Umbrella Parameter | 1 (Global) | 1 (Global) | 1 (Global) | 1 (Global) |
| Max WebAuth Parameter | No limit | No limit | No limit | No limit |
| Max URL filters | 16 | 16 | 16 | 16 |
| Max URLs per filter | 20 | 20 | 20 | 20 |
| Max Accounting Lists | 8 | 8 | 8 | 8 |
| Max AAA Method Lists | 100 | 100 | 100 | 100 |
| Max PMK Cache size | 64K | 64K | 128K | 128K |

# Meraki Scale



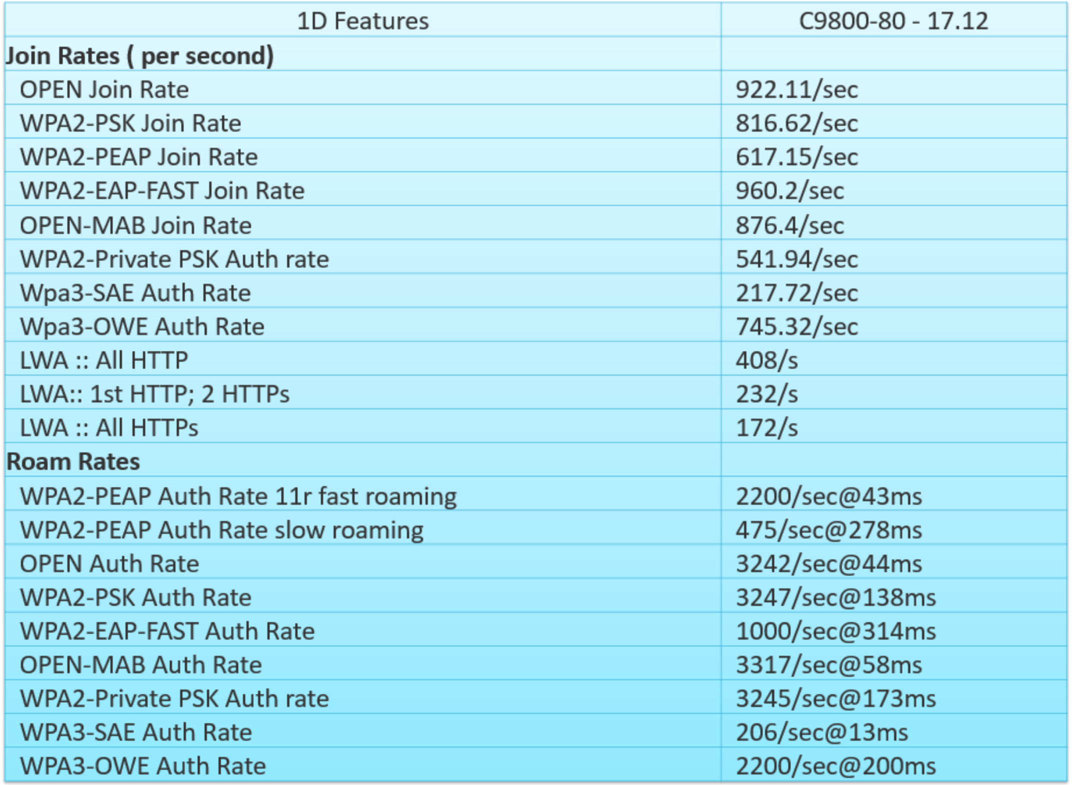
| Item | Scope | Limit |
|---|---|---|
| Maximun Devices | Per Network | 1000 |
| Maximun Devices | Per Organization | 25000 |
| Maximun Networks | Per Organization | 20000 |
| Maximum Licensed Devices | Per Organization | 25000 |
| Maximim SSIDs | Per Network | 15 |
| Maximim SSIDs | Per Organization | 15000 |
| Maximum Clients | Per Network | 50000 |



| | MX67 | MX68 | MX75 | MX85 | MX95 | MX105 | MX250 | MX450 |
|---|---|---|---|---|---|---|---|---|
| **Maximum Site to Site VPN Tunnel Count** | 50 | 50 | 75 | 200 | 500 | 1,000 | 3,000 | 5,000 |
| **Recommended Maximum Site to Site VPN Tunnel Count** | 50 | 50 | 75 | 100 | 250 | 500 | 1,000 | 1,500 |

Best practice as always not to deploy past 80% maximum

# C9800 Control Plane Performance



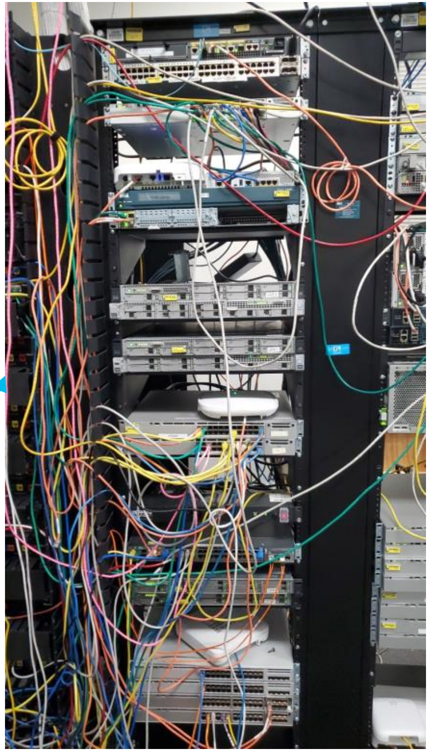
| 1D Features | C9800-80 - 17.12 |
|---|---|
| **Join Rates ( per second)** | |
| OPEN Join Rate | 922.11/sec |
| WPA2-PSK Join Rate | 816.62/sec |
| WPA2-PEAP Join Rate | 617.15/sec |
| WPA2-EAP-FAST Join Rate | 960.2/sec |
| OPEN-MAB Join Rate | 876.4/sec |
| WPA2-Private PSK Auth rate | 541.94/sec |
| Wpa3-SAE Auth Rate | 217.72/sec |
| Wpa3-OWE Auth Rate | 745.32/sec |
| LWA :: All HTTP | 408/s |
| LWA:: 1st HTTP; 2 HTTPs | 232/s |
| LWA :: All HTTPs | 172/s |
| **Roam Rates** | |
| WPA2-PEAP Auth Rate 11r fast roaming | 2200/sec@43ms |
| WPA2-PEAP Auth Rate slow roaming | 475/sec@278ms |
| OPEN Auth Rate | 3242/sec@44ms |
| WPA2-PSK Auth Rate | 3247/sec@138ms |
| WPA2-EAP-FAST Auth Rate | 1000/sec@314ms |
| OPEN-MAB Auth Rate | 3317/sec@58ms |
| WPA2-Private PSK Auth rate | 3245/sec@173ms |
| WPA3-SAE Auth Rate | 206/sec@13ms |
| WPA3-OWE Auth Rate | 2200/sec@200ms |

# Firewall Ports and Reachability

- Different services require different ports to be open for connectivity.
- This can be between devices or devices and cloud
- Config guides and release notes can be a helpful source for this information
- Two comprehensive guides are available for Catalyst and Meraki
  - Meraki - https://documentation.meraki.com/General_Administration/Other_Topics/Upstream_Firewall_Rules_for_Cloud_Connectivity
  - Catalyst - https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113344-cuwn-ppm.html

# Architecture/scale example for events center

- Conference lets out and 15K subscribers will roam from conference center to the hotel.
  - Using open SSID with Web Auth (as an example)
  - Watch out for “Pull out your phones and…”
  - RF discussion not covered here (in RF Design Section).
  - Central Switching used to minimize large L2 domains (L3 to the AP) but similar design considerations are made for local switching.

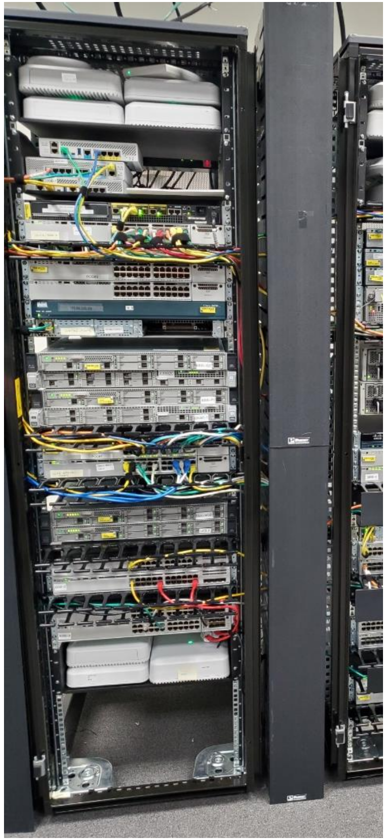


Know your requirements first!!

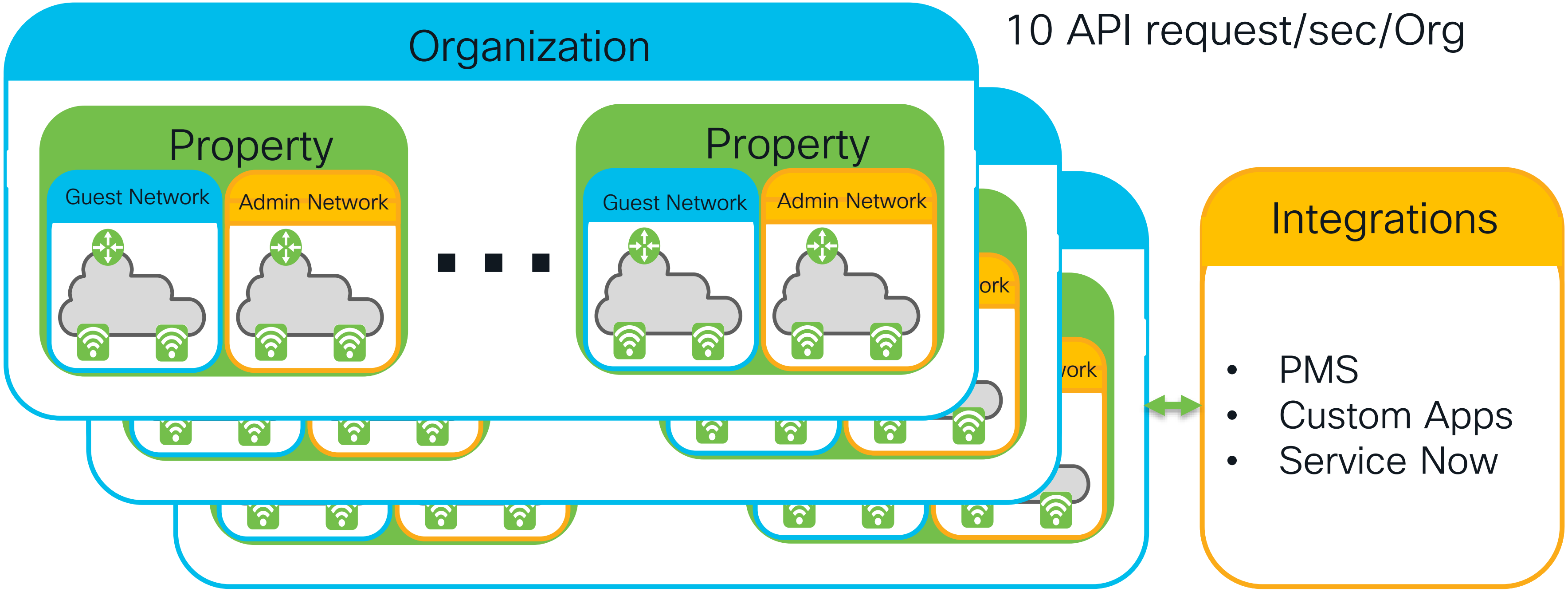
# Architecture/scale example for events center

## Design considerations (PLAN!)

- Where are the L3 roaming boundaries?
- Dot1x authentication rates (75-150 Auth/sec per node depending on types)
- MAB (400+ Auth/sec per node depending on type)
- 15K concurrent subscribers (AAA/WLC/DHCP/Switch)
  - CAM table on core switch…are there multiple controllers?  Multiple hops to GW?
  - Subnet sizes/VLAN Groups
- Enable Proxy ARP to minimize broadcast/unicast traffic
- Pure capacity phones (1-8Mbps streaming) target < 100 clients per AP/Radio
- Idle timer
  - Reducing this will help with WLC capacity
  - Increasing this will reduce re-authentication as clients sleep, move, etc.



# How to scale cloud horizontally



10 API request/sec/Org

- PMS
- Custom Apps
- Service Now

# Example two large hospitality customers

Reduced tickets by 10x

Worldwide Scale:

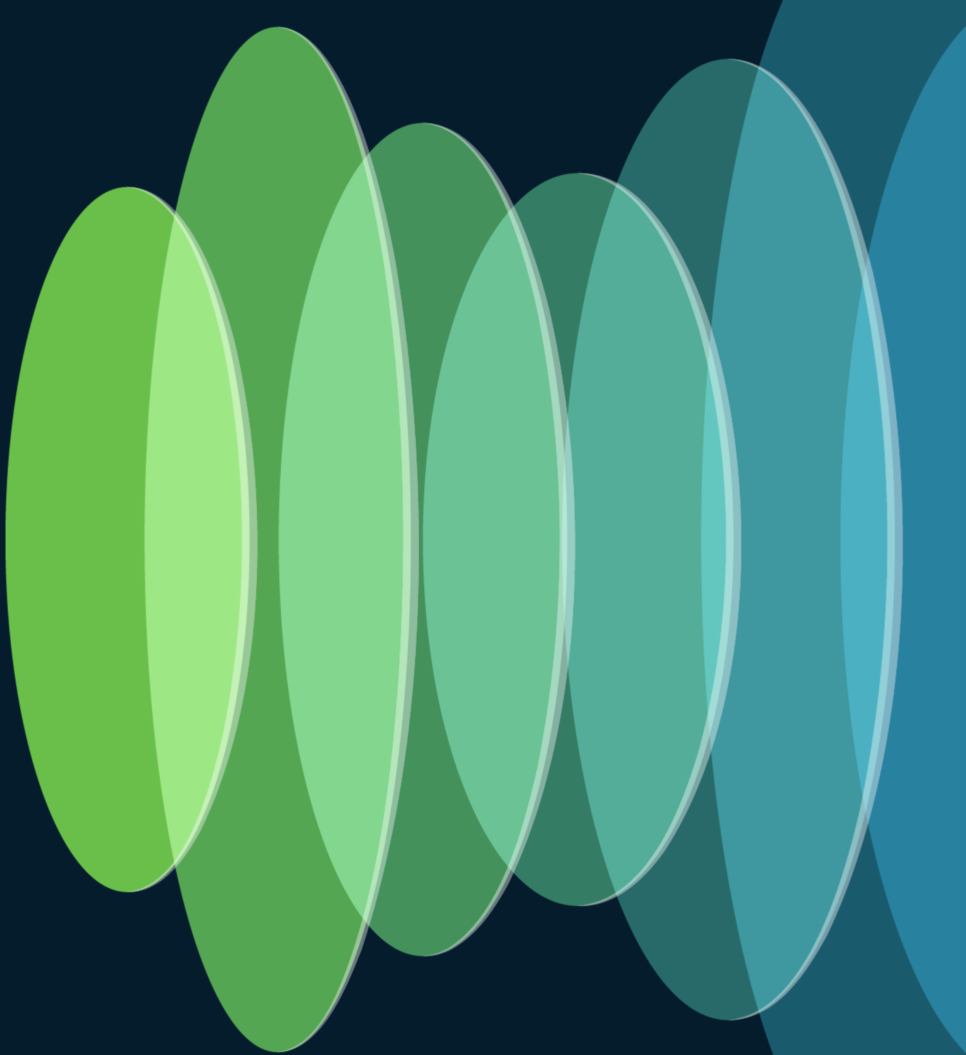
- 1 New property every 36 hours
- 44 Organizations (align with countries and logical divisions)
- 16000 Networks (two per hotel, Admin and Guest)
- 1.2M APs
- 30M clients

Process:

- Hotel Owner picks integrator
  - Design/Survey
  - Maps, Networks, Device configurations and Organizations as required
- Automation with APIs key to making this sort of scale work.

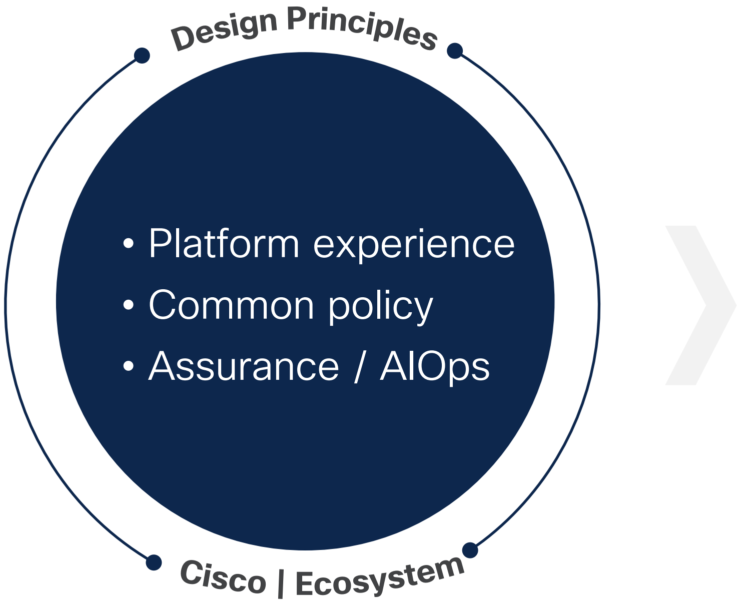
# Architectures

## What are the options and why would one fit better than the other?



# Key design principles for **Campus and Branch**

## Cisco Networking Cloud



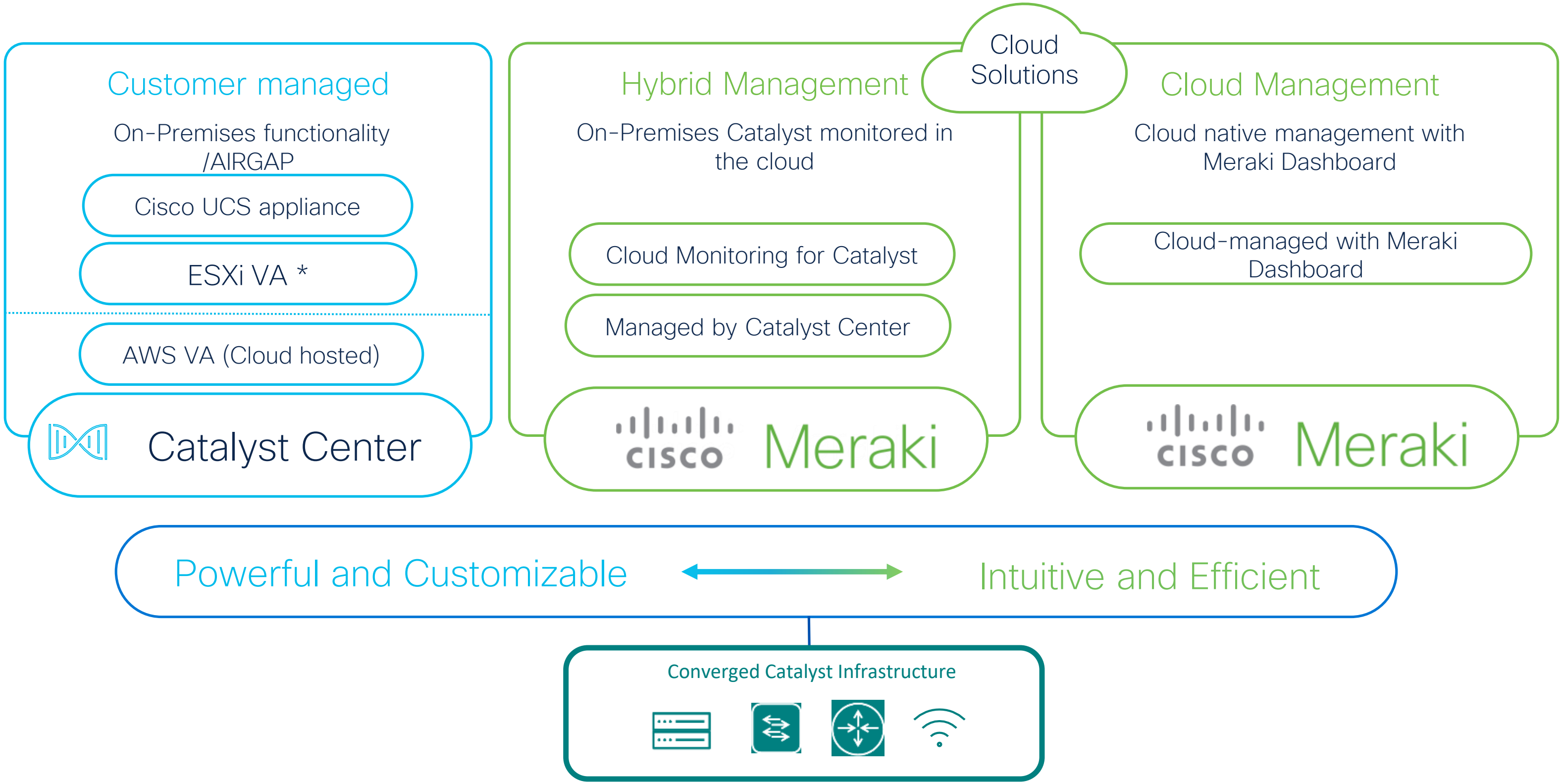
- Platform experience
- Common policy
- Assurance / AIOps

Digital Experience Assurance

Simplified, AI-Native Operations

End-to-End Secure Networking

# Meeting Our Customers Where they are



Cloud Solutions

Customer managed

On-Premises functionality /AIRGAP

Cisco UCS appliance

ESXi VA *

AWS VA (Cloud hosted)

Catalyst Center

Hybrid Management

On-Premises Catalyst monitored in the cloud

Cloud Monitoring for Catalyst

Managed by Catalyst Center

cisco Meraki

Cloud Management

Cloud native management with Meraki Dashboard

Cloud-managed with Meraki Dashboard

cisco Meraki

Powerful and Customizable ⟷ Intuitive and Efficient

Converged Catalyst Infrastructure

* DN-SW-APL (90-day lead time) – Scaled to 44 core parity

# Controller / Centralized Data Plane

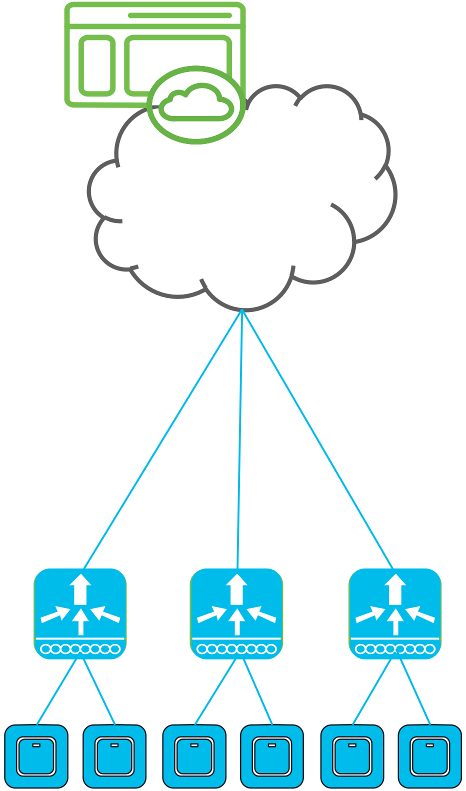
1RU

**CW9800H1 / CW9800H2**
6000 APs, 64,000 clients,
4 x 25Gbps / 2 x 40Gbps

**CW9800M**
3000 APs**,** 32,000 clients
4 x 10Gbps and 2 x 25Gbps

- Supports all APs not currently past end of support
- Feature compatibility with 9800- controllers
- Interoperable with 9800- controllers
  - Mobility L2/L3
  - RRM
  - Anchors

# Cloud Monitored C9800 Wireless Controller



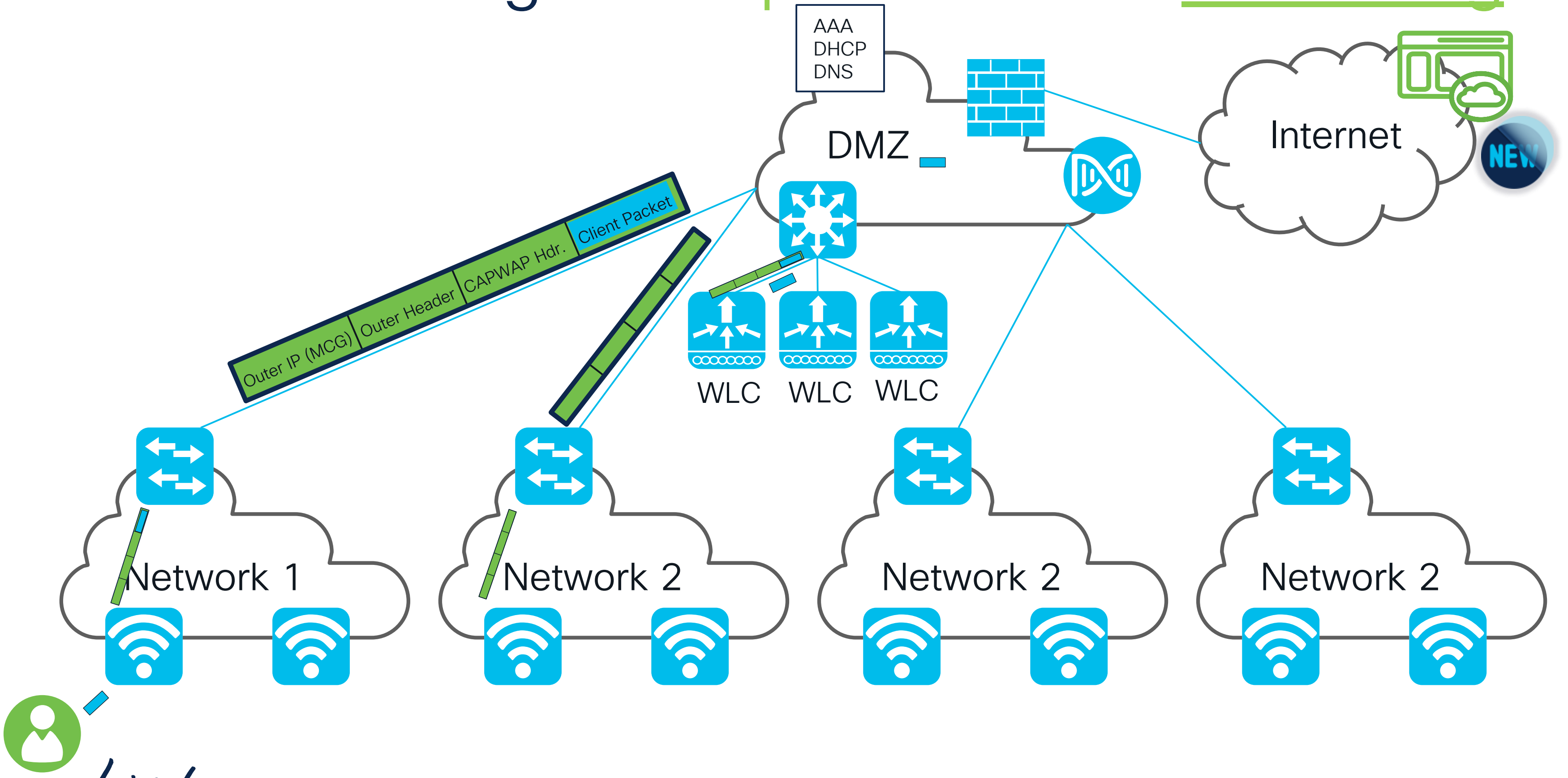
| Requirements | |
|---|---|
| Software | |
| | Cisco IOS® XE 17.12.3 |
| Licensing | |
| | Cisco DNA Essentials<br>Cisco DNA Advantage |

**Table 2. Firmware and scale support[1]**

| Wireless LAN Controller | | Meraki dashboard |
|---|---|---|
| Firmware: IOS XE 17.12.3/17.15.1 or later | | |
| Catalyst 9800-L | Up to 250 access points/3000 clients | 25,000 total devices per organization |
| Catalyst 9800-40 | Up to 1300 access points/10,000 clients | 1000 devices per network |
| Catalyst 9800-80 | Up to 2000 access points/20,000 clients | 50,000 clients per network |

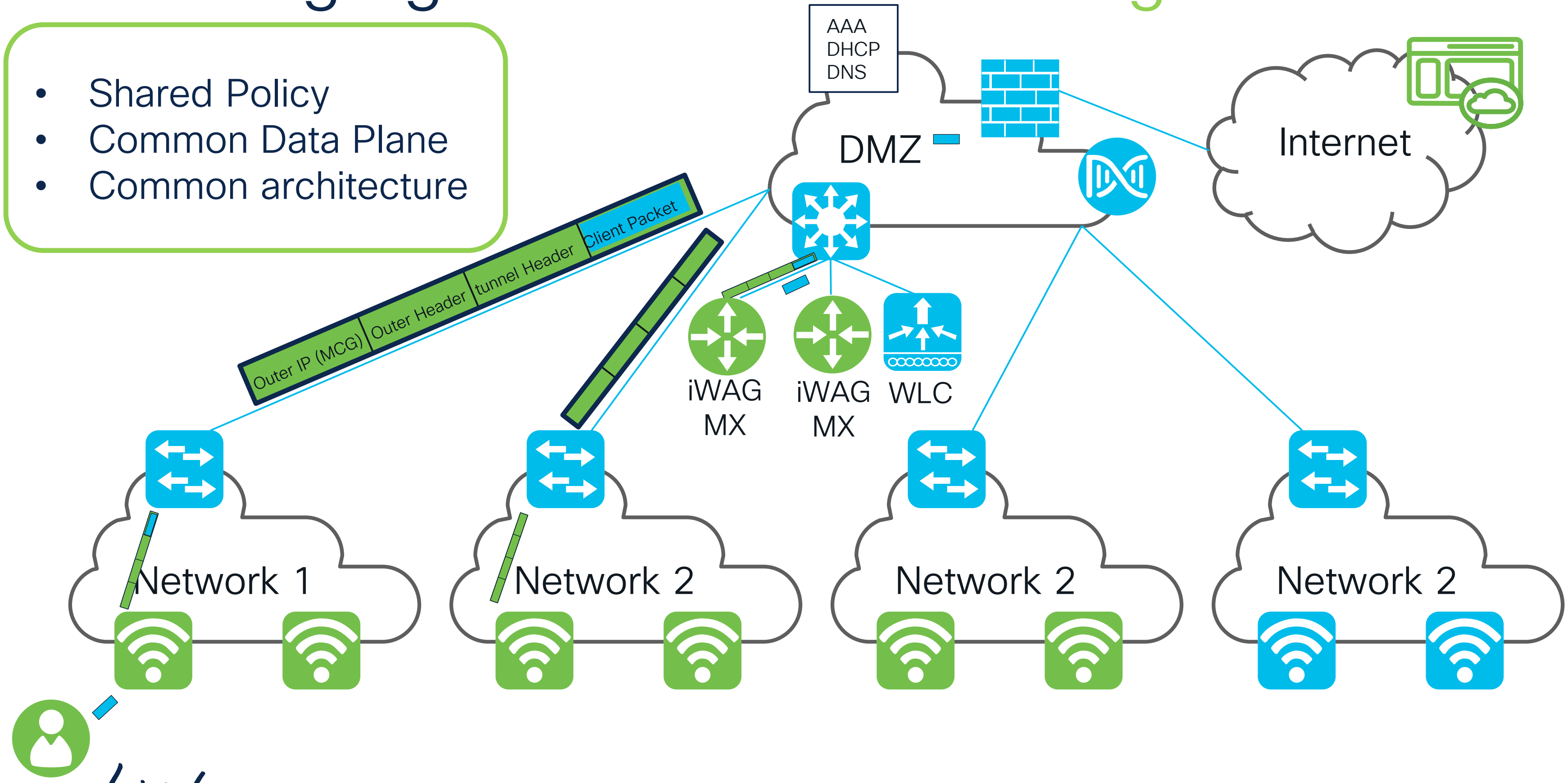
[1]Scale to be supported at launch contingent upon final testing

# Central Switching with Optional Cloud Monitoring



# Central Agregation with Cloud Management!

- Shared Policy
- Common Data Plane
- Common architecture



# L3 Access in Wireless

## Network Simplification & Security

### 1 Segmentation

For Security

- Macro Segmentation with VRF Support
- Support for Overlapping IP
- Flexible routing to services

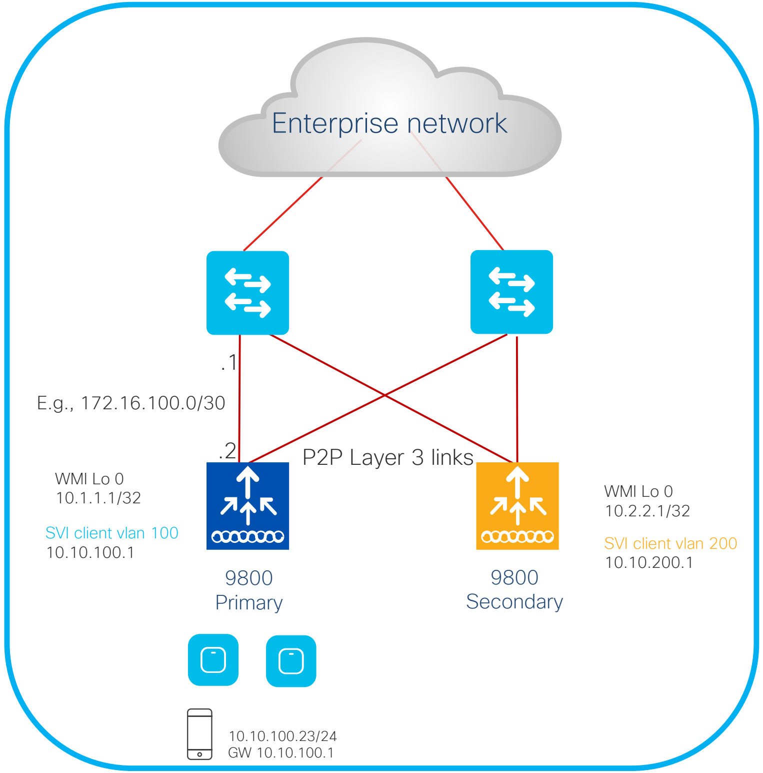
Managed Service Providers :

- Airports
- Multi-dwelling units

### 2 Optimized Network Design

- Less constrains on AGGR switch (ARP, MAC tables)
- Better load balancing and high availability with ECMP
- L3 routing based faster network reconvergence
- IOS-XE 17.13.1+

# L3 forwarding topology – Full L3 mode



All WLANs are configured for L3 forwarding

Routing and uplink load balancing, Equal Cost Multi-path (ECMP) is configured between 9800 and aggregation switches

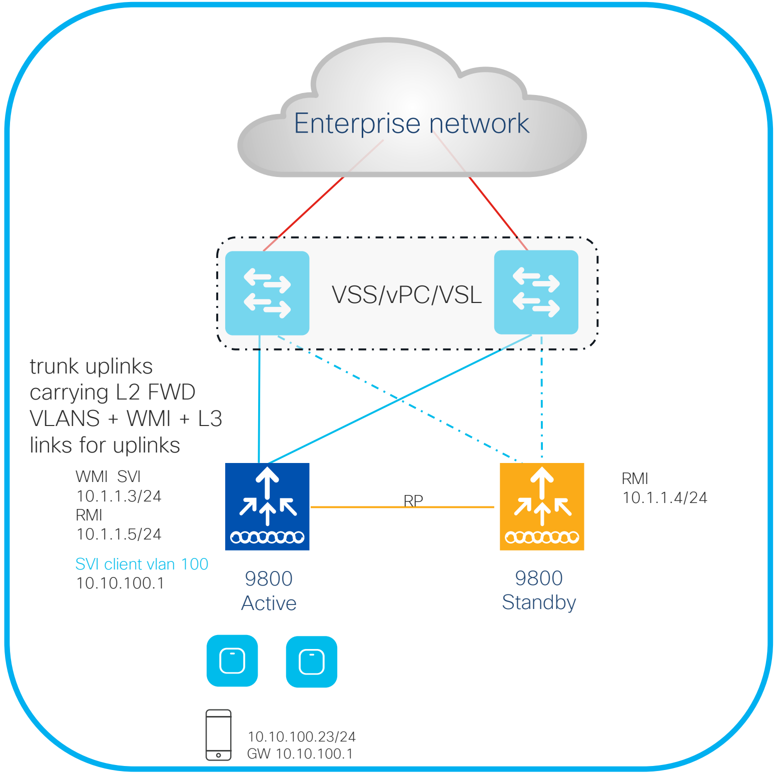
Uplinks are L3 P2P links (each uplink is usually a LAG)

WMI is on a Loopback interface

SVI for client WLANs to terminate client subnets

High Availability: N+1 Supported

# L3 forwarding topology – L3/L2 mixed mode



Mix of L2 and L3 forwarding SSIDs

Recommended wired topology: switches are configured in VSS/VSL/VPC

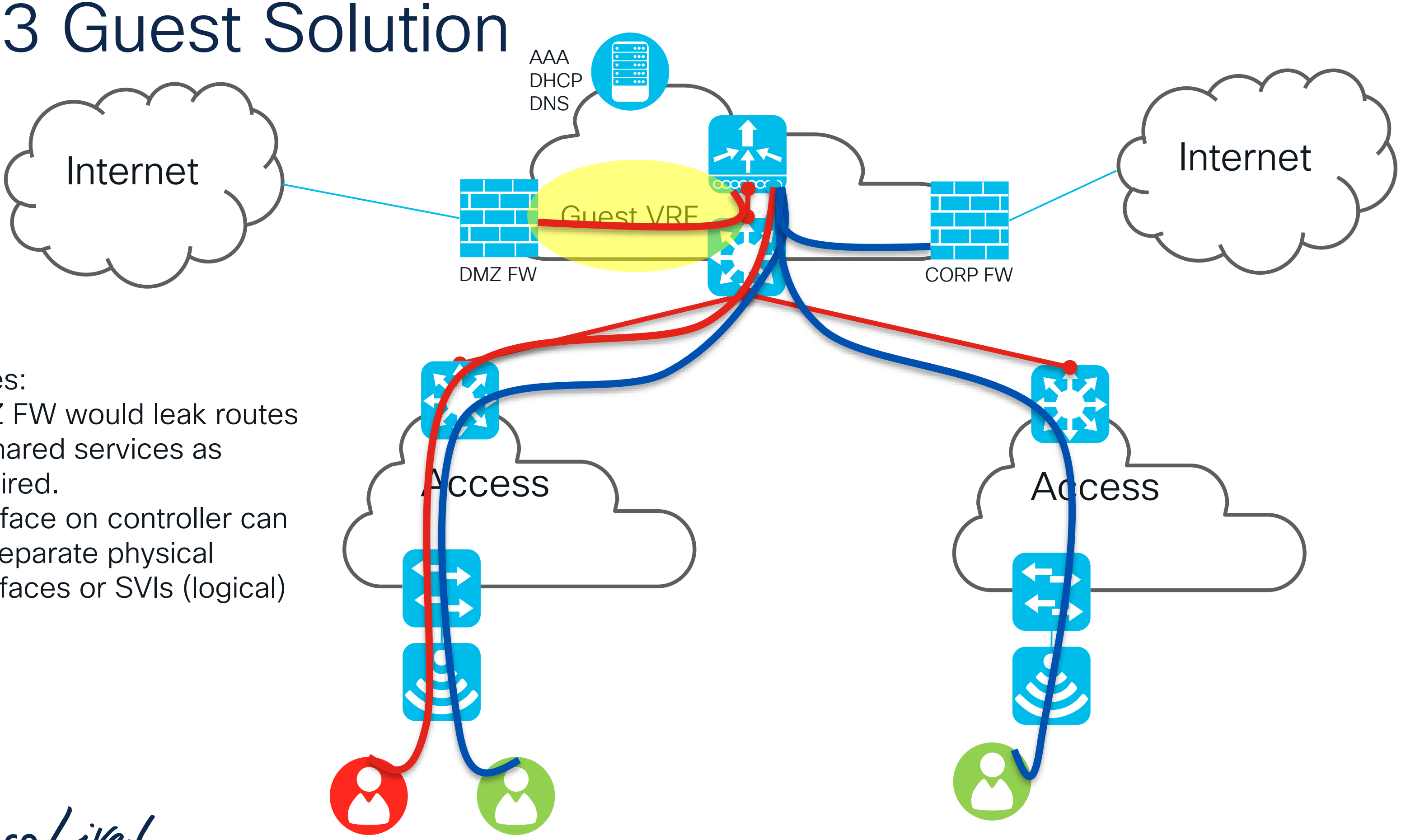
Uplinks are L2 802.1q trunks. SVIs for the P2P L3 links, and SVIs to terminate client subnets for L3 forwarding WLANs

WMI can be configured as SVI to support SSO

Uplinks are L2 802.1q trunks, SVIs for the P2P L3 links and client subnets for L3 forwarding WLANs.

High Availability: SSO or N+1 Supported

# L3 Guest Solution



Notes:
DMZ FW would leak routes to shared services as required.
Interface on controller can be separate physical interfaces or SVIs (logical)

# L3 Access – Profile Configuration

L3 Access enable/disable configuration will be available under policy profile

By default, L3 Access will be disabled under policy profile

Configuration:

```
C9800(config)# wireless profile policy [Policy Profile]
C9800(config-wireless-policy)# [no] l3-access
```

Verification:

```
#On WLC
C9800 # show wireless profile policy detailed  [Policy Profile] | inc L3
#On Specific Client
C9800 # show wireless client mac-address [Client MAC] detail | inc L3
```

# L3 Access – OSPF

OSPF can be enabled in the interfaces/SVIs with or without VRF support

## Configuration: Without VRF

```
C9800(config)#Interface [Interface name]
no switchport
ip address <IP Address> <Mask>
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 <passwd>
negotiation auto
no mop enabled
no mop sysid

router ospf 1
network <IP-Address> <mask> area 1
network <IP-Address> <mask> area 1
```

## Configuration: With VRF

```
C9800(config)#Interface [Interface name]
no switchport
 ip address <IP Address> <Mask>
 vrf forwarding <VRF Name>
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 <passwd>
 negotiation auto
 no mop enabled
 no mop sysid

router ospf 1
 network <IP-Address> <mask>area 1
 network <IP-Address> <mask>area 1
```

# L3 Access – NAT Support

## Configuration: NAT Outside

```
C9800(config)# interface [Interface name]
ip address 62.1.1.15 255.255.0.0
no ip proxy-arp
ip nat outside
end
```

## Configuration: NAT Inside

```
C9800(config)#interface [Interface name]
ip address 155.1.1.6 255.255.0.0
no ip proxy-arp
ip nat inside
end
```

## Configuration: Dynamic

```
C9800(config)# ip access-list extended Guest
10 permit ip 155.1.1.0 0.0.0.255

ip nat pool NAT_Pool 62.1.1.101 62.1.1.101 netmask 255.255.255.252
ip nat inside source list Guest pool Guest_NAT_Pool overload
```

# L3 Access – DHCP Support

## Configuration: Without VRF

```
C9800(config)#interface [Interface name]
 vrf forwarding guest
 ip address 55.55.55.2 255.255.255.0
 no ip proxy-arp
 no autostate
 no mop enabled
 no mop sysid
end
```

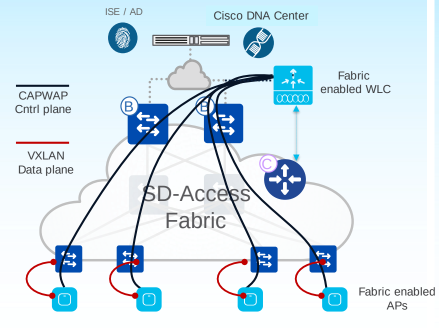
## Configuration: With VRF

```
C9800(config)# dhcp pool [Pool Name]
 vrf guest
 network 55.55.55.0 255.255.255.0
 default-router 55.55.55.2

C9800(config)# interface Loopback1
 vrf forwarding guest
 ip address 7.7.7.1 255.255.255.0
end
```

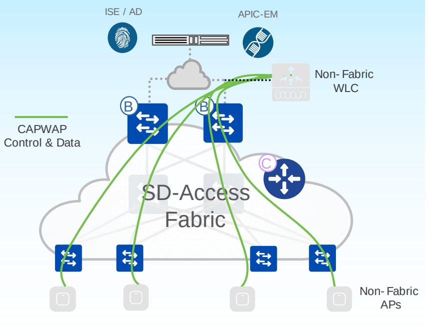
# Wireless in and on the fabric

## SD- Access Wireless



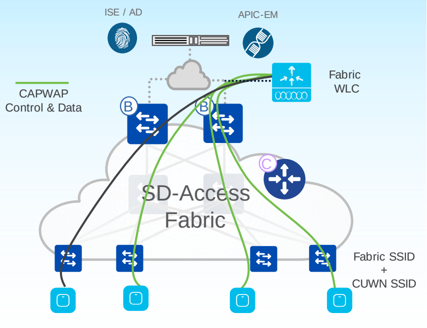
- CAPWAP Control Plane, VXLAN Data plane
- WLC/APs integrated in Fabric, SD- Access advantages
- Requires software upgrade (8.5+)
- Optimized for 802.11ac Wave 2 and 11ax APs

## CUWN wireless Over The Top (OTT)



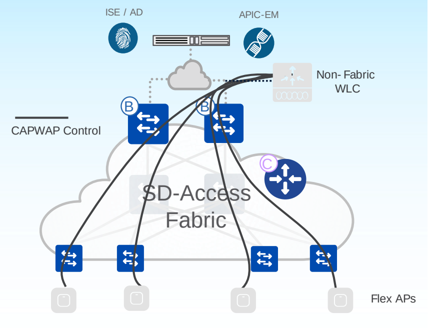
- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport
- Supported on any WLC/AP software and hardware

## Mixed Mode



- non- Fabric SSID: client traffic is CAPWAP encapsulated to WLC
- Fabric SSID: client traffic is VXLAN encapsulated

## FlexConnect Over The Top (OTT)

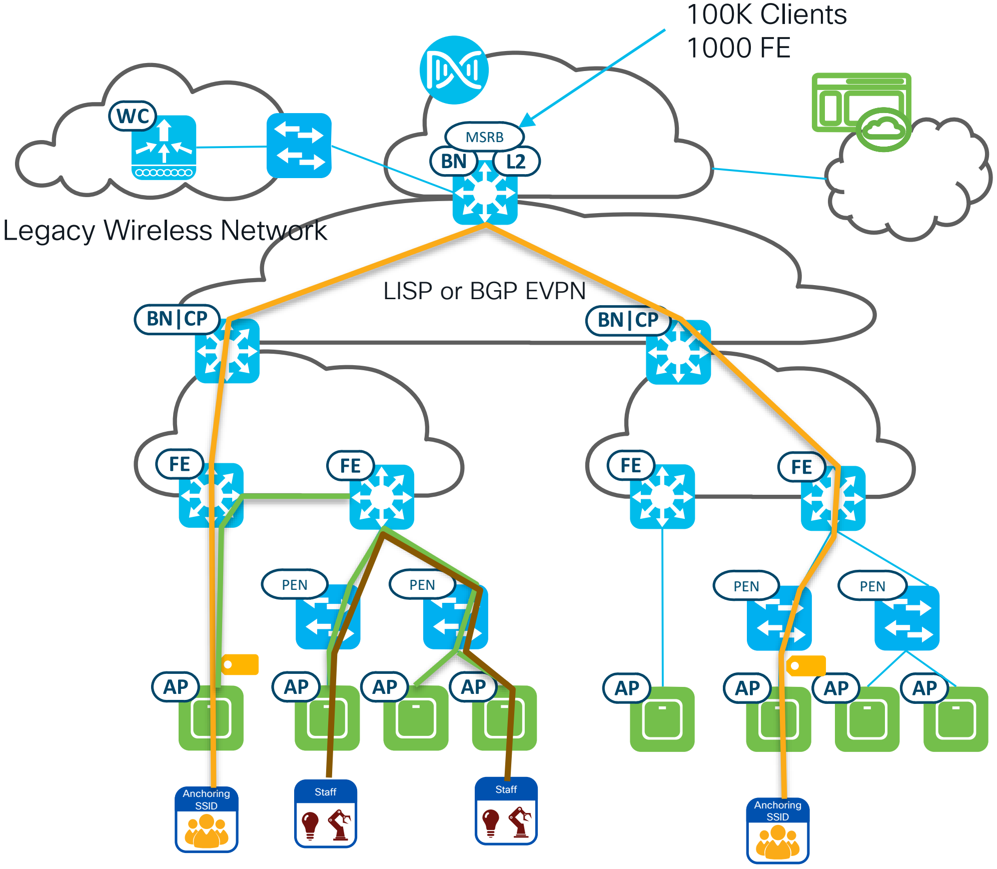


- CAPWAP for Control Plane
- Data plane is locally switched. Wireless traffic is treated like wired traffic.

## Fabric Wireless Advantage

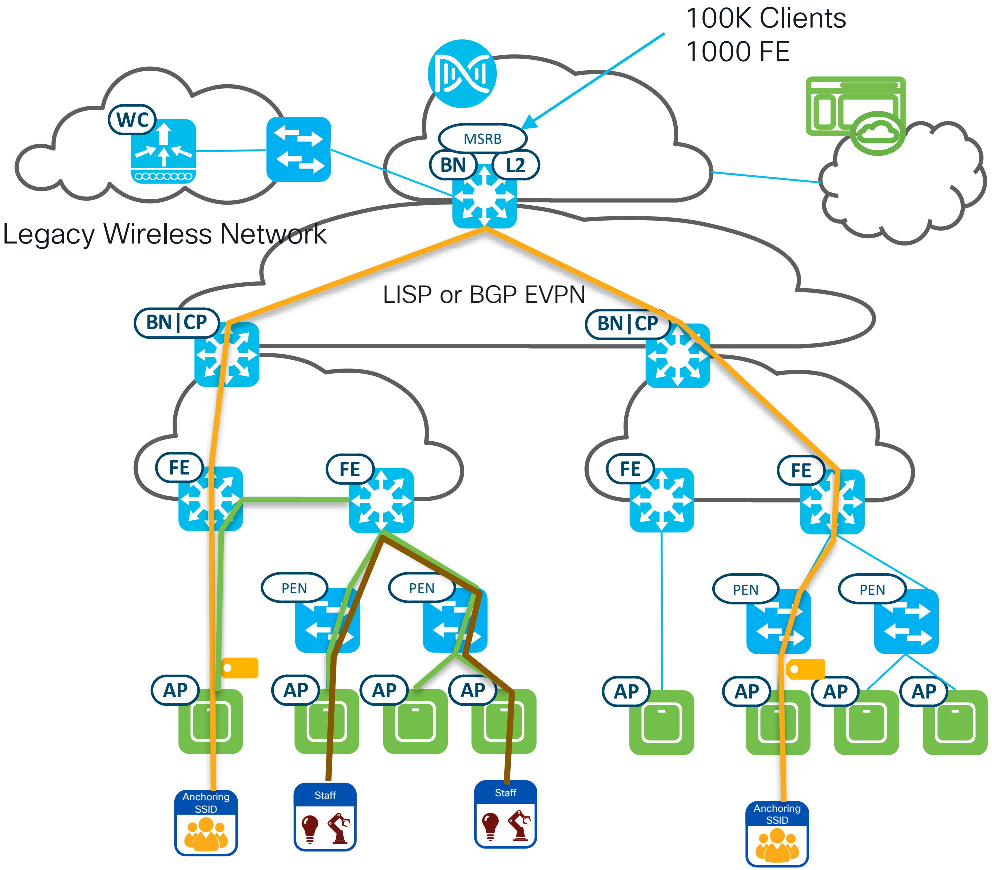
- Overlay uses alternate forwarding attributes to provide additional services
- Policy is applied irrespectively of network constructs (VLAN, subnet, IP)
- Easily implement Network Segmentation (w/o implementing MPLS)
- Provide L2 and L3 flexibility (w/o stretching VLANs)

# Meraki Wireless in the fabric



- Scalable
- Client mobility allowed across entire network
- No additional hardware needed with fabric
- Two management domains with policy integrated via ISE
- Macro and Micro Segmentation

# Meraki Wireless in the fabric

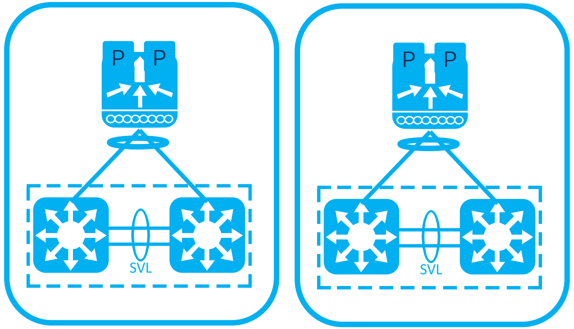


- Basic construct is to allow the fabric to manage all the IP roaming
- No additional gateways needed outside the fabric
- IP roaming can be within a fabric site or throughout the entire fabric domain
- Wireless fast roaming (key caching) preformed by L2 connection between APs.
  - Limited to APs within a Meraki network (~800)
  - Limited to within the fabric site (L2 broadcast)
- Micro-segmentation SGTs can be supported provided access layer switching supports CTS and is advantage.
- Use of enhanced forwarding for client VLANs to improve IP roaming time (<100ms)
- Mobility (hard roam but keep the same IP) is allowed across the fabric sites and across cloud and controller-based deployment.

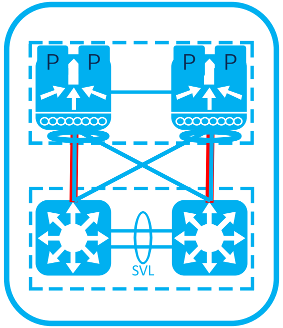
# High Availability

## How do I include this in my design

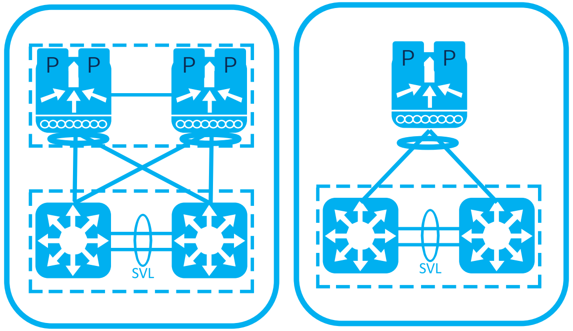
# High Availability Architectures for WLCs



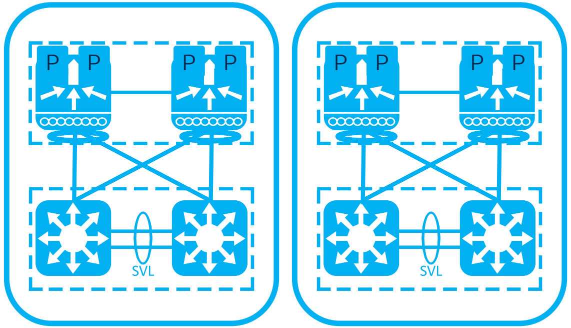
AP Fail-Over (N+1)



SSO



SSO + One

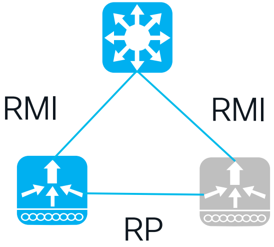


SSO + SSO

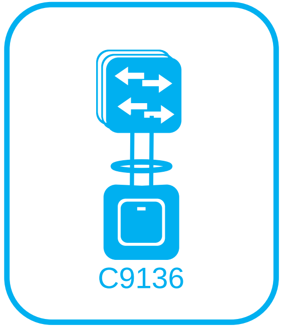
Note: LACP/PAGP Supported

# SSO Notes

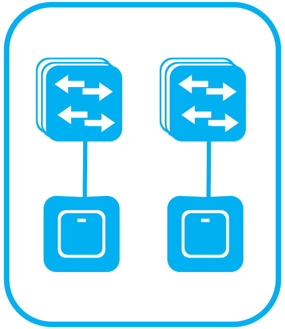
- Same SW Version/Form Factor
- Maximum RP link latency = 80 ms RTT
- Minimum bandwidth = 60 Mbps
- Minimum MTU = 1500
- Supported in Virtual Machines through virtual switch
- RMI allows for secondary inter-link in the event RP goes down
- RMI is a secondary IP on the management SVI (must be same subnet a mgmt IP)
- RMI also provides a Gateway check
  - 1 Second intervals
  - 4  consecutive ICMP followed by 4 ARP means gateway is down.
  - Redundant controller no longer a option



# High Availability Architectures for APs



AP Dual Connection



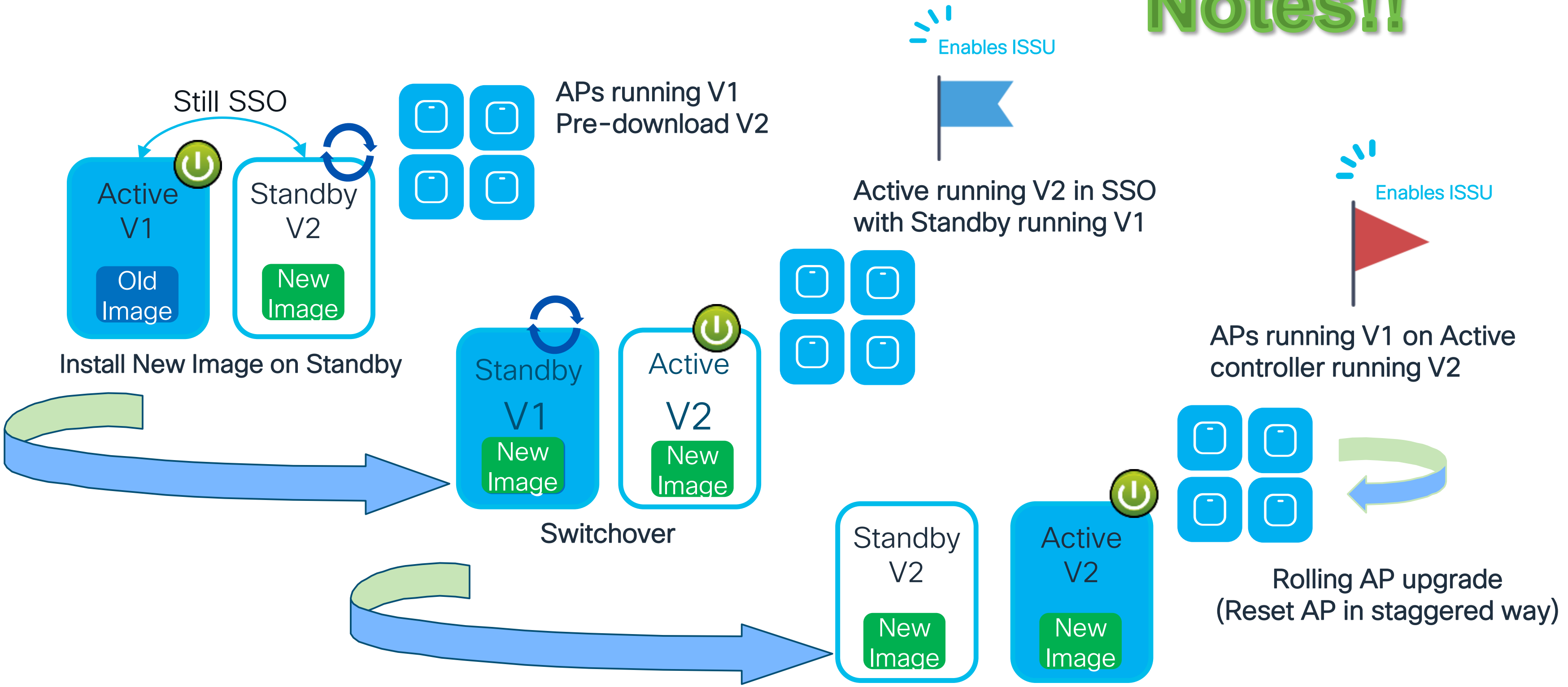
Overlapping Coverage

Switching for AP HA

- Perpetual PoE
- Fast PoE
- Stack Power
- Stackwise
- Stagger Switches

# ISSU Process

Read the Release Notes!!



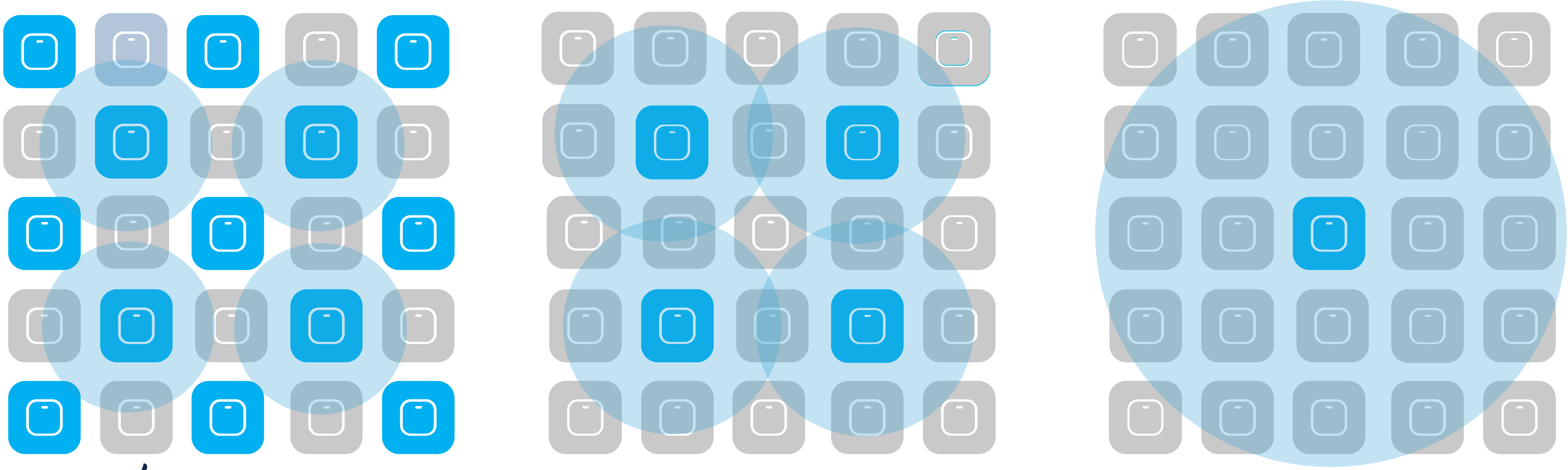
Install New Image on New Standby

Note: "Hitless" and "ISSU" are not the same thing

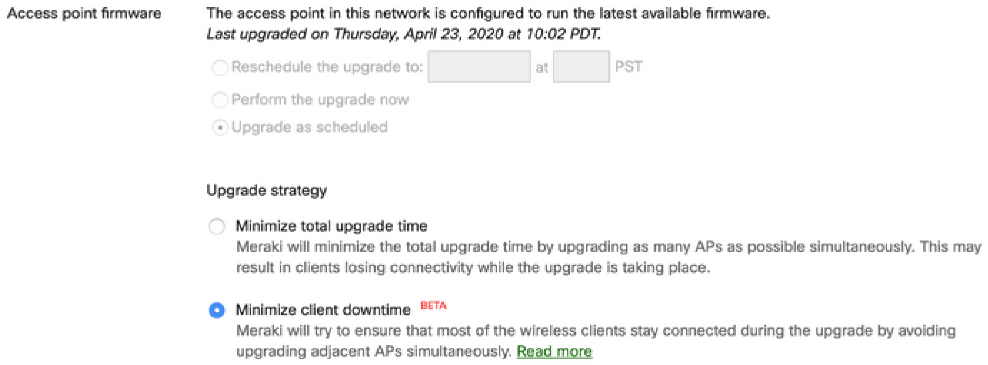
# Neighbor Marking for Rolling AP Upgrade
(N+1 Also)

User selects % of APs to upgrade in one go [5, 15, 25]

- For 25%, Neighbors marked = 6 [Expected number of iterations ~ 5]
- For 15%, Neighbors marked = 12 [Expected number of iterations ~ 12]
- For 5%, Neighbors marked = 24 [Expected number of iterations ~ 22]



# Meraki Minimize Client Down Time



Access point firmware

The access point in this network is configured to run the latest available firmware.
*Last upgraded on Thursday, April 23, 2020 at 10:02 PDT.*

○ Reschedule the upgrade to: ____ at ____ PST

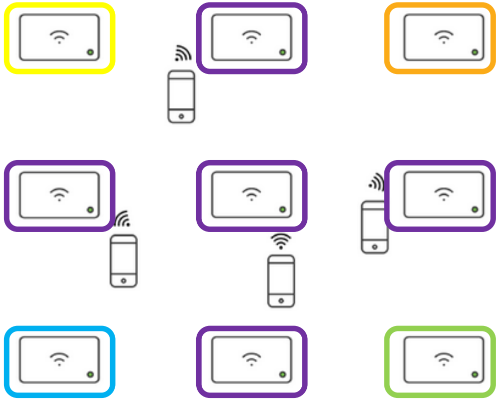
○ Perform the upgrade now

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



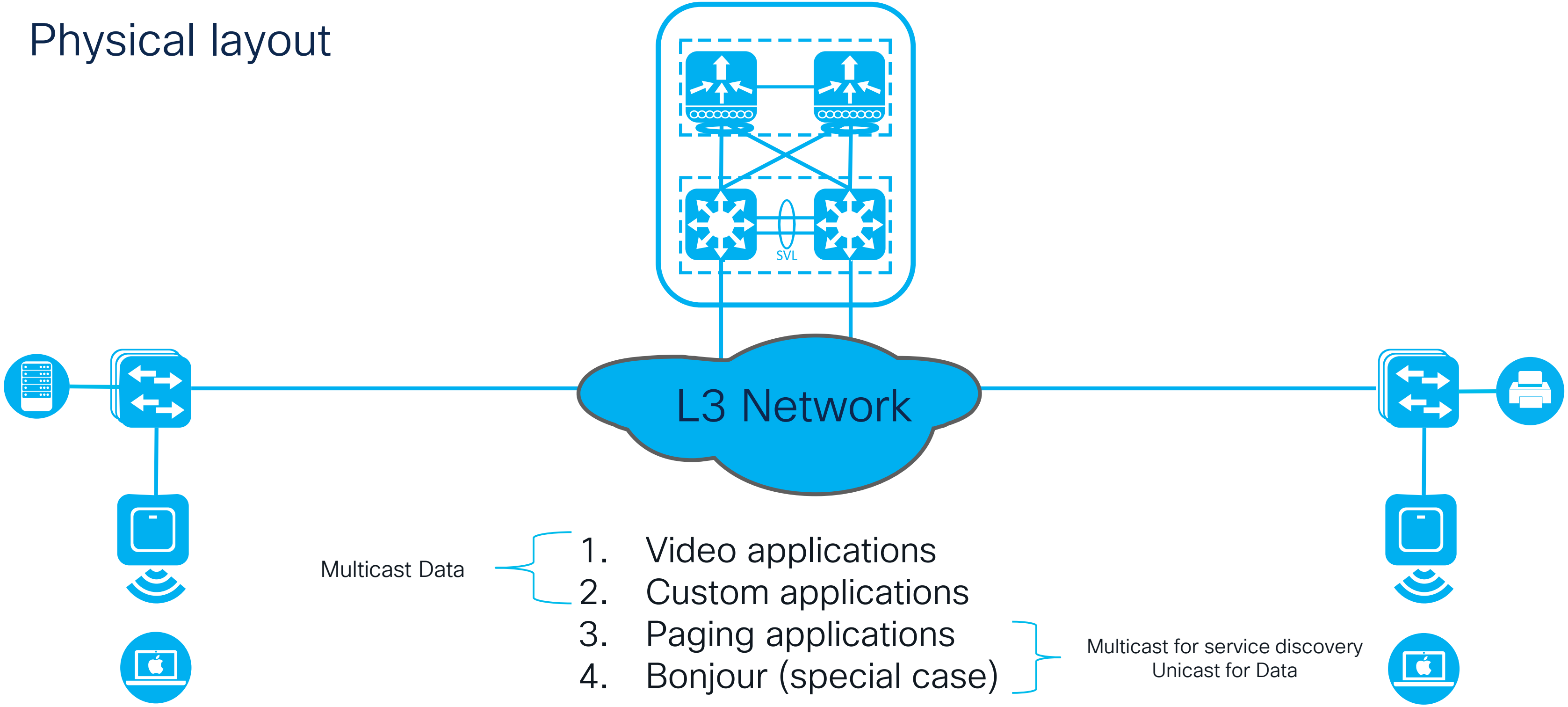
- APs are logically divided into groups so that clients can join a neighboring AP
- Groups are upgraded one at a time
- Increases upgrade time but decreases down time.

# Multicast

## What is it and how does it affect my design

# Multicast

## Physical layout



Multicast Data

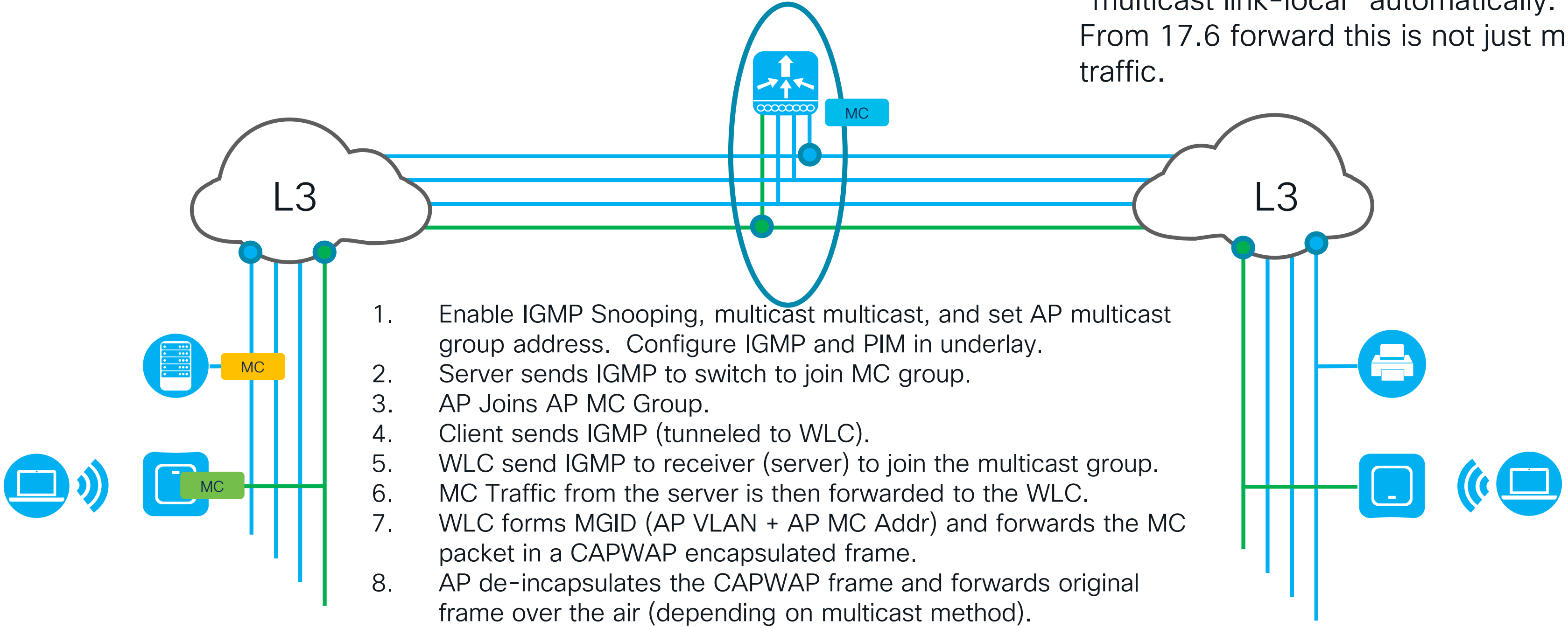
1. Video applications
2. Custom applications
3. Paging applications
4. Bonjour (special case)

Multicast for service discovery
Unicast for Data

# Multicast-Multicast vs Multicast-Unicast

## Local Mode (central switching)

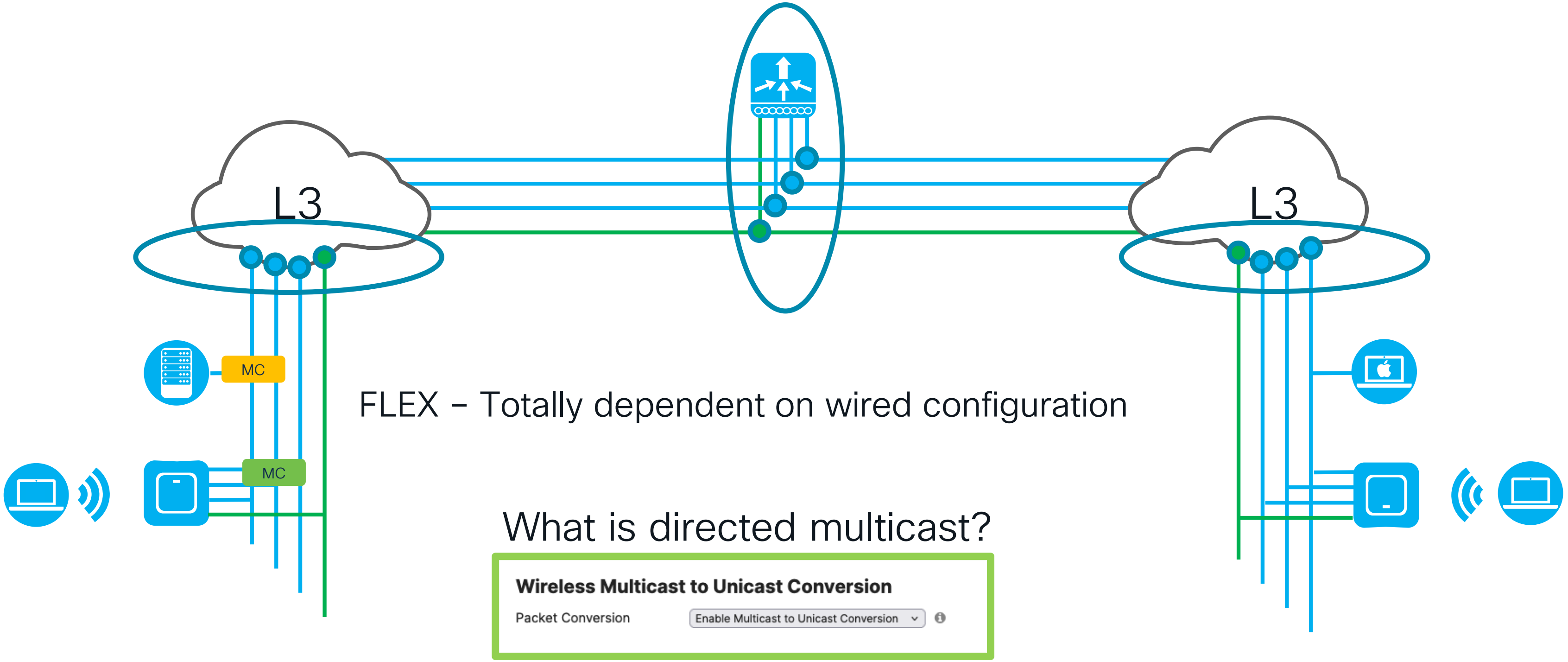
Note: Enabling Multicast enables “multicast link-local” automatically. From 17.6 forward this is not just mDNS traffic.



1. Enable IGMP Snooping, multicast multicast, and set AP multicast group address. Configure IGMP and PIM in underlay.
2. Server sends IGMP to switch to join MC group.
3. AP Joins AP MC Group.
4. Client sends IGMP (tunneled to WLC).
5. WLC send IGMP to receiver (server) to join the multicast group.
6. MC Traffic from the server is then forwarded to the WLC.
7. WLC forms MGID (AP VLAN + AP MC Addr) and forwards the MC packet in a CAPWAP encapsulated frame.
8. AP de-incapsulates the CAPWAP frame and forwards original frame over the air (depending on multicast method).

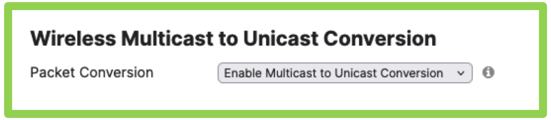
# Multicast-Multicast vs Multicast-Unicast

## Flexconnect Mode or Meraki (local switching)



FLEX – Totally dependent on wired configuration

What is directed multicast?

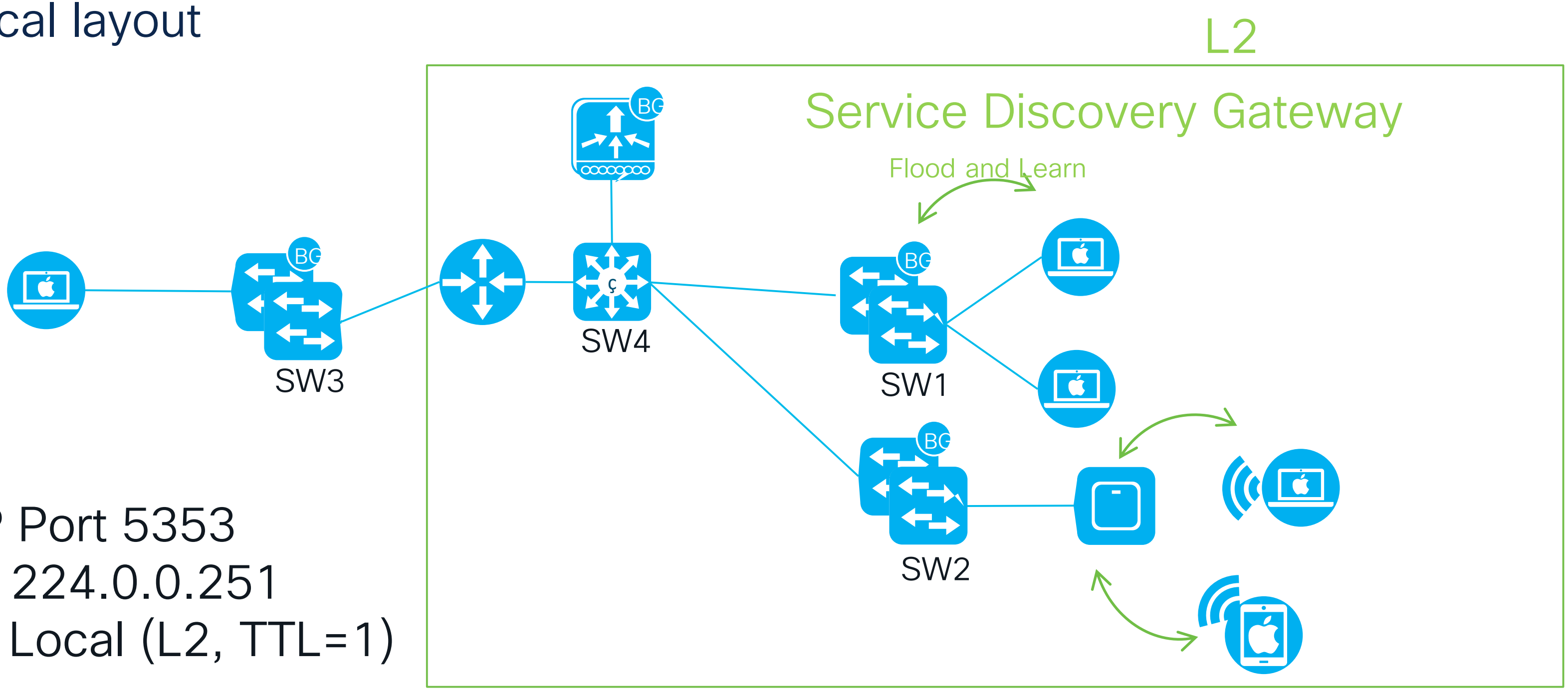


**Wireless Multicast to Unicast Conversion**

Packet Conversion: Enable Multicast to Unicast Conversion

# Bonjour/mDNS Example

## Physical layout

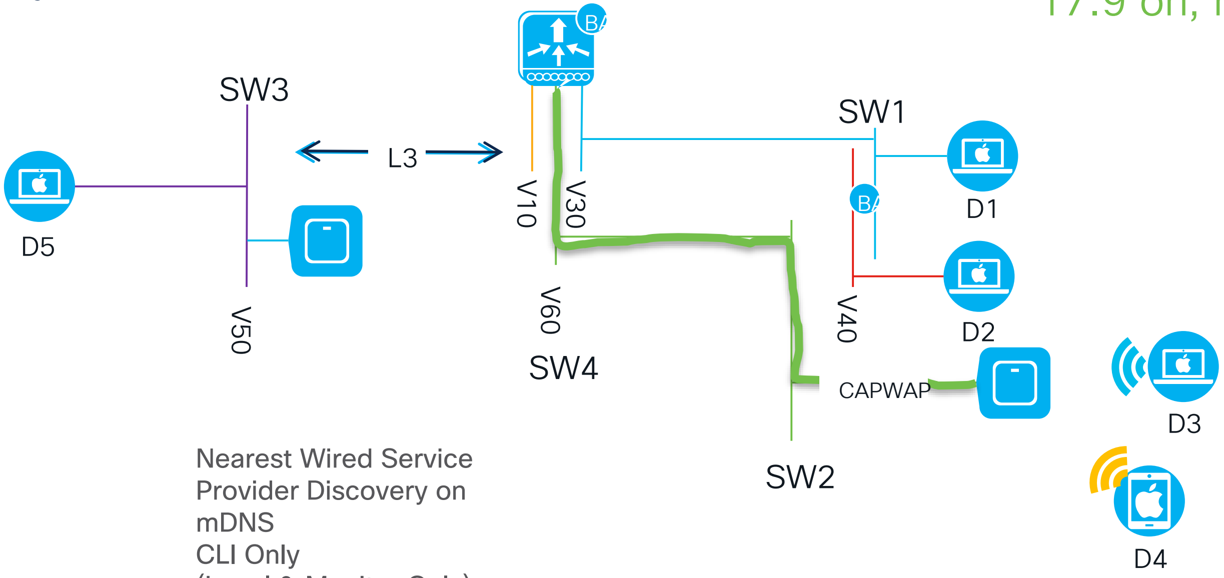


UDP Port 5353
MC: 224.0.0.251
Link Local (L2, TTL=1)

# Bonjour/mDNS Example

## Logical layout

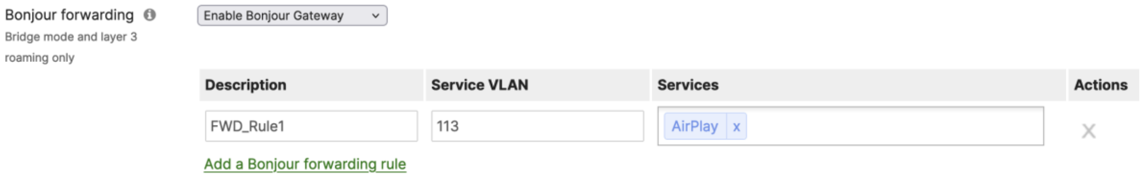
Effects Control Plane/CPU
Use location
17.9 on, no SVI required



Nearest Wired Service Provider Discovery on mDNS
CLI Only
(Local & Monitor Only)

UDP Port 5353
MC: 224.0.0.251
Link Local (L2, TTL=1)
BA = Bonjour Agent

# Managing mDNS rules can be challenging

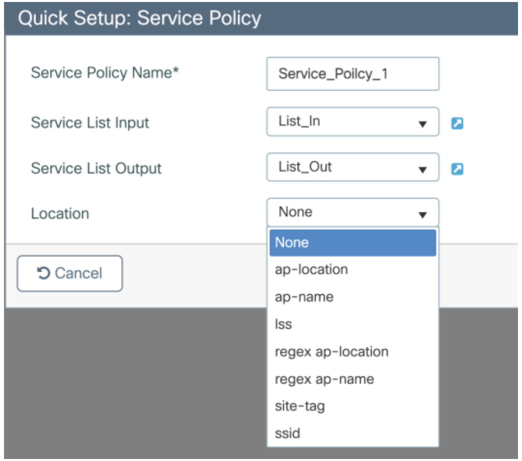


Bonjour forwarding
Bridge mode and layer 3 roaming only

Enable Bonjour Gateway

| Description | Service VLAN | Services | Actions |
|---|---|---|---|
| FWD_Rule1 | 113 | AirPlay x | X |

Add a Bonjour forwarding rule



Quick Setup: Service Policy

Service Policy Name*: Service_Poilcy_1

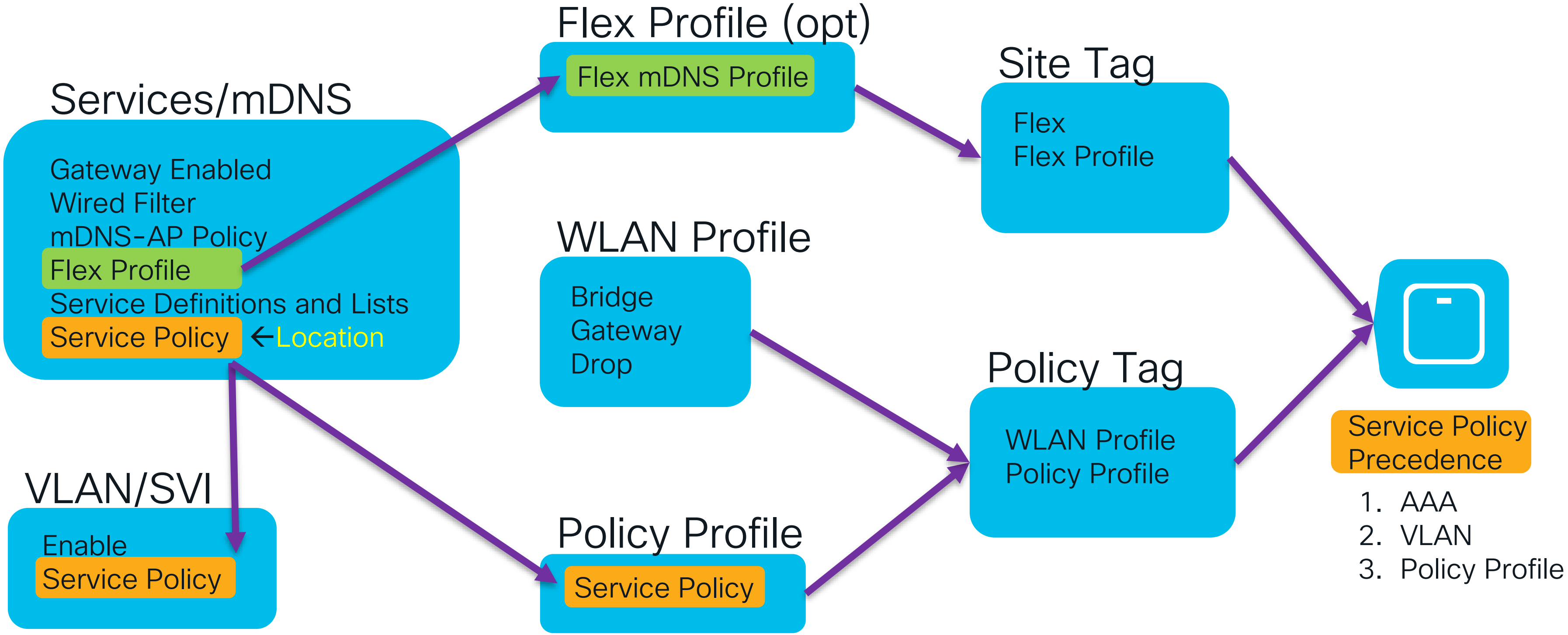
Service List Input: List_In

Service List Output: List_Out

Location: None

What if I want to use location specific or AP specific broadcasts while using locally switch data?

# Configure mDNS in C9800



Services/mDNS

Gateway Enabled
Wired Filter
mDNS-AP Policy
Flex Profile
Service Definitions and Lists
Service Policy ←Location

Flex Profile (opt)

Flex mDNS Profile

Site Tag

Flex
Flex Profile

WLAN Profile

Bridge
Gateway
Drop

Policy Tag

WLAN Profile
Policy Profile

VLAN/SVI

Enable
Service Policy

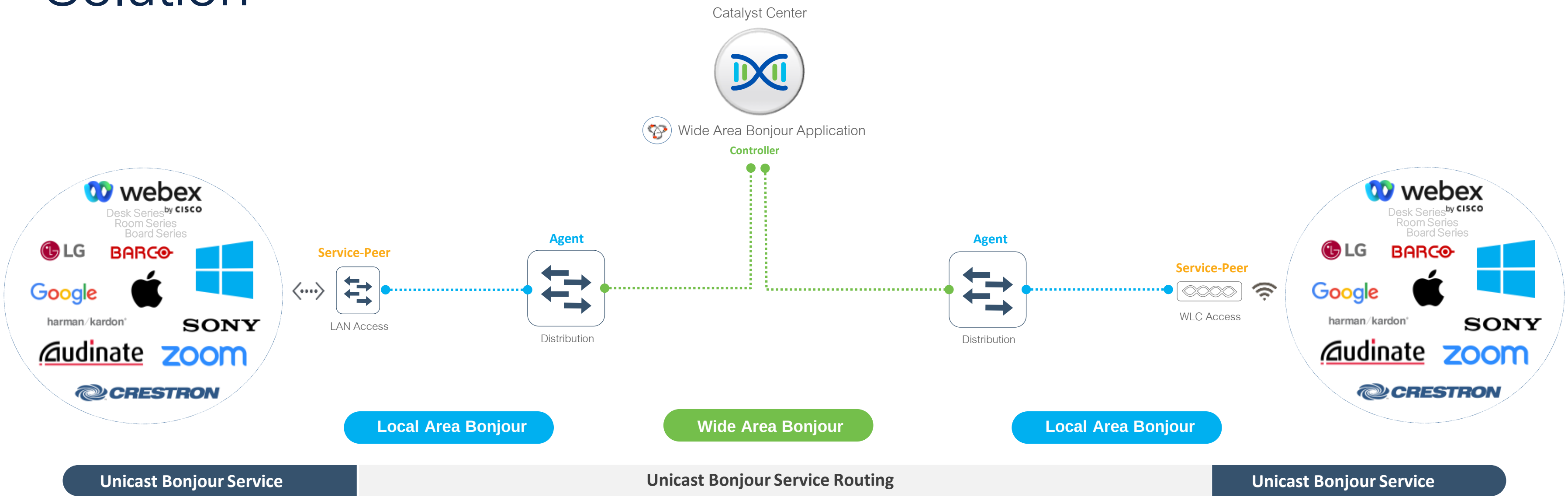
Policy Profile

Service Policy

Service Policy Precedence

1. AAA
2. VLAN
3. Policy Profile

# C9000 Offers Most Comprehensive Wide Area mDNS Solution



### Hierarchical

2-Tier Service Routing

Structured Role and Function

mDNS Flood-Free Networks

### Secure

Policy-Based Service Management

IT controlled deterministic services

Protected network flood boundaries

### Location

Deep granular location-based service

Location-aware Wide Area Bonjour

Flexible design any Enterprise Network

### Performance

Improved system performance

Increase network bandwidth

Flexible design any Enterprise Network

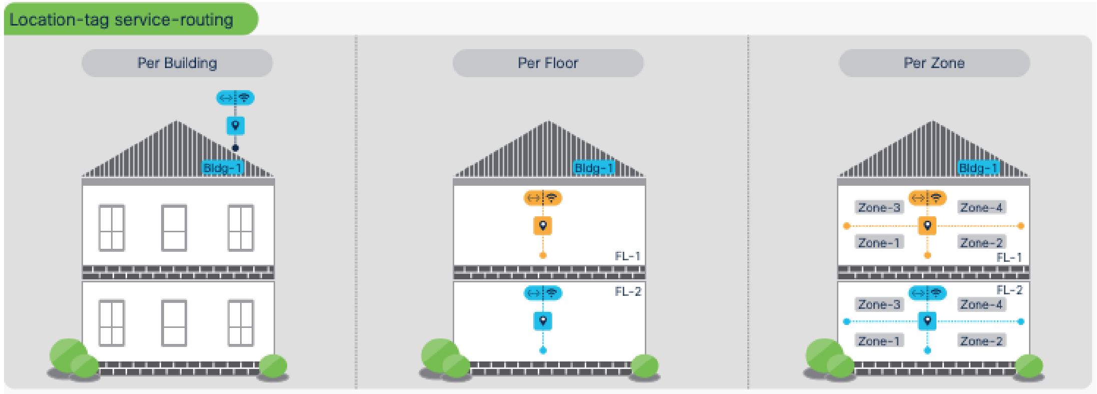
### Battery Life

May assist improve battery-life

On-demand Query response mode

Increase Wireless network bandwidth

# How does this solve locally switch Flex or Meraki



**Per Building** – Gateway can be in the distribution switch (assuming L2 to the access) and can form peering relationships with access switches

**Per Floor** – Gateway can reside at the access layer switch or multiple peer groups from the distribution layer

**Per Zone** – Gateway on the access switch can port group configurations for an interface or group of interfaces

# Per Zone Configuration (only on Access Switch)

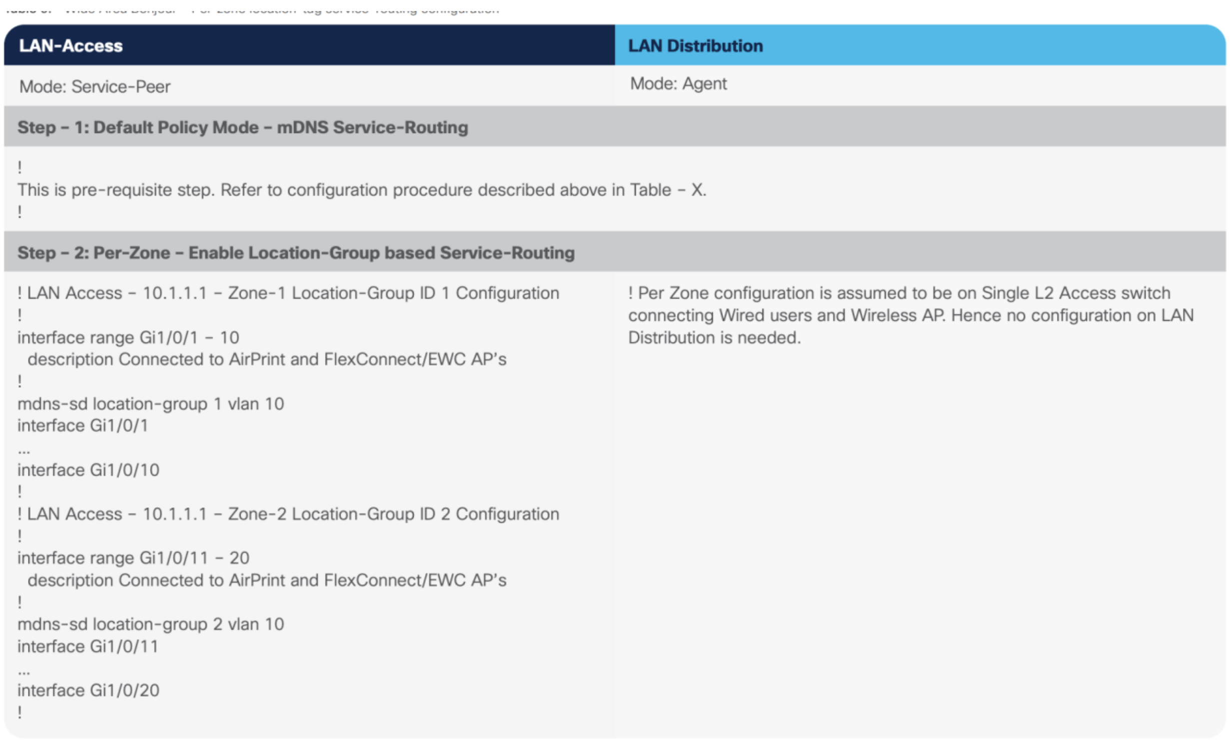
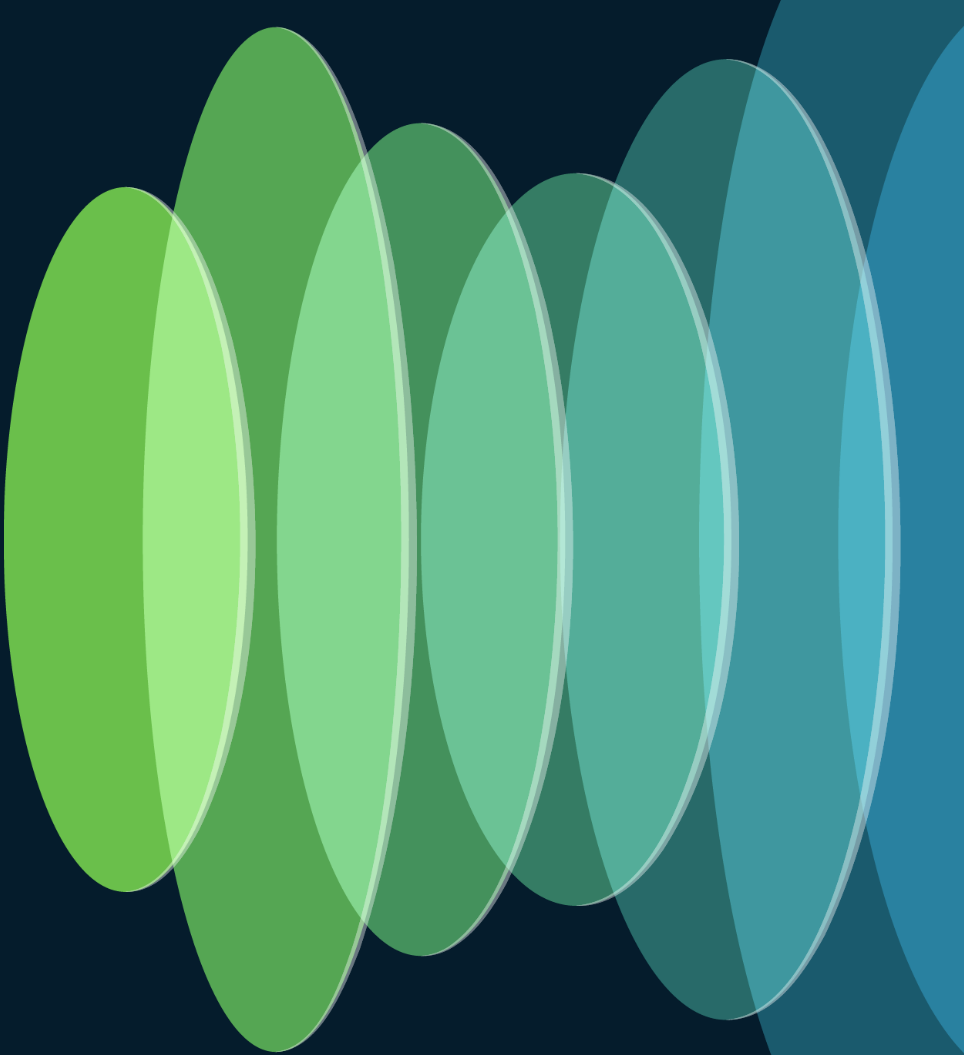


Table 6: Wide Area Bonjour – Per Zone location-tag service-routing configuration

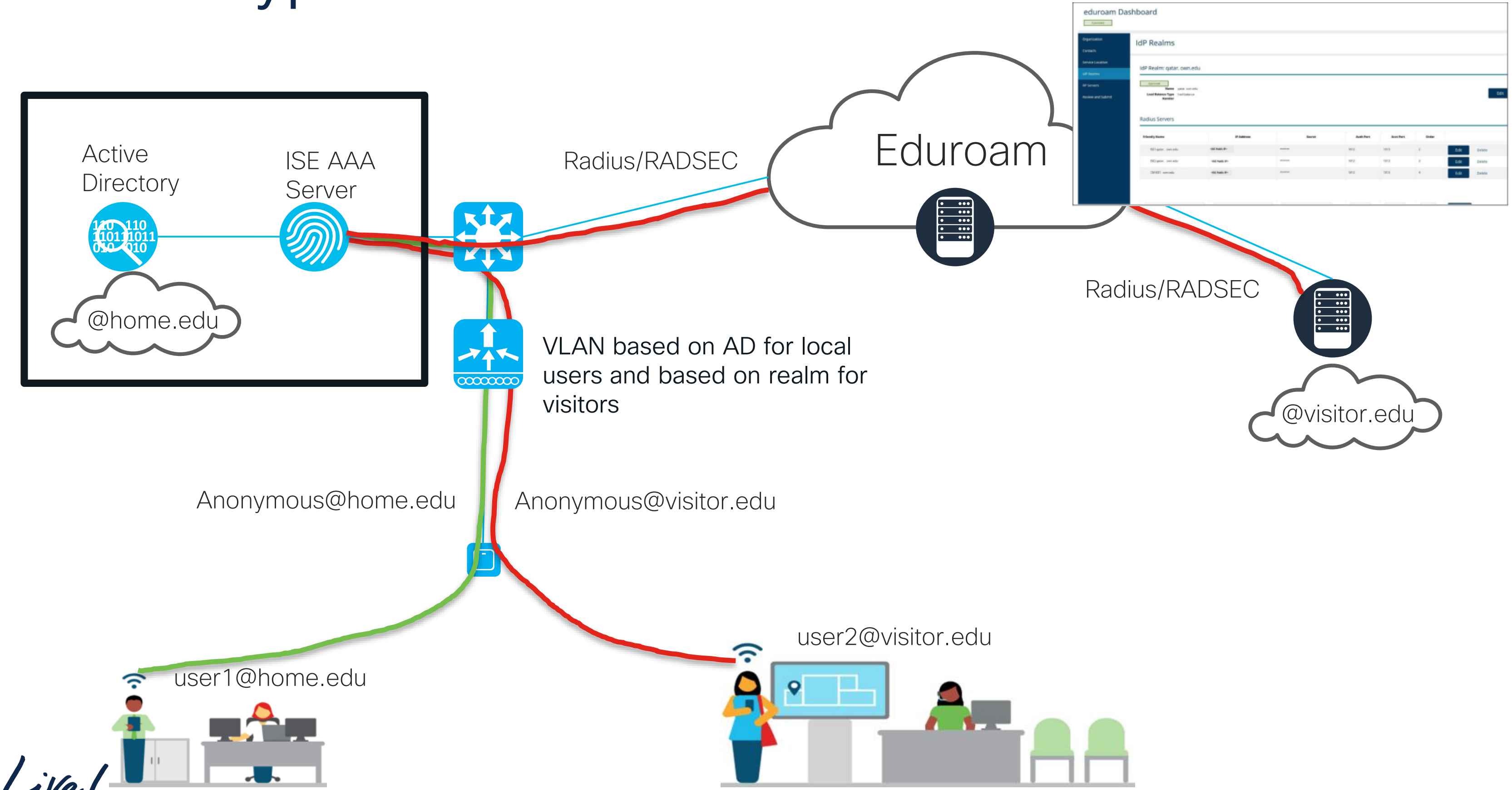
| LAN-Access | LAN Distribution |
|---|---|
| Mode: Service-Peer | Mode: Agent |
| **Step – 1: Default Policy Mode – mDNS Service-Routing** | |
| !<br>This is pre-requisite step. Refer to configuration procedure described above in Table – X.<br>! | |
| **Step – 2: Per-Zone – Enable Location-Group based Service-Routing** | |
| ! LAN Access – 10.1.1.1 – Zone-1 Location-Group ID 1 Configuration<br>!<br>interface range Gi1/0/1 – 10<br>  description Connected to AirPrint and FlexConnect/EWC AP's<br>!<br>mdns-sd location-group 1 vlan 10<br>interface Gi1/0/1<br>...<br>interface Gi1/0/10<br>!<br>! LAN Access – 10.1.1.1 – Zone-2 Location-Group ID 2 Configuration<br>!<br>interface range Gi1/0/11 – 20<br>  description Connected to AirPrint and FlexConnect/EWC AP's<br>!<br>mdns-sd location-group 2 vlan 10<br>interface Gi1/0/11<br>...<br>interface Gi1/0/20<br>! | ! Per Zone configuration is assumed to be on Single L2 Access switch connecting Wired users and Wireless AP. Hence no configuration on LAN Distribution is needed. |

# Eduroam

## A different approach to an old requirement



# Eduroam Typical Authentication



eduroam Dashboard

Submitted

Organization
Contacts
Service Location
IdP Realms
RP Servers
Review and Submit

IdP Realms

IdP Realm: qatar. own.edu

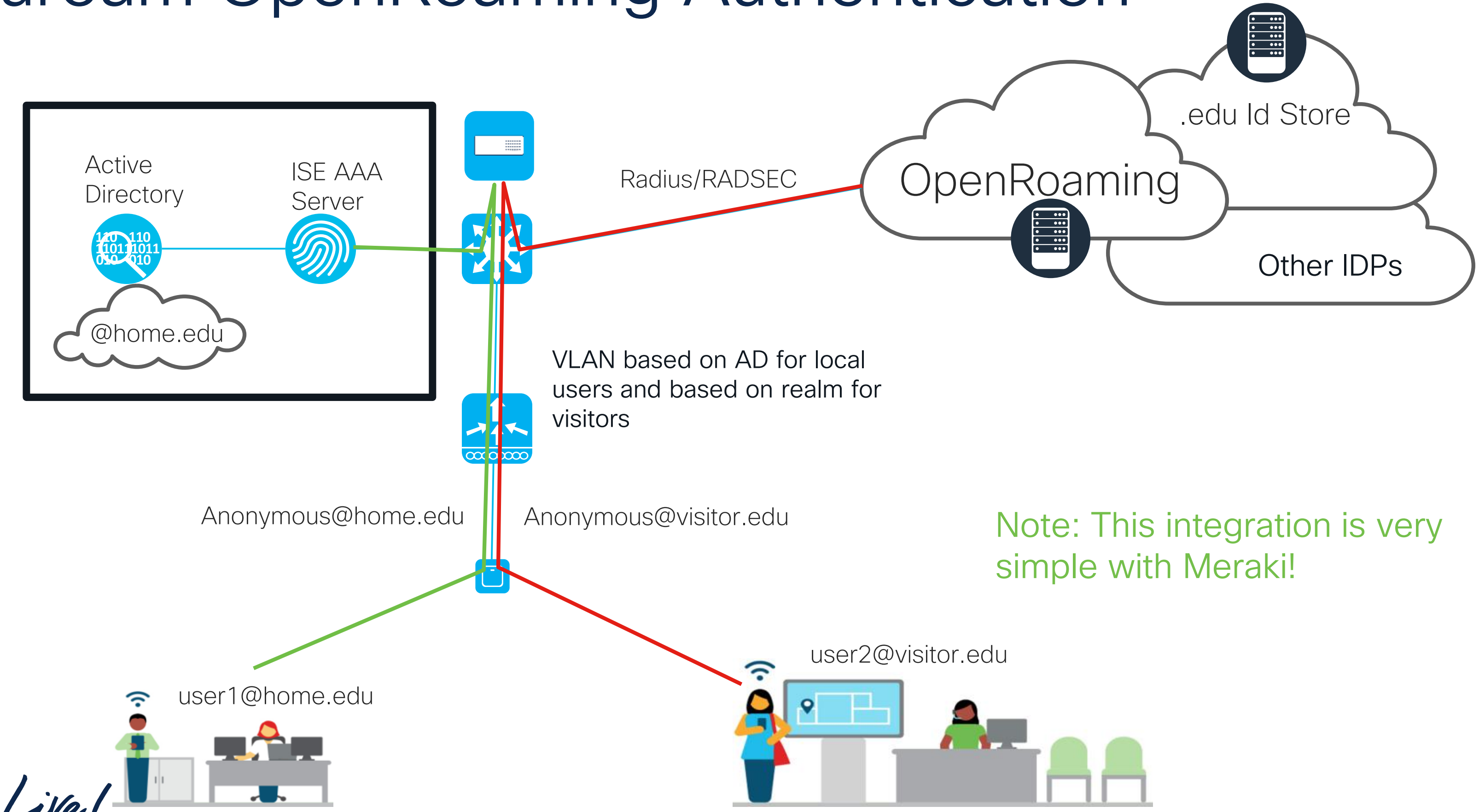
Approved
Name qatar. own.edu
Load Balance Type Handler FastBalance

Edit

Radius Servers

| Friendly Name | IP Address | Secret | Auth Port | Acct Port | Order | | |
|---|---|---|---|---|---|---|---|
| ISE1.qatar. own.edu | <ISE Public IP> | ****** | 1812 | 1813 | 2 | Edit | Delete |
| ISE2.qatar. own.edu | <ISE Public IP> | ****** | 1812 | 1813 | 3 | Edit | Delete |
| CM-ISE1 own.edu | <ISE Public IP> | ****** | 1812 | 1813 | 4 | Edit | Delete |

# Eduroam OpenRoaming Authentication



VLAN based on AD for local users and based on realm for visitors

Note: This integration is very simple with Meraki!

# Eduroam Considerations

* 17.12 added support for Transition Mode

- Be sure network is sized to support additional Eduroam users
- Local AAA (ISE) is authenticating server for local Eduroam users.
- Visitors AAA is authenticating server for visiting Eduroam users.
- Outer identities are anonymous and routed.
- Can use standard forms of EAP:
  - PEAP
  - EAP-TLS
  - EAP-TTLS
  - EAP-FAST
- Can use configuration assistance tool (CAT) for client to simplify onboarding.
- Typical process is to create 2 WLANs with the same name for 2.4 & 5, and 6GHz. *

# iPSK/mPSK/UDN /WPN

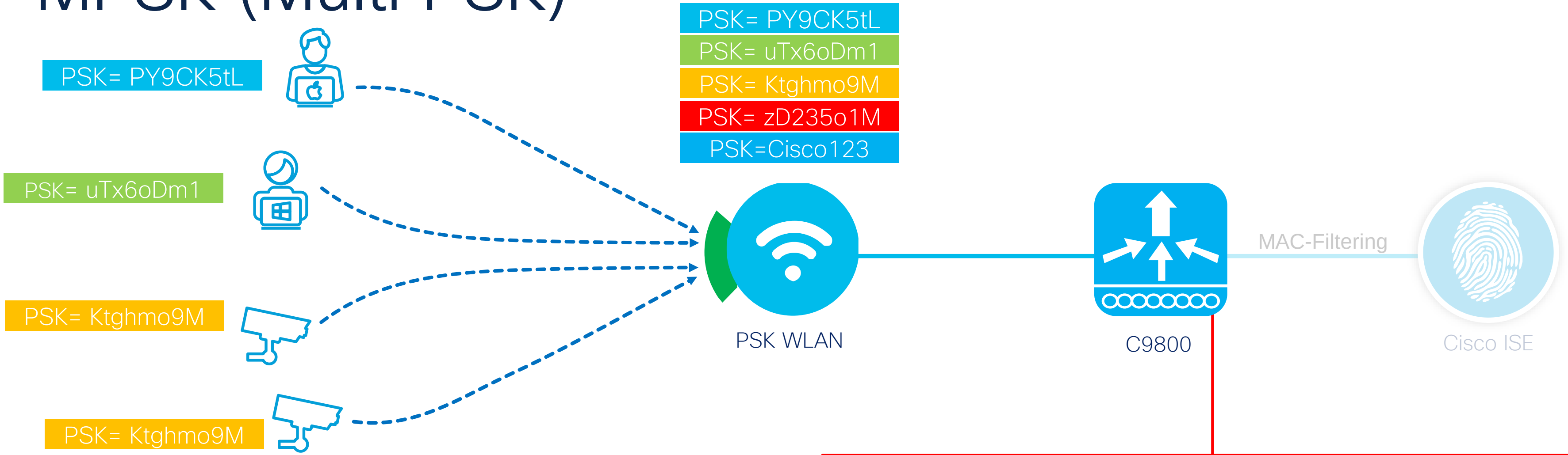
## What is it and how can I use this in my design

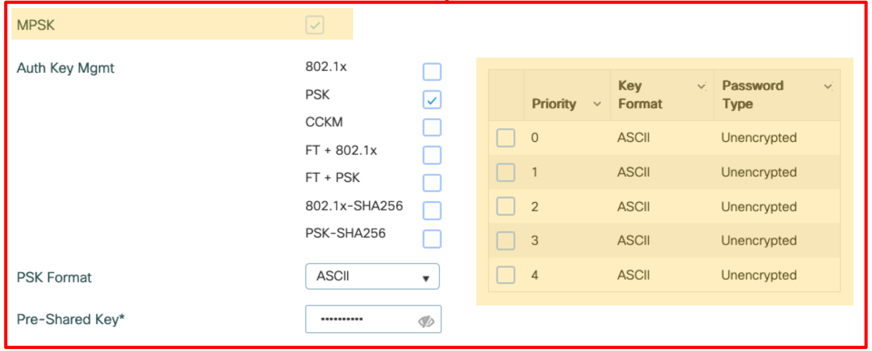
# Multiple User PSK Options

| Method | WPA3 support | AAA mandatory | Backend Provision | User experience | Segmentation | Stack |
|---|---|---|---|---|---|---|
| MPSK | No | No | Un bounded MAC | Very easy | P2P Blocking | Catalyst |
| Easy PSK | No | Yes, Nomadix# (FT not supported) | Un bounded MAC | Very easy | VLAN override | Catalyst |
| iPSK | Yes | Yes | Requires MAC onboarding | Easy | Unicast | Both |
| WPN | No | No | Use of Splash Accesss portal for MAC onboarding | Easy | Unicast/Multicast | Meraki |
| UDN+ | Yes | Yes | Use of Splash Accesss portal for MAC onboarding | Easy | Unicast/Multicast | Catalyst |

# -Also works with Rgnets now https://www.reddit.com/r/RGNets/comments/t9zgzr/multiple_psk/

# MPSK (Multi PSK)





MPSK ☑

Auth Key Mgmt
- 802.1x □
- PSK ☑
- CCKM □
- FT + 802.1x □
- FT + PSK □
- 802.1x-SHA256 □
- PSK-SHA256 □

PSK Format: ASCII

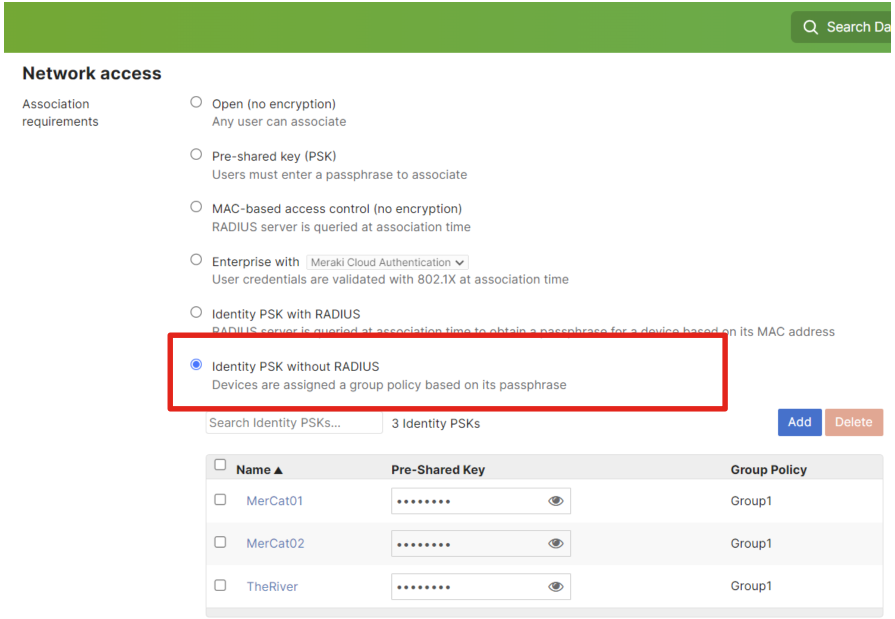
Pre-Shared Key*: ..........

| | Priority | Key Format | Password Type |
|---|---|---|---|
| □ | 0 | ASCII | Unencrypted |
| □ | 1 | ASCII | Unencrypted |
| □ | 2 | ASCII | Unencrypted |
| □ | 3 | ASCII | Unencrypted |
| □ | 4 | ASCII | Unencrypted |

- Can configure up to 5 different PSK per WLAN
- (Optional) ISE may be used for validating MAC address
- Supported with C9800 16.10+, not AireOS
- No WPA3 support (Catalyst or Meraki)

# Meraki “iPSK without RADIUS”

- This is the like MPSK on Catalyst
- 50 iPSKs per SSID in the firmware versions MR 27.X, 28.X, and 29.X
- 5,000 iPSKs per SSID in the firmware versions MR 30.1 and newer
- Unicast and multicast are not blocked when clients have a different iPSK, unless L2 isolation is enabled. With
  - L2 isolation enabled unicast, and multicast are blocked in all cases
- WPA3 is not supported
- VLANs can be assigned to different PSKs on same VLAN using the Dashboard, ISE is not required.



**Network access**

Association requirements

○ Open (no encryption)
Any user can associate

○ Pre-shared key (PSK)
Users must enter a passphrase to associate

○ MAC-based access control (no encryption)
RADIUS server is queried at association time

○ Enterprise with Meraki Cloud Authentication
User credentials are validated with 802.1X at association time

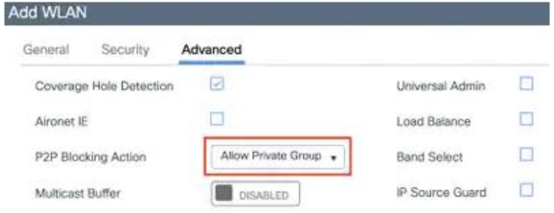
○ Identity PSK with RADIUS
RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

● Identity PSK without RADIUS
Devices are assigned a group policy based on its passphrase

Search Identity PSKs... 3 Identity PSKs

| □ | Name ▲ | Pre-Shared Key | Group Policy |
|---|---|---|---|
| □ | MerCat01 | •••••••• | Group1 |
| □ | MerCat02 | •••••••• | Group1 |
| □ | TheRiver | •••••••• | Group1 |

# IPSK (Identity PSK) p2p blocking



Add WLAN

General | Security | **Advanced**

Coverage Hole Detection ☑

Aironet IE □

P2P Blocking Action: Allow Private Group ▾

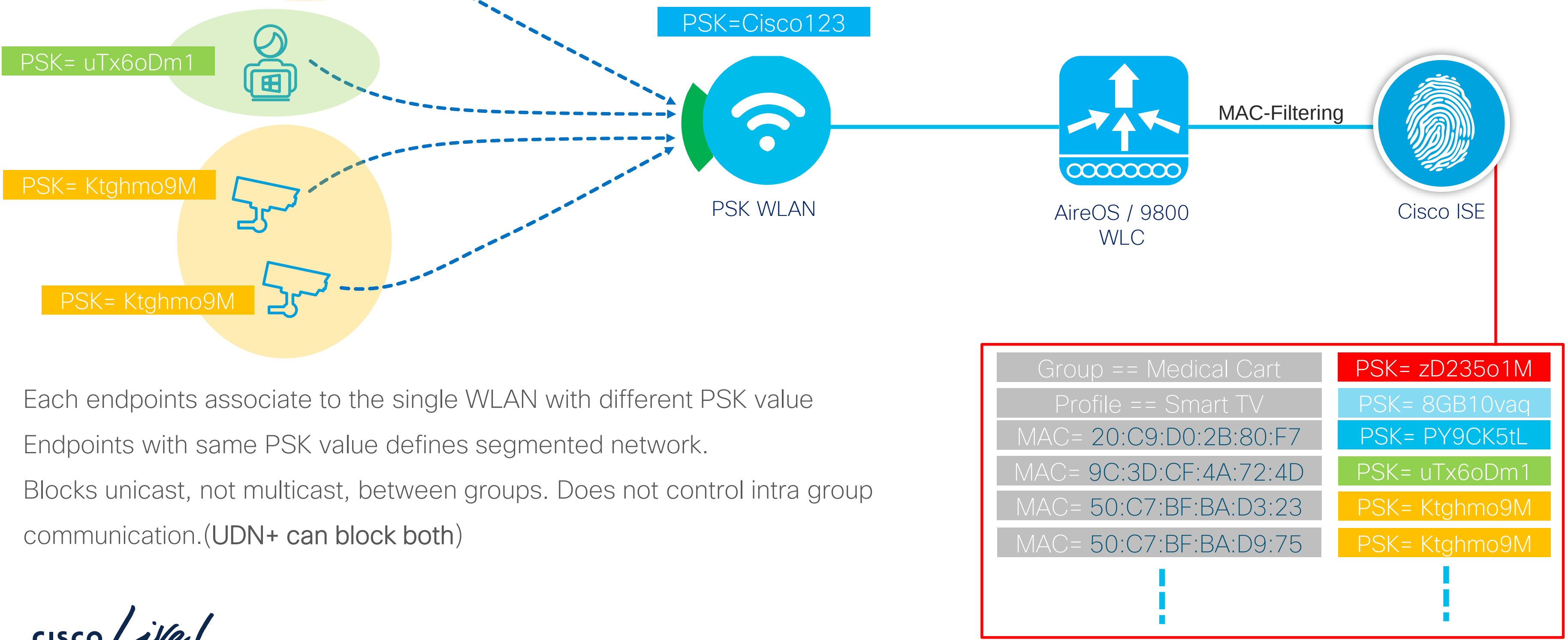
Multicast Buffer: DISABLED

Universal Admin □

Load Balance □

Band Select □

IP Source Guard □



| | |
|---|---|
| Group == Medical Cart | PSK= zD235o1M |
| Profile == Smart TV | PSK= 8GB10vaq |
| MAC= 20:C9:D0:2B:80:F7 | PSK= PY9CK5tL |
| MAC= 9C:3D:CF:4A:72:4D | PSK= uTx6oDm1 |
| MAC= 50:C7:BF:BA:D3:23 | PSK= Ktghmo9M |
| MAC= 50:C7:BF:BA:D9:75 | PSK= Ktghmo9M |

- Each endpoints associate to the single WLAN with different PSK value
- Endpoints with same PSK value defines segmented network.
- Blocks unicast, not multicast, between groups. Does not control intra group communication.(UDN+ can block both)

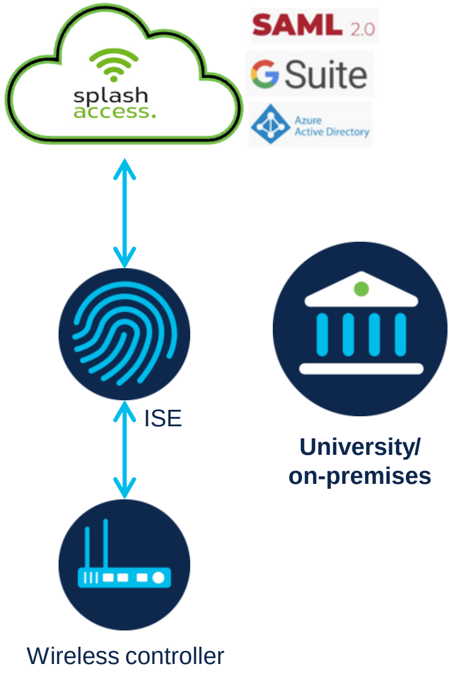
# Catalyst UDN+ with splash access*

Log in to the user portal (registers or enter voucher Azure AD, iDP, name/email)

Portal generates unique password for the user if using iPSK with QR code. User add their own devices MAC address from the portal to register the device.

Splash pushes the registered MAC addresses, and iPSK to the ISE endpoint group.

User devices joins the iPSK enabled SSID ( with MAC filtering).



(*) UK based Cisco Technology Partner https://www.splashaccess.com/

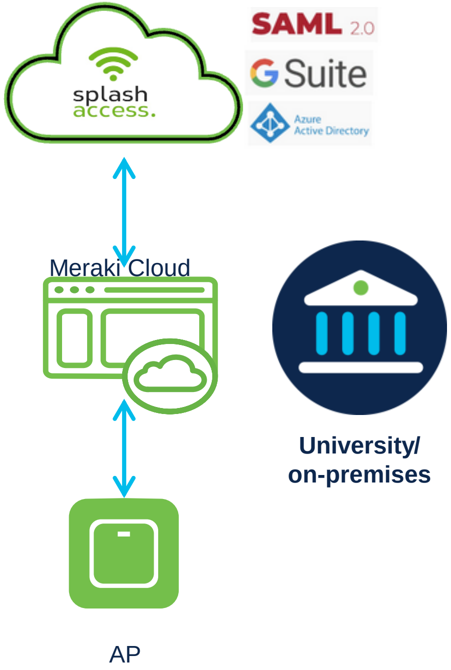
# Meraki WPN with splash access*

Log in to the user portal (registers or enter voucher Azure AD, iDP, name/email)

Portal generates unique password for the user if using iPSK with QR code. User add their own devices MAC address from the portal to register the device.

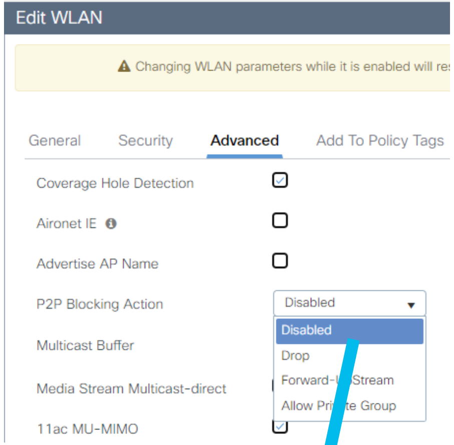
Splash pushes the registered MAC addresses, and iPSK via API to Meraki Cloud and assigned to group policy as configured in Splash

User devices joins the iPSK enabled SSID ( with MAC filtering).



(*) UK based Cisco Technology Partner https://www.splashaccess.com/

# UDN+ Isolation



Edit WLAN

⚠ Changing WLAN parameters while it is enabled will re

General | Security | Advanced | Add To Policy Tags

Coverage Hole Detection ☑

Aironet IE ⓘ □

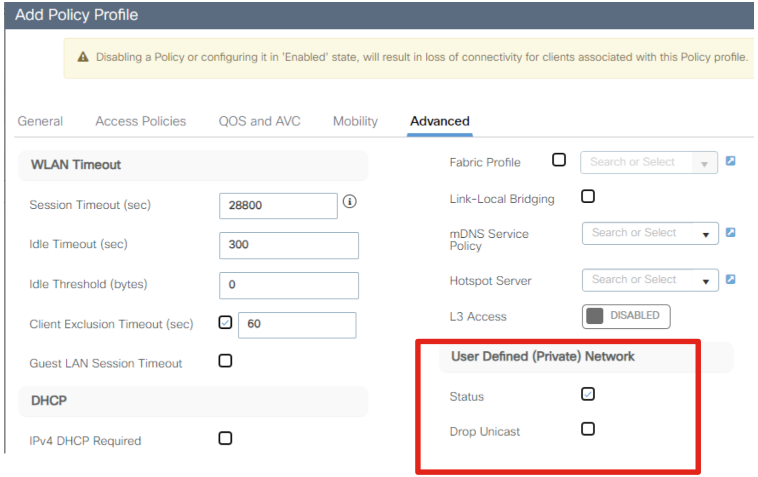
Advertise AP Name □

P2P Blocking Action: Disabled ▾
- Disabled
- Drop
- Forward-U Stream
- Allow Pri te Group

Multicast Buffer

Media Stream Multicast-direct

11ac MU-MIMO ☑



Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General | Access Policies | QOS and AVC | Mobility | Advanced

**WLAN Timeout**

Session Timeout (sec): 28800 ⓘ

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

Guest LAN Session Timeout □

**DHCP**

IPv4 DHCP Required □

Fabric Profile □ Search or Select ▾

Link-Local Bridging □

mDNS Service Policy: Search or Select ▾

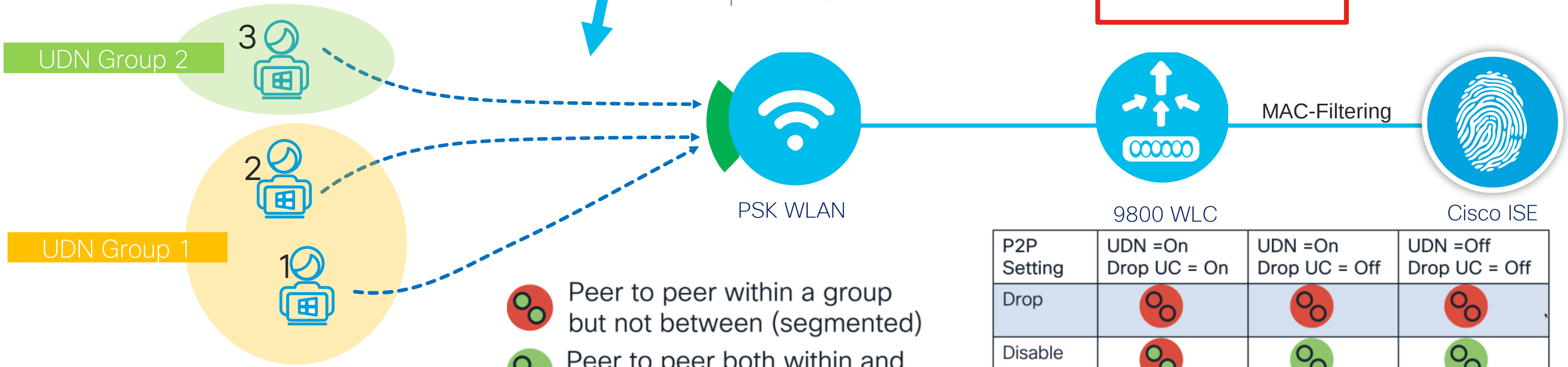
Hotspot Server: Search or Select ▾

L3 Access: DISABLED

**User Defined (Private) Network**

Status ☑

Drop Unicast □



🟥🟢 Peer to peer within a group but not between (segmented)

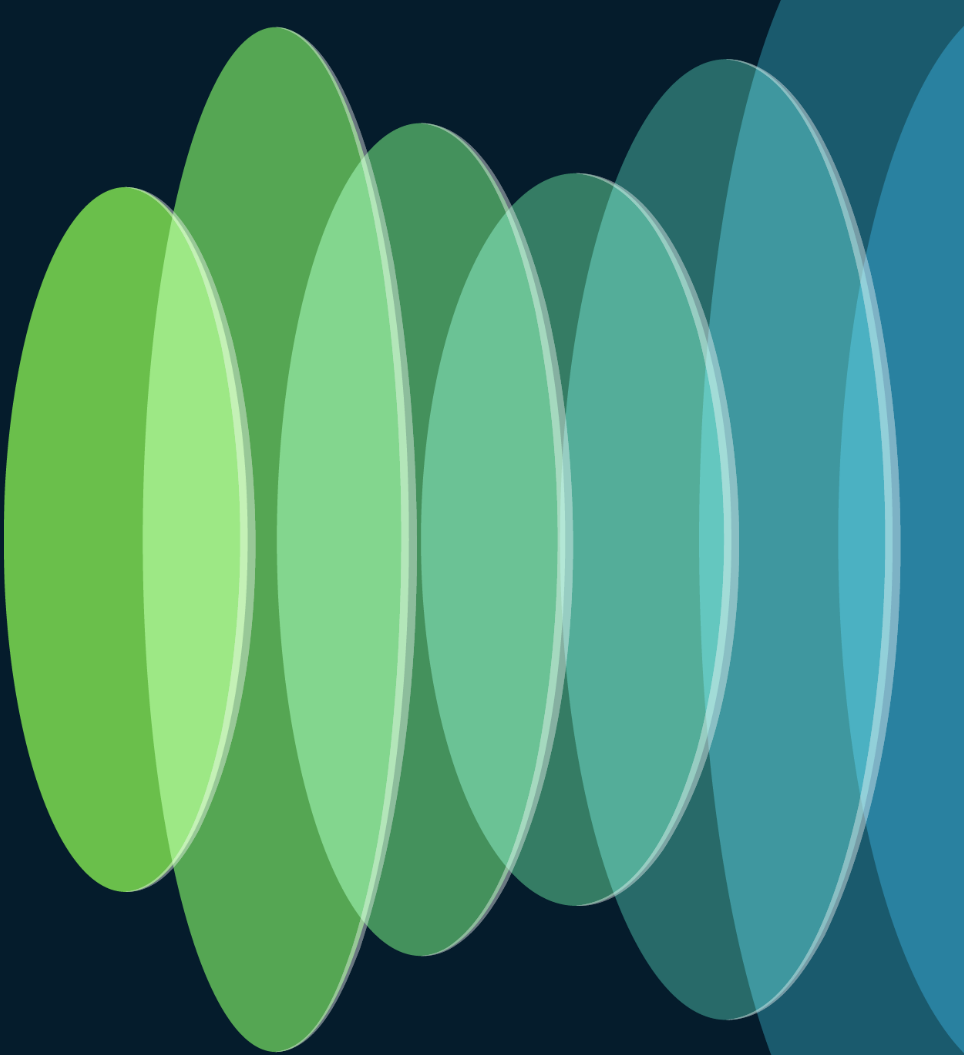
🟩 Peer to peer both within and between groups (no segmentation)

🟥 No peer to peer allowed

| P2P Setting | UDN =On<br>Drop UC = On | UDN =On<br>Drop UC = Off | UDN =Off<br>Drop UC = Off |
|---|---|---|---|
| Drop | 🟥 | 🟥 | 🟥 |
| Disable | 🟥🟢 | 🟩 | 🟩 |
| Forward Upstream | 🟥 | 🟥 | 🟥 |
| Allow Pvt Group | 🟥🟢 | 🟥🟢 | 🟥🟢 |

# Useful References

Things to use later for your designs



# Really good tools

- https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!wireless-troubleshooting-tools/wireless-troubleshooting-tools
  - Wireless Config Analyzer Express – WCAE
  - WLAN Poller
  - WiFi Hawk
  - Wireless Debug Analyzer
  - WLC Config Converter BETA
- Power Calculator Tool - http://tools.cisco.com/cpc/launch.jsp

# Useful References

- WiFi 6E 6GHz WW allocations: https://www.wi-fi.org/countries-enabling-wi-fi-in-6-ghz-wi-fi-6e
- 9800 Best Practices: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/guide-c07-743627.html
- 6GHz Deployment Paper: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/ghz-unlicensed-spectrum-reg-wp.html
- Blog part 1: https://blogs.cisco.com/networking/wi-fi-6e-something-old-something-new-something-borrowed-something-blue-part-1
- Blog part 2: https://spaces.at.internet2.edu/display/eduroam/eduroam-US+Knowledge+Base
- ISE Scale Documents: https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html

# Unplugged

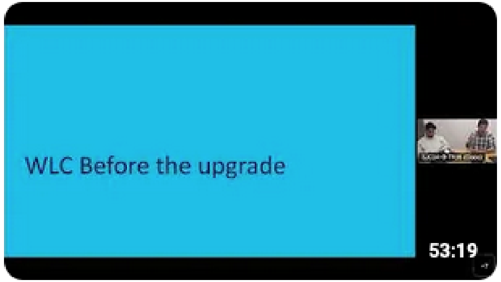
- New content every two weeks
- 60+ Videos
- Both Catalyst and Meraki
- Topics in Migration, Operations,
- Standards, AI Ops and many others!

Unplugged Connectivity

Cisco Cloud Monitored Wireless LAN Controller (Part 2 - Using the Dashboard)

Cisco Unplugged
A recurring live series to keep you in tune with the world of Wi-Fi
Over 26,000 views to date, with over 835 subscribers!
YouTube
youtube.com/@getunplugged
Las Vegas,NV
Unplugged
Dan Klamert
Al Dumdei | Scott Clayton | Ian Procyk

youtube.com@getunplugged



Back to School Cisco Wireless Best Practices (Summer 2023 - Session #1)

# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](http://www.CiscoLive.com/on-demand)

Contact me at: aldumdei@cisco.com

The bridge to possible

# Thank you

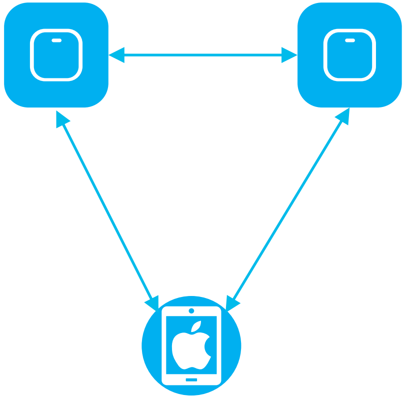
#CiscoLive

# Additional material for design reference

# RF Design

## Legacy bands and 6GHz

# General design guidelines



- Three things to watch
  - AP Downlink
  - Client Uplink
  - AP Neighbors
- It’s all about SNR and time
  - Directional antennas help to reduce interference in high-capacity areas.
  - Increase basic rates, decrease SSID count
  - RX SOP can be your friend
  - Use of .11v & .11k action frames are good but do take airtime
    - .11K can cause high CPU.
  - .11r very helpful for 11r compatible clients (especially .1x like Open Roaming)*

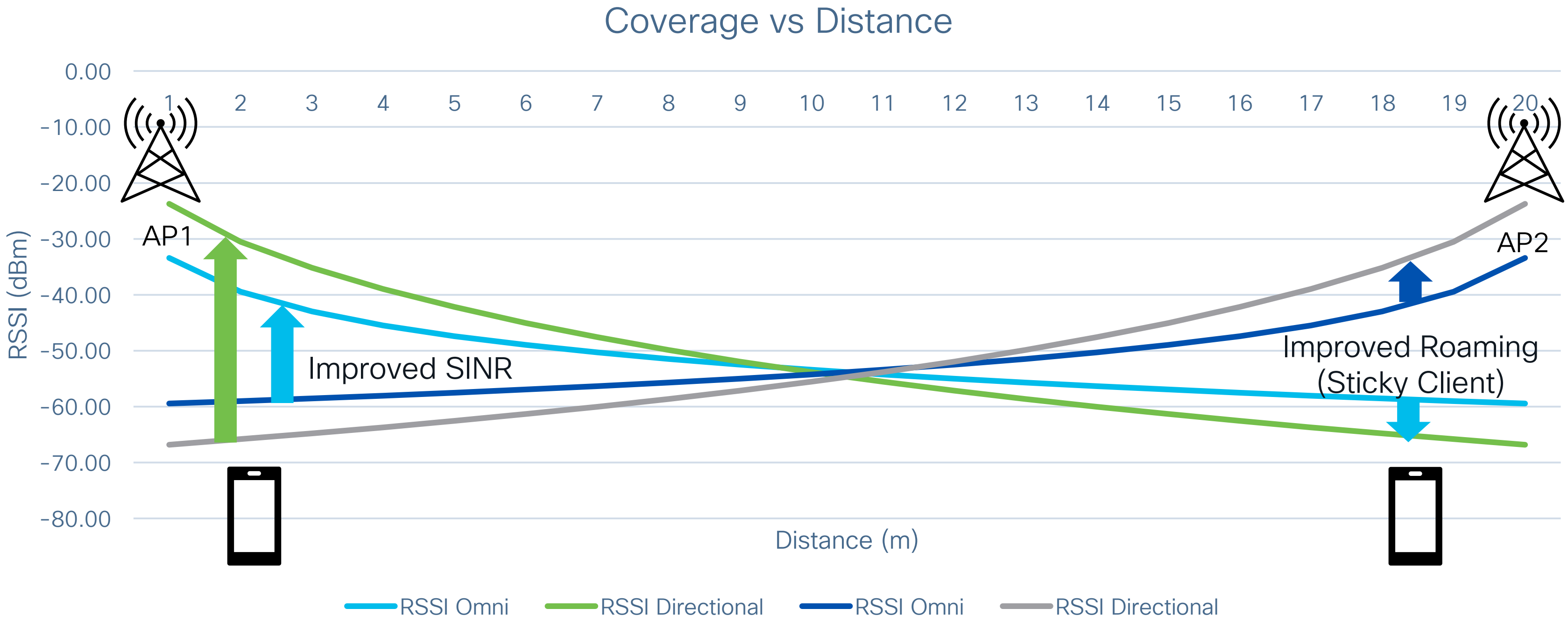
Early versions of RX-SOP

* Note: Not currently supported with CoA enabled on Meraki

# High Density RF Design

- You cannot compensate for poor RF design with optimization!
- The challenge is more what do the APs not hear than what they hear.
- Find APs with highest client counts (Catalyst Center Assurance Network Health)
  - Adjust TPC for more even distribution
  - Band Select and Load balancing are secondary effects
- The 9104s make sure you understand orientation
  - Portrait or Landscape
  - DCA/TPC not useful as sidelobes are very low and hence very little AP2AP
    - Manual RF plan
    - Use a RF design tool to help with this.

# Why directional antennas

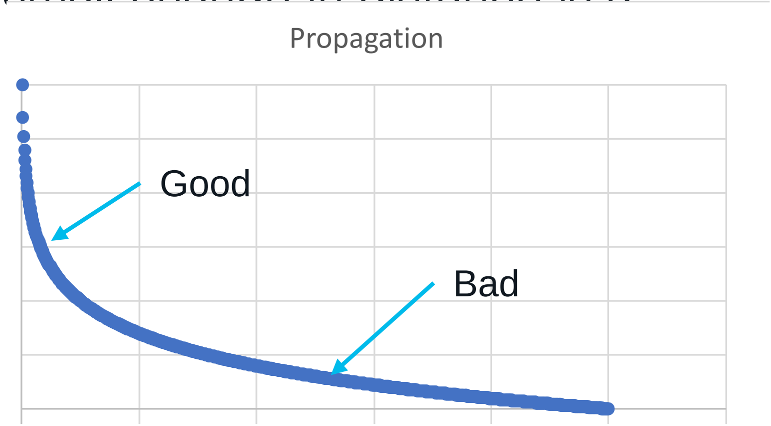


# Things that make design challenging

- Fire walls and beams (especially behind walls)
- Stair wells and elevators
- Esthetics
- Clean room/OR
- Small rooms with cinder block construction
- Building/Classrooms that are very close together

# Designing for location

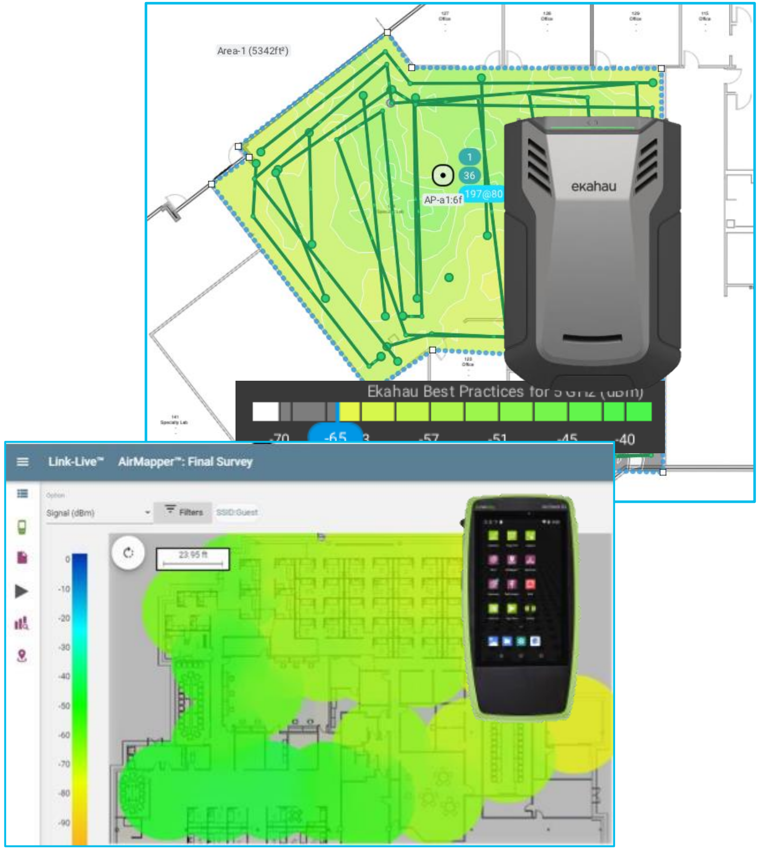
- For RSSI based location what is desirable is a small change in distance is a big change in RSSI
- Need >3 APs @ dispersed angles (-75dBm)
- Location only with within AP perimeter.
- Walls and floors add distance
- Directional antennas:
  - Directional antenna help the rate of signal change between APs.
  - Important that you get the right AP MAC addresses in the right location and the right direction for the antenna.



# Predictive vs Measured

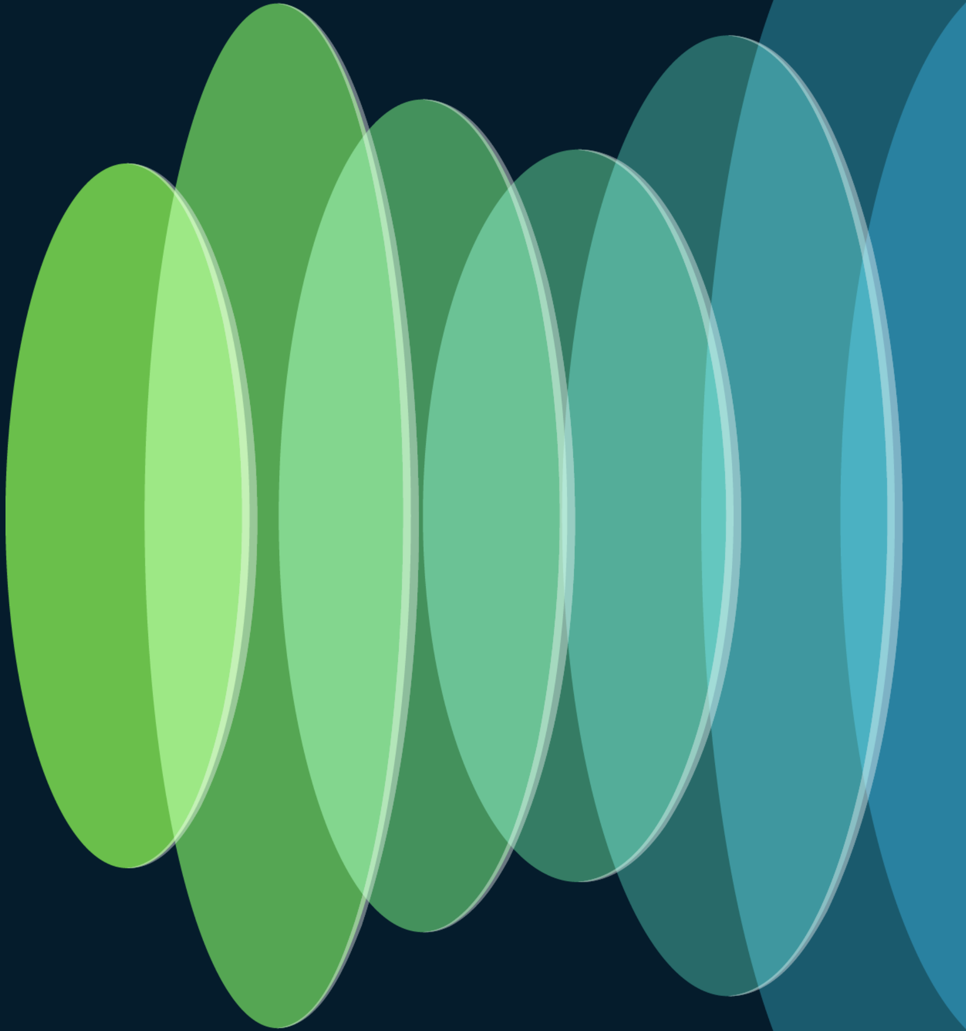
## When is good enough, good enough?

- A Measured Site Survey is an actual measurement of the RF Coverage in each space
- Ekahau and NetAlly both have Instruments specifically for measuring Wi-Fi
- Predictive Surveys often good enough
  - Garbage in, garbage out
  - Bound predictive with measurements



# 6GHz

## How do I use it in my design



# Things to note about 6GHz LPI

- FCC 5dBm/MHz, 30dBm Max, ETSI 10dBm/MHz, 23dBm Max.
- Typically, 1:1 overlay if existing APs at power level 3 or higher.
- 6GHz Mandates WPA 3 which include PMF mandatory.
- Only “permanently attached integrated” antennas can be used.
- No wildcard probing allowed.
- Introduces 4 new methods of discovery:
  - Reduced Neighbor Report (RNR) Out-of-Band discovery.
  - Preferred Scanning Channels (PSC) In-Band discovery.
  - Fast Initial Link Setup (FILS) In band discovery.
  - Unsolicited Probe Response (UPR) In band discovery.

# 9166D1 Wi-Fi 6 Indoor Access Point

## Cisco® Catalyst® 9166D1-x

Directional, Tri-Radio with 12 Spatial Streams!

### Penta-Radio Architecture

1. 2.4 GHz Client Radio: 4x4:4SS
2. 5 GHz Client Radio: 4x4:4SS
3. 6 GHz Client Radio 4x4:4SS (XOR to 5GHz)
4. Dedicated tri-band auxiliary radio
5. 2.4 GHz IoT Radio

### 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

### Internet of Things Capabilities

- Built-In Environmental Sensors
- Application Hosting Technology
- USB port with 4.5 W power output

### 5 Multigigabit (mGig) PoE Port

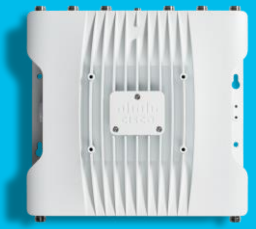
- Optional DC Power

Subject to change

*2/5/6 mode

† SW support post-FCS

# 6GHz Outdoor Options



IW9167E/I

IW9167E-STA

IW9165E/D

9163E

## 6GHz Outdoors

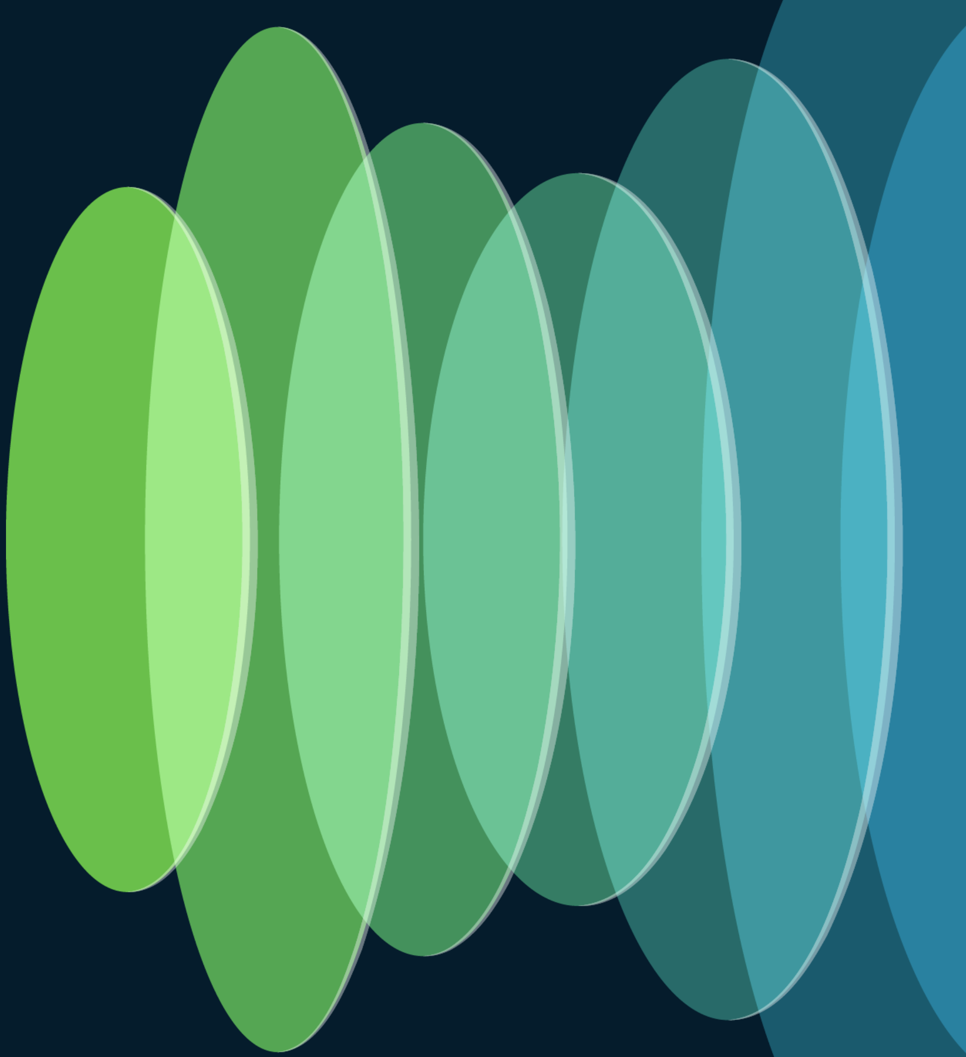
1. Must meet FCC Standard Power Requirements
    1. Must comply with AFC
    2. GPS/GNSS
2. Must be only Outdoor/SP (reconfigurable is not acceptable)
3. Not Mobile
4. Can use external antennas
5. Can (should be) weatherized

# Design Considerations

- No external antennas options for high ceiling designs
- Wide variety of clients behavior
  - Some clients only use RNR which means you must transmit legacy bands.
  - Roaming from WPA 2 to WPA 3 is reauthentication
  - Roaming between WLANs with different policy profiles requires reauthentication.
  - Clients are often looking for strong signals at 6GHz to join (>-65dBm)
  - Can have RNR with PSC and FILS or UBR

# AI RRM

## The next generation of RF management



# Exceptional Wi-Fi with Cisco's AI-Enhanced RRM

Radio resource management leveraging the power of machine learning

## Customer experiences

### Traditional RRM

- **Optimizations** are reactive to that point in time.
- **Configurations** require a high level of RF expertise to be made optimal.
- **Visibility** into RRM decisions and benefits is limited to the Command-Line Interface (CLI).
- **Troubleshooting** requires CLI access and knowledge of debug commands.

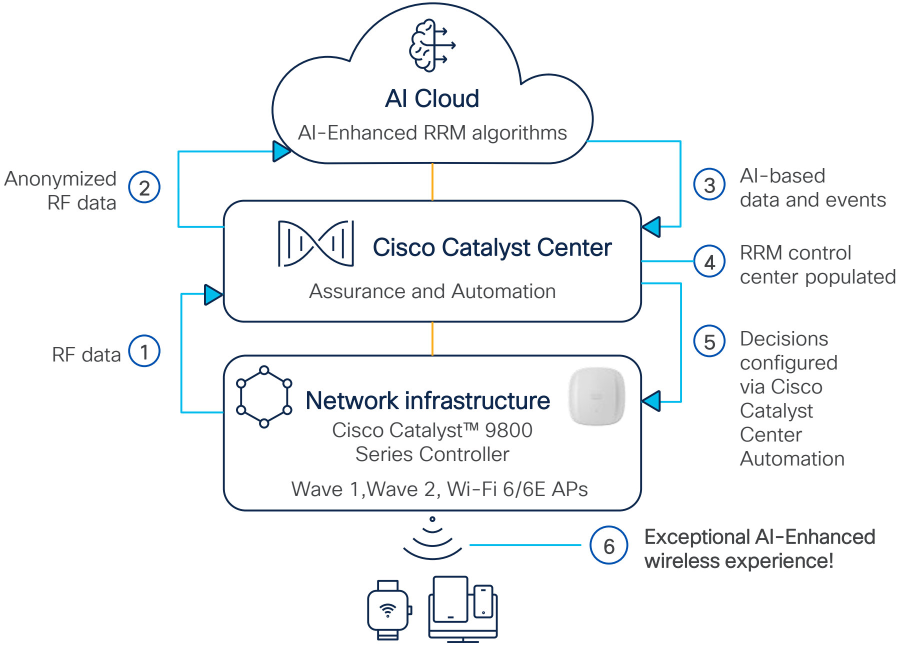
## Product capability

### AI-Enhanced RRM

- **Optimizations** are proactive and use Machine Learning (ML) to analyze 2 weeks' worth of RF data to find patterns by leveraging Cisco's AI Cloud.
- **Configurations** are simplified, have a concept of busy hours, and have actionable insights when AI-Enhanced RRM detects a more optimal setting.
- **Visibility** into RRM decision history and benefits are displayed on an aesthetic dashboard through Cisco Catalyst Center Assurance.
- **Troubleshooting** is made easy with a button to download all CLI output in a zip file.

## Customer benefits

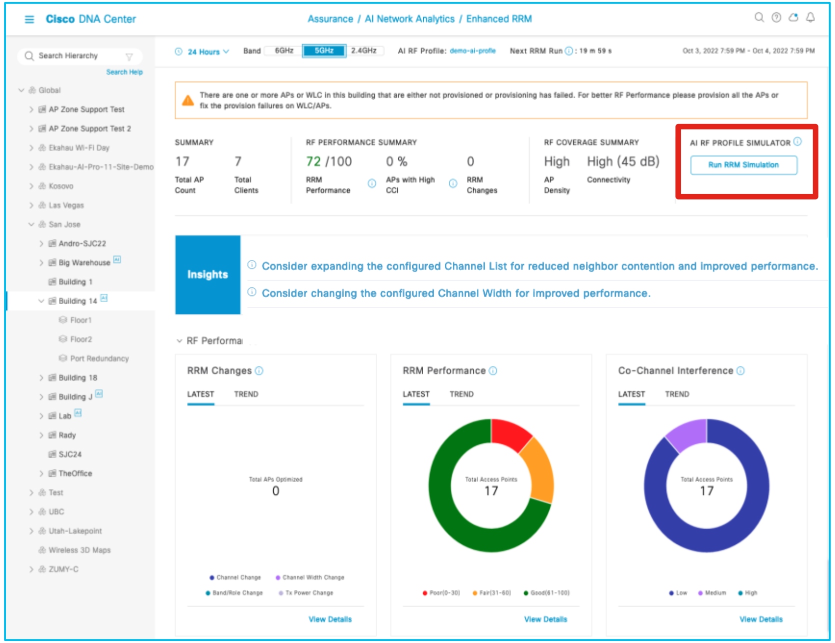
- An improved end-user experience through the AI-driven self-optimizing RF.
- A reduction in network operational cost by letting AI-Enhanced RRM take care of wireless optimizations, which is more efficient than traditional RRM.


AI Cloud
AI-Enhanced RRM algorithms
Anonymized RF data
2
3
AI-based data and events
Cisco Catalyst Center
Assurance and Automation
4
RRM control center populated
RF data
1
5
Decisions configured via Cisco Catalyst Center Automation
Network infrastructure
Cisco Catalyst™ 9800 Series Controller
Wave 1,Wave 2, Wi-Fi 6/6E APs
6
Exceptional AI-Enhanced wireless experience!

**Supported WLCs:** Catalyst 9800-CL, 9800-L, 9800-40 9800-80
**Supported access points:** All Wave 2, Wi-Fi 6/6E APs
**Suggested software versions:** Cisco Catalyst Center 2.3.7.4+ (WLC not managed) or 2.3.5 (Wi-Fi 6E), Cisco IOS® XE 17.9.5+

# AI Enhanced RRM

- What is RRM?
- The goal for AI Enhanced RRM since the beginning has been to provide clear, and actionable information
- Insights give Actionable suggestions on how to improve the configurations
- Break up profiles on sites. Dis-similar floors can use different profiles
- No longer requires Catalyst Center to Manage the controller!
- All of the APs on the WLC are assigned the AI RF Profile (small interruption)
- All the sites on a controller must be assigned. A WLC can either run legacy RRM or AI Enhanced RRM but not both
- The RF group Group Leader Changes from WLC to CC/Cloud
- Loss of cloud WLC fails back to group leader



AI RF Profile: demo-ai-profle

Next RRM Run : 19 m 59 s

Oct 3, 2022 7:59 PM - Oct 4, 2022 7:59 PM

There are one or more APs or WLC in this building that are either not provisioned or provisioning has failed. For better RF Performance please provision all the APs or fix the provision failures on WLC/APs.

SUMMARY: 17 Total AP Count; 7 Total Clients

RF PERFORMANCE SUMMARY: 72 /100 RRM Performance; 0 % APs with High CCI; 0 RRM Changes

RF COVERAGE SUMMARY: High AP Density; High (45 dB) Connectivity

AI RF PROFILE SIMULATOR: Run RRM Simulation

Consider expanding the configured Channel List for reduced neighbor contention and improved performance.

Consider changing the configured Channel Width for improved performance.

# Security Concerns

## Basic Concepts in Wireless Security

# Wireless Security

What’s your policy!!

## Manage the Environment

- ✓ Rogue Management
  Basic Wireless Security
- ✓ WIPS
  Advanced Wireless Security
- ✓ Cisco CleanAir
  Visibility of non-WiFi interferers
- ✓ Switch-port Tracing
- ✓ RLDP

## Protection

- ✓ PMF or MFP (RMF)
  Secure the control
- ✓ Authentication
  Access
- ✓ Authorization
  To what?
- ✓ RBAC
  Least required, TACACs
- ✓ Encryption
  AES, CCMP, GCMP
- ✓ PSIRTS
  Vulnerabilities
- ✓ Key Management
  802.1x, PSK,SAE,OWE
- ✓ DHCP Spoofing
  Hide GiAddr, DNCP Snooping

## Segmentation

- ✓ Tagging
  VLAN, SGT
- ✓ ACL
  IP ACL, SG ACL, dACL, URL ACL
- ✓ Routing
  PBR, VRF, P2P
- ✓ Fabric
  Macro/Micro

# Use Cases

- 3 Band SSID
- All WPA3
- Control of devices

BOH/Office

- Separate 2.4+5 and 6GHz
- WPA 2 legacy
- WPA 3 6GHz
- Same SSID

General Use

- Separate 2.4+5 and 6GHz
- WPA 2 legacy
- WPA 3 6GHz
- Different 6GHz SSID

Special Case

- Separate 2.4+5 and 6GHz
- WPA 2 transition legacy
- WPA 3 6GHz
- Same 6GHz SSID

Not recommended

## 17.12 adds support for Transition Mode 1 profile to rule them all!

- BOH/Office
  - If you can control the devices.
  - Cisco has this deployed in certain offices
  - Fast roaming works across bands
- General use
  - Accommodates legacy clients
  - Not fast roaming between bands
  - Some clients may “bounce” causing disruption to client and network loading.
  - Typically recommended for Eduroam
- Special Case
  - Like General Use
  - Can help reduce the bounce in general use
  - RNR is still effective
  - Clients will often stay at 5GHz
- Not recommended
  - It works
  - Client may think they are on WPA3 when on WPA2

# WPA3-Personal – SAE

## Simultaneous Authentication of Equals (SAE)

1 Protection against brute force “dictionary” attacks, passive attacks for Personal deployment (Dragonfly Handshake)

2 **Natural password selection:** Allows users to choose passwords that are easier to remember

3 **Forward secrecy:** Protects data traffic even if a password is compromised after the data was transmitted

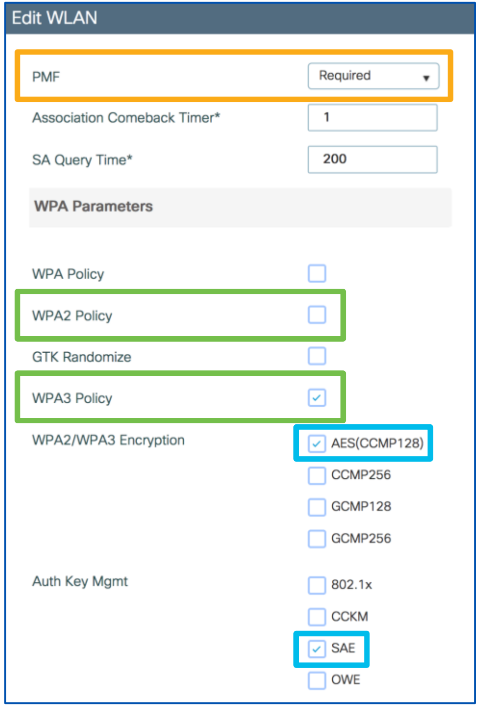
4 **Transition mode:** Coexistence of WPA2 and WPA3, easy adoption

5

6 PMF enabled (protected management frames)

Note: 9800 17.10 and later IOSXE supports iPSK with WPA3, Merak support is roadmap for WPA3 with iPSK

# WPA3 SAE - Getting the configuration right



Edit WLAN

| | |
|---|---|
| PMF | Required ▾ |
| Association Comeback Timer* | 1 |
| SA Query Time* | 200 |

**WPA Parameters**

| | |
|---|---|
| WPA Policy | □ |
| WPA2 Policy | □ |
| GTK Randomize | □ |
| WPA3 Policy | ☑ |
| WPA2/WPA3 Encryption | ☑ AES(CCMP128)<br>□ CCMP256<br>□ GCMP128<br>□ GCMP256 |
| Auth Key Mgmt | □ 802.1x<br>□ CCKM<br>☑ SAE<br>□ OWE |

Example for **WPA3-Personal only** (**WPA3-SAE**):

- Layer 2 Security Mode = WPA2 + WPA3
- PMF = Required
- WPA2 Policy unchecked, WPA3 Policy checked
- WPA2/WPA3 Encryption = AES(CCMP128)
- Auth Key Mgmt = SAE (then configure the passphrase too)

Note: technically, this should not be called “PSK”.

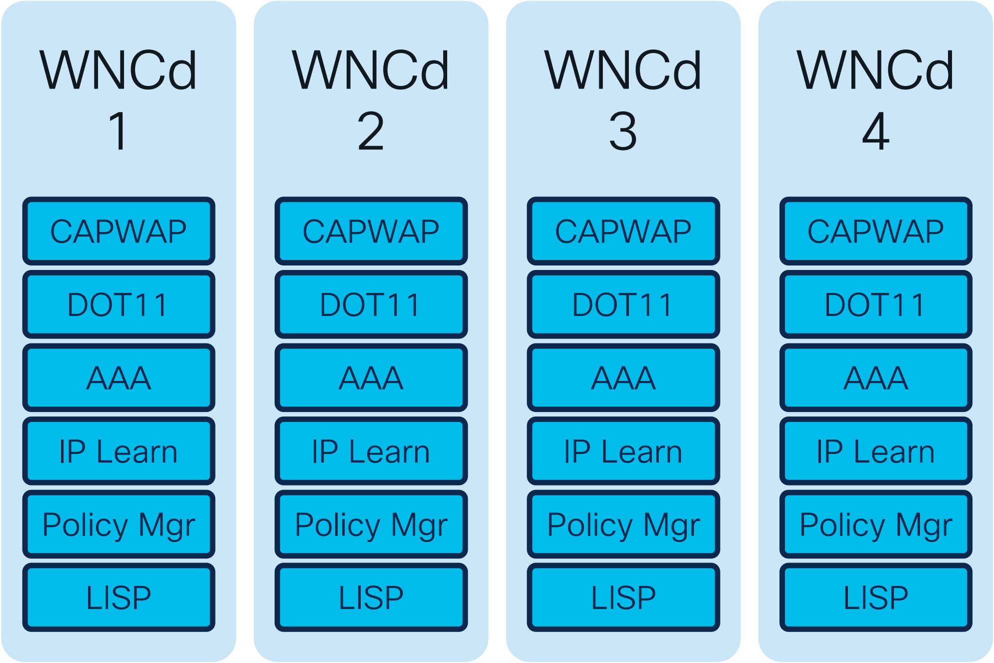
# WNCd

## What is it and how does it affect my design

# WNCd, what is it

- AireOS was single threaded, a task was received, scheduled and processed.
  - This worked ok but when it became busy it affected everything.
  - Sort of all or nothing approach
- IOS-XE (C9800) added multithreaded support
  - The Wireless Network Control daemon (WNCd) was created
  - The number of WNCd processes varied from 1 to 8 based on the size of the Wireless Lan Controller.
  - Each process runs independent of the other processes.
  - The processes are responsible for managing AP and Client sessions

# More about WNCd



WNCd 1

CAPWAP
DOT11
AAA
IP Learn
Policy Mgr
LISP

WNCd 2

CAPWAP
DOT11
AAA
IP Learn
Policy Mgr
LISP

WNCd 3

CAPWAP
DOT11
AAA
IP Learn
Policy Mgr
LISP

WNCd 4

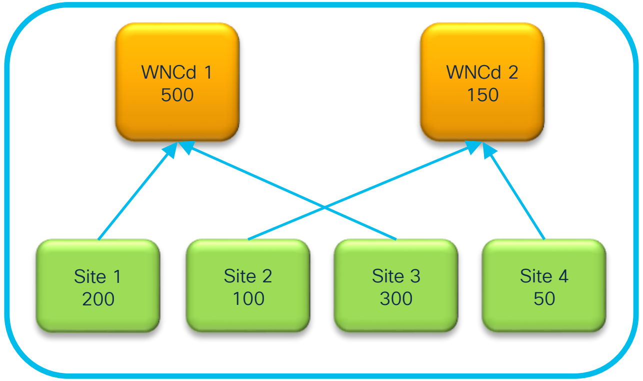
CAPWAP
DOT11
AAA
IP Learn
Policy Mgr
LISP

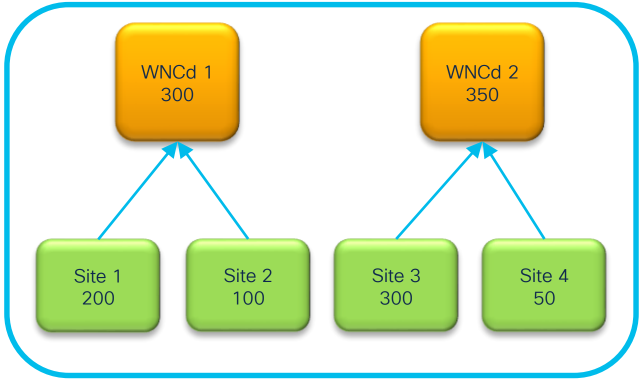
| Platform | WNCd Instances |
|---|---|
| EWC (AP or C9k switch) | 1 |
| C9800-L | 1 |
| C9800-CL (S) | 1 |
| C9800-CL (M) | 3 |
| C9800-40 | 5 |
| C9800-CL (L) | 7 |
| C9800-80 | 8 |

# How does this affect my design

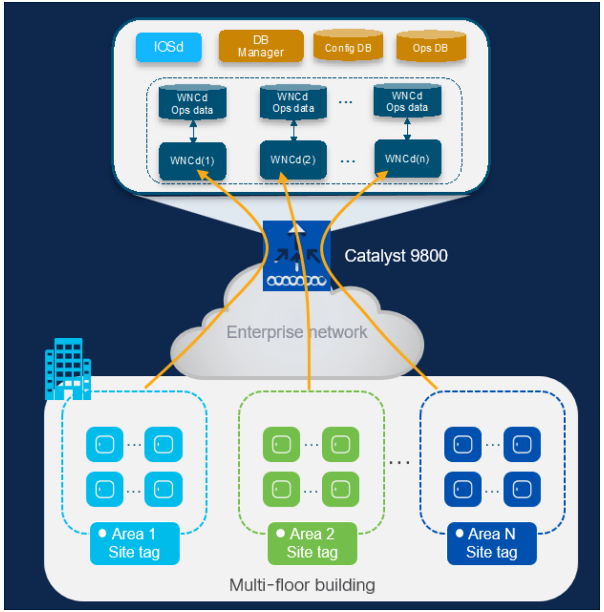
17.12 Automatic WNCd Load Balancing

- High CPU can cause APs to drop.
- Target less than 500 APs per WNCd.
- Roaming between APs on different WNCd process will add latency to the roam.
- Site Tags are used to map APs to WNCd process.
- Three methods of assigning Site Tags to WNCd processes.
  - Old – round robin
  - New – weighted grouping
  - New- RRM Neighbor based load balancing





# WNCd load balancing updates



Existing

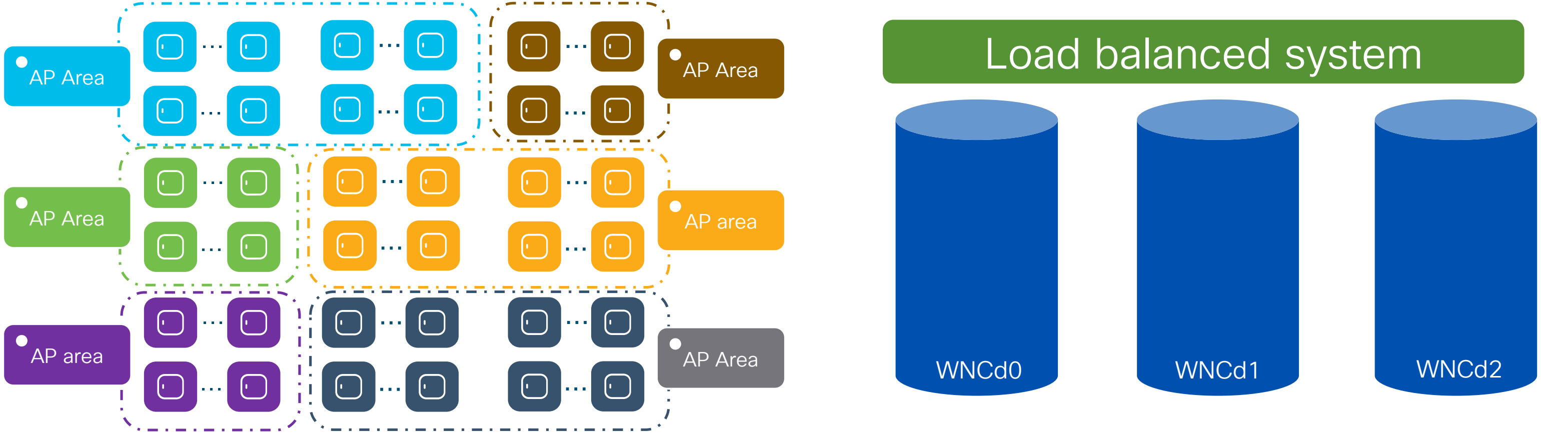
- Site Tag Based
- load input for large sites

## Recommendations for Local mode:

- Starting 17.9.3, "**load**" parameter can be configured, so site tags are allocated to WNCd based on the compute load
- Usually "**load**" equal to the number of APs

- What if customer cannot define named site tags (no AP names, no APs on maps) or simply doesn't want to do it?
- Starting 17.12.1, we have a solution! (RRM based) **Auto WNCd load balancing**
- RRM based Auto WNCd load balancing simplifies the site tag design

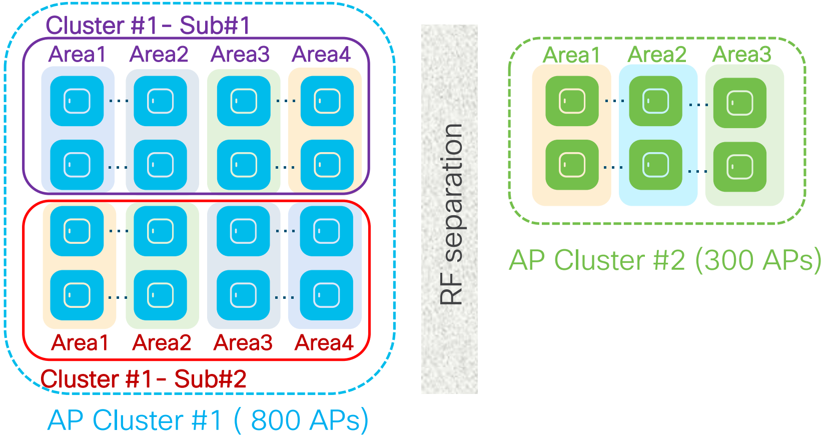
# RRM based Auto WNCd load balancing



## Key Points

- RF-based automatic clustering APs for even WNCd distribution
- On demand/Scheduled (Requires stable RF Env for best clustering)
- Off by default, supersedes site tag & load-based distribution

# RRM based auto WNCd load balancing



## Inner workings of load balancing algorithm

- AP clusters (**neighbourhood**) based on RSSI received from AP neighbour report on 5GHz
- Further division with **sub-neighbourhoods** if the # of APs goes above a defined size (400)
- Create **areas** from each sub-neighbourhood. Each area size will be MAX 100 AP. A sub-neighbourhood can have up to 4 areas.
- Assign areas to WNCd processes to optimize APs to WNCd load balancing

# WNCd Example #1

- High probe count can cause high WNCd CPU.
  - Poor coverage can drive up client probe rates
    - Coverage between buildings in campus
    - Areas where clients are entering and exiting
    - Outdoor areas
  - High roaming can increase client probe rates
    - Class lets out
    - Event starting or ending
  - If an AP goes offline this cascades

Solution

- Fix the coverage issues
- Reduce probe queue depth

# WNCd Example #2

- High volumes of mDNS traffic cause WNCd CPU
  - mDNS gateway should be enable to limit mDNS
  - Enabling Apple Continuity cause high volumes of mDNS
    - Typically meant for home use.
    - Dormitory student use
    - Guest rooms guest use
  - Monterey update allows MacBook to advertise as TV
    - Classrooms
    - Meeting/conference rooms

### Solution

- With mDNS gateway enabled, removed any service not required for the venue.
- For services that are enabled assign them to specific locations.

# Typical Use Cases

## Example design requirements and solutions

# University Campus (requirements)

- Periodic High Roaming times (Class Break)
  - High authentication/AAA
  - High dot11 activity
  - High probing
  - mDNS

# University Campus

- Design strategies
  - Group dorm and classrooms in the same WNCd
  - Reduce probe queue depth
  - Enable fast roaming/key caching
  - If local AAA (ISE) use distributed architecture with load balancing
  - Ensure good coverage where roaming will occur
  - See WNCd Example 2 for mDNS solutions
  - Clean Air shows hundreds of thousands of interferers…disable that band on Clean Air

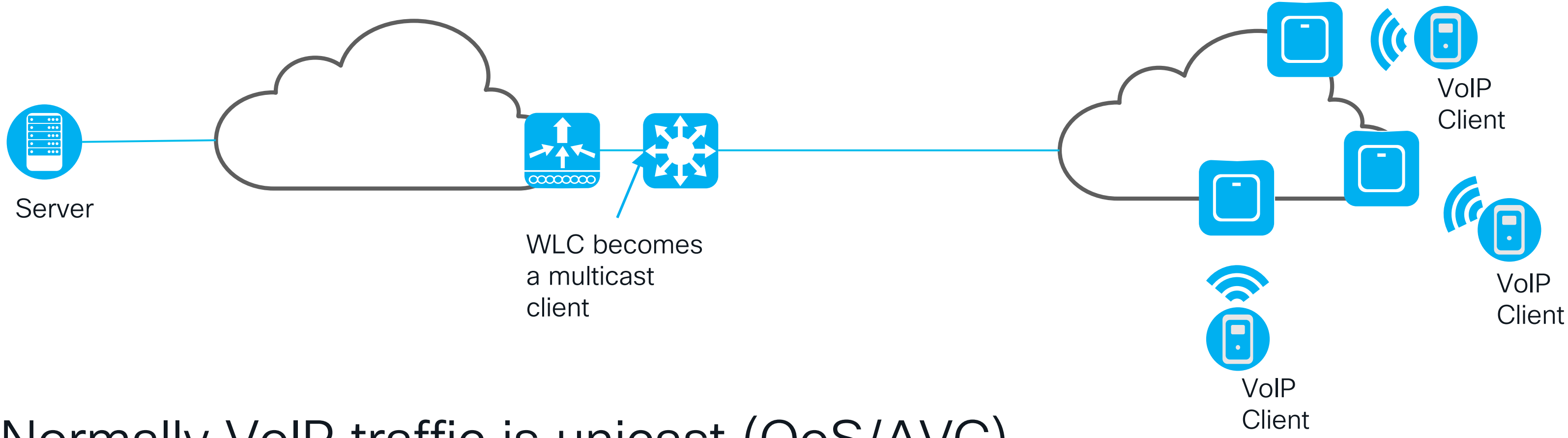
# Event Center (Requirements)

- Coverage is good but:
  - High client counts (>200)
  - High roaming loads at certain times
  - Wide range of clients and client behavior

# Event Center

- Design Solutions
  - Disable .11K as this is only useful at peak times and hit WNCd CPU
  - Watch out for high numbers of clients in authenticating state
    - May need to decrease EAP timeout to flush sessions not established (default is good)
  - Look for APs set to abnormally high-power levels.
  - Consider more directional antennas and APs
  - Do not enable passive client
  - Check for high ARP rates and police (>2000 Packets/sec)
  - In the case of multiple controllers on one core switch mac address capacity (CAM) is a concern.

# Hospital VoIP/Badge Paging



- Normally VoIP traffic is unicast (QoS/AVC)
- Paging is multicast
  - Server send message to clients which Multicast Group to join
  - All members join the group and get page from one of the clients

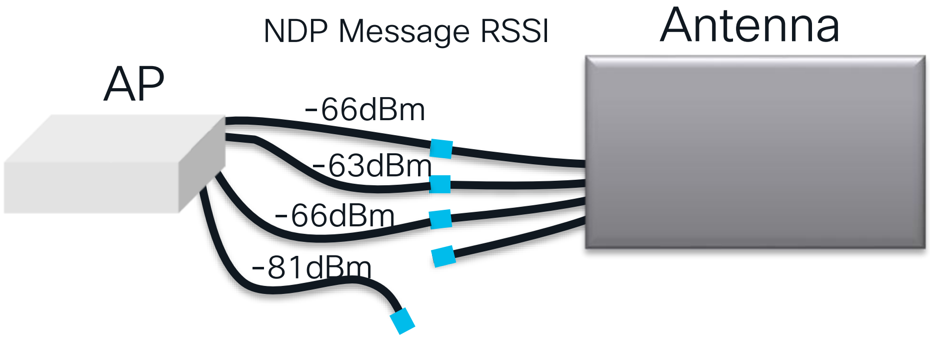
# Hospital VoIP/Badge Paging

- Design solutions
  - Enable IGMP snooping
  - Enabled Multicast-Multicast mode on the WLC
  - PIM Sparse Mode is used
    - L3 interfaces for AP management need PIM
    - L3 interfaces on the switch connecting to the WLC need PIM.

# Industrial/Manufacturing/Warehouse

- High ceiling environments
  - Ceiling height installations above 25 feet may benefit from directional antennas aimed downward at an angle or straight down, the Wi-Fi 6E CW9166D works well in this environment.
  - Omnidirectional antennas can be effective when lowered closer to the floor level, approximately 20 feet or lower.
- Predictive analysis surveys can be helpful to predetermine approximate AP locations and density. These environments may have sources of RFI and/or EMI that will impact a design and are most likely found during an onsite active site survey.
- Automated Guided Vehicles (AGV's) often use a workgroup bridge (WGB) for wireless connectivity. Cisco has two solution options for WGB via On-Prem Catalyst and Cisco Ultra Reliable Wireless Backhaul (CURWB). When using Cisco Cloud Meraki wireless then consider deploying in combination with CURWB for WGB requirements.
- Industrial often has legacy wireless client devices
  - Aging devices may only support 2.4 or partial 5GHz (pre UNII-2e)
  - May not support modern security requirements, good use case for iPSK

# Broken Antenna (for external antennas)



Some tuning required:

| Default values/Tuned Values | |
|---|---|
| Status | Disabled/Enabled |
| rssi-failure-threshold | 40 (dB)/15 (dB) |
| weak-rssi | -60 (dBm)/-65 (dBm) |
| detection-time | 12 min/12 min |

- Syslog or Traps
- Works with 4 or 8 antenna connections
- Use 2.4 and 5GHz if possible, for correlation

Syslog example (C9130 AP w/8 lead DART connector):

```
Broken Antenna Report from AP <mac> slot:0 band:2.4ghz dart:yes broken_antennas:D
Broken Antenna Report from AP <mac> slot:1 band:5ghz dart:yes broken_antennas:DEFGH
```

# Configuration Example and Default Values

```
vwlc(config-ap-profile)#antenna monitoring rssi-failure-threshold ?
  <10-90>        RSSI failure threshold value in dB

vwlc(config-ap-profile)#antenna monitoring weak-rssi ?
  <-90 - -10>        Weak RSSI value in dBm

vwlc(config-ap-profile)#antenna monitoring detection-time ?
  <9-180>        Configure the detection time in minutes
```

```
vwlc#sh ap name 3800-AP config general

 Cisco AP Name   : 3800-AP
================================================
...
AP broken antenna detection  : Enabled
    RSSI threshold         : 40
    Weak RSSI              : -80
    Detection Time         : 120
```

```
vwlc#sh ap profile name rf-profile-24g detailed

AP Profile Name: rf-profile-24g
.
.
AP broken antenna detection :
  Status             : ENABLED
  RSSI threshold       : 40
  Weak RSSI            : -80
  Detection Time       : 120
```