Designing Enterprise Wireless Networks for Challenging Environments

Tales from the Wi-Fi Crypts

Al Dumdei

BRKEWN-2054

Cisco Webex App

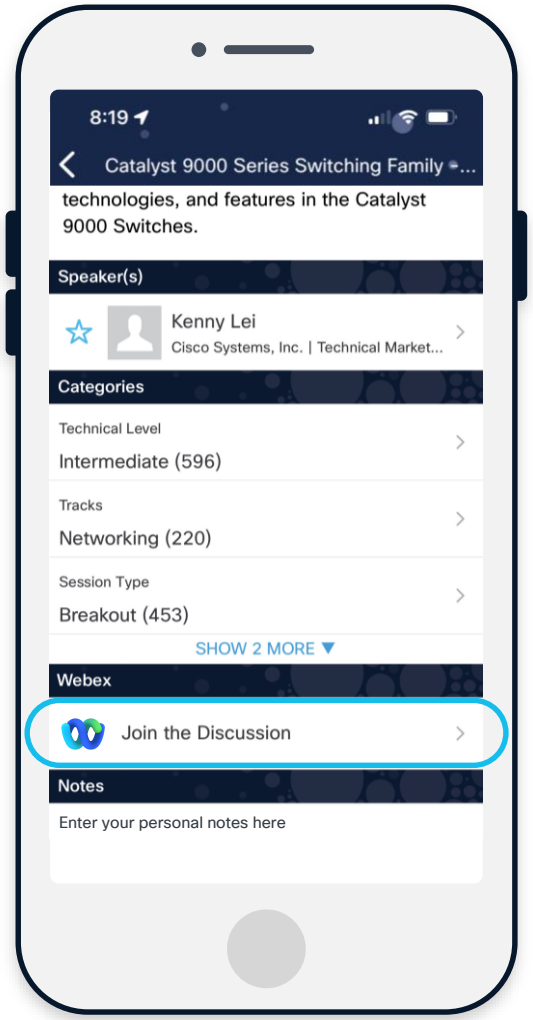
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 13, 2025.



https://ciscolive.ciscoevents.com/ciscolivebot/**#BRKEWN-2054**

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

Agenda



01 Introduction

02 Higher Ed Design

03 Healthcare/Voice Design

04 Large Venue Design

05 Design References

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

Use Cases

From the crypts



Higher Ed

Higher Ed has design challenges around topics like **scale**, Multi-Dwelling Units (**MDU**), and **consistent performance** on a wide variety of devices. This sector has a lot of overlapping challenges with other sectors.

Healthcare/Voice

Health Care has design challenges with multitude of older devices providing challenges with **security and SSID sprawl**. In addition, **phones** and badges are often part of the Wi-Fi design adding challenges around multicast and QoS.

Large Venue

Large venues (Stadiums, Airports, Convention Centers and the like) bring in challenges related to high density. **Good design principles** including the use of **6GHz spectrum** are required, and an understanding of how different **timer settings** can work together to improve (or reduce) the effectiveness of the venue. Client adoption and perception is key.

Other

Good to know references and links.

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

Design Constructs

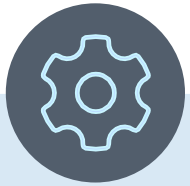


Wired considerations for wireless architectures



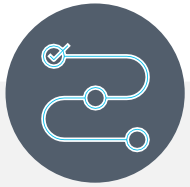
Switching

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



Segmentation

- VLAN
- VRF
- SGT
- Fabric



Gateway Requirements

- CAM Table
- Throughput
- IP helper

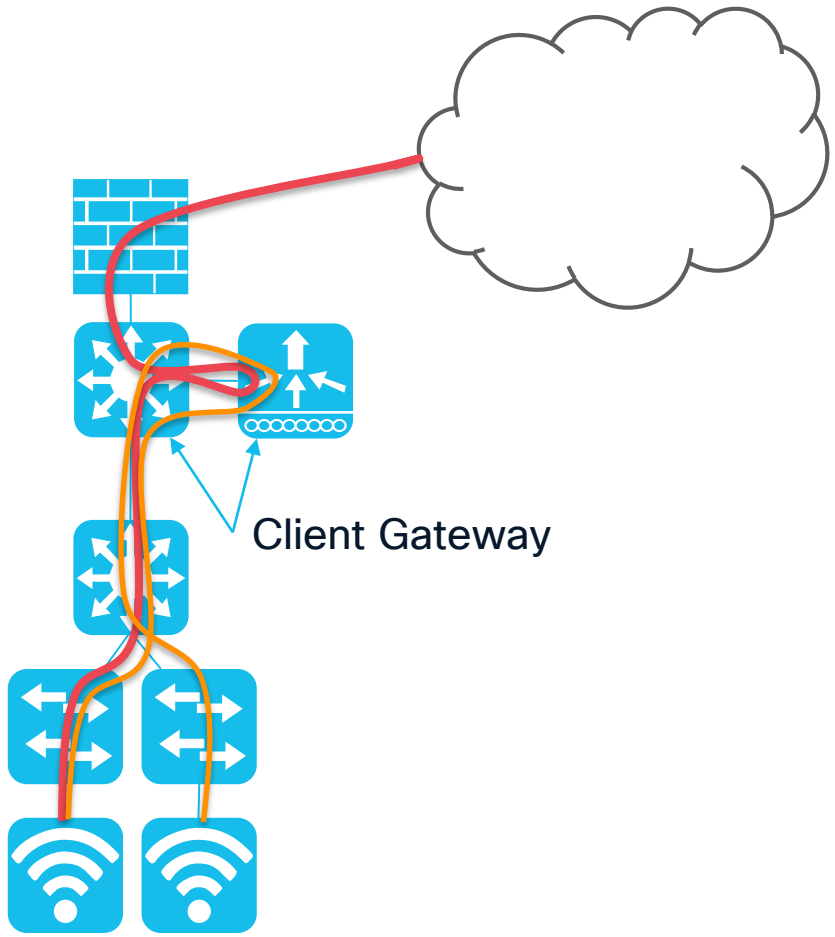


Cloud Considerations

- Private vs Public
- Must be FlexConnect LS
- Manageability

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

Some Basics – Central Switching



Central Switching/Tunnel

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

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

CW9800 / Centralized Data Plane



1RU



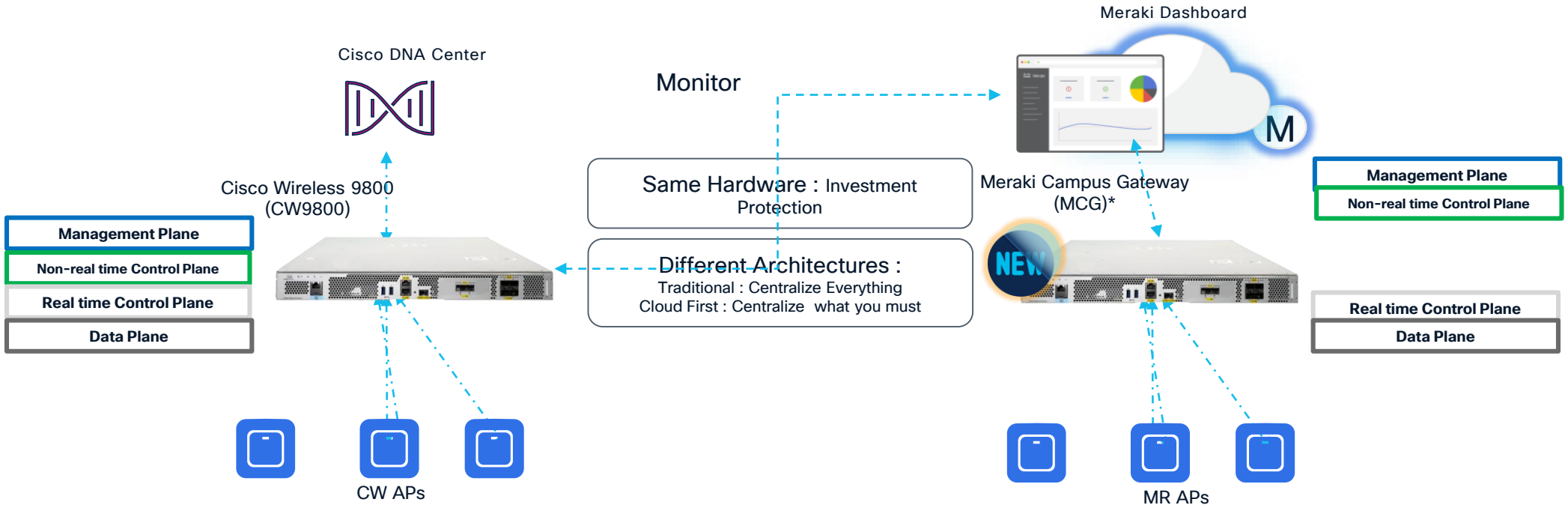
CW9800H1 / CW9800H2
6000 APs, 64,000 clients,
4 x 25Gbps / 2 x 40Gbps

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
- 17.14.1 first release, 17.15.3 is 1st gold star “candidate”

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

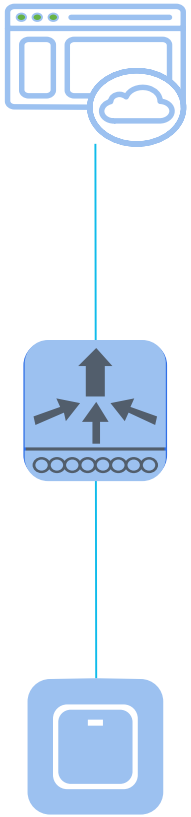
Campus Gateway Centralized Data Plane



On-Prem > Cloud enabled Hybrid With Monitoring > Cloud Managed

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

Just a bit deeper on the CG



Meraki Dashboard

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

Non-real time Control Plane
- AutoRF
- AirMarshall
- Rogues

Meraki Campus Gateway

Data Plane
- Data plane termination
- VLAN termination
- ARP proxy
- Multicast optimizations

Real time Control Plane
- Roaming – Key management
- AAA Auth Proxy

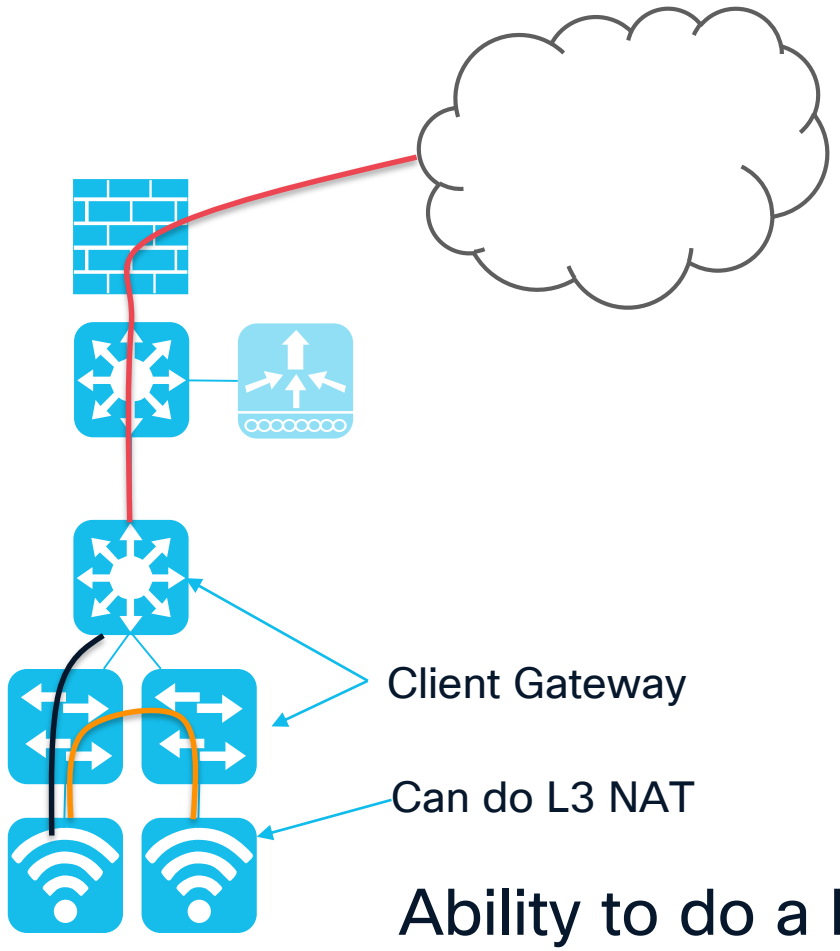
MR AP

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

Real time Control Plane
- Client Authentication
- Client state

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

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

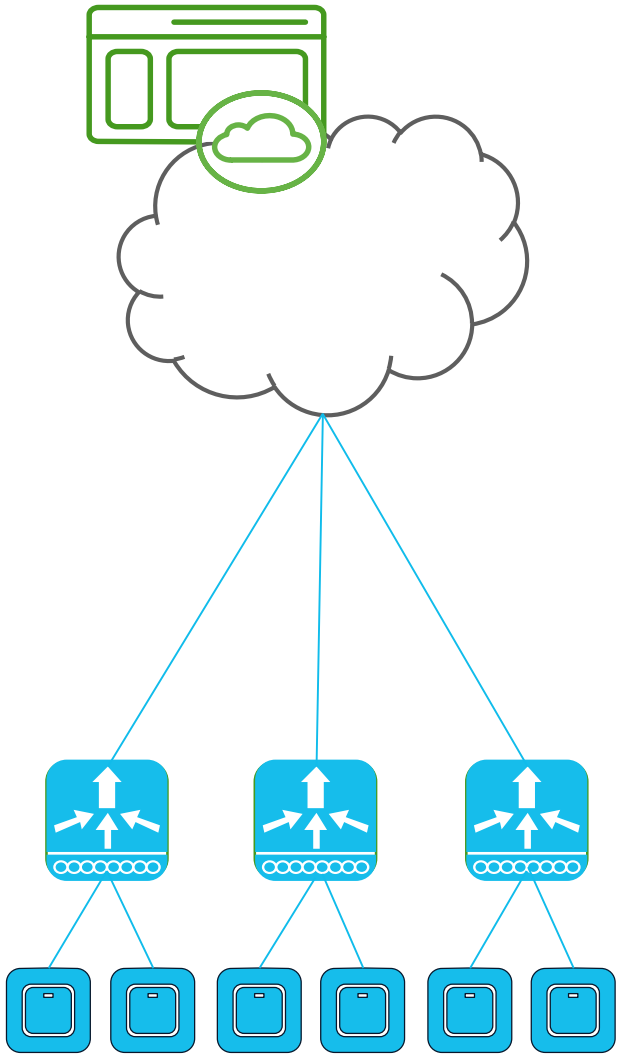
© 2025 Cisco and/or its affiliates. All rights reserved.

Architectures

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



Cloud Monitored C9800 Wireless Controller



Requirements	
Software	
	Cisco IOS® XE 17.12.3
Licensing	
	Cisco DNA Essentials Cisco DNA Advantage

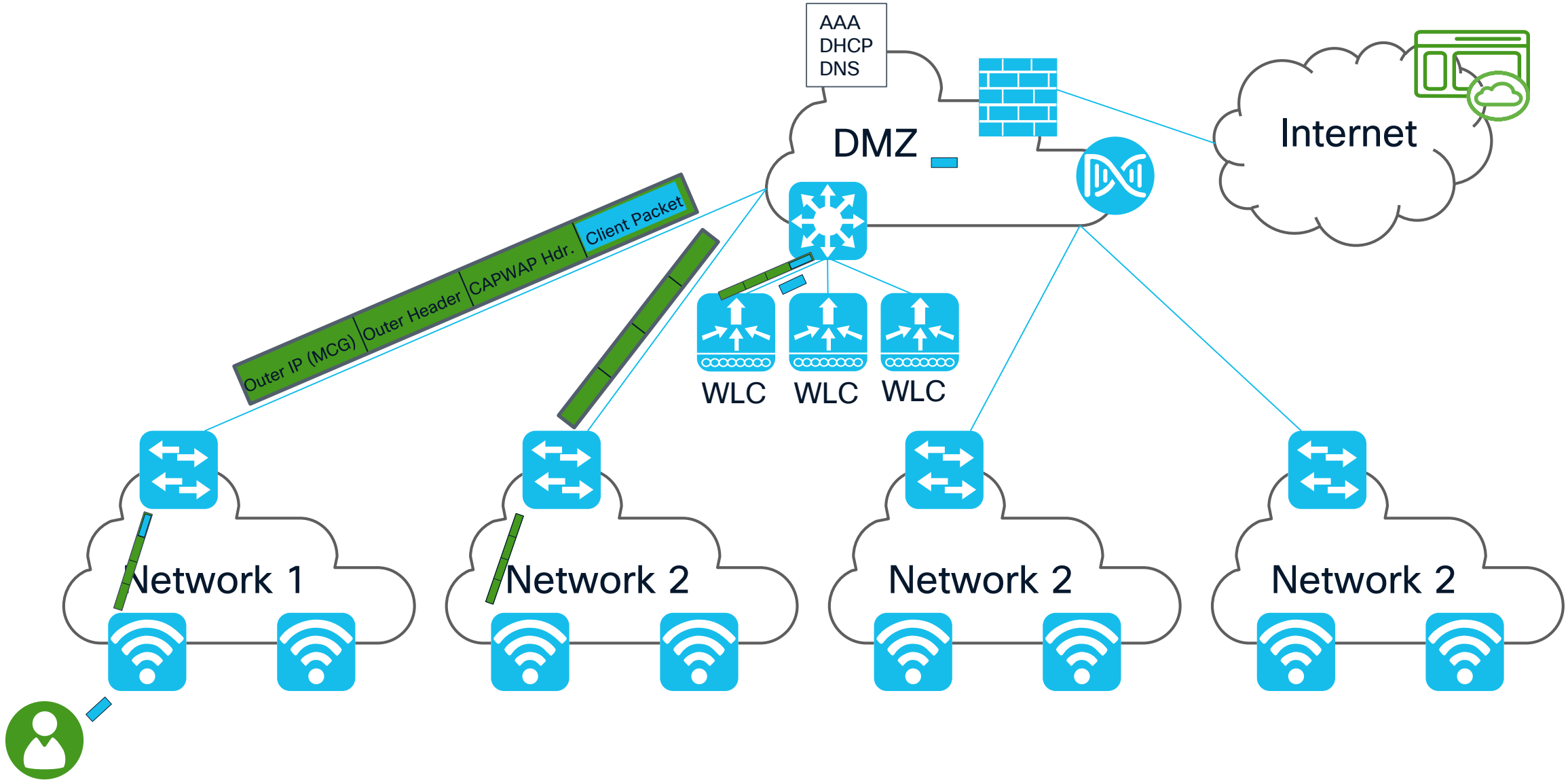
Table 2. Firmware and scale support[1]

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]* CW9800M/H coming soon

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

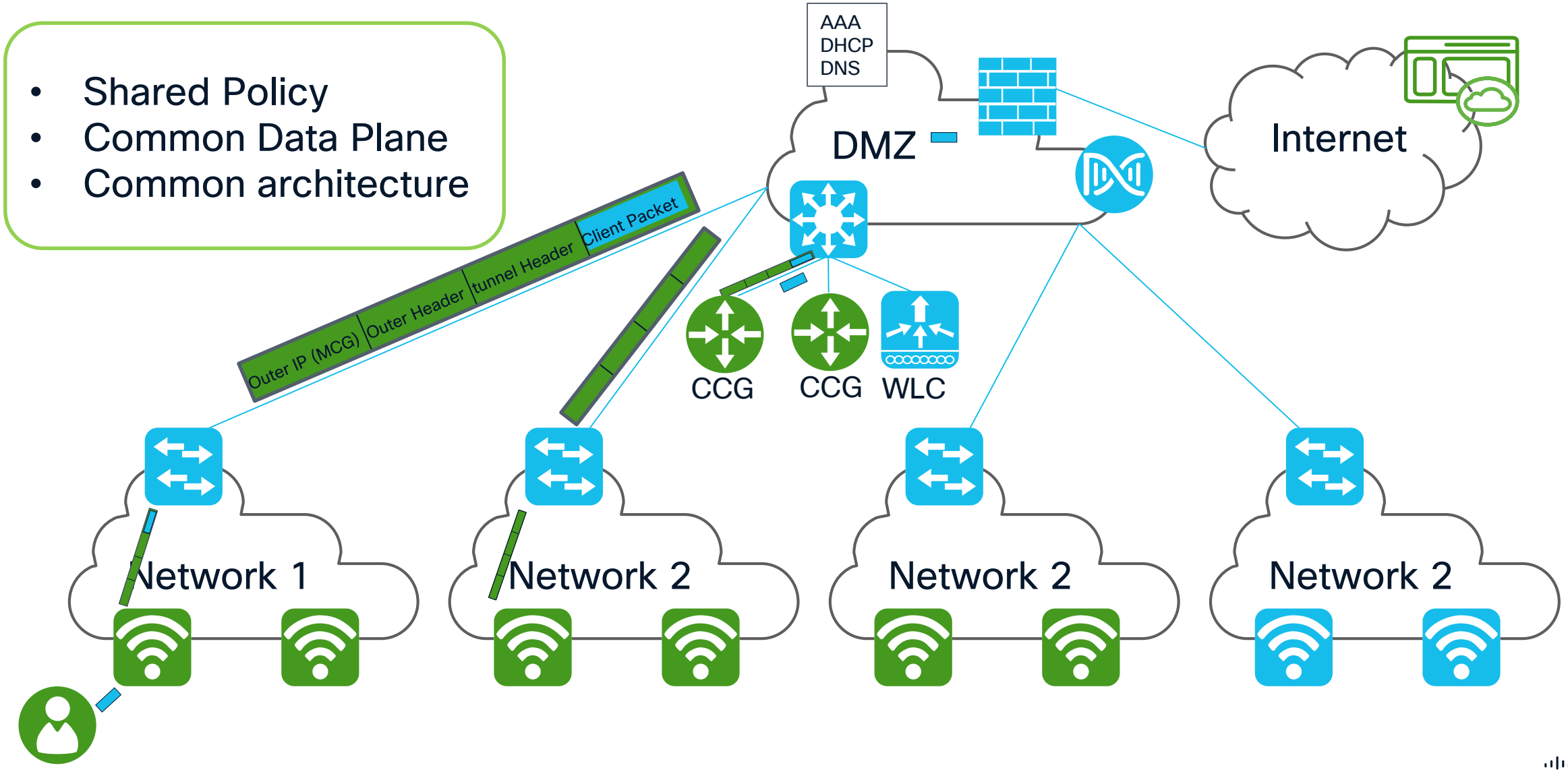
Central Switching On Prem with Optional Cloud Monitoring



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

Central Aggregation with Cloud Monitor and Management!

- Shared Policy
- Common Data Plane
- Common architecture



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

L3 Access in Wireless

1 Segmentation

For Security

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

Managed Service Providers :

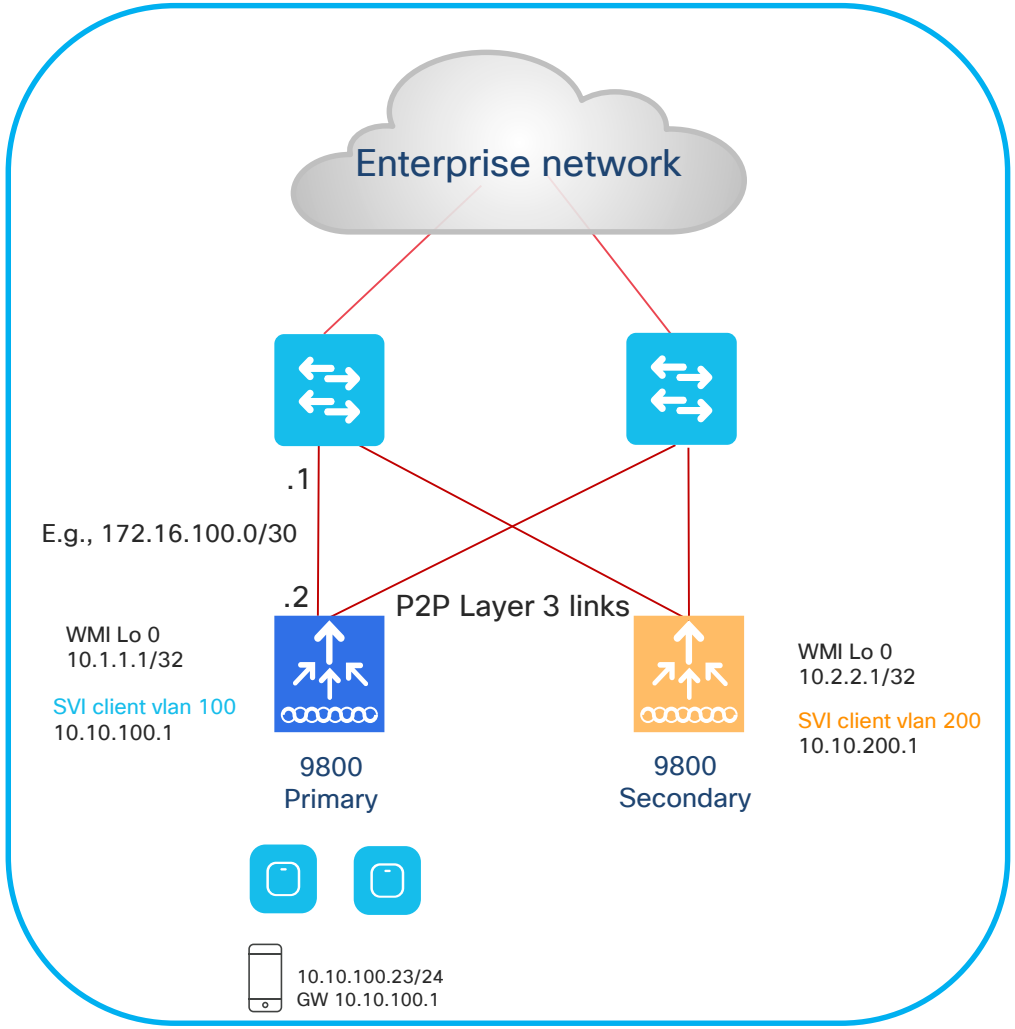
- Airports
- Multi-dwelling units

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**

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

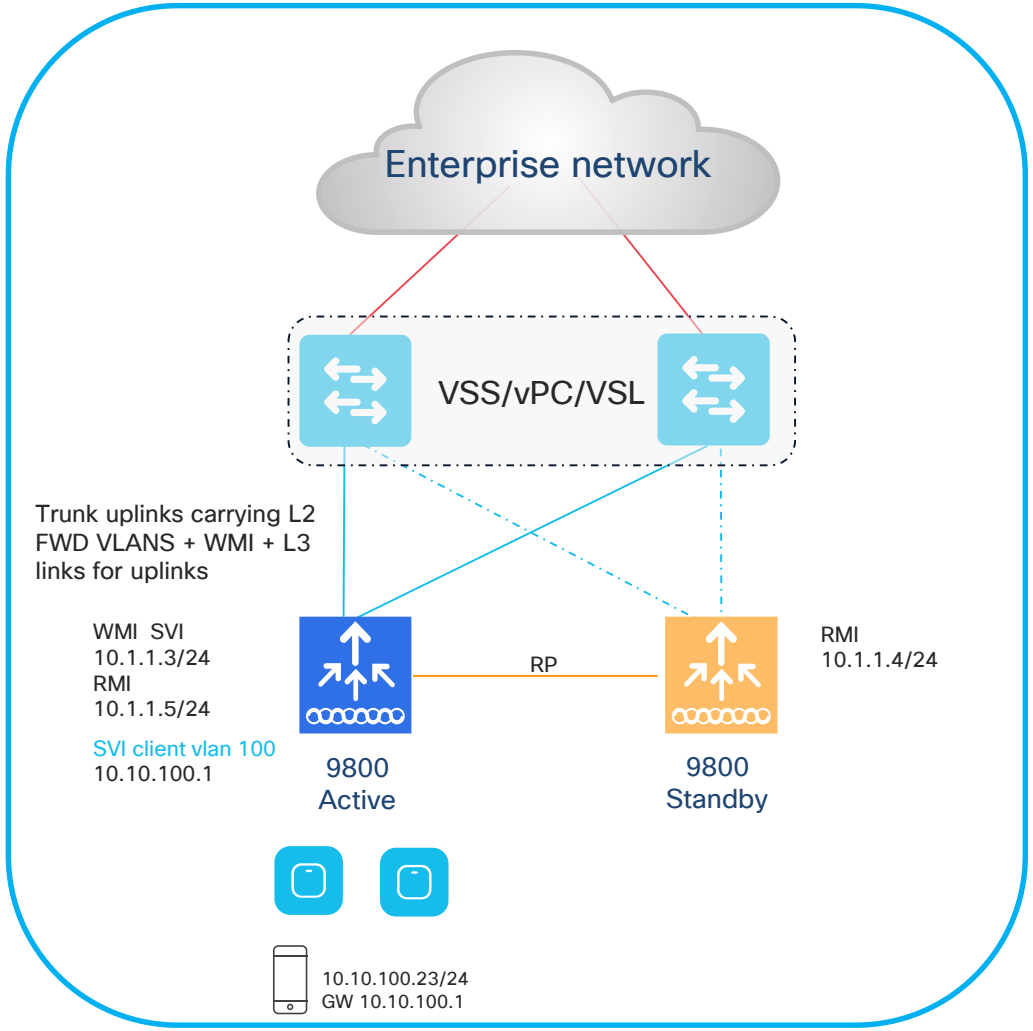
L3 forwarding topology – Full L3 mode



- 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

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

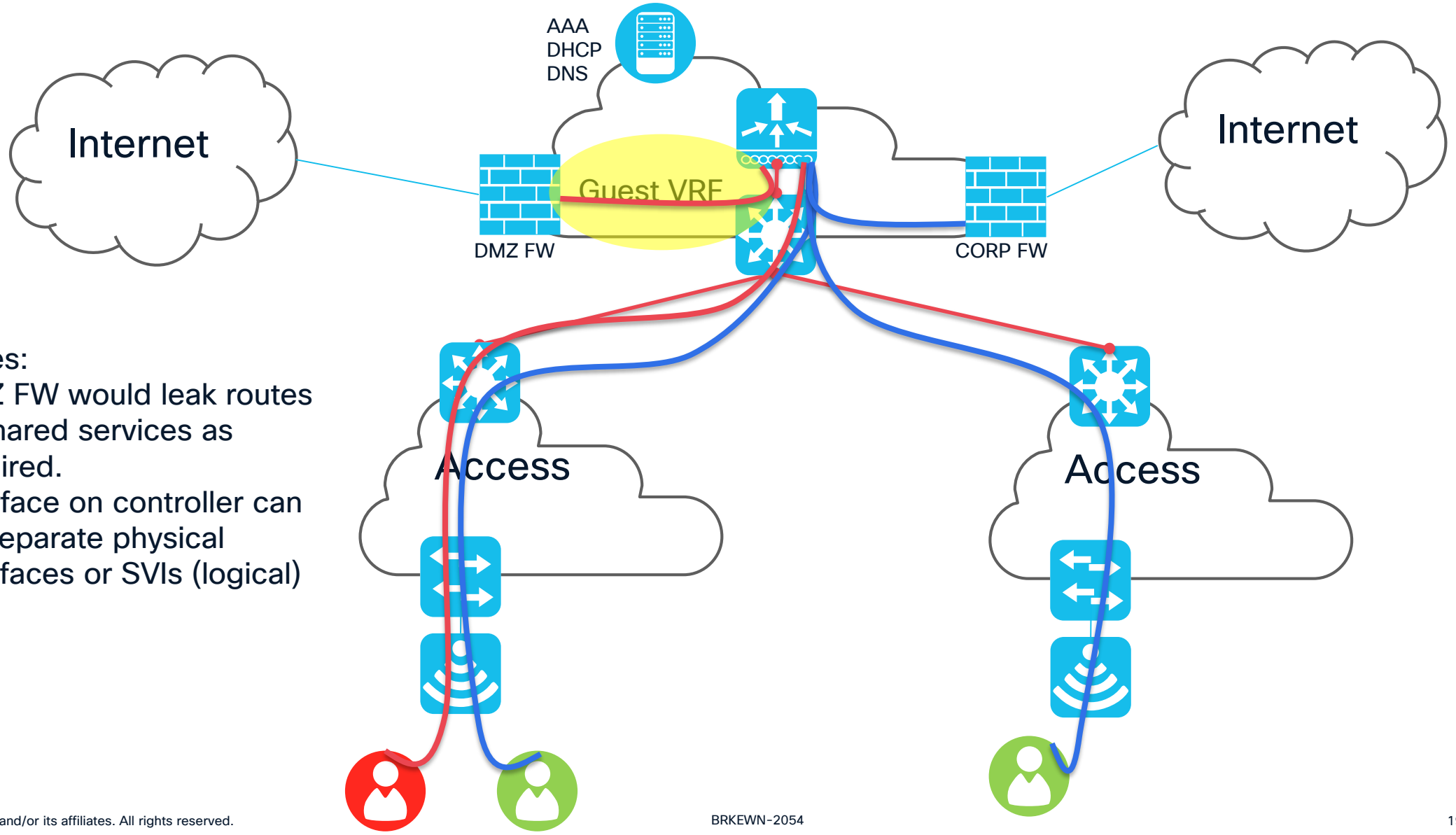
L3 forwarding topology – L3/L2 mixed mode



- 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
- RMI can be configured with SVI in WMI subnet (L2)
- High Availability: SSO or N+1 Supported

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

L3 Guest Solution (Hybrid L2/L3)



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

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

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:

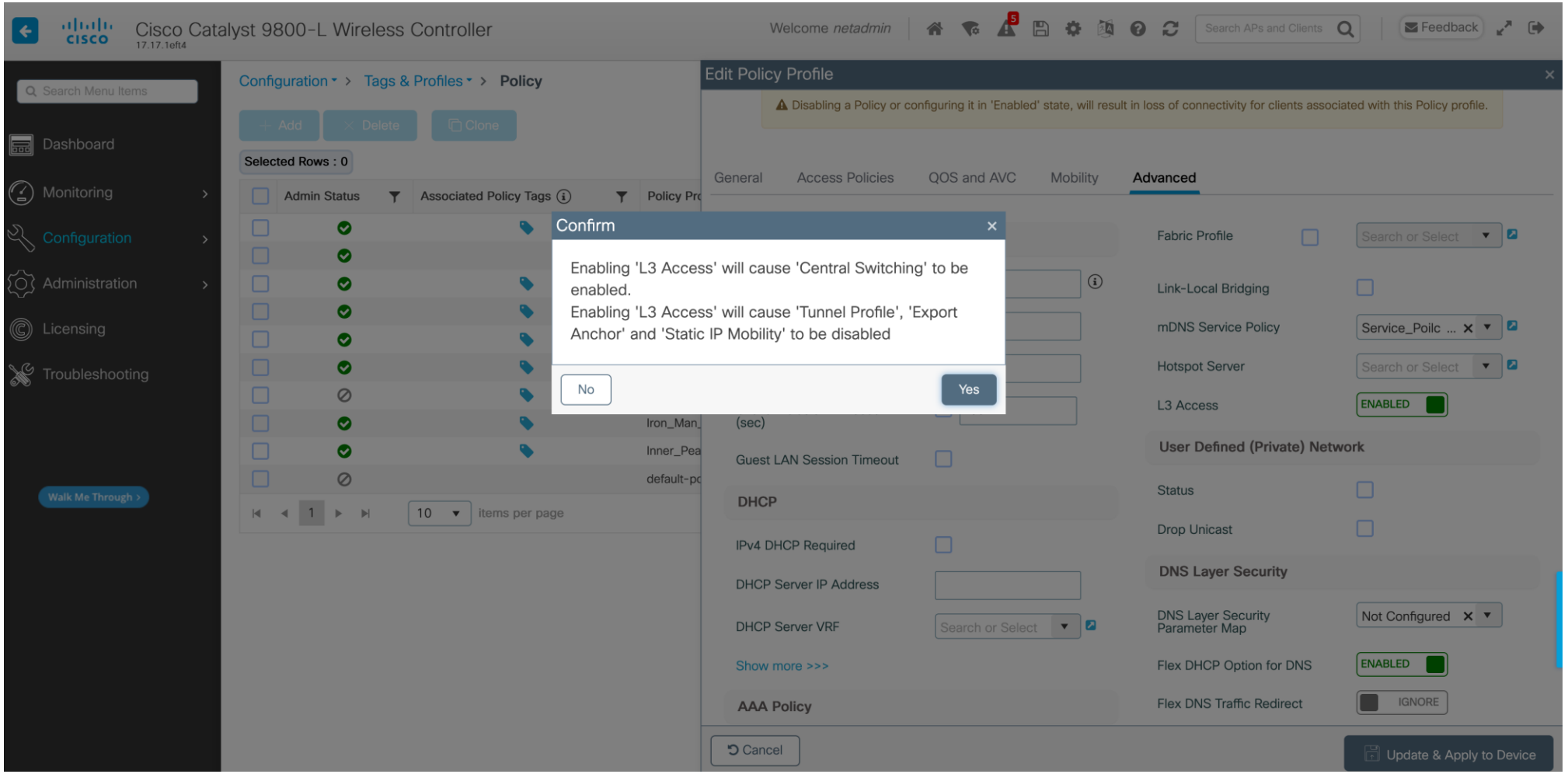
```
C9800(config)# wireless profile policy [Policy Profile]
C9800(config-wireless-policy)# [no] l3-access
```

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
```

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

Enable L3 in the Policy Profile



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

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
```

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

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
```

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

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
```

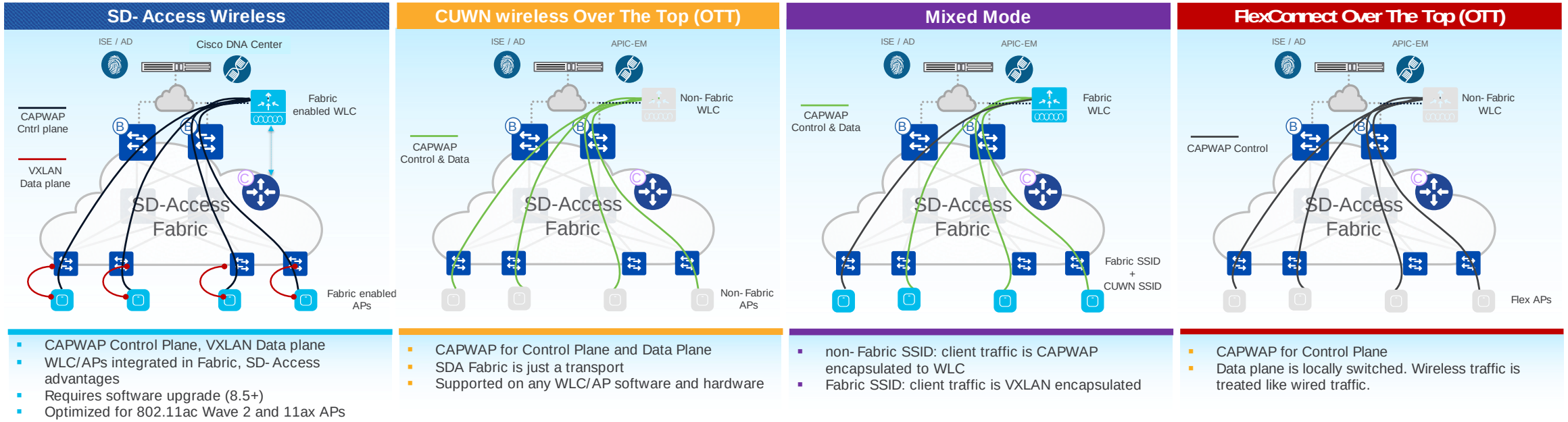
Configuration: With VRF

```
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
```

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

Wireless in and on the fabric



- 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

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

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

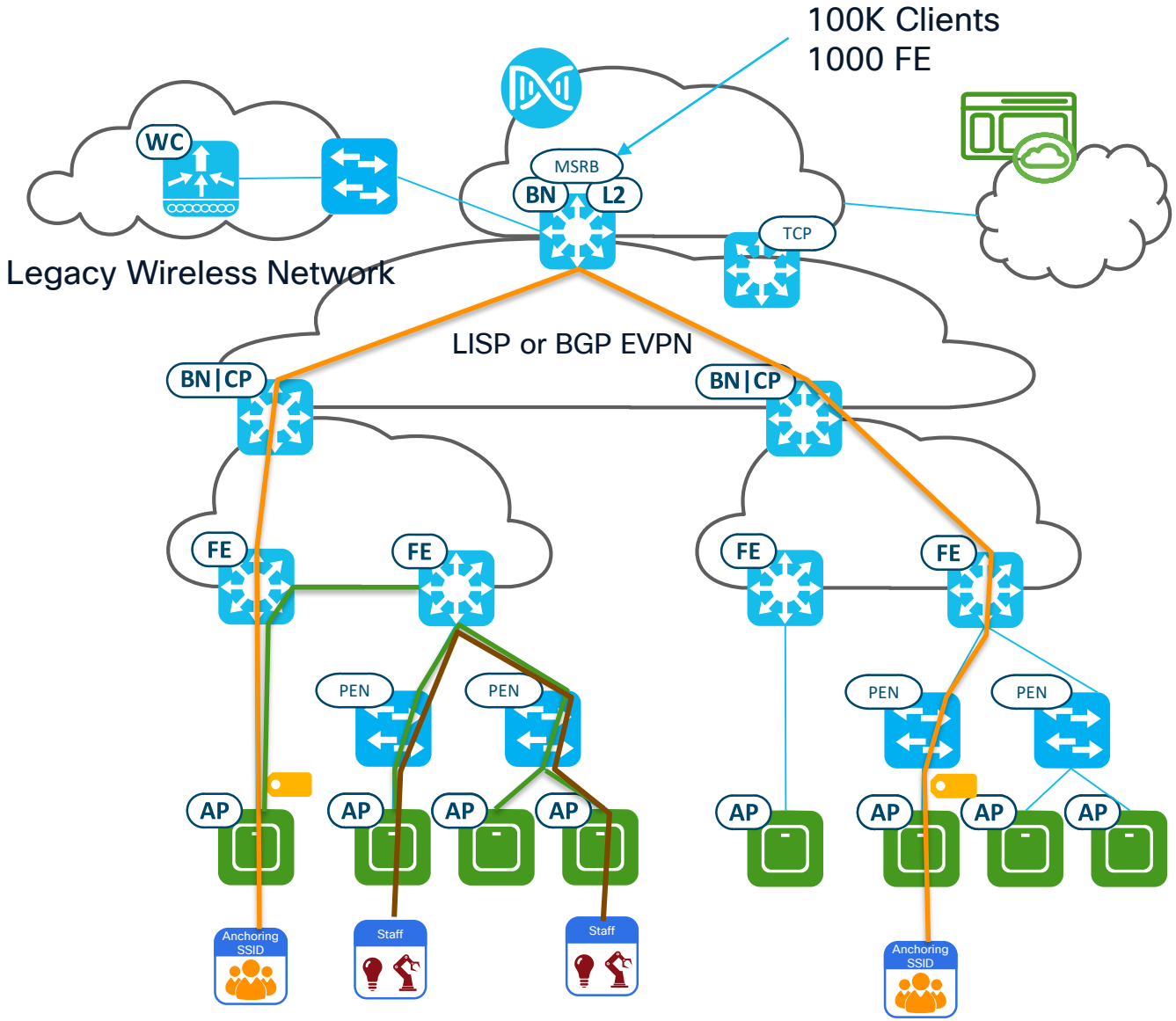
- CAPWAP for Control Plane
- Data plane is locally switched. Wireless traffic is treated like wired traffic.

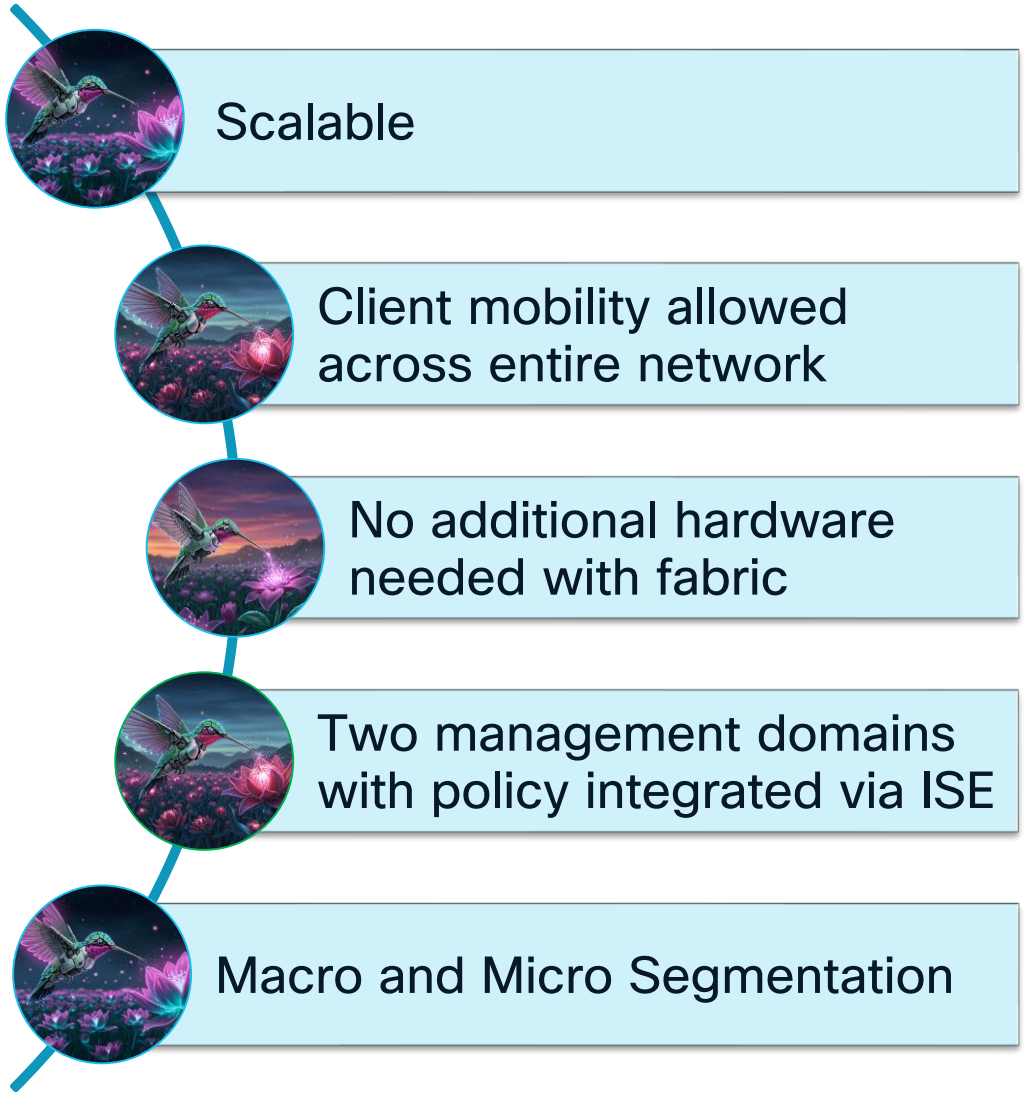
Fabric Wireless Advantage

- 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)

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

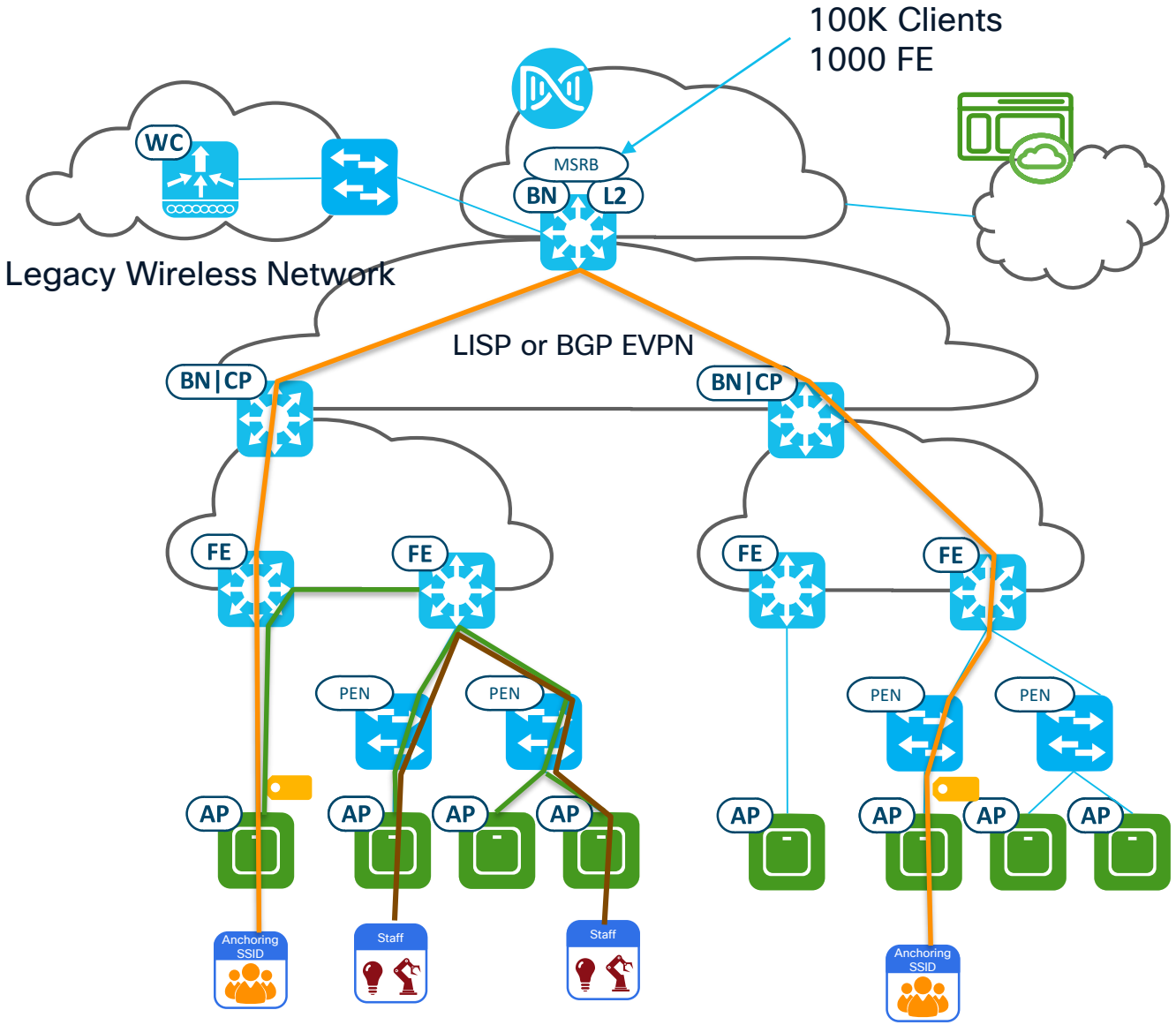
Meraki Wireless in the fabric





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

Meraki Wireless in the fabric

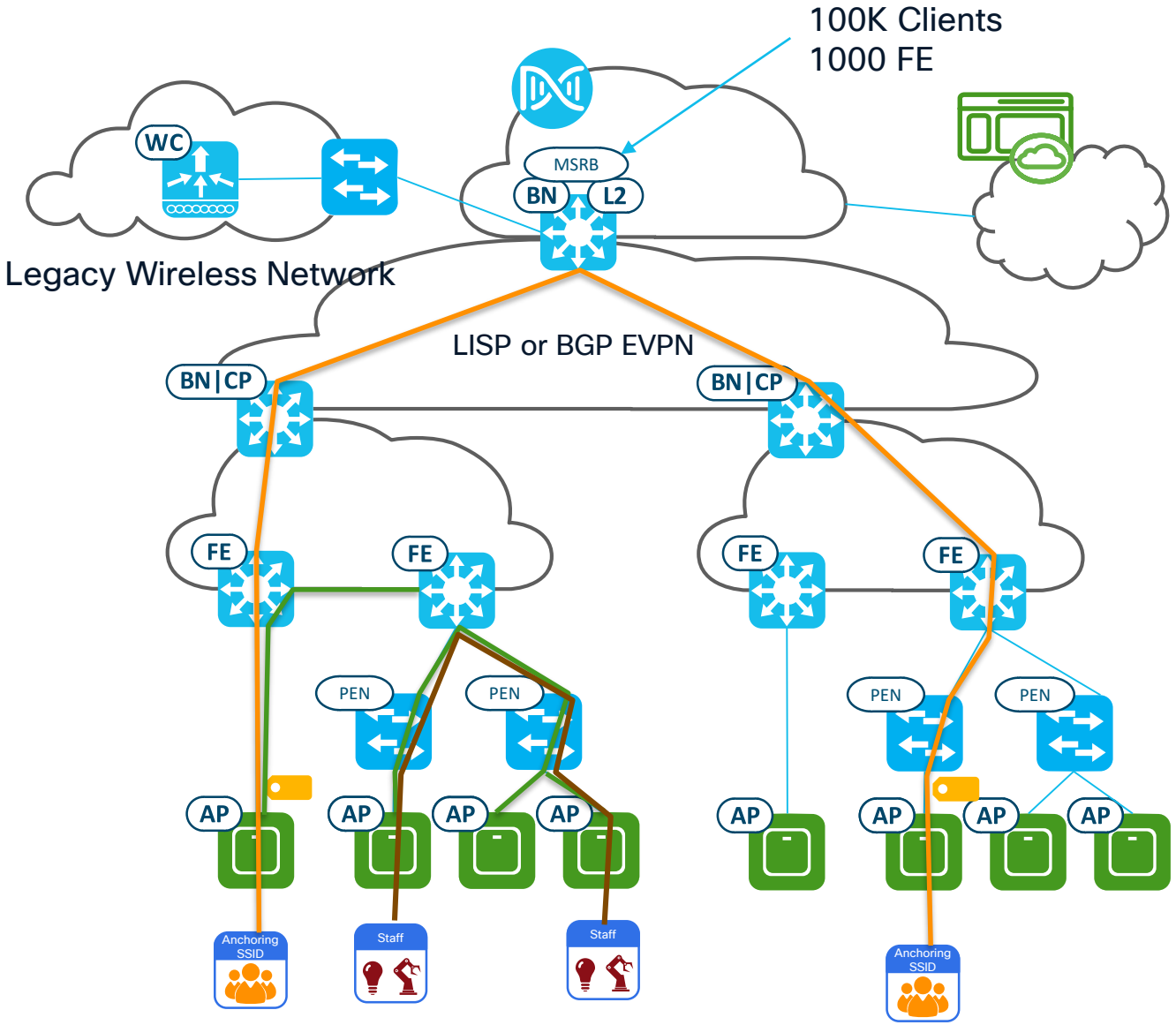


- Basic construct is to allow the fabric to manage all the IP roaming
- IP roaming can be within a fabric site or throughout the entire fabric domain
- Wireless fast roaming (key caching) preformed by L2 connection between APs.
- Micro-segmentation SGTs can be supported.
- Use of enhanced forwarding for client VLANs to improve IP roaming time (<100ms)

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

Meraki Wireless in the fabric

REFERENCE



- 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.

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

Drill into design requirements





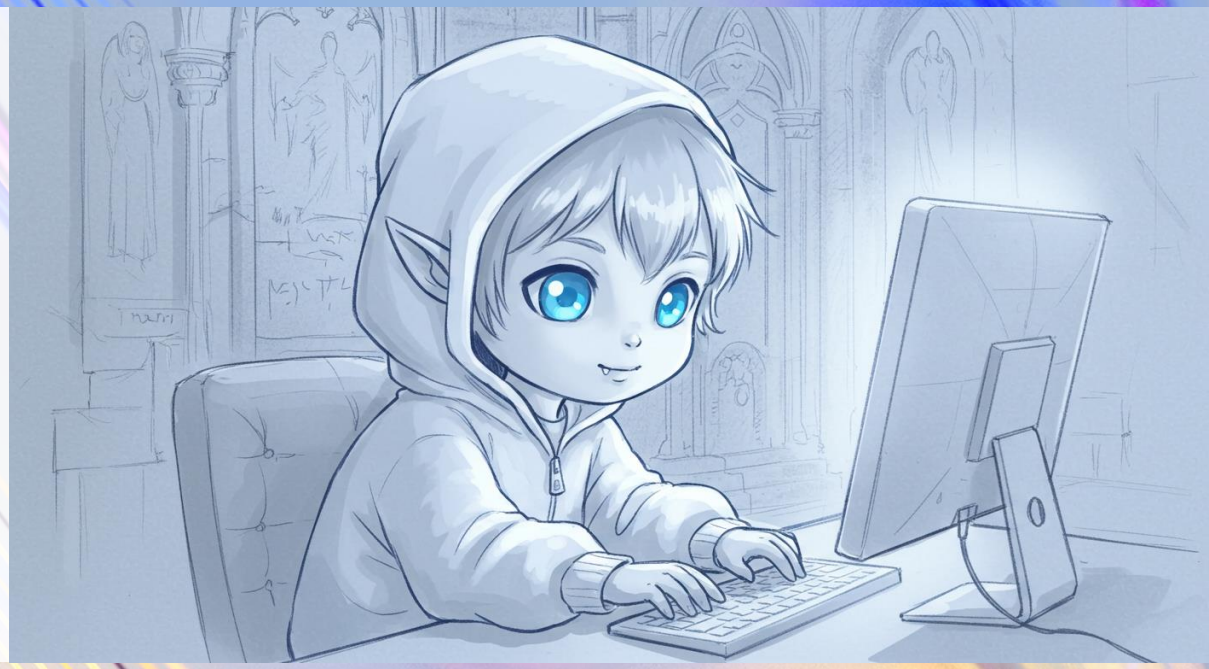


© 2025 Cisco and/or its affiliates. All rights reserved.

Higher Ed

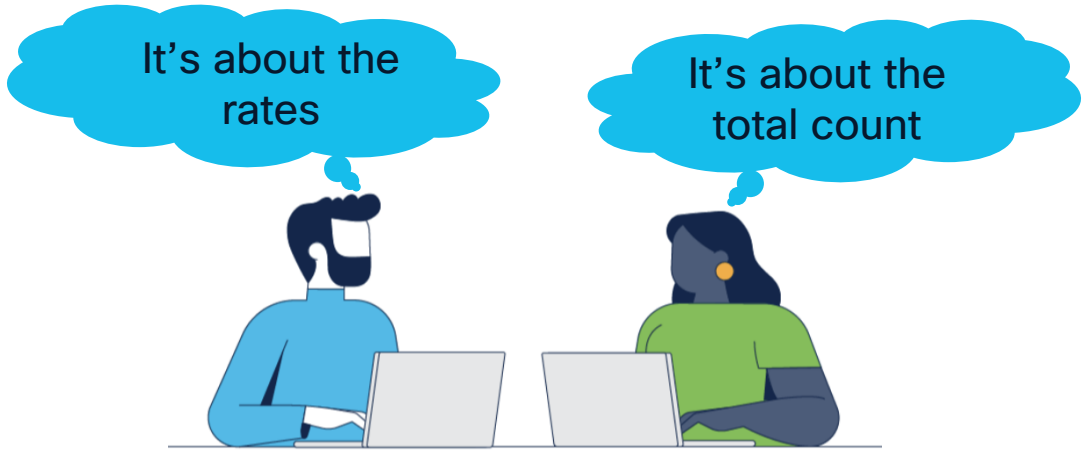
- Scale – 100K+
- Multi-Dwelling Units
- Consistent Performance

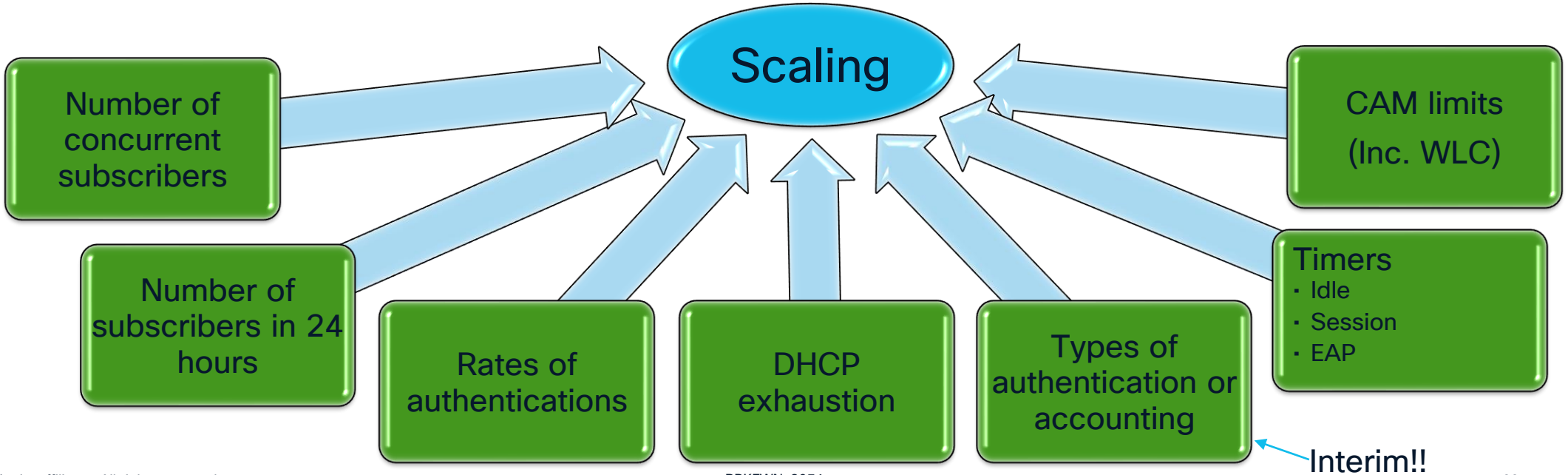
Scale
What to watch for



Think scale!

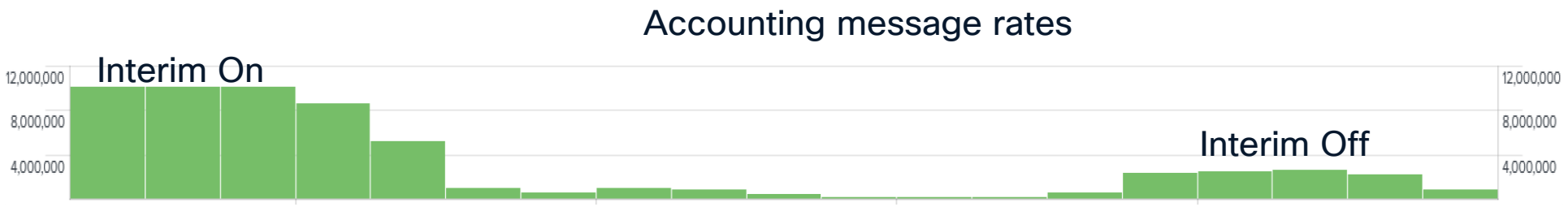




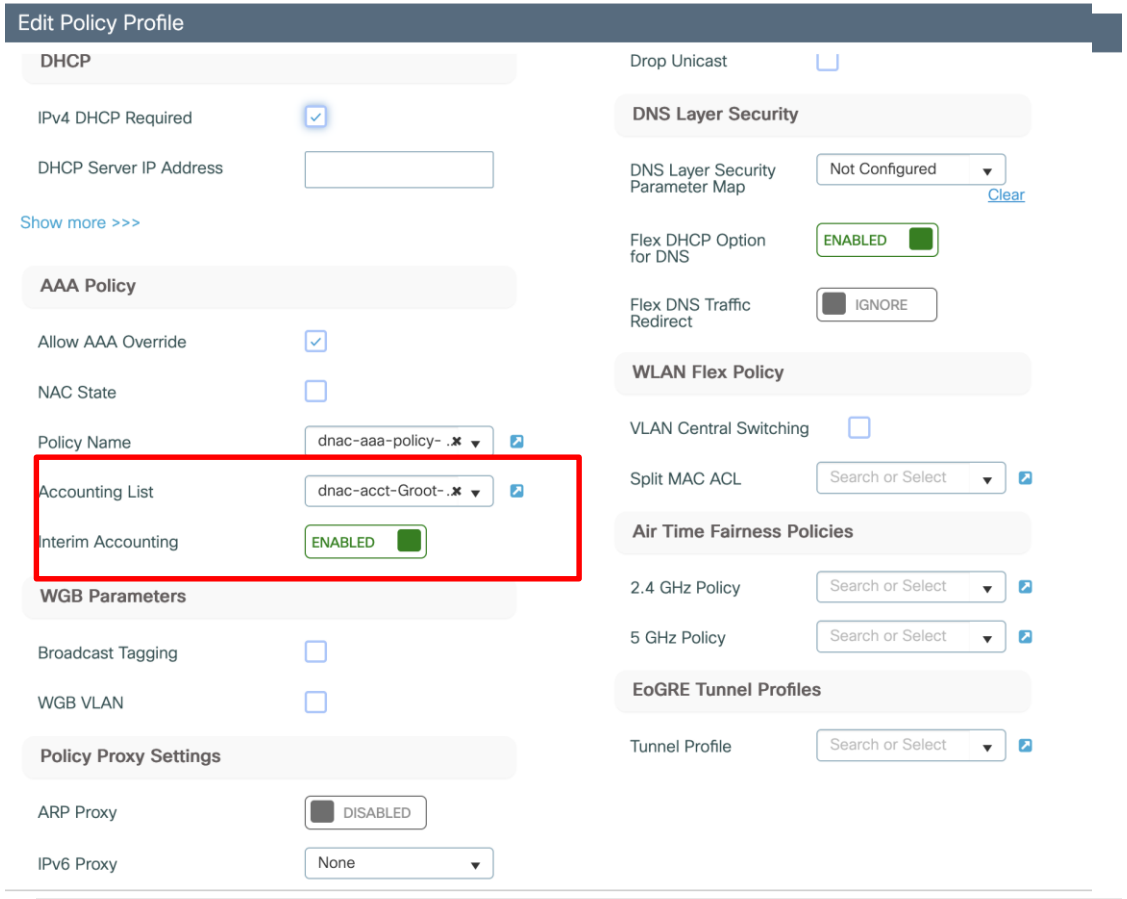


© 2025 Cisco and/or its affiliates. All rights reserved.

What does Interim Accounting do



- On by default
- Occurs on device roam
- Configured in Policy Profile



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

Watch Out



Thanks to the Wireless Escalation team for these updates!

- Radius messages are occasionally seen from the RMI interface in SSO pair.
  - Be sure to add both the wireless management an the RMI address as network devices in AAA
  - Only a concern if using SSO with RMI
- AirDrop sessions from Apple clients seen as threat causing high CPU due to AWIPS.
  - Disable AWIPS
  - Most customers do not have a policy for WIPS. If no policy good practice is to disable. AWIPs or Air Marshal. At the very least, remove “Airdrop Session” from the profile.
  - CSCwo69382, CSCwo69408, CSCwo67268
- Radius Load Balancing not to be used with CWA, only with l2 auth such as 802.1X/MAB
- WiFi7 deployment, beware of strict client compliance checks for SSID config

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

C9800 Scale Numbers

Note: 9800H scale = 9800-80, 9800M scale = 9800-40

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 ACI 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

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

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

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

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

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

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

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

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

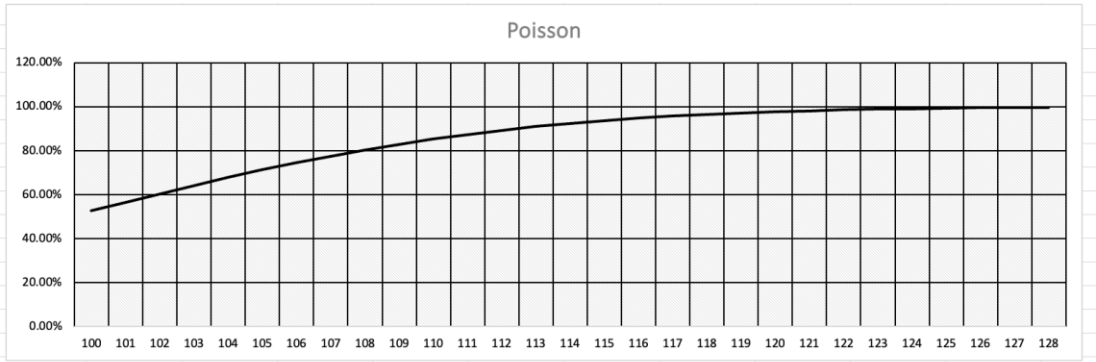
© 2025 Cisco and/or its affiliates. All rights reserved.

...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

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

TPS Example

Peak busy period = 5 minutes
Clients/busy period = 50000
T = 50000/(5*60) = 167 clients/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

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

Scale/WNCd

What is it and how does it affect my design

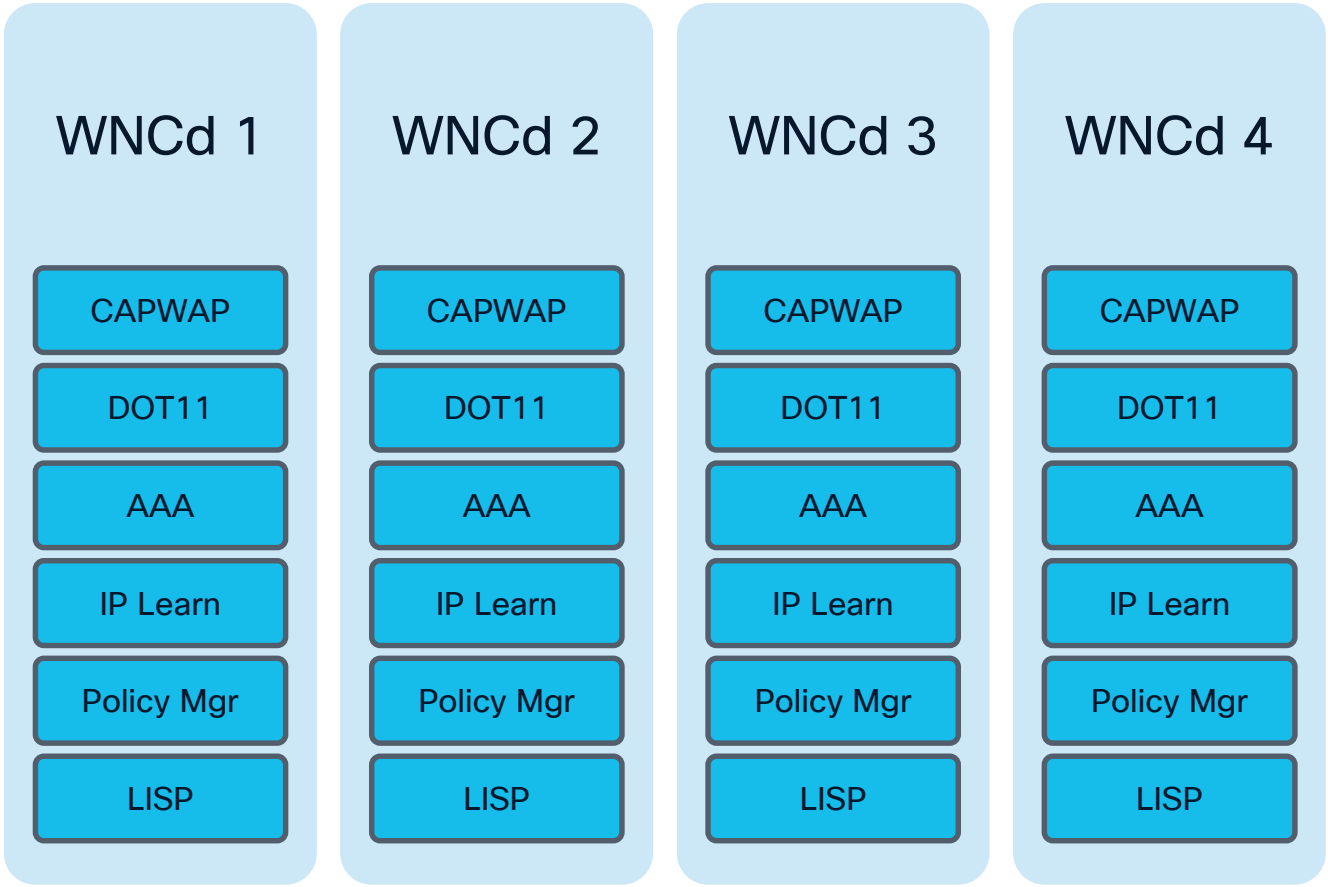


WNCd, what is it

- 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.
  - Each process runs independently.
  - The processes are responsible for managing AP and Client sessions.

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

More about WNCd



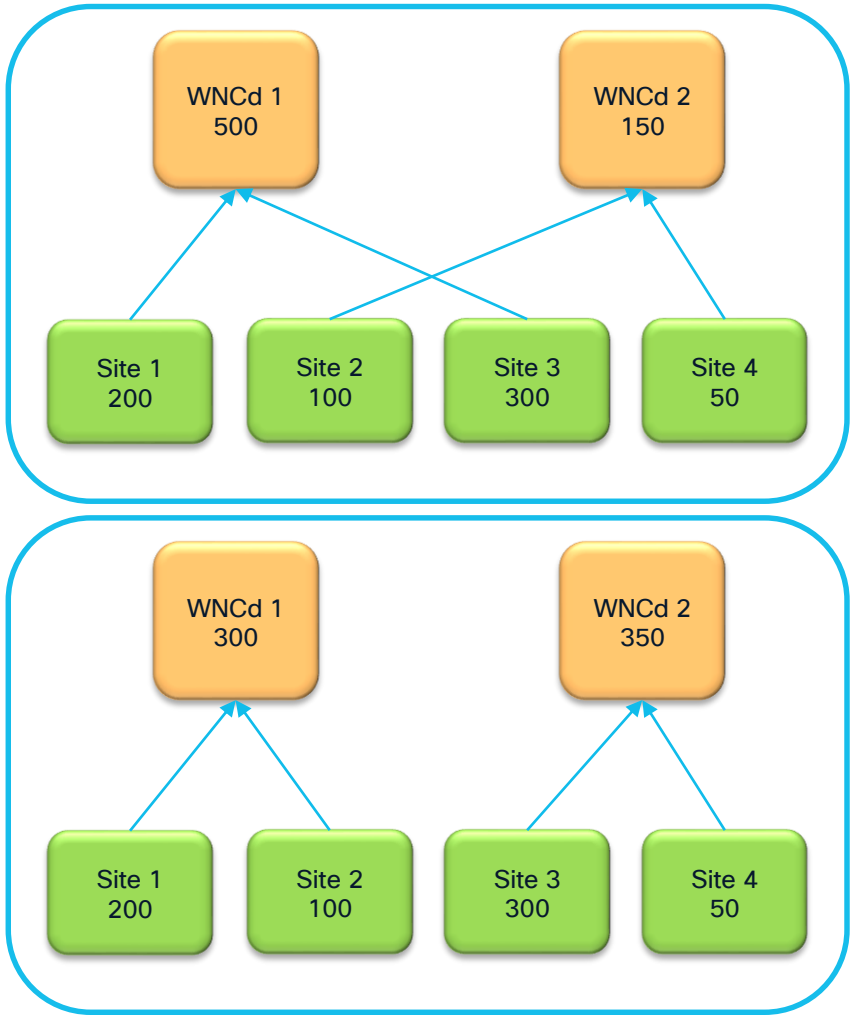
Platform	WNCd Instances
EWC (AP or C9k switch)	1
C9800-L	1
C9800-CL (S)	1
C9800-CL (M)	3
C9800-40/M	5
C9800-CL (L)	7
C9800-80/H	8

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

How does this affect my design

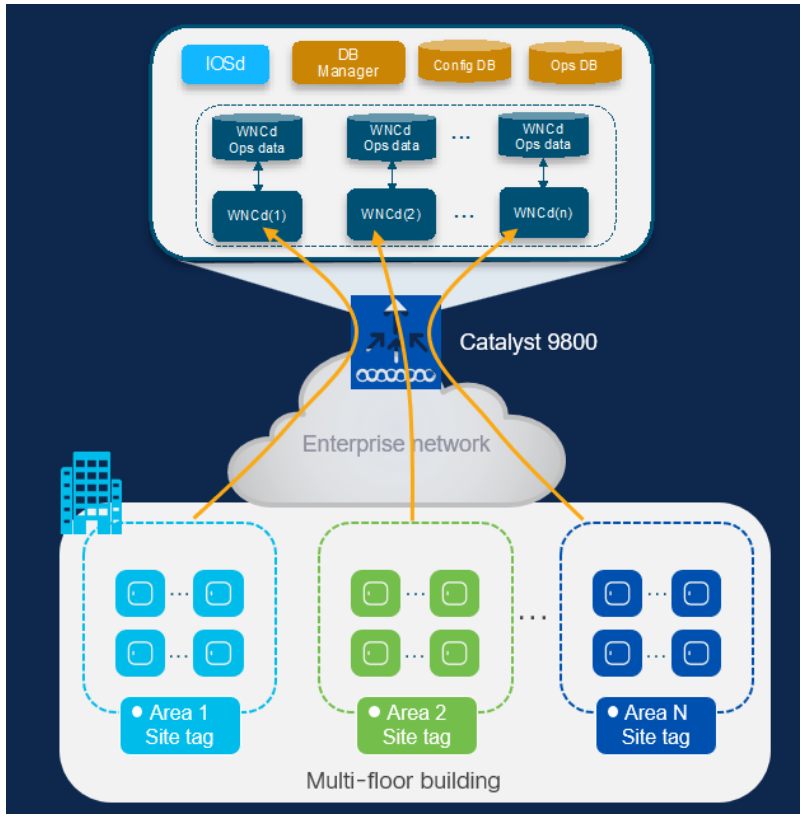
- High CPU can cause APs to drop.
- Target less than 500 APs per WNCd.
- Roaming between APs on different WNCd process will add latency to the roam.
- Site Tags are used to map APs to WNCd process.
- Three methods of assigning Site Tags to WNCd processes.
  - Old – round robin
  - New – weighted grouping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

17.12.1+ Automatic WNCd Load Balancing



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

WNCd load balancing updates



Existing

- Site Tag Based
- load input for large sites

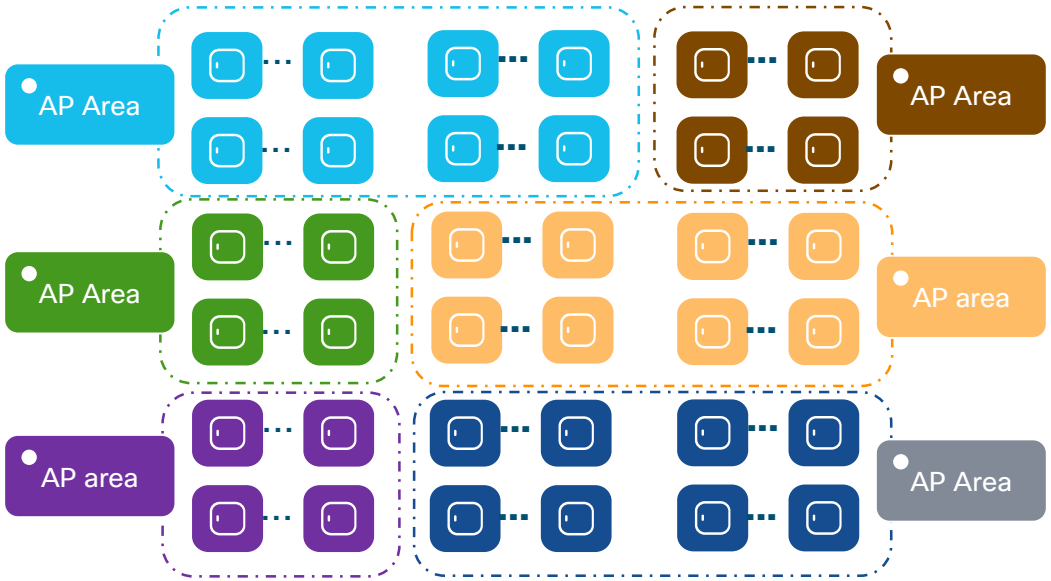
Recommendations for Local mode:

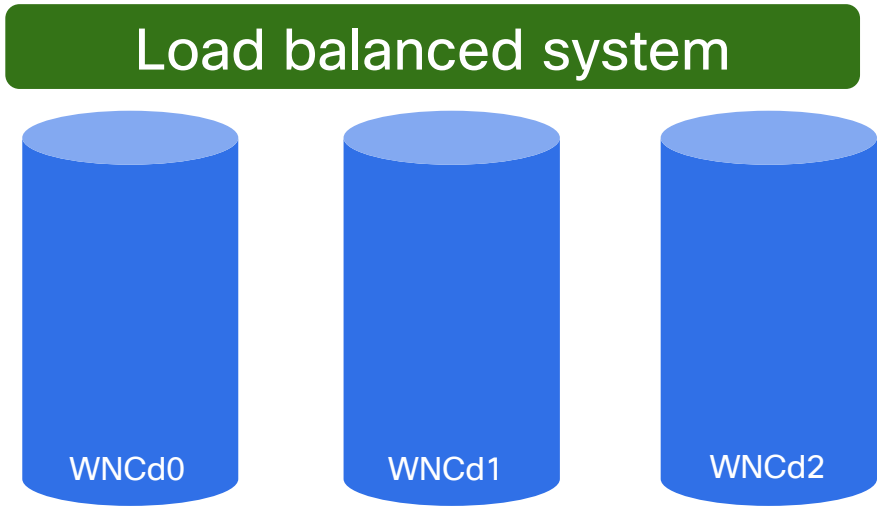
- Starting 17.9.3, "**load**" parameter can be configured, so site tags are allocated to WNCd based on the compute load
- Usually "**load**" equal to the number of APs

- 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

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

RRM based Auto WNCd load balancing



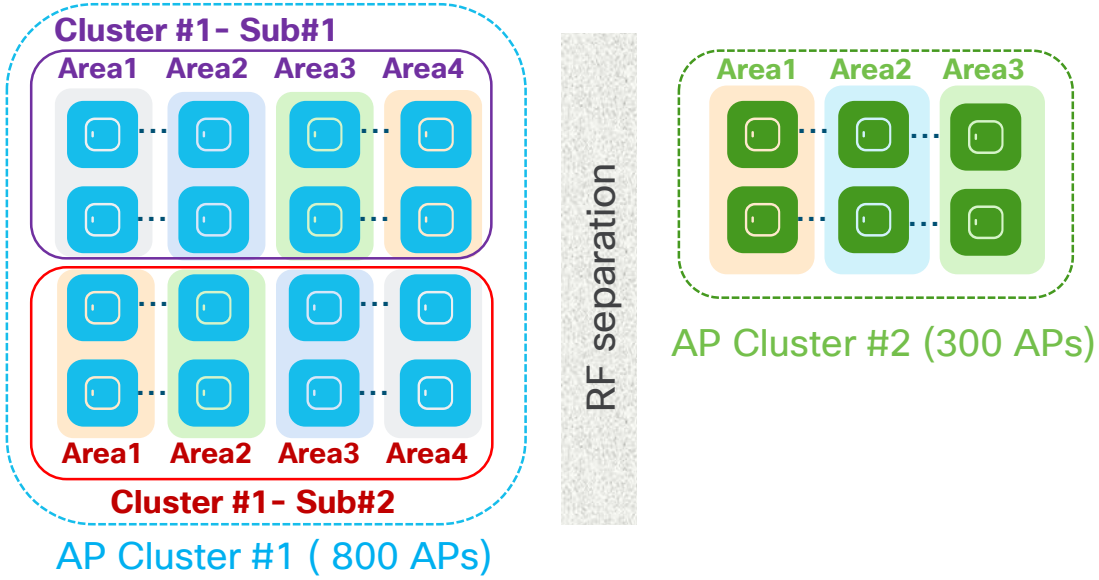


Key Points

- 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

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

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

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

University Campus General

- 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
  - Clean Air shows hundreds of thousands of interferers…disable that band on Clean Air

* External load balancing recommended

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

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

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

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.

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

MDU



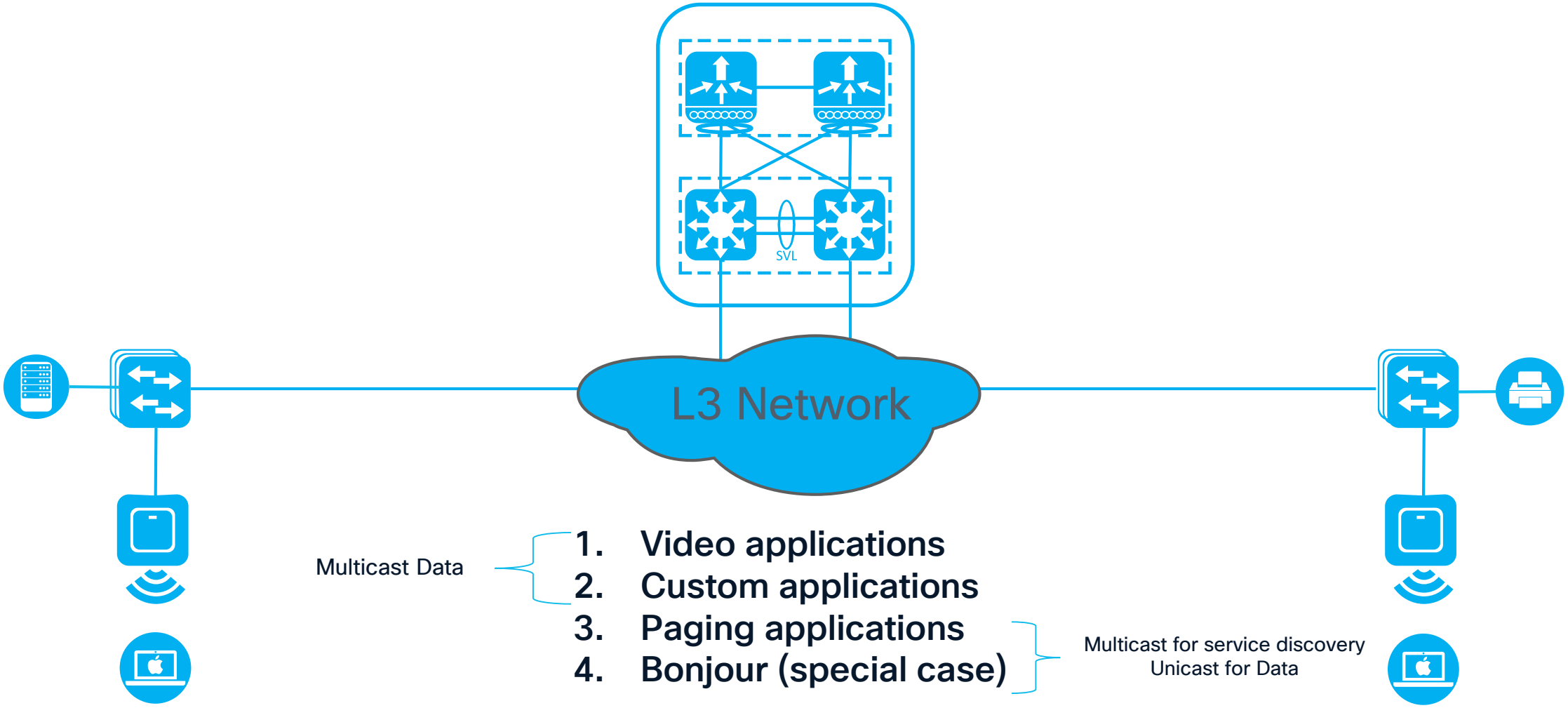
First a bit about Multicast

What is it and how does it affect my design



Multicast

Physical layout

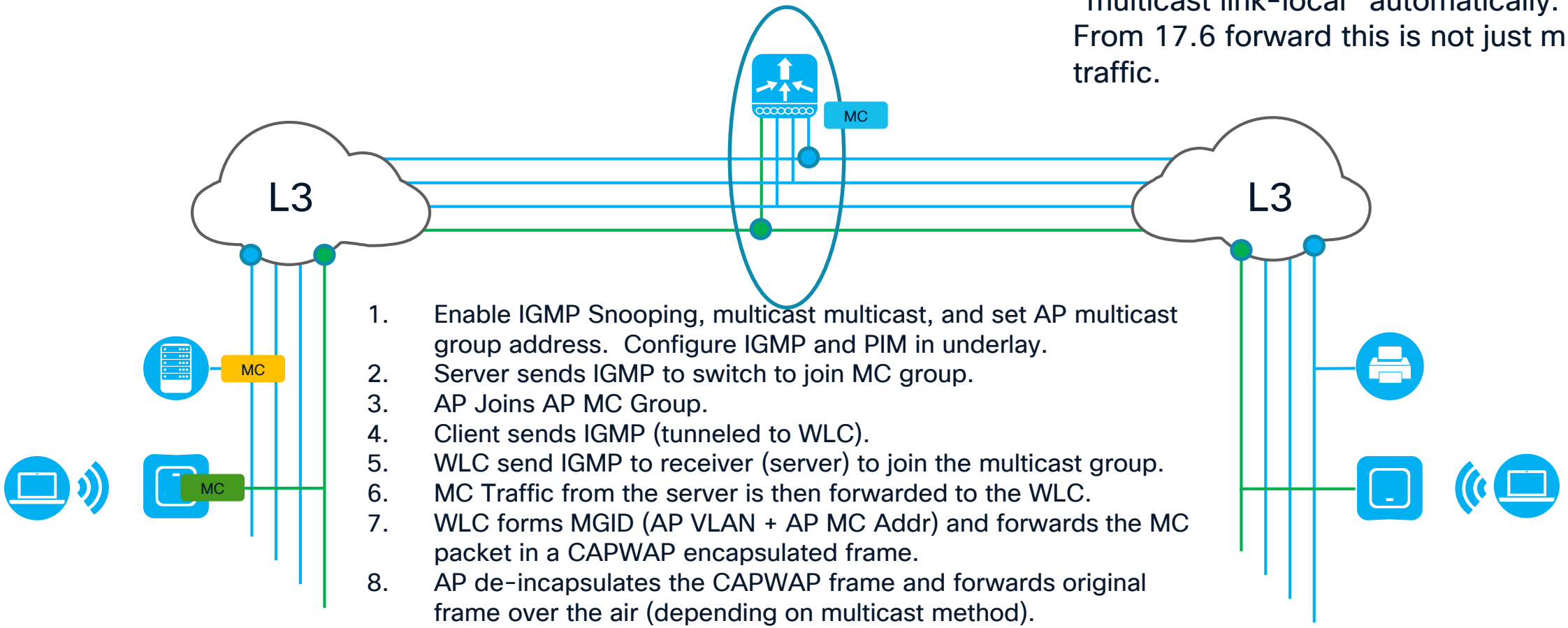


© 2025 Cisco and/or its affiliates. All rights reserved.

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.

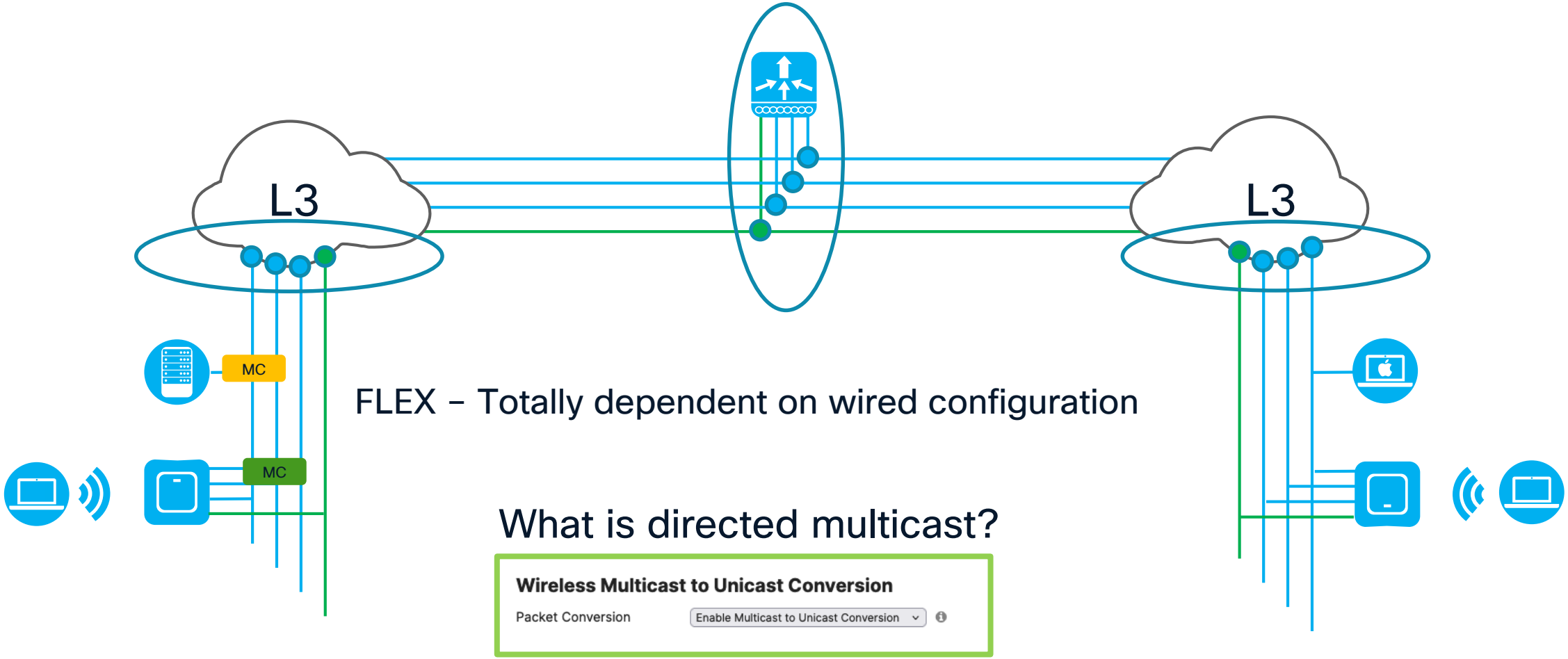


1. Enable IGMP Snooping, multicast multicast, and set AP multicast group address. Configure IGMP and PIM in underlay.
2. Server sends IGMP to switch to join MC group.
3. AP Joins AP MC Group.
4. Client sends IGMP (tunneled to WLC).
5. WLC send IGMP to receiver (server) to join the multicast group.
6. 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).

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

Multicast-Multicast vs Multicast-Unicast

Flexconnect Mode or Meraki (local switching)



FLEX – Totally dependent on wired configuration

What is directed multicast?

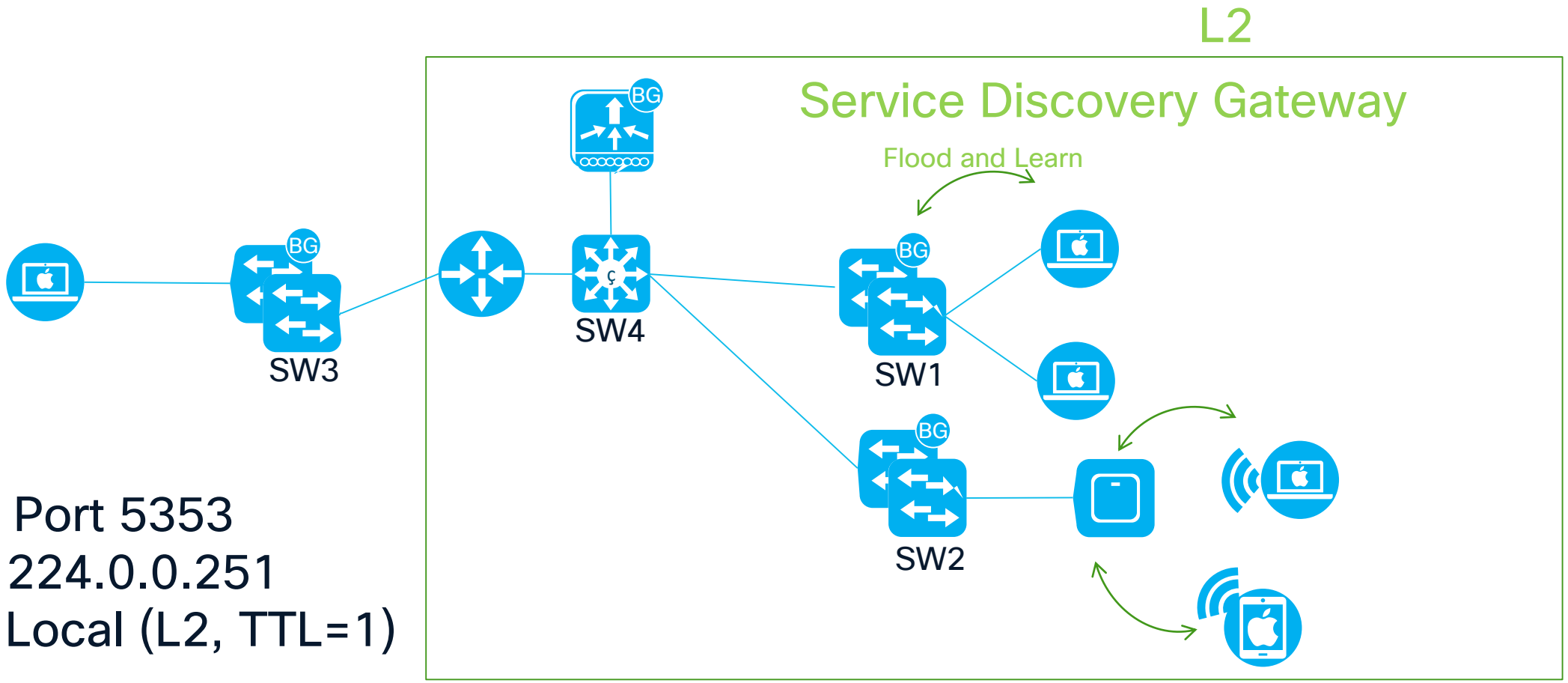
Wireless Multicast to Unicast Conversion

Packet Conversion | Enable Multicast to Unicast Conversion

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

Bonjour/mDNS Example

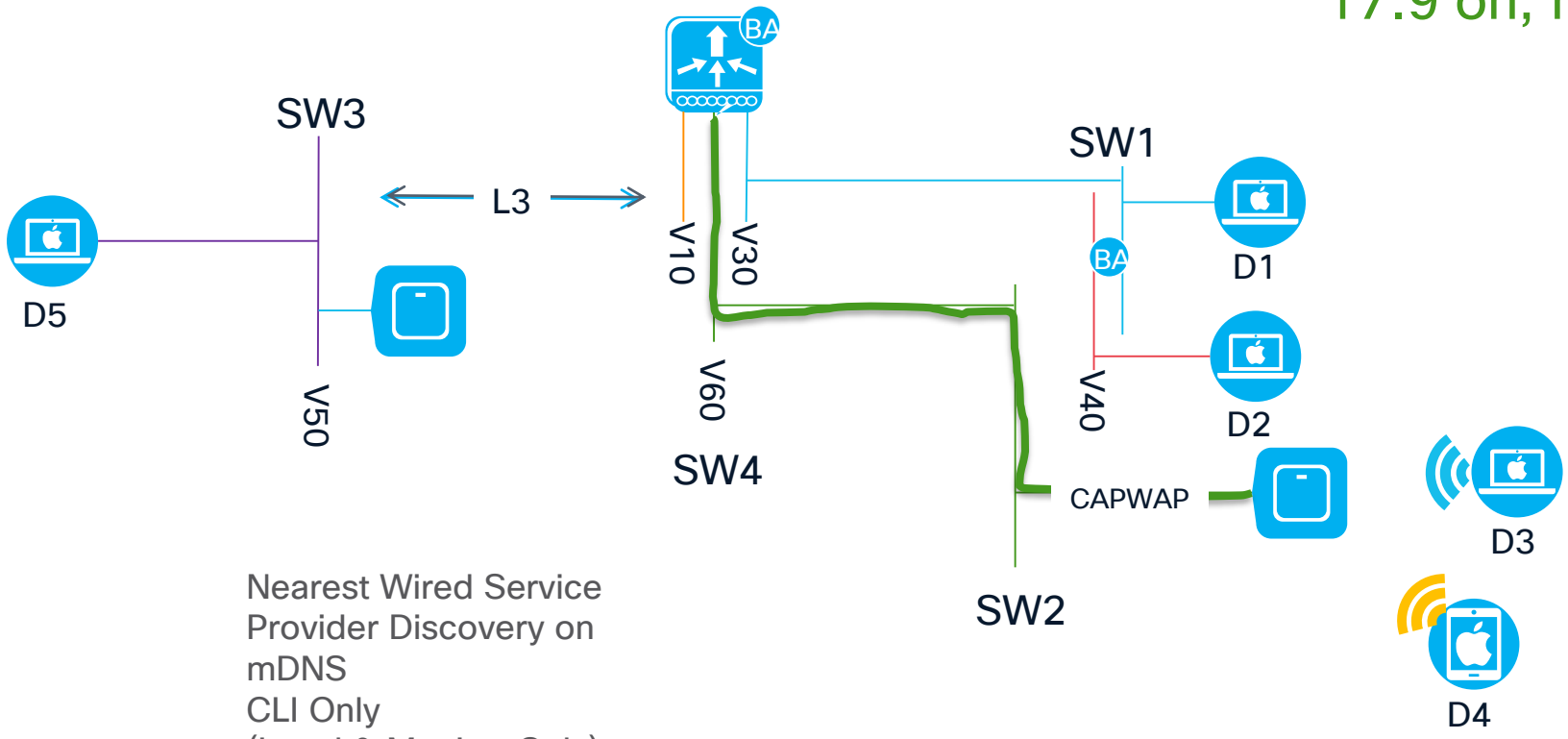
Physical layout



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

Bonjour/mDNS Example

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



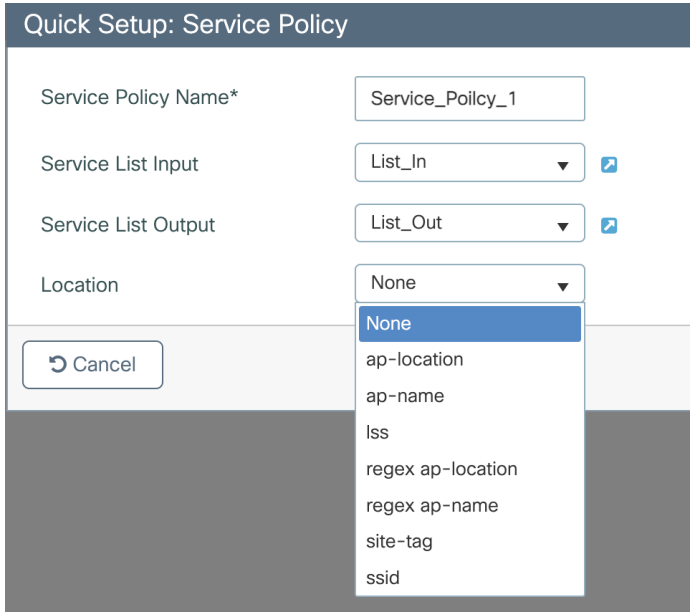
Nearest Wired Service Provider Discovery on mDNS
CLI Only
(Local & Monitor Only)

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

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

Managing mDNS rules can be challenging

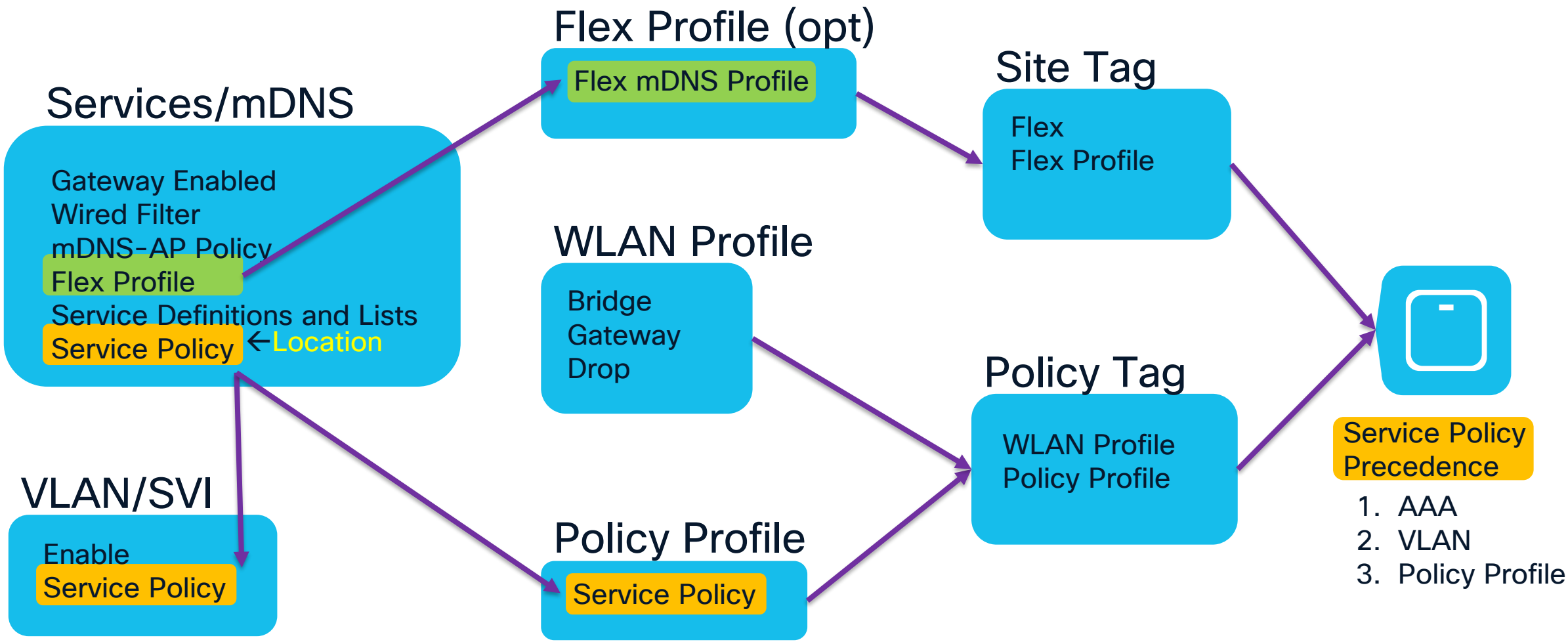




What if I want to use location specific or AP specific broadcasts while using locally switch data?

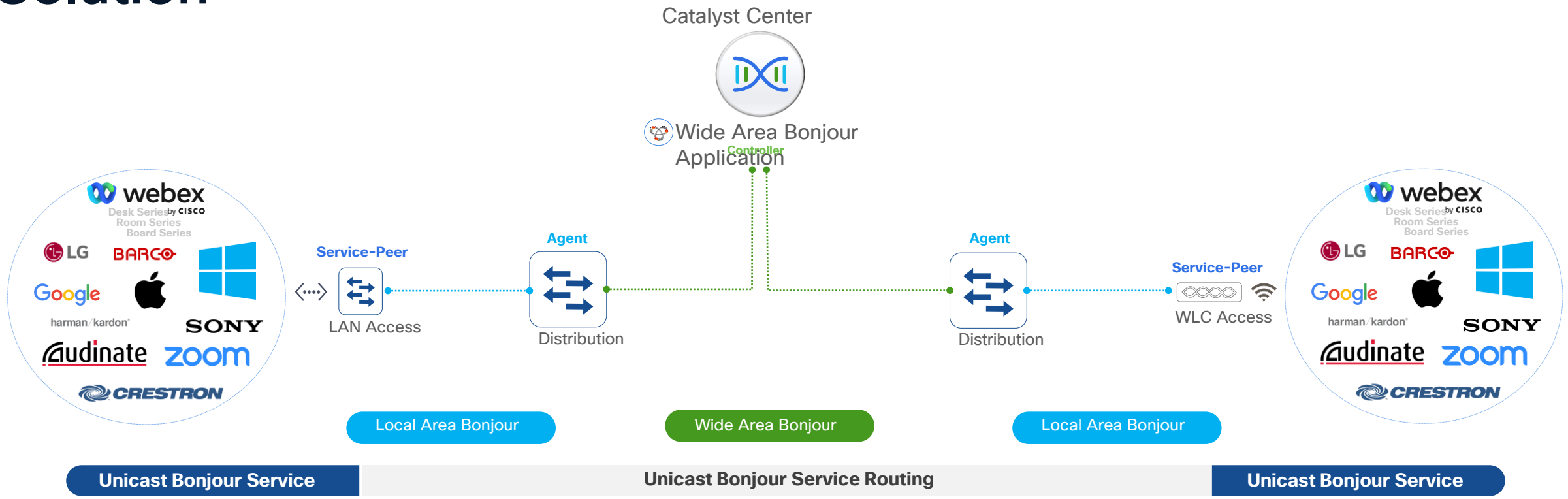
© 2025 Cisco and/or its affiliates. All rights reserved.

Configure mDNS in C9800



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

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

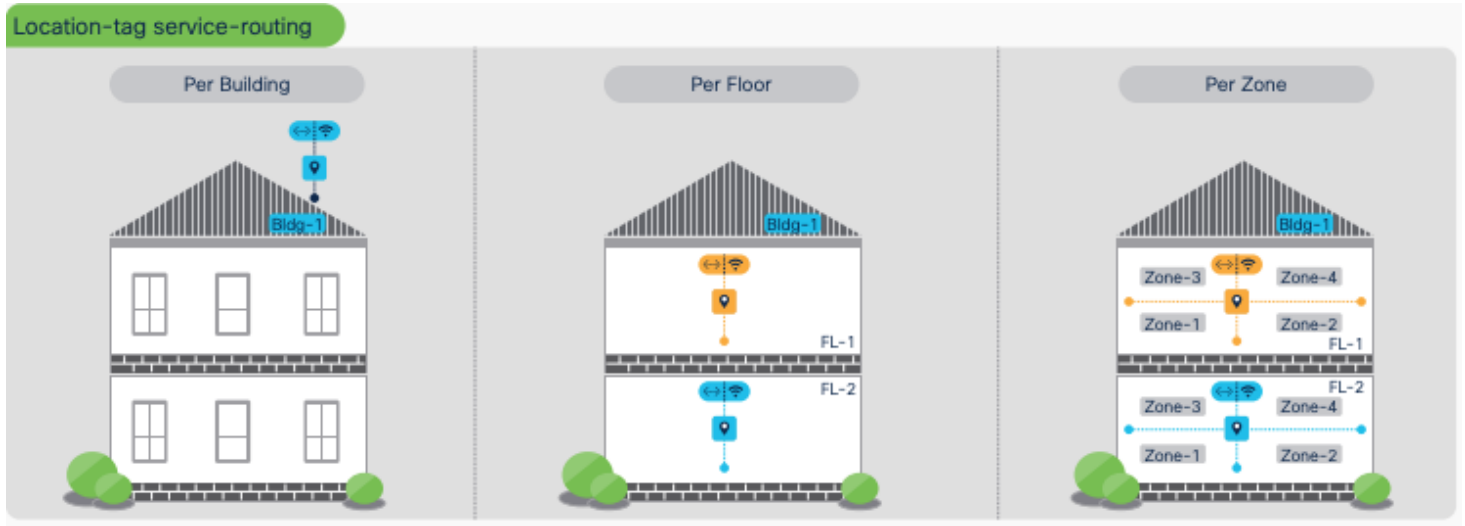
Improved system performance
Increase network bandwidth
Flexible design any Enterprise Network

Battery Life

May assist improve battery-life
On-demand Query response mode
Increase Wireless network bandwidth

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

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

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

Per Zone Configuration (only on Access Switch)

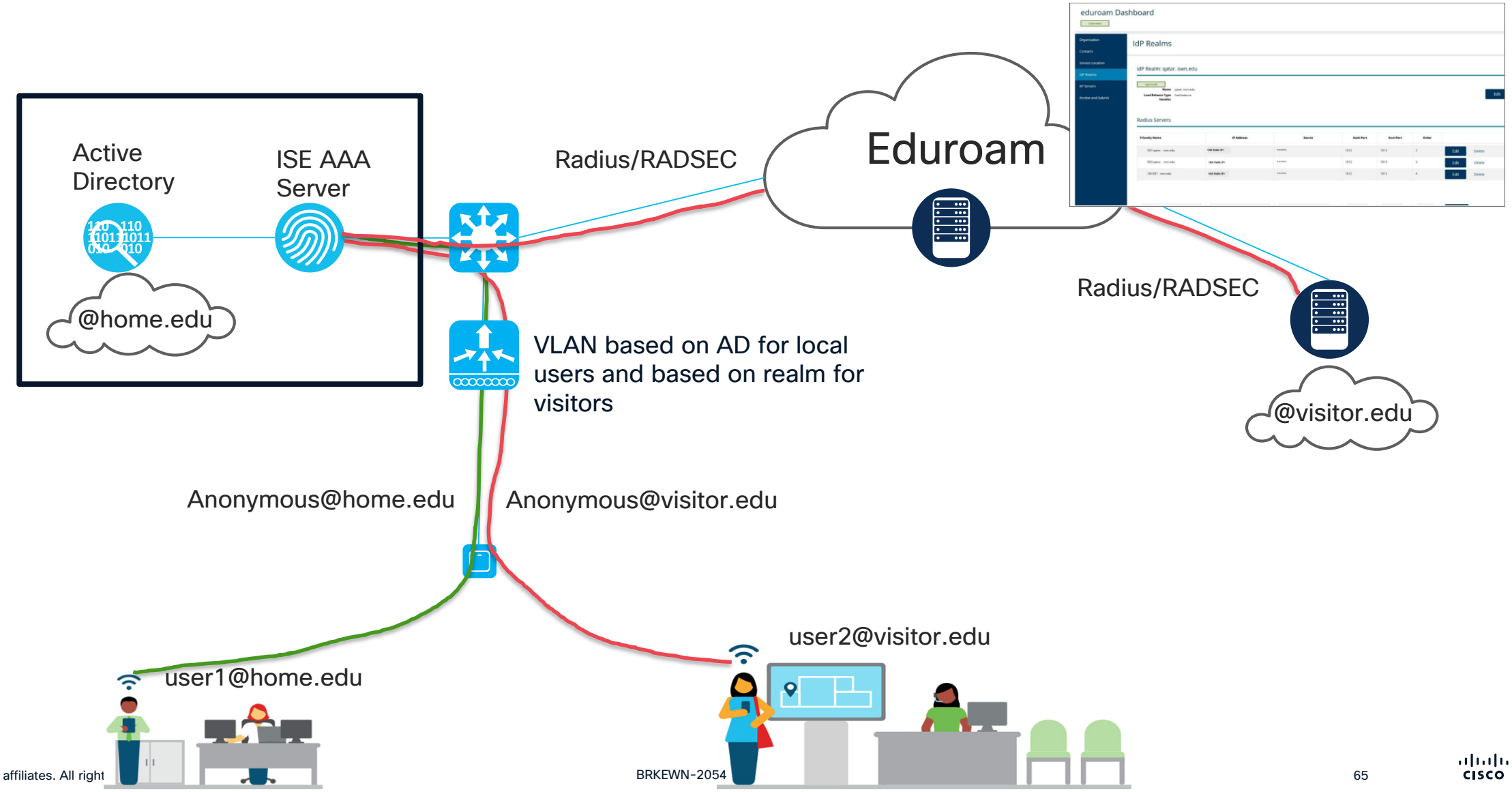
LAN-Access	LAN Distribution
Mode: Service-Peer	Mode: Agent
Step – 1: Default Policy Mode – mDNS Service-Routing	
! This is pre-requisite step. Refer to configuration procedure described above in Table – X. !	
Step – 2: Per-Zone – Enable Location-Group based Service-Routing	
! LAN Access – 10.1.1.1 – Zone-1 Location-Group ID 1 Configuration ! interface range Gi1/0/1 – 10 description Connected to AirPrint and FlexConnect/EWC AP's ! mdns-sd location-group 1 vlan 10 interface Gi1/0/1 … interface Gi1/0/10 ! ! LAN Access – 10.1.1.1 – Zone-2 Location-Group ID 2 Configuration ! interface range Gi1/0/11 – 20 description Connected to AirPrint and FlexConnect/EWC AP's ! mdns-sd location-group 2 vlan 10 interface Gi1/0/11 … interface Gi1/0/20 !	! 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.

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

Eduroam

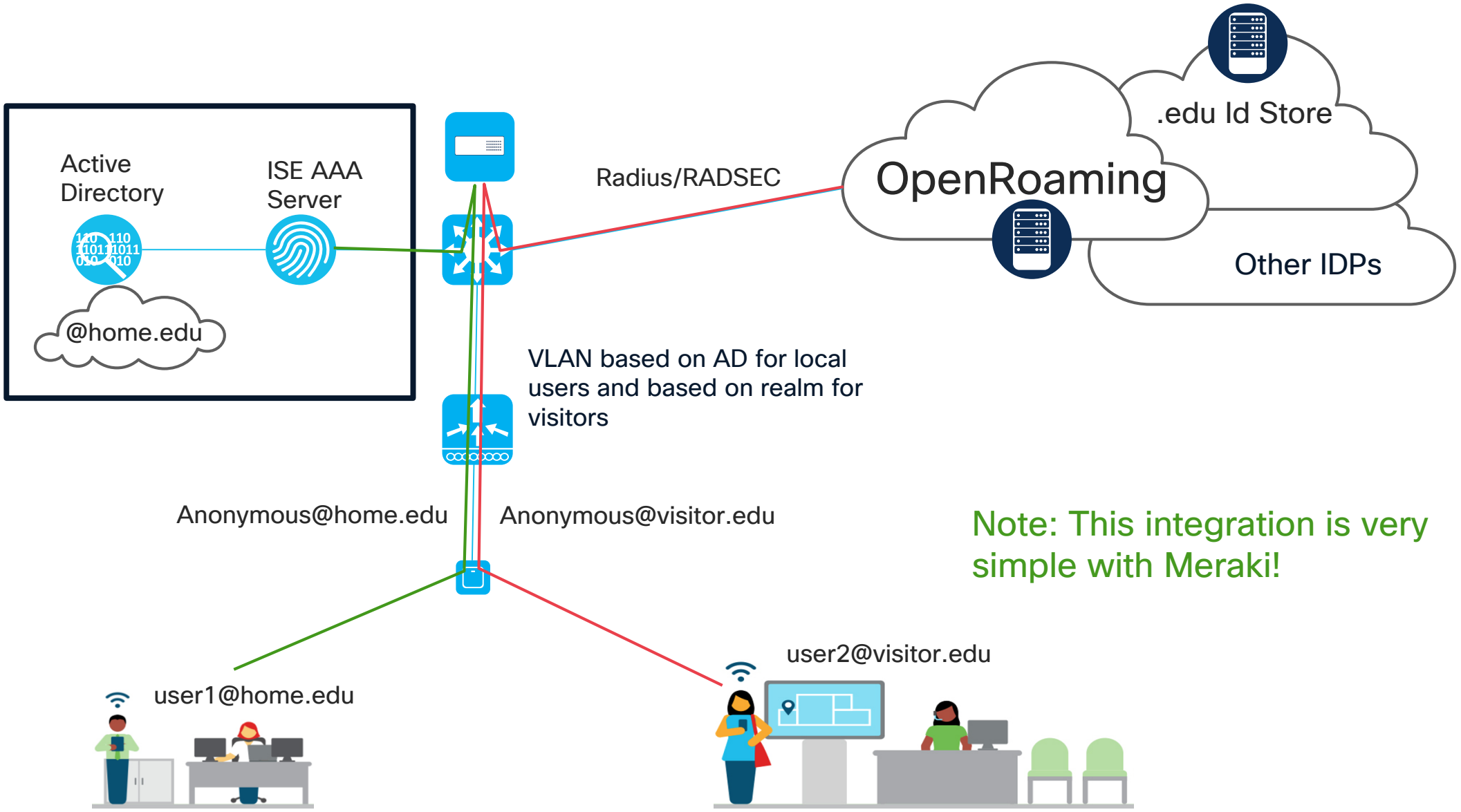
A different approach to an old requirement

Eduroam Typical Authentication



© 2025 Cisco and/or its affiliates. All right

Eduroam OpenRoaming Authentication



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. *

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

iPSK/mPSK/UDN/WPN

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



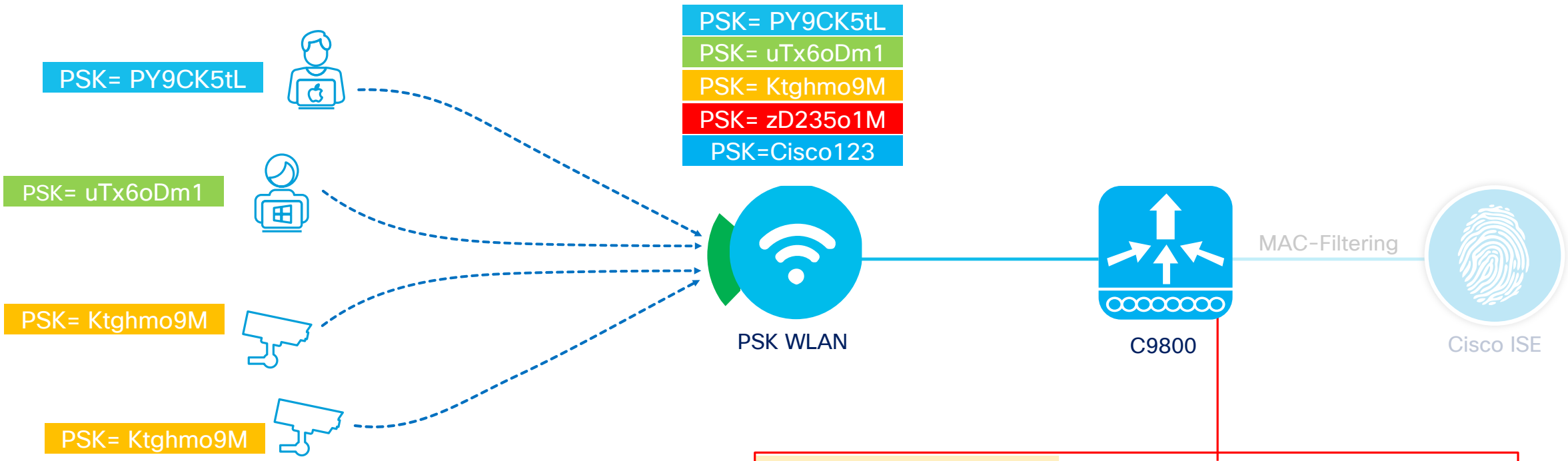
Multiple User PSK Options

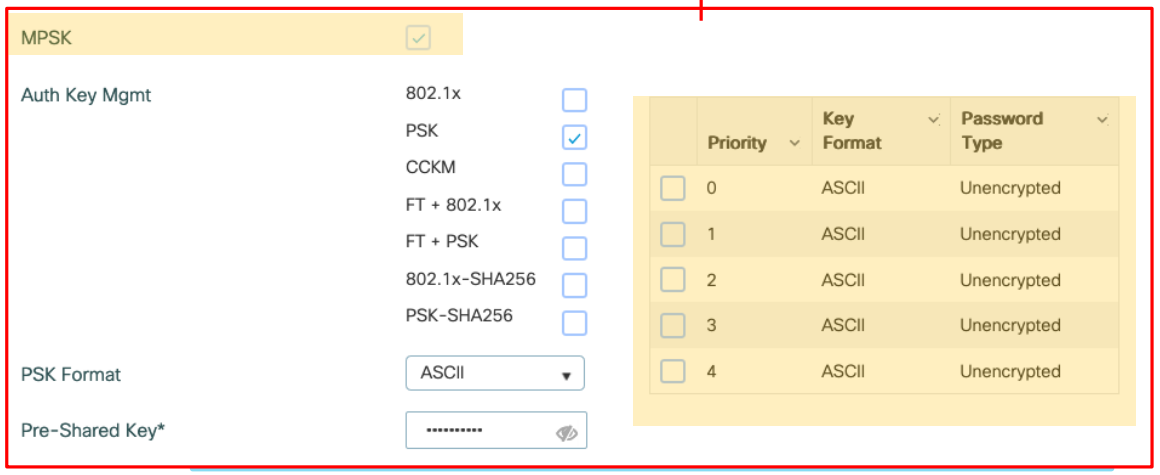
Method	WPA3 support	AAA mandatory	Backend Provision	User experience	Segmentation	Stack
MPSK	No	No	Un bounded MAC	Very easy	P2P Blocking	Catalyst
Easy PSK	No	Yes, Nomadix# (FT not supported)	Un bounded MAC	Very easy	VLAN override	Catalyst
iPSK	Yes	Yes	Requires MAC onboarding	Easy	Unicast	Both
WPN	No	No	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/ or Cloud4Wi https://cloud4wi.com/

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

MPSK (Multi PSK)



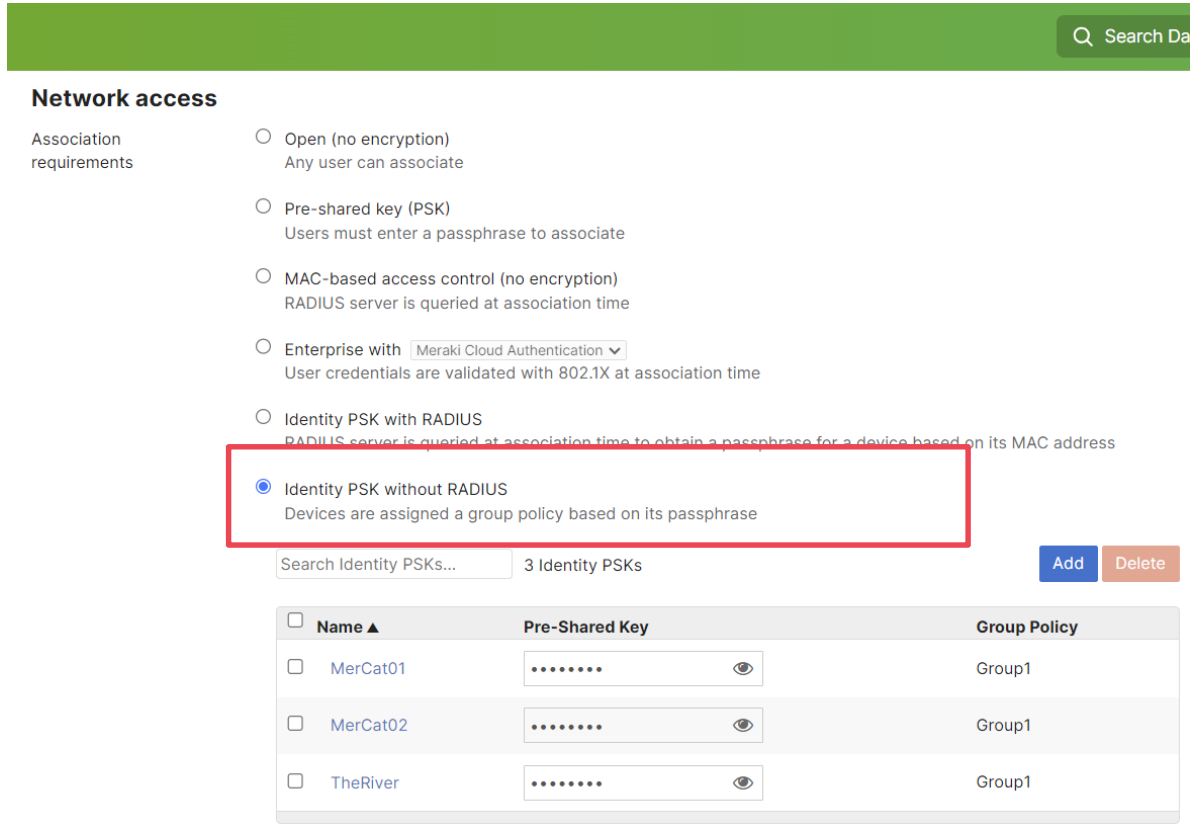


- Can configure up to 5 different PSK per WLAN
- (Optional) ISE may be used for validating MAC address
- Supported with C9800 16.10+, not AireOS
- No WPA3 support (Catalyst or Meraki)

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

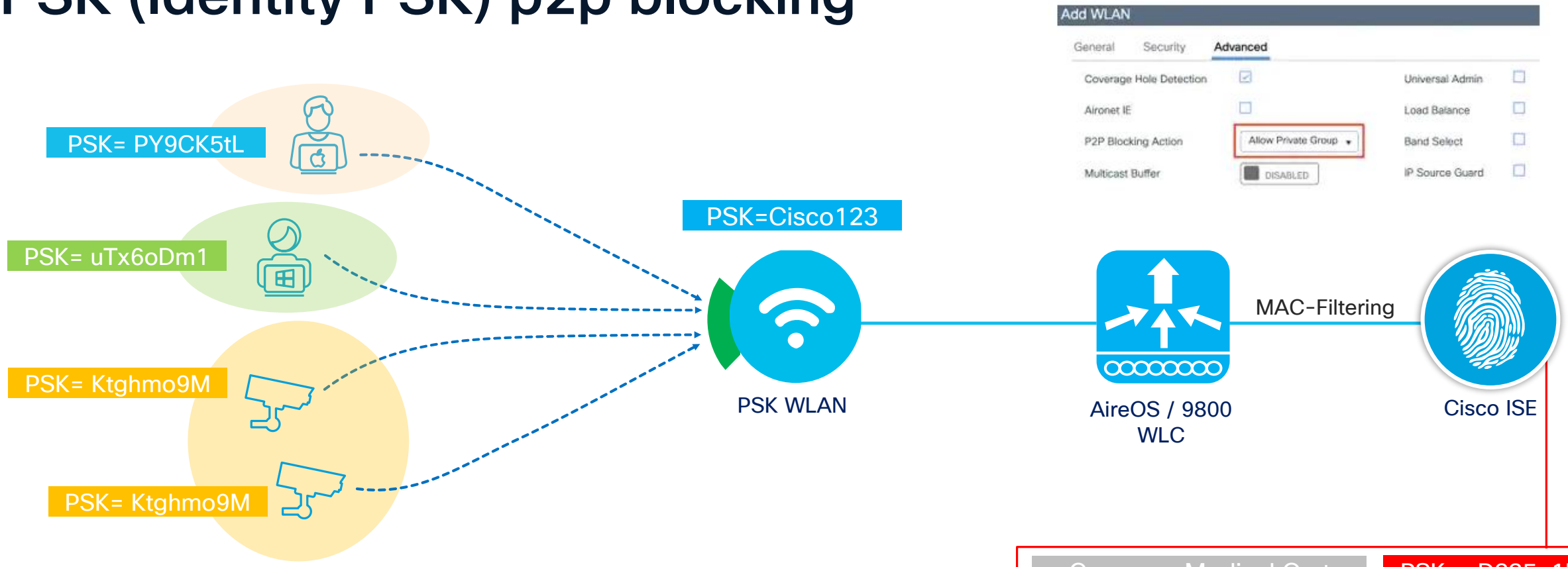
Meraki “iPSK without RADIUS”

- 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.



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

IPSK (Identity PSK) p2p blocking



- 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**)

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

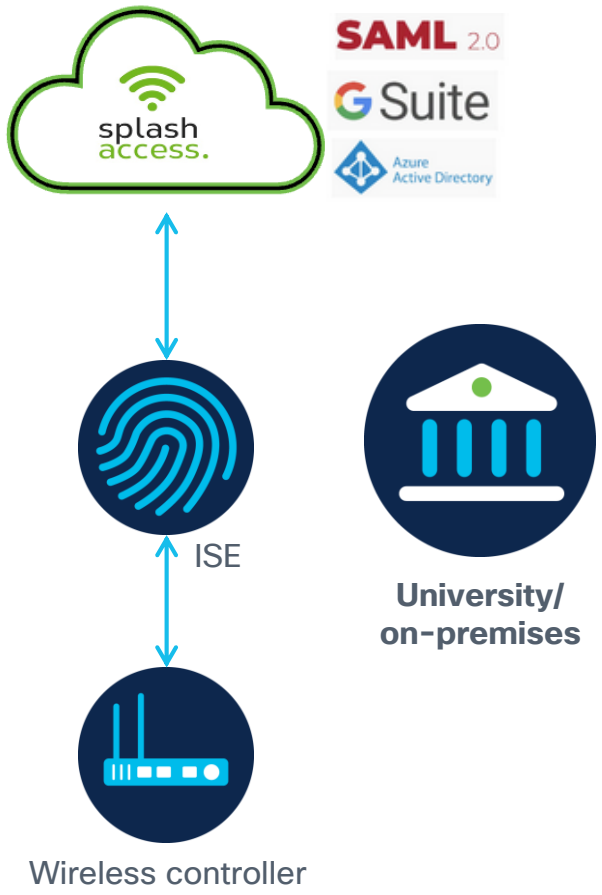
Catalyst UDN+ with splash access*

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/

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

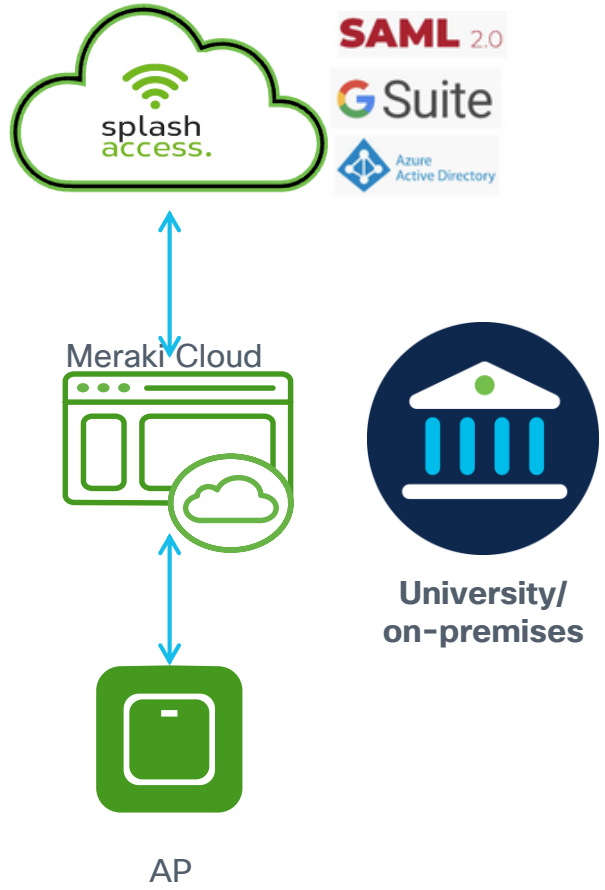
Meraki WPN with splash access*

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

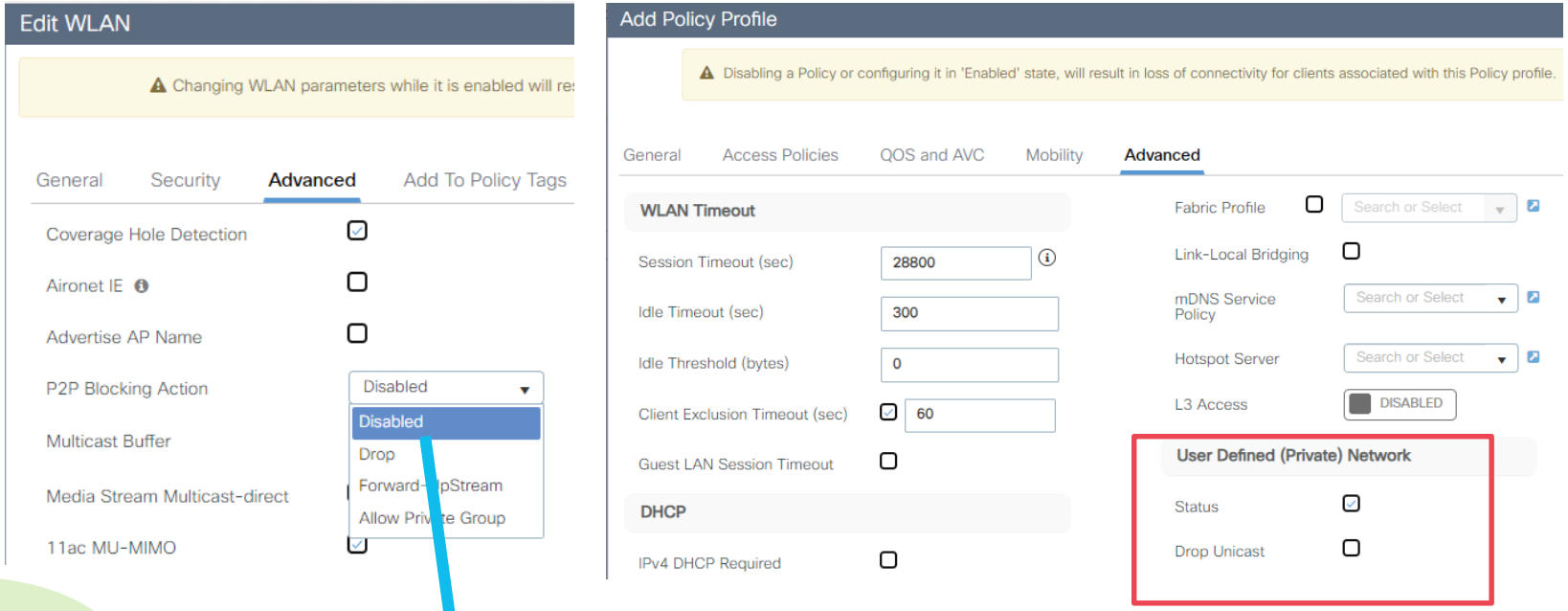
User devices joins the iPSK enabled SSID (with MAC filtering).

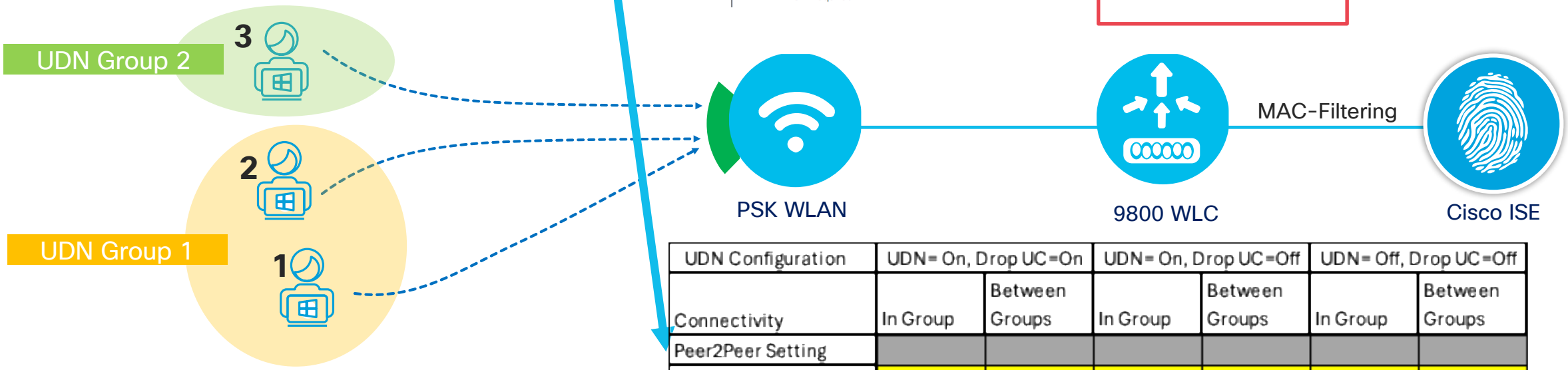


(*) UK based Cisco Technology Partner https://www.splashaccess.com/

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

UDN+ Isolation





UDN Configuration	UDN= On, Drop UC=On		UDN= On, Drop UC=Off		UDN= Off, Drop UC=Off	
Connectivity	In Group	Between Groups	In Group	Between Groups	In Group	Between Groups
Peer2Peer Setting						
Drop	No	No	No	No	No	No
Disable	Yes	No	Yes	Yes	Yes	Yes
Fwd Upstream	Unreach	Unreach	Unreach	Unreach	Unreach	Unreach
Allow Private Group	Yes	No	Yes	No	Yes	No

Allow UC between group but block MC

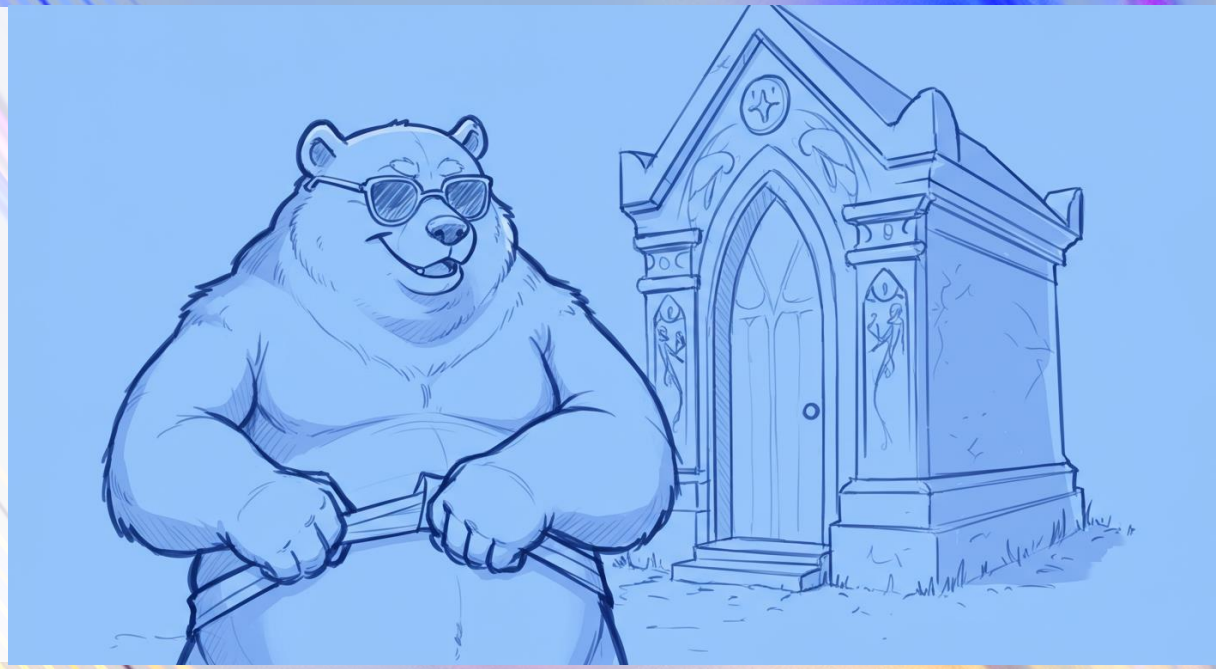
© 2025 Cisco and/or its affiliates. All rights reserved.

Consistent Performance

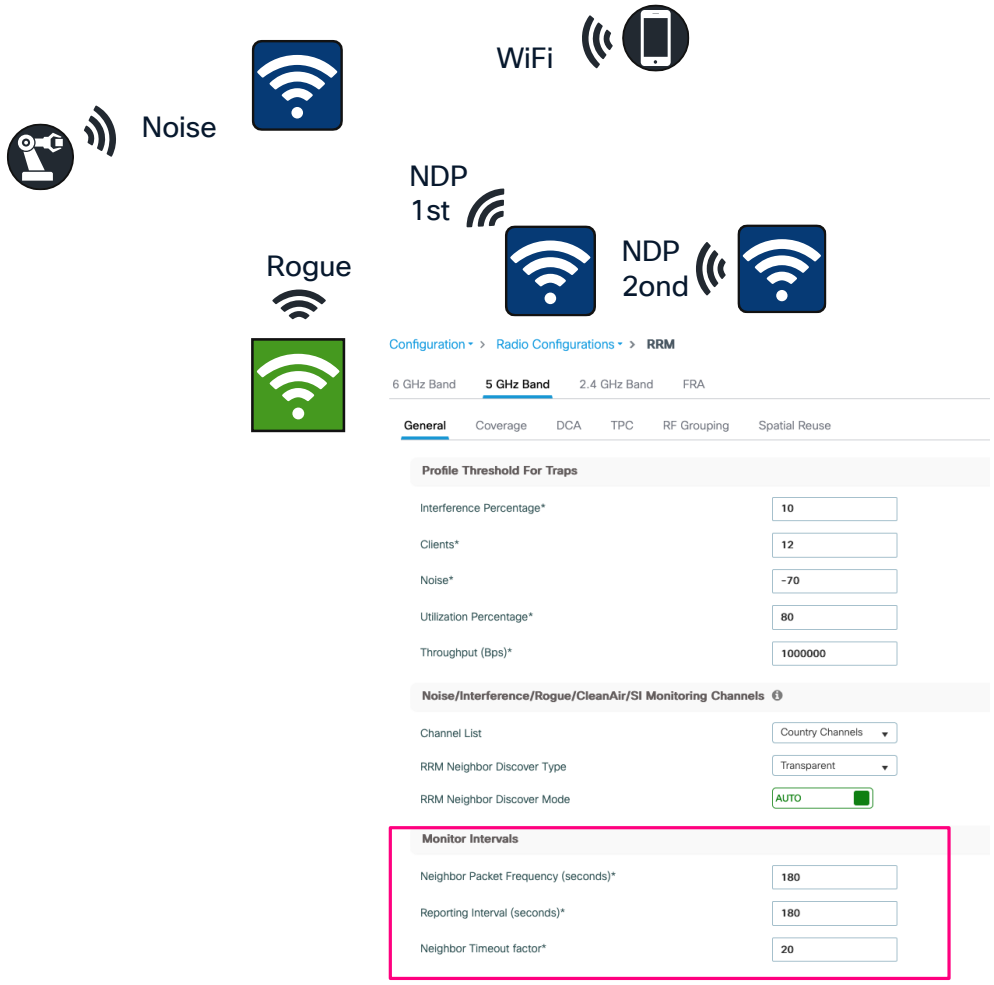


RRM

RRM Update/Review



Off Channel Scanning and Neighbor Discovery Protocol (NDP)



- NDP sent on all channels every 180 sec*
- NDP sent at Power Level 1@6Mbps
- Specific Multicast Address
- Be aware:



  - Neighbor timeout factor * neighbor timeout frequency = Neighbor Timeout
  - Neighbor Timeout should be greater than DCA Cycle

* 6GHz default is 600 Seconds

```
waikiki-en-9800-3(config)#ap dot11 5ghz rrm monitor neighbor-timeout-factor ?
  <5-60>  Timeout factor
```

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

NDP Thoughts

- NDP Messages are transmitted by default every:
  - 2.4GHz – 180 sec (3 ch typically)
  - 5GHz – 180 sec (21-22 ch typically)
  - 6GHz – 600 sec (59 ch typically)
- Now a scanning radio now does all the above at the same interval.
- Some (outdoor APs) still use in-band scanning due to the difference in antennas selected. This is selectable (Auto, Off-channel).
- NDP messages are transmitted on all channels in the selected channel list (i.e. Country, DCA, All).
- NDP is transmitted by serving radio.
- The current dwell time with scanning radios is 1.2 secs (50ms for inband).

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

NDP Usage

- Transmit Power Control (TPC) – To be discussed
- Flexible Radio Assignment (FRA) – To be discussed
- Rogue detection – If it is not transmitting the correct NDP then it is a rogue
- CleanAir correlation – APs that are part of the same group can determine if the interference is the same source
- AP RF Distance – This is changing to favor FTM* and UWB**.

* FTM = Fine Time Measurements

** UWB = Ultra-Wide Band

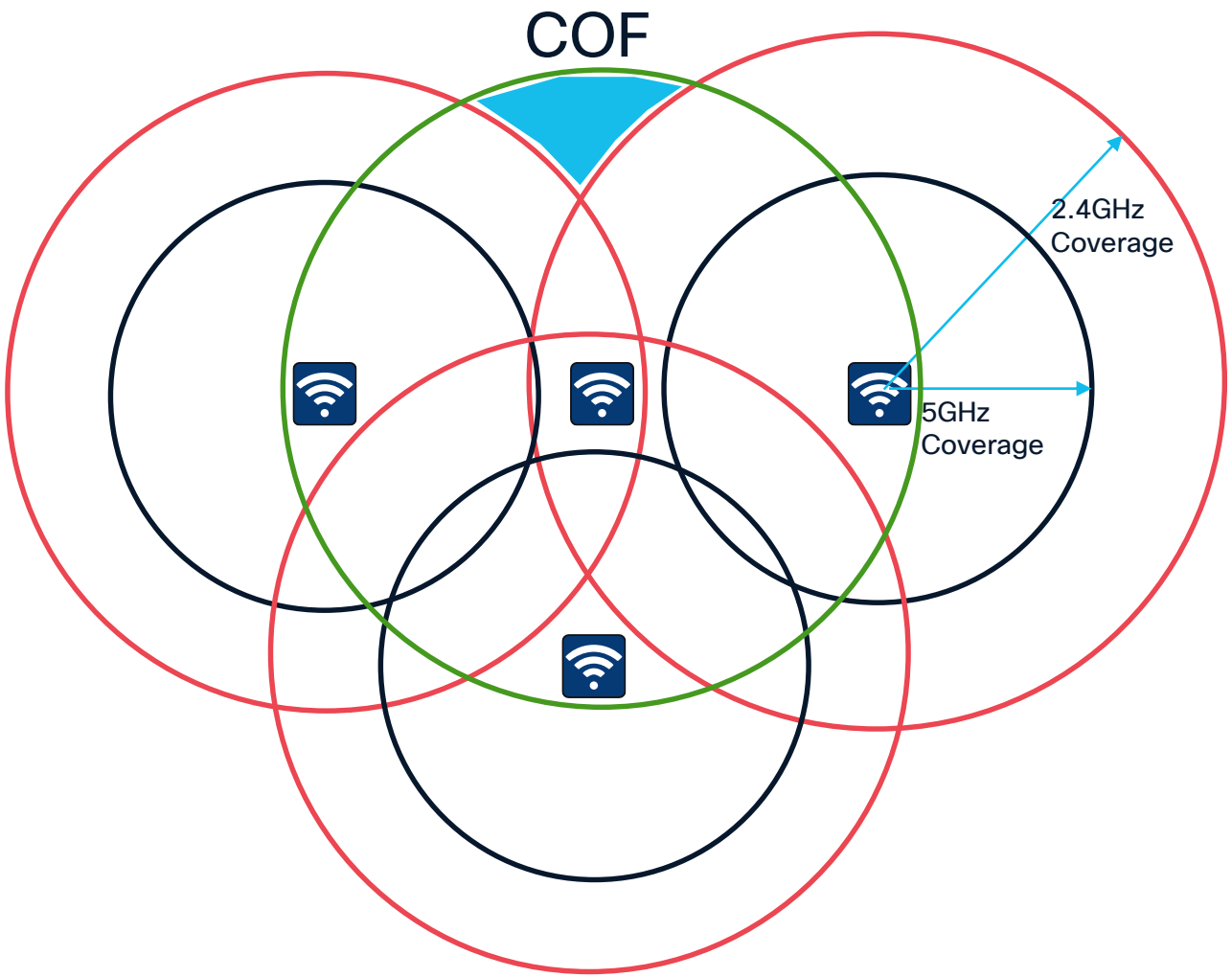
© 2025 Cisco and/or its affiliates. All rights reserved.

RF Group Leader

- The RF group leader does the RRM calculations for all participating WLCs in the RF group
- The RF group leader is assigned based on WLC capability; highest IP breaks the tie.
- Based on number of APs there can be more than 1 RF group leader. A 9800-80 can manage up to 12000 APs in one group.
- Chosen leaders can be different for different bands, but this breaks FRA so static assignment may be in order 
- AP Neighborhoods are formulated using >-80dBm NDP RSSI
- The global RRM configurations of the RF Group Leader take precedence over non-Group leaders.

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

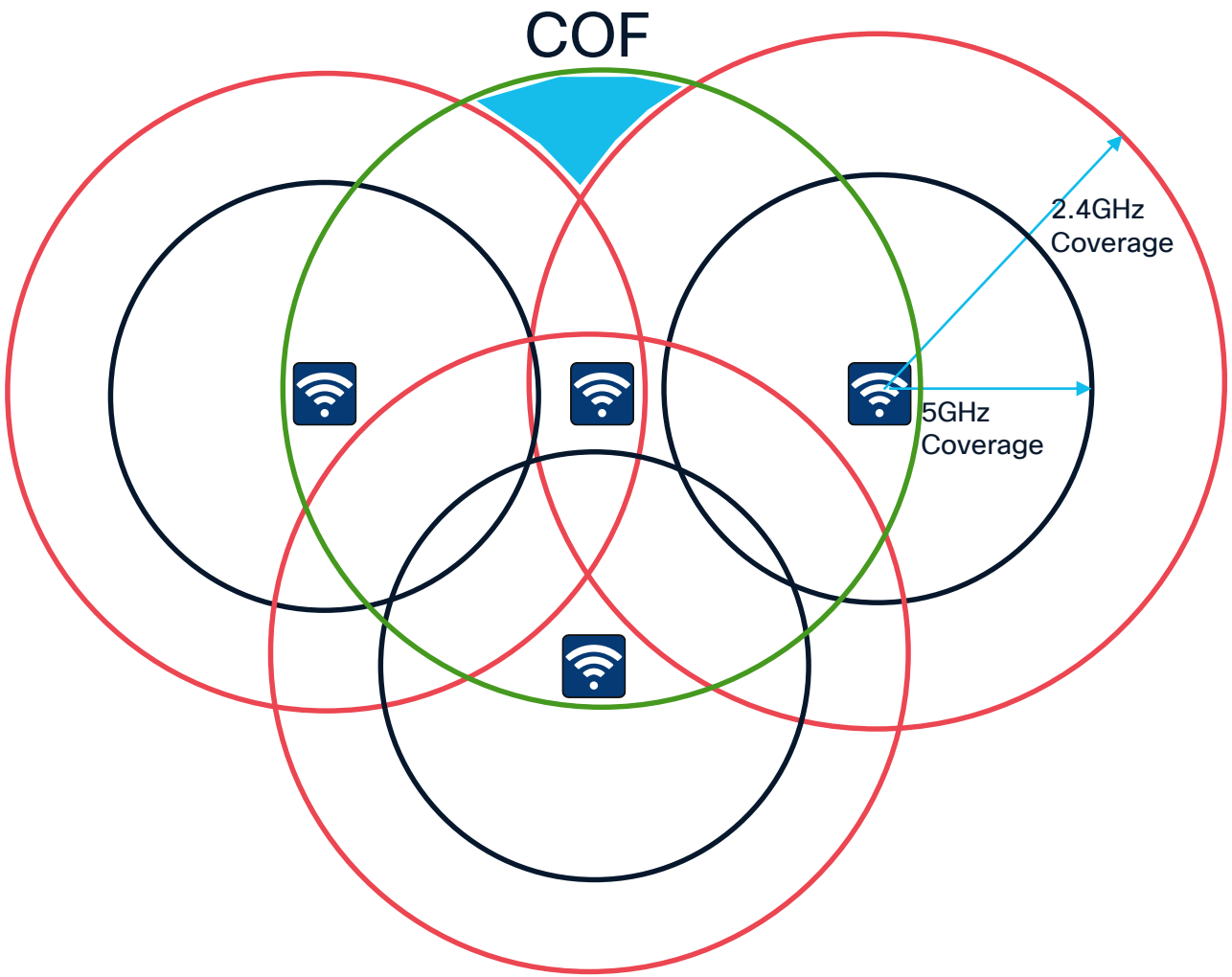
FRA and Coverage Overlap Factor (COF)



- NDP messages used to calculate overlap
- Calculation based on NDP measurements
- Be aware this does not account for APs with unique SSIDs
- COF would be adjusted based on geometry and sensitivity
- Must be enabled then set sensitivity and interval.
- Some APs force channel separation
- Radio (not assigned monitor) will wait for DCA for channel assignment.
- CHD can revert FRA!
- Consider manual mode and set APs based on COF

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

FRA and Coverage Overlap Factor (COF)



- NDP messages used to calculate overlap
- -67dBm cell edge
- Certain radios have flexible use typically TX/RX 2.4 or 5GHz
- Calculation based on NDP measurements
  - Location of APs
  - Size of cells
  - Uses 4 strongest APs
- Be aware this does not account for APs with unique SSIDs
- COF would be adjusted based on geometry
  - Low (100%) AP surrounded by others
  - Medium (95%) APs surrounded on one side
  - High (90%) AP down a hallway
  - Higher (85%)
  - Even Higher (80%)
  - Super High (50%)
- Start with Manual mode and watch COF
- Must be enabled then set sensitivity and interval.
- Some APs force channel separation
- Radio (not assigned monitor) will wait for DCA for channel assignment.
- CHD can revert FRA!
- Consider manual mode and set APs based on COF

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

Dynamic Channel Allocation

- Information collected from off channel scanning
- The Cost Metric (as sort of complex SINR) is calculated for every AP in-band (same channel, overlapping channels, noise, load). Result is a dB value.
- $E_j = W_s \sum_{i=1}^{N} S_i \ \mu_i \ adj\left(c_i - j\right) \ + \ W_n \sum_{c} N_c \ adj\left(c - j\right) \ + \ W_i \sum_{c} I_c \ adj\left(c - j\right)$
- APs are then stack ranked. Calculations are then done alternating worst case and a random value in the stack
- Normalized Cumulative Cost Function (NCCF) is calculated. Think of this as a “goodness” value. It looks at the first and second hop neighbors and determines improvement of each.
- $CCF(N(N(X)) = \sum_{i=1}^{|N(N(X))|} \frac{M(X_i)}{|N(N(X))|}$ If CM(x)>5dB, M(x)=1, If CM(x)<-5dB, M(x)–1, otherwise 0
- Determination to change the channel is then based on sensitivity

	High Sensitivity	Medium Sensitivity	Low Sensitivity
CF Improvement	5 /5 dB	10/15 dB	20/20 dB
Normalized CCF	0.1	0.2	0.5

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

DCA Notes

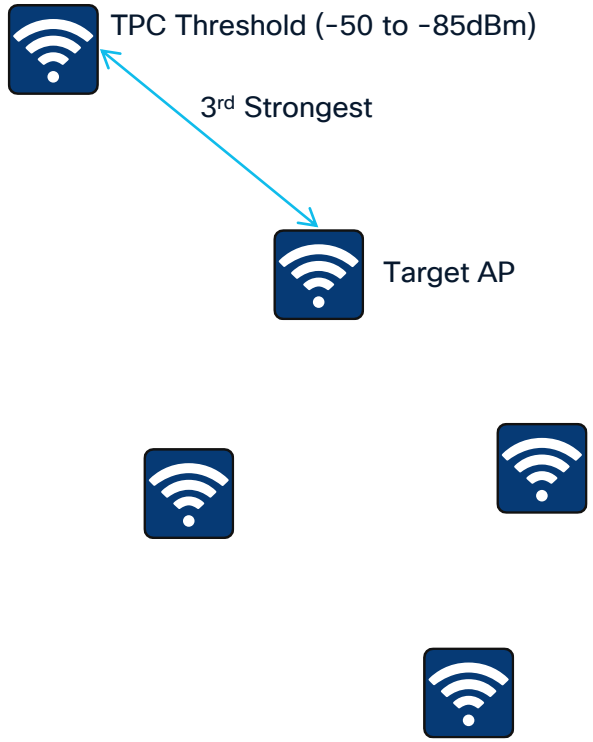
- This method assures the change is good for both the AP and the rest of the neighboring APs.
- Account for secondary channel thresholds higher than primary
- Penalties are applied for DFS occurrences
- Zero Wait DFS
- Startup mode
  - 10 min cycle/ 100 minutes long
  - NCCF not accounted for
  - Pinning and Cascading can occur

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

TPC

- 3rd strongest AP is identified and the effective pathloss is calculated $-1(RSSI_W - Tx_W(P_{max}))$
- Adjusts target AP power to have 3rd strongest AP “hear” the target AP a the the TPC Threshold.
- Hysteresis is applied
- Less than 3 neighbors uses a power smoothing technique (average of surrounding values).
- TPC Min/Max used to bound TPC. Typically, a min at 5GHz and a max at 2.4GHz.
- By selecting channel aware TPC will take into account channel activity not just NDP RSSI.





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

Client Network Preference

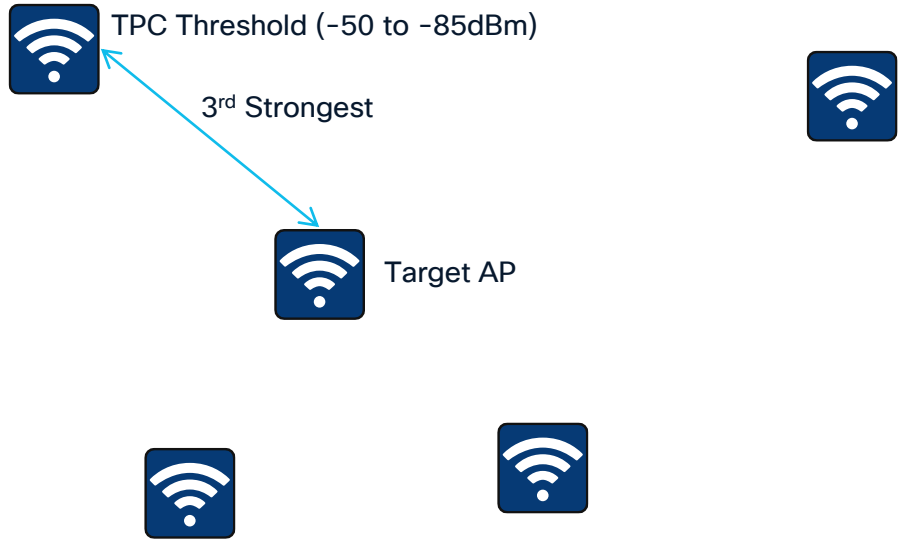
RRM Algorithm	Connectivity	Throughput	Default
DCA	Higher Bias on current Channel Low Sensitivity for DCA (override in DCA) Prefer current channel when Voice/Video	Less bias on current channel High DCA Sensitivity (override in DCA) All 11n capable clients	No Change from Current DCA behavior
DTPC	DTPC should not reduce power when weak signal clients detected (<-79)	DTPC will not increase power when number of clients is over the configured max threshold	No Change from current TPC behavior
DBS	Prefer Current bandwidth Prefer current Primary channel Lower bias on client type Voice/Video clients increased contribution	Favor Higher Channel Widths Higher bias for high capacity (11n,11ac) client types present	No Change from current DBS behavior
FlexDFS/ED–RRM	Priority on maintaining primary channel Voice/Video client increased contribution	Priority on higher bandwidth channel width	No Change from current flexDFS/ED-RRM behavior
FRA	No Band/Role switching when more than 3 clients exist	Band-switching, regardless of clients	Defaults to connectivity profile

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

TPC



- Again, based on neighbor messages (NDP)
- NDP Message transmitted at full power
- 3rd strongest AP is identified and the effective pathloss is calculated -1($RSSI_W$ – $Tx_W(P_{max})$)
- Adjusts target AP power to have 3rd strongest AP “hear” the target AP a the the TPC Threshold.
- Hysteresis is applied
  - Increase threshold – >3dB
  - Decrease threshold – >-6dB
  - Power change by only 1 (3dB) each iteration
- Less than 3 neighbors uses a power smoothing technique (average of surrounding values).
- TPC Min/Max used to bound TPC. Typically, a min at 5GHz and a max at 2.4GHz.



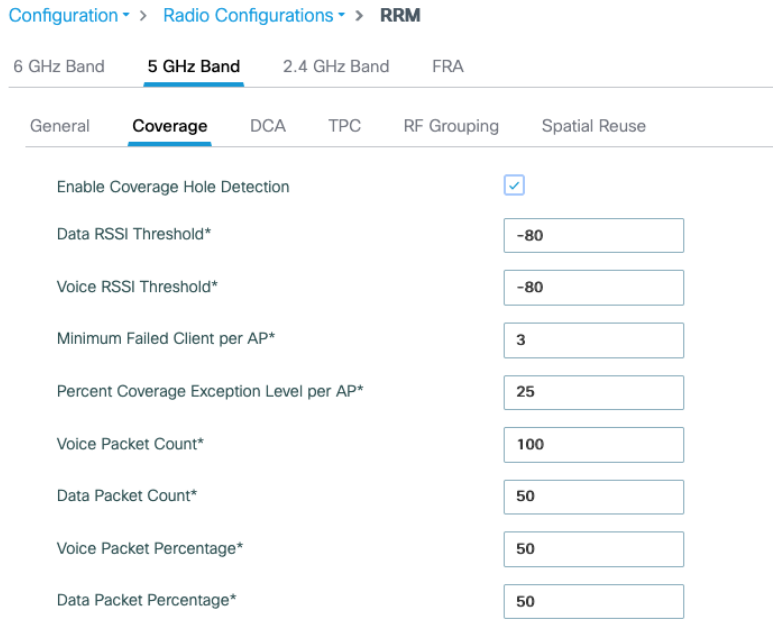


© 2025 Cisco and/or its affiliates. All rights reserved.

Coverage Hole Detection

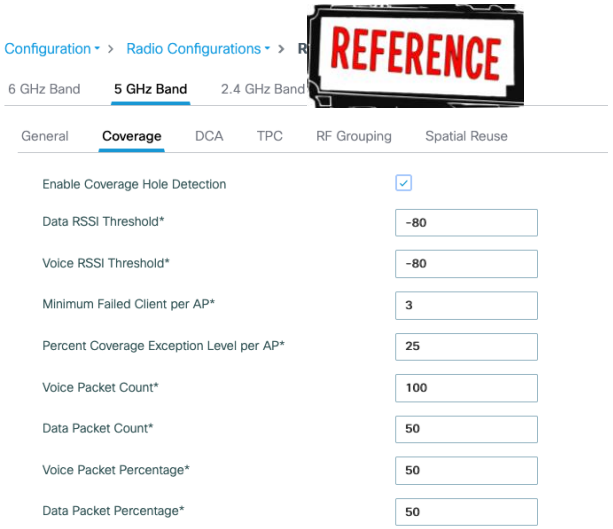
- Adjust power up in the event of coverage hole detected.
- Must meet minimum failed client count AND percent failed clients
- WLC then looks to see if it sees the client stronger (above the threshold) on other APs
- Power can only be increase by 1 (3dB)
- Optimized roaming shares these thresholds (Config>wireless>Adv)
- Be aware if the situation changes the AP may take some time to cycle back with regular TPC.





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

Coverage Hole Detection



- Not run on group leader…run on APs controller
- Based on client RSSI (1dB Bins between -90 and -60dBm)
- Client falling below threshold for >5sec is **marked** (alarm)
- If the client stay below threshold for >90 sec becomes **actionable**
- Must meet minimum failed client count AND percent failed clients
- WLC then looks to see if it sees the client stronger (above the threshold) on other APs
- Power can only be increase by 1 (3dB)
- Optimized roaming shares these thresholds (Config>wireless>Adv)
- Be aware if the situation changes the AP may take some time to cycle back with regular TPC.



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

Dynamic Bandwidth Selection

- Bandwidth decision based on:
  - *Associated client capabilities and types*
  - *RF Neighbor Channel Widths*
  - *OBSS channel Overlap ratios*
  - *Channel Utilization*
  - *Non Wi-Fi Noise*
  - *Wi-Fi interference*
- *Creates a ”bias” that is added to the calculated channel metric*
- *Then a “recommendation” is made on channel bandwidth*

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

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

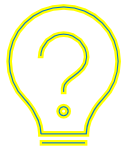
General Use

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

Special Case

- Single 2.4+5 + 6GHz
- WPA 2 transition legacy (2.4/5GHz)
- WPA 3 (all bands)
- Same 6GHz SSID

Typical WPA Personal or Enterprise



17.12 added 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.
- Special Case
  - Like General Use
  - Can help reduce the bounce in general use
  - RNR is still effective
  - Clients will often stay at 5GHz
- Typical for WPA Personal or Enterprise
  - Keep the same Cipher Suite if possible
  - Client may think they are on WPA3 when on WPA2
  - Open/OWE work but not for 6GHz.

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

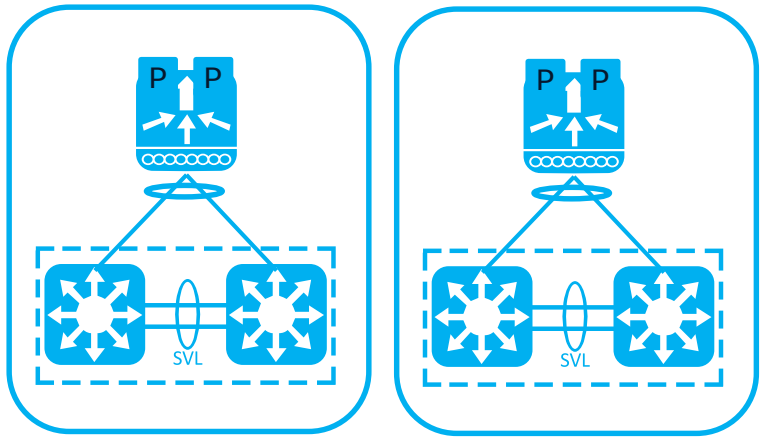
Healthcare

- SSID Sprawl
- Security
- Voice

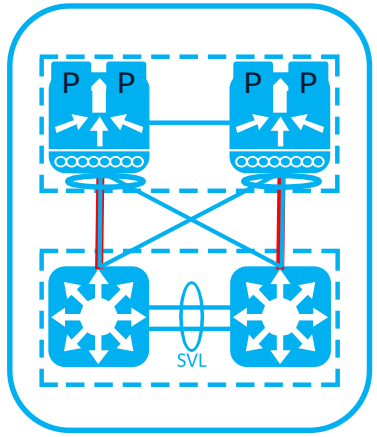
High Availability

How do I include this in my design

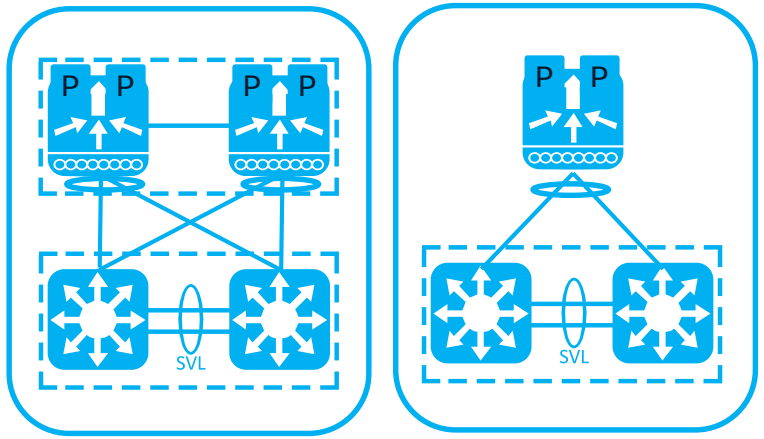
High Availability Architectures for WLCs



AP Fail-Over (N+1)

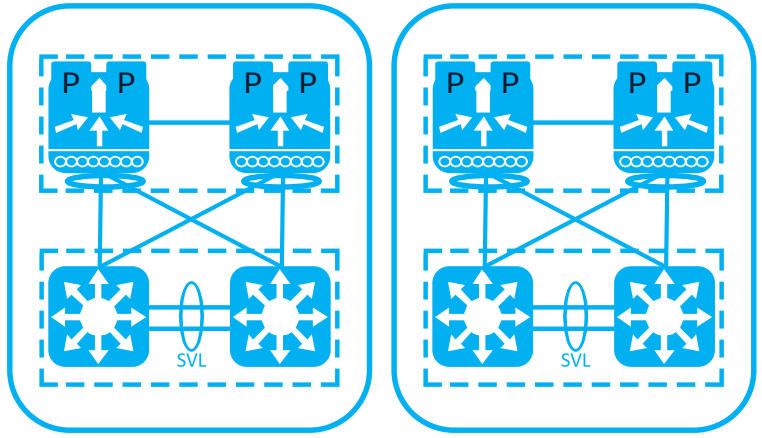


SSO



SSO + One

Note: LACP/PAGP Supported

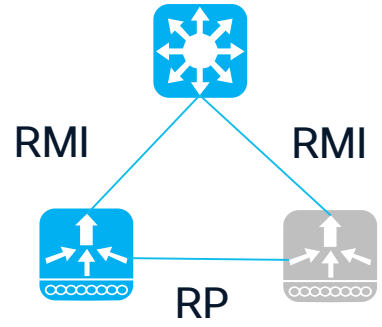


SSO + SSO

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

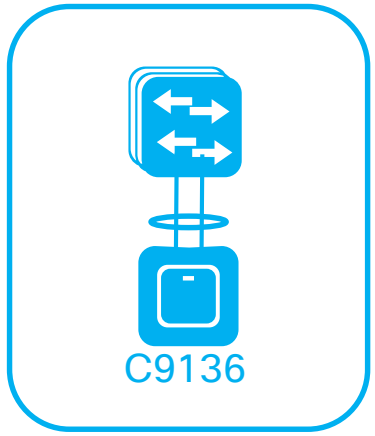
SSO Notes

- 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 an option

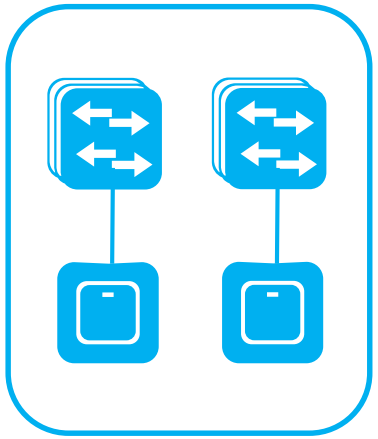


© 2025 Cisco and/or its affiliates. All rights reserved.

High Availability Architectures for APs



AP Dual Connection



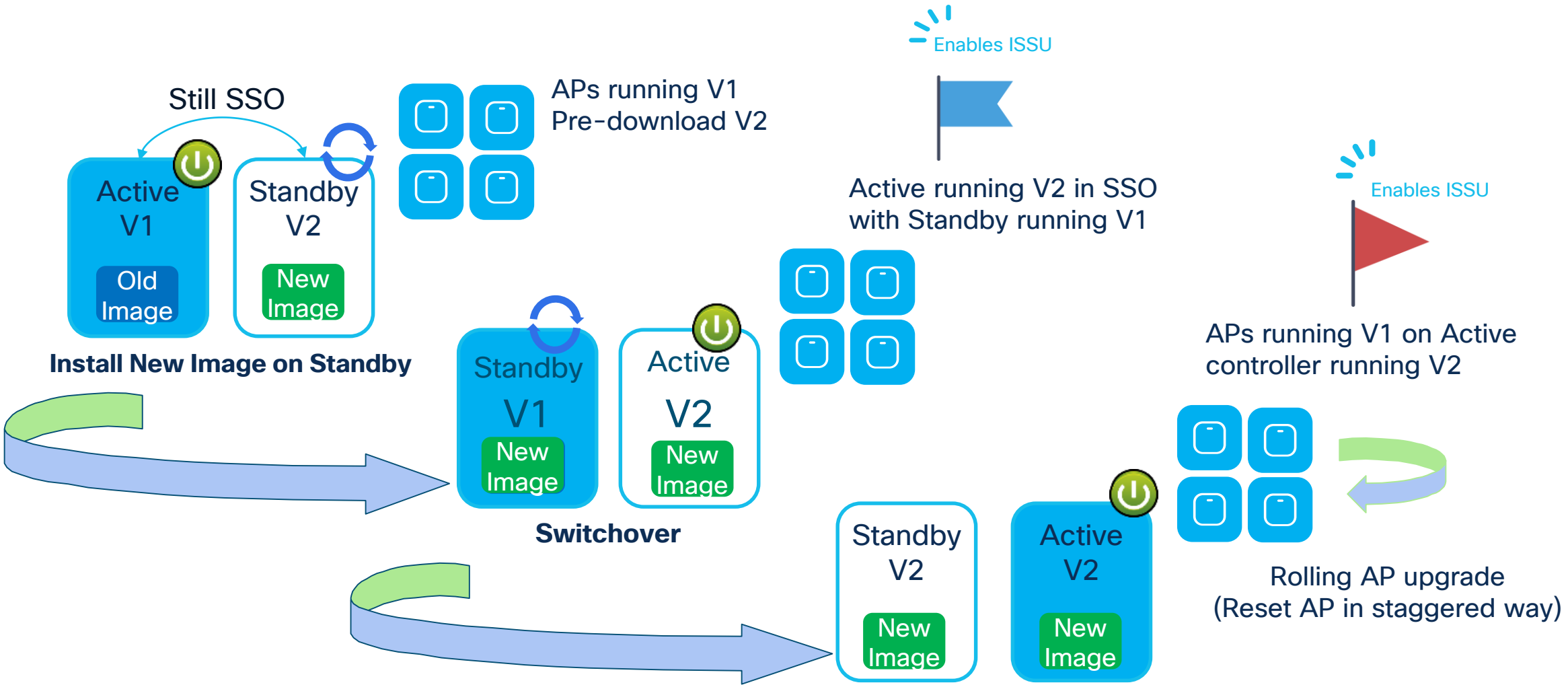
Overlapping Coverage

Switching for AP HA

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

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

ISSU Process



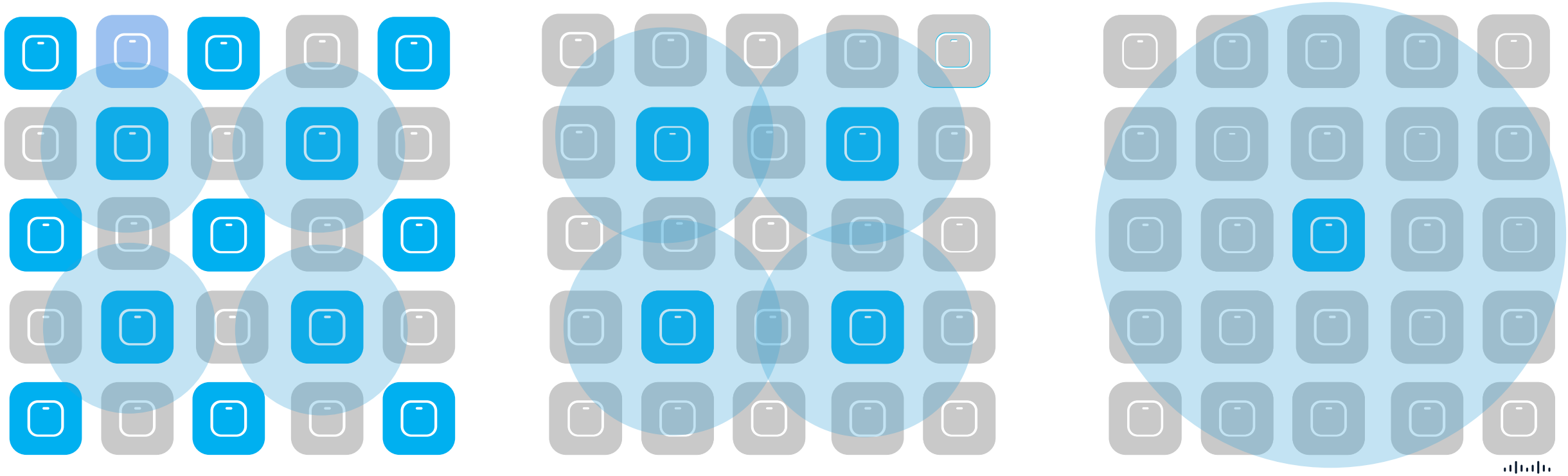
Note: “Hitless” and “ISSU” are not the same thing

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

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

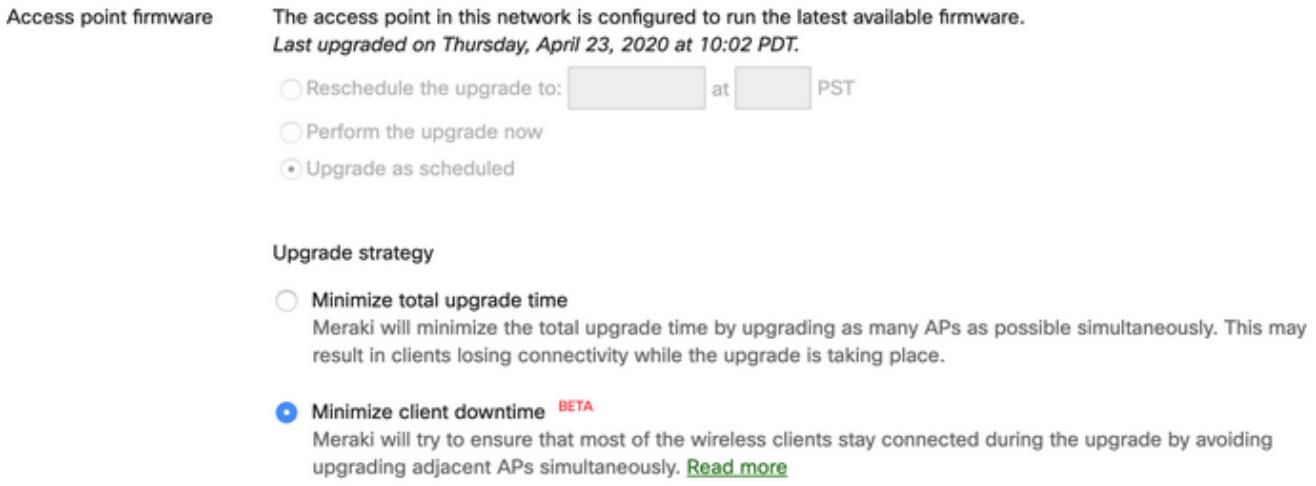
User selects % of APs to upgrade in one go [5, 15, 25]

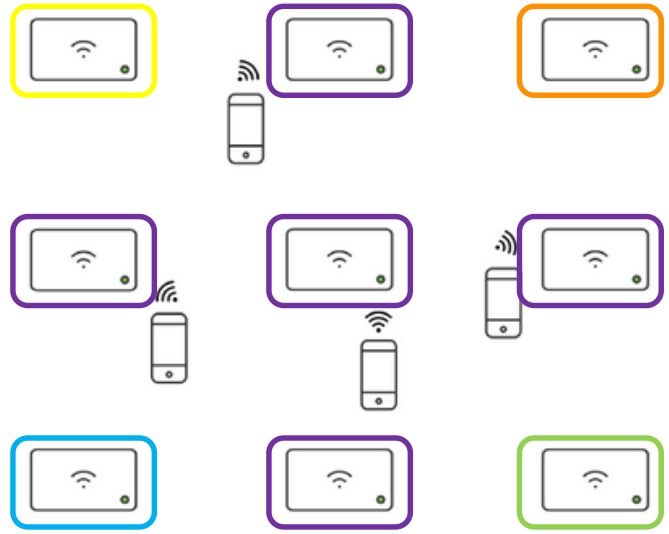
- For 25%, Neighbors marked = 6 [Expected number of iterations ~ 5]
- For 15%, Neighbors marked = 12 [Expected number of iterations ~ 12]
- For 5%, Neighbors marked = 24 [Expected number of iterations ~ 22]



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

Meraki Minimize Client Down Time





- 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.

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

SSID Sprawl
What can be done?

SSID Sprawl

	2.4GHz	5GHz	6GHz
WPA2 Enterprise + 802.11r	✓	✓	✗
WPA2 AES PSK (iPSK)	✓	✓	✗
Open (Guest)	✓	✓	✗
OWE (Guest)	✗	✓	✓
WPA3 + 11r	✗	✓	✓
WPA2 Enterprise Legacy	✓	✓	✗

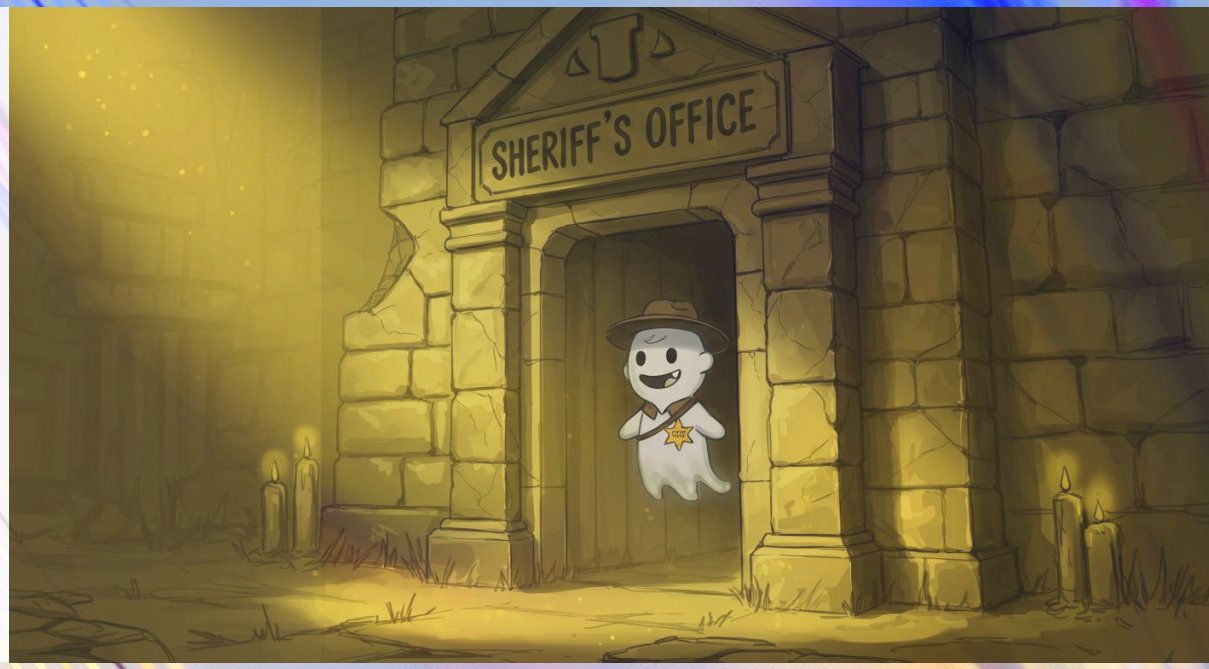
Windows clients, Apple clients, Old Honeywell equipment, other medical equipment.

Consider transition mode

Offer SSIDs only on the bands required.

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

Security Concerns
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

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

What is “Transition Mode”

- Allow the use of the SSID for both WPA2 and WPA3
  - Clients can join the same BSS as either WPA2 or WPA3
  - Clients can join an AP in the ESS and roam with WPA2 or WPA3
  - Moving from WPA2 to WPA3 (either direction) is not a fast roam.
  - Client could for example “move” from WPA2 at 2.4GHz to WPA3 at 5GHz

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

Transition Modes

- Considerations
  - Authentication (Open, PSK/SAE, Dot1X)
  - Band (2.4,5, 6GHz)
  - Security (WPA2, WPA3)
  - Standard (802.11ax, 802.11be)
  - Configuration (same profile, different profiles)
- 6GHz
  - There is no “transition mode” for 6GHz. 
    - The WFA WPA3 specification paragraph 11 clearly states that there is no transition mode for 6GHz in any mode or standard.
  - An ESS can be created with transition mode for 2.4/5GHz and then WPA3 only for 6GHz.

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

WPA2 vs WPA3

- WPA3
  - *00-0F-AC:3 (FT with 802.1X/SHA256)*
  - *00-0F-AC:5 (802.1X with SHA256)*
  - *00-0F-AC:8 (SAE)*
  - *00-0F-AC:9 (FT with SAE)*
  - *00-0F-AC:12 (802.1X in 192-bit mode)*
  - *00-0F-AC:13 (FT with 802.1X using SHA-384)*
  - *00-0F-AC:24 (SAE using group-dependent hash)*
  - *00-0F-AC:25 (FT with SAE using group-dependent hash)*
  - *MFPC (Management Frame Protection Capable) = 1, MFPR (Management Frame Required) = 1*
- WPA2
  - *00-0F-AC:1 (802.1X)*
  - *00-0F-AC:2 (PSK)*
  - *00-0F-AC:3 (FT with 802.1X/SHA256)*
  - *00-0F-AC:5 (802.1X with SHA256)***
  - *00-0F-AC:4 (FT with PSK)*
  - *00-0F-AC:6 (PSK using SHA-256),*
  - *00-0F-AC:20 (PSK using SHA-384)*
  - *00-0F-AC:19 (FT over PSK using SHA-384)*

** Optional support of AC:3 and AC:5 in WPA2, allowed in controller WLAN configuration

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

WFA Defined WPA2/WPA3 AKMs from WFA WPA3 Spec



1.4 Types of Security Associations

When an AP and STA establish secure connectivity, the type of security association depends on their respective configuration. With respect to this specification, the type of security association can be either WPA2 or WPA3. A detailed summary of the values of fields in the RSNE and RSNXE and the resultant type of association is given in Table 2.

A WPA3 security association is an RSNA in which PMF and one of the following AKMs was negotiated to be used:

- 00-0F-AC:8, 00-0F-AC:24 (SAE)
- 00-0F-AC:9, 00-0F-AC:25 (FT with SAE)
- 00-0F-AC:5 (802.1X)
- 00-0F-AC:3 (FT with 802.1X)
- 00-0F-AC:12 (802.1X in 192-bit mode)

© 2025 Wi-Fi Alliance. All Rights Reserved.
Used with the permission of Wi-Fi Alliance under the terms as stated in this document.

- 00-0F-AC:13 (FT with 802.1X using SHA-384)

A WPA2 security association is an RSNA in which one of the following AKMs was negotiated to be used:

- 00-0F-AC:2 (PSK)
- 00-0F-AC:4 (FT with PSK)
- 00-0F-AC:1 (802.1X)
- 00-0F-AC:3 (FT with 802.1X)

NOTE: WPA2 STAs and APs might support the SHA-256 AKMs (00-0F-AC:3 and 00-0F-AC:5) with PMF for Enterprise

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

Transition mode for WPA-Enterprise

- Dot1X (Enterprise)
  - A client can authenticate using WPA2 or WPA3 with dot1x
    - At least AKM selector 00-0F-AC:1 and 00-0F-AC:5.
    - MFPC=1, MFPR=0*
    - No WEP, TKIP, WPA1
    - A handful off other specifics (see WPA3 specification PP 3.4)
    - There are several new AKMs for WPA3
  - At 6GHz (no transition mode) 802.1X SHA-1 AKM not allowed, and PMF always used.
  - Transition mode does not specify which Pairwise Cipher be careful with using different ciphers. This can cause roaming issue 

* MFPC = Management Frame Protection Capable, MFPR = MFP Required

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

Transition Mode on dot1X can be confusing

WPA2 Only

```
Tag: RSN Information
   Tag Number: RSN Information (48)
   Tag length: 30
   RSN Version: 1
   Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Cipher Suite type: AES (CCM) (4)
   Pairwise Cipher Suite Count: 1
   Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
         Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
         Pairwise Cipher Suite type: AES (CCM) (4)
   Auth Key Management (AKM) Suite Count: 2
   Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) WPA (SHA256)
      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
         Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
         Auth Key Management (AKM) type: WPA (1)
      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA256)
         Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
         Auth Key Management (AKM) type: WPA (SHA256) (5)
   RSN Capabilities: 0x00e8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentic…
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key…
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GT…
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GT…
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
      .0.. .... .... .... = OCVC: False
   PMKID Count: 0
   PMKID List
   Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Management Cipher Suite type: BIP (128) (6)
```

WPA2/WPA3 Transition Mode

```
Tag: RSN Information
   Tag Number: RSN Information (48)
   Tag length: 30
   RSN Version: 1
   Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Cipher Suite type: AES (CCM) (4)
   Pairwise Cipher Suite Count: 1
   Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
         Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
         Pairwise Cipher Suite type: AES (CCM) (4)
   Auth Key Management (AKM) Suite Count: 2
   Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) WPA (SHA256)
      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
         Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
         Auth Key Management (AKM) type: WPA (1)
      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA256)
         Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
         Auth Key Management (AKM) type: WPA (SHA256) (5)
   RSN Capabilities: 0x00e8
      .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authenticatio
      .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 s
      .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/S
      .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/S
      .... .... .1.. .... = Management Frame Protection Required: True
      .... .... 1... .... = Management Frame Protection Capable: True
      .... ...0 .... .... = Joint Multi-band RSNA: False
      .... ..0. .... .... = PeerKey Enabled: False
      ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
      .0.. .... .... .... = OCVC: False
   PMKID Count: 0
   PMKID List
   Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
      Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Group Management Cipher Suite type: BIP (128) (6)
```

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

Transition mode for WPA-Personal

- PSK/SAE
  - Transition mode is available for 2.4/5GHz
    - WPA2 PSK and WPA3 SAE
    - Must enable 00-0F-AC:2 and 00-0F-AC:8
    - Should enable 00-0F-AC:6 and 00-0F-AC:24
  - SAE only on 6GHz
  - MFPC (Management Frame Protection Capable) = 1, MFPR (Management Frame Required) = 0
  - Minimum of CCMP-128 for Wi-Fi7 add GCMP-256 Pairwise Cipher Suite
  - Transition mode has vulnerability to downgrade attack
  - SAE has “Dragonblood” vulnerability (side channel)
  - Hunt and Peck not allowed with Wi-Fi 7 features (EHT/MLO) or 6GHz.
    - Hashing is the required option.

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

Transition mode for WPA-Personal



- PSK/SAE
  - Transition mode is available for 2.4/5GHz
    - WPA2 PSK and WPA3 SAE
    - Must enable 00-0F-AC:2 and 00-0F-AC:8
    - Should enable 00-0F-AC:6 and 00-0F-AC:24
  - SAE only on 6GHz
  - Transition mode has vulnerability to downgrade attack
    - Transition disable fixes this but…
    - Clients that move to APs not offering WPA3 may get stuck
  - SAE has “Dragonblood” vulnerability (side channel)
    - SAE does not share key, instead it basically provides an element that shows it knows the password. This prevents offline attack as is it is interactive. RFC 7664
    - When deriving that elements (Password Element) it used a random selection method that looked for a solution that showed even division (even modulo) on elliptic curve.
    - Based on the length of time attackers could deduce or reduce the set of elements.
  - Hunt and Peck not allowed with Wi-Fi 7 features (EHT/MLO) or 6GHz.
    - Hashing is the required option.
  - MFPC (Management Frame Protection Capable) = 1, MFPR (Management Frame Required) = 0
  - Minimum of CCMP-128 for Wi-Fi7 add GCMP-256 Pairwise Cipher Suite

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

Example Transition WPA2/3 Personal Transition Mode

```
Auth Key Management (AKM) Suite Count: 3
Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256) 00:0f:ac (Ieee 802.11) FT using SAE (SHA256)
  Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: PSK (2)
  Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: SAE (SHA256) (8)
  Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT using SAE (SHA256)
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: FT using SAE (SHA256) (9)
RSN Capabilities: 0x00e8
  .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
  .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
  .... .... .... 10.. = RSN PTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
  .... .... ..10 .... = RSN GTKSA Replay Counter capabilities: 4 replay counters per PTKSA/GTKSA/STAKeySA (0x2)
  .... .... .1.. .... = Management Frame Protection Required: True
  .... .... 1... .... = Management Frame Protection Capable: True
  .... ...0 .... .... = Joint Multi-band RSNA: False
  .... ..0. .... .... = PeerKey Enabled: False
  ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
  .0.. .... .... .... = OCVC: False
```

Can be false

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

Transition mode for Open/OWE

- Open/OWE Transition mode
  - Transition mode exists only for 2.4/5GHz
    - OWE transition mode defined prior to 6GHz availability
    - 6GHz specification explicitly forbids the use of OWE transition mode
  - Two SSID
    - OWE is set to hidden so clients will not try to join natively
    - Open SSID broadcasts the information of hidden OWE SSID in transition element.
    - See WFA Enhance Open Technology Overview paragraph 2.2(Login required)
  - OWE Transition Mode will not help client adoption/use of 6GHz!
  - Recommend using two SSIDs, one with WPA2/Open at 5GHz and a second one at WPA3/OWE at 5&6GHz. But then there is Apple...

https://support.apple.com/en-us/102285

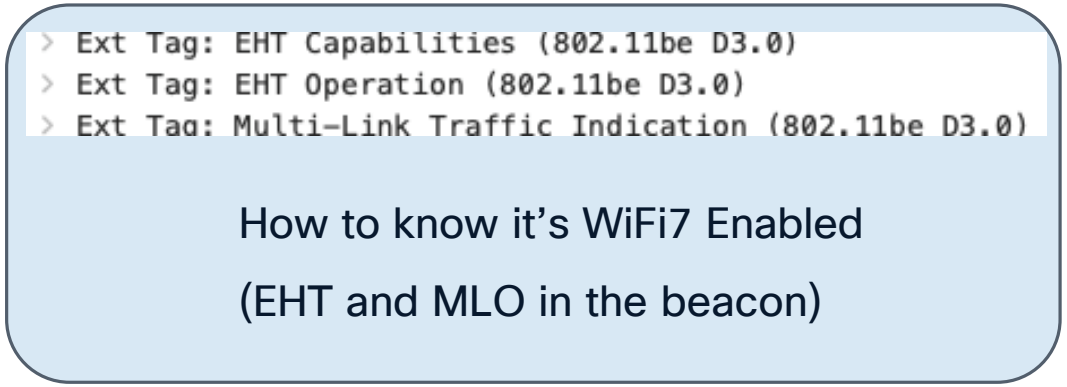




© 2025 Cisco and/or its affiliates. All rights reserved.

Wi-Fi 7

- No PSK AKM or 802.1X SHA-1 AKM
  - AP can advertise these AKM but
  - STA that joins as EHT or MLO shall not use these AKMs
- No Open allowed with EHT or MLO
- No OWE Transition mode with EHT or MLO
- Specific to WPA3 and EHT/MLO (Before 17.18)
  - Must include AKM 00-0F-AC:24/25 with GCMP-256
  - Must use Hash-to-Element (IEEE P802.11be/D7.0 pp12.12.9)
  - Must include AKM 00-0F-AC:8/9 (deviation)
  - WPA2 PSK/802.1x with PMF (deviation)
  - 802.1x-SHA256 (AC:5) with PMF
  - Suite-B-192 with PMF



Not Allowed by WPA3 Specification

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

WiFi-7 Evolution with Code Version

Non-compliant beacons

Clients can try to negotiate non-compliant connection

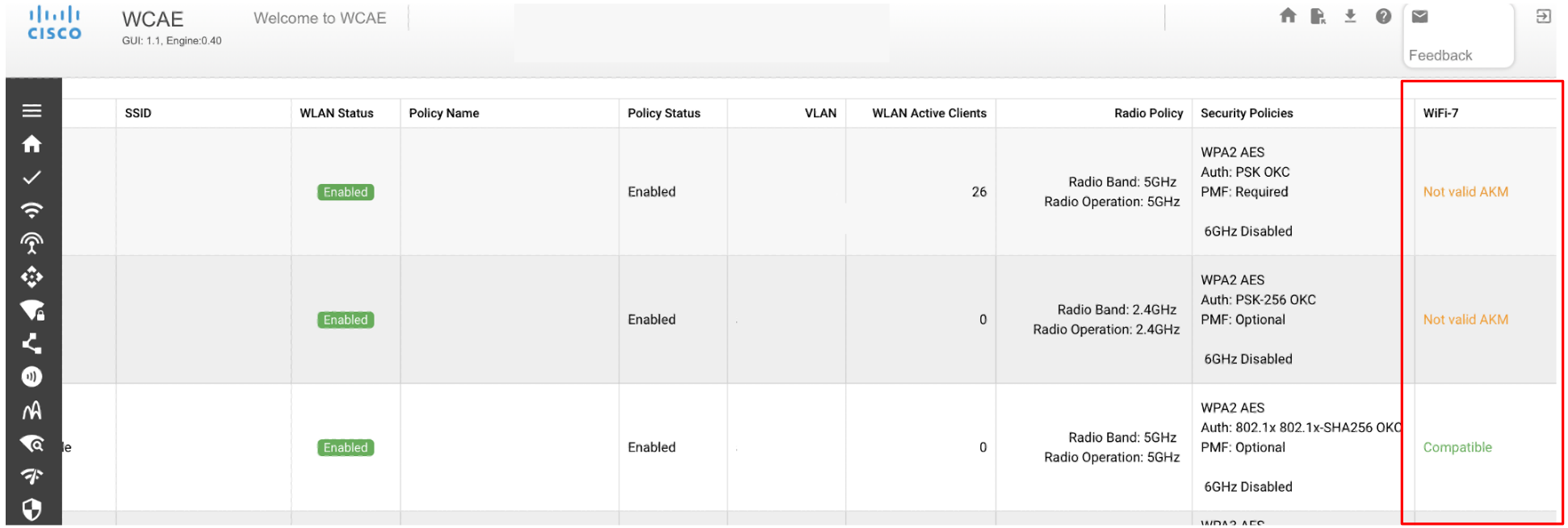
17.15.3 ➔

Non-compliant beacons

Clients not allowed to negotiate non-compliant connection

17.18.1 ➔

Beacons are compliant



SSID	WLAN Status	Policy Name	Policy Status	VLAN	WLAN Active Clients	Radio Policy	Security Policies	WiFi-7
	Enabled		Enabled		26	Radio Band: 5GHz Radio Operation: 5GHz	WPA2 AES Auth: PSK OKC PMF: Required 6GHz Disabled	Not valid AKM
	Enabled		Enabled		0	Radio Band: 2.4GHz Radio Operation: 2.4GHz	WPA2 AES Auth: PSK-256 OKC PMF: Optional 6GHz Disabled	Not valid AKM
	Enabled		Enabled		0	Radio Band: 5GHz Radio Operation: 5GHz	WPA2 AES Auth: 802.1x 802.1x-SHA256 OKC PMF: Optional 6GHz Disabled	Compatible

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

Wi-Fi 7 Still evolving…



Phone a friend: Thanks to Shreyas Trivedi for proving his test results!! Check out his WiFi7 blog also!

- In certain cases, if a WLAN is configured with non WiFi7 compliant security(say SAE/AKM8) then this can cause clients to get stuck and not be able to join (not down grade). Future enhancements will address this behavior by dynamically downgrading beacon as per configured security.
- Clients do not roam between different Cipher Suite. Example: *00-0F-AC:8 (SAE) with CCM128 does not roam to 00-0F-AC:24 GCMP256*
- While Wi-Fi 7 has a technique (STR/MLMR) to use two radios simultaneously (Multi-Link Operation) many clients do not support combination of 5GHz and 6GHz. Typically, there are two options:
  - Dual Band Simultaneous (DBS) and High Band Simultaneous (HBS).
    - DBS is 2.4GHz and (5GHz or 6GHz)
    - HBS is 5 GHz and/or 6 GHz

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

Wi-Fi 7 Still evolving...Continued

- Different devices have different restrictions
  - Both channels must have the same bandwidth configured for efficient MLO scheduling.
  - Scheduling behaviors are not consistent and in many cases traffic thresholds need to be exceeded before MLO occurs.
  - Wi-Fi 7 MLO has the flexibility for different methods for MLO. For example, one radio transmits but two radios receive. In some case both radios can transmit and receive. In the latter case, it can starve out other clients that are only one transmit radio.
  - Some clients while Wi-Fi 7 capable, only have one transmitter and one receiver (iPhone16 for example). It will however support up to 3 links (one at a time) where many others will only support 2.
  - Wi-Fi 7 also allows for a very large acknowledgement to be sent, reducing the ping-ponging between data send and acknowledgement returned. Not all clients support this.

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

AKM Selection Order

Personal

1. FT Authentication over SAE using group-dependent hash 00-0F-AC:25
2. SAE Authentication using group-dependent hash 00-0F-AC:24
3. FT Authentication over SAE 00-0F-AC:9
4. SAE Authentication 00-0F-AC:8
5. FT Authentication over PSK 00-0F-AC:4
6. PSK using SHA-256 00-0F-AC:6
7. PSK 00-0F-AC:2

Enterprise

1. FT Authentication over IEEE Std 802.1X using SHA-256 00-0F-AC:3
2. Authentication using IEEE Std 802.1X using SHA-256 00-0F-AC:5
3. Authentication using IEEE Std 802.1X 00-0F-AC:1

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

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.

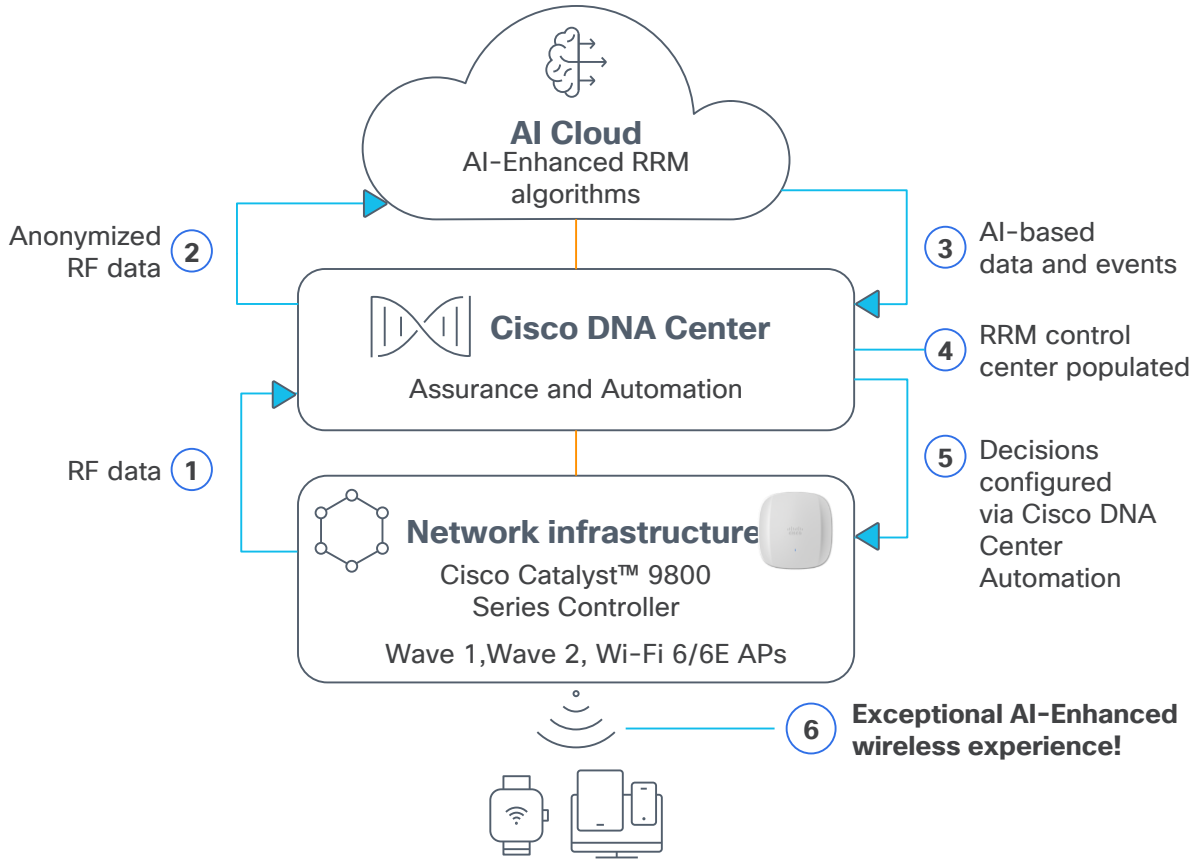
Product capability

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 DNA 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.

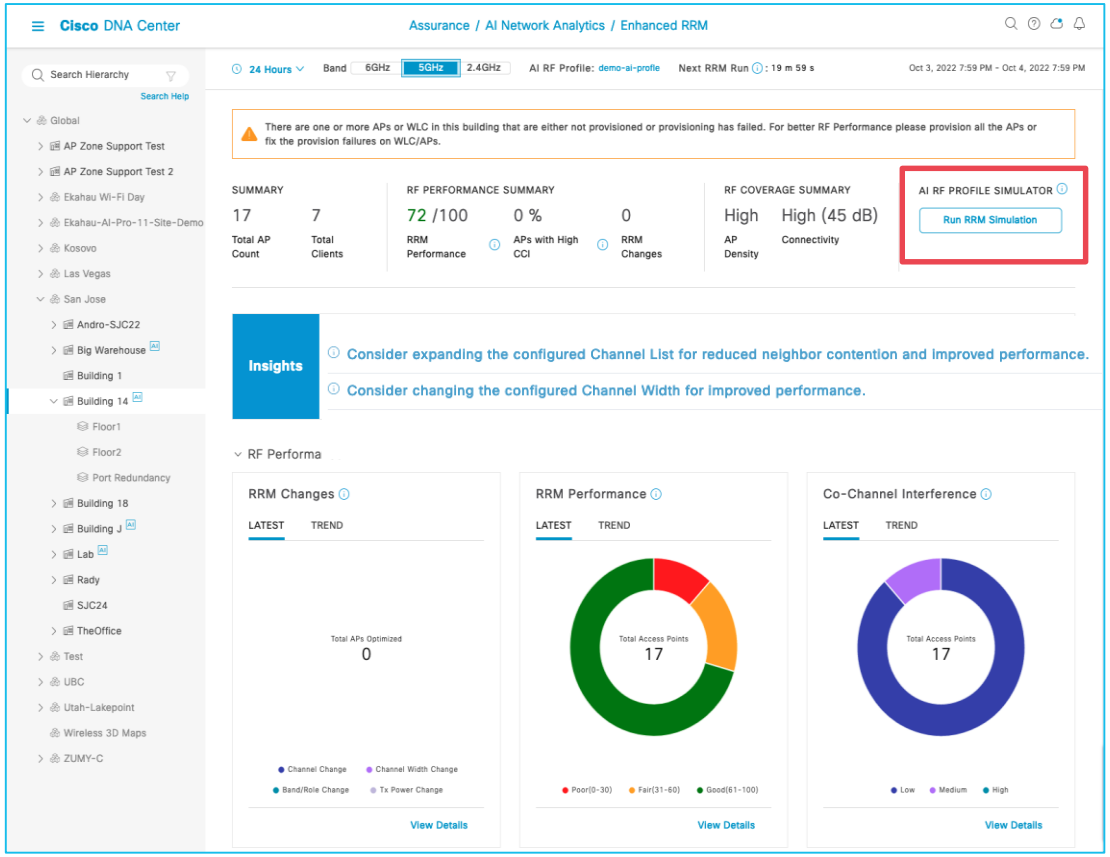


Supported WLCs: Catalyst 9800-CL, 9800-L, 9800-40 9800-80
Supported access points: All Wave 2, Wi-Fi 6/6E APs
Suggested software versions: Cisco DNA Center 2.3.7.4+ (WLC not managed) or 2.3.5 (Wi-Fi 6E), Cisco IOS® XE 17.9.5+

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

AI Enhanced RRM

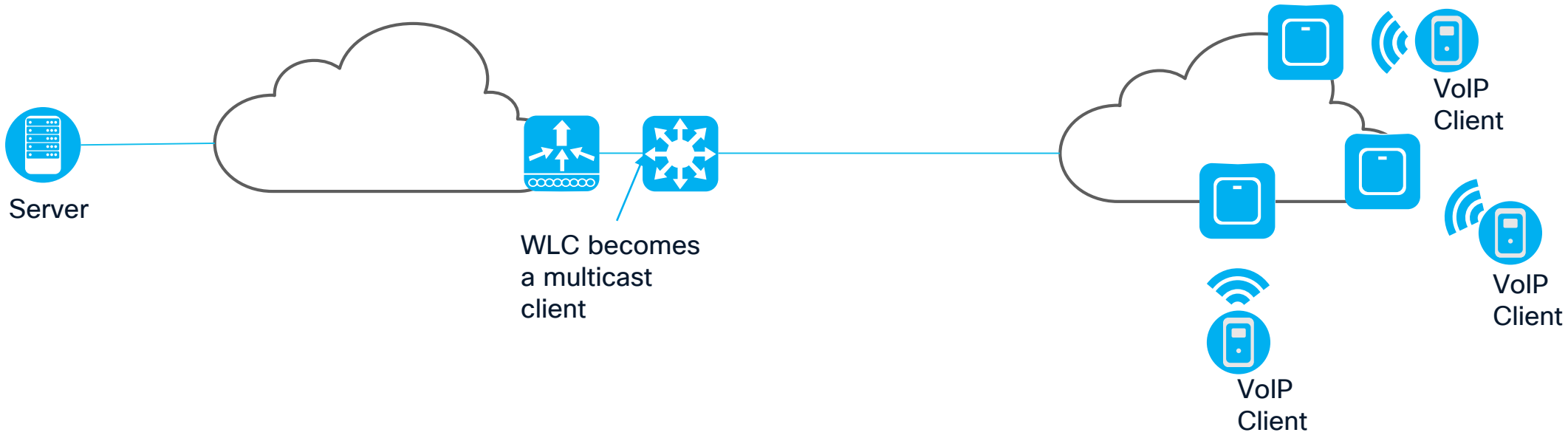
- Provide clear, and actionable information
- Insights give Actionable suggestions
- Break up profiles on sites. Dis-similar floors can use different profiles
- No longer requires DNAC to Manage the controller!
- All of the APs on the WLC are assigned the AI RF Profile (small interruption)
- All the 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 DNAC/Cloud
- Loss of cloud WLC fails back to group leader



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

Voice
Design Considerations

Hospital VoIP/Badge Paging



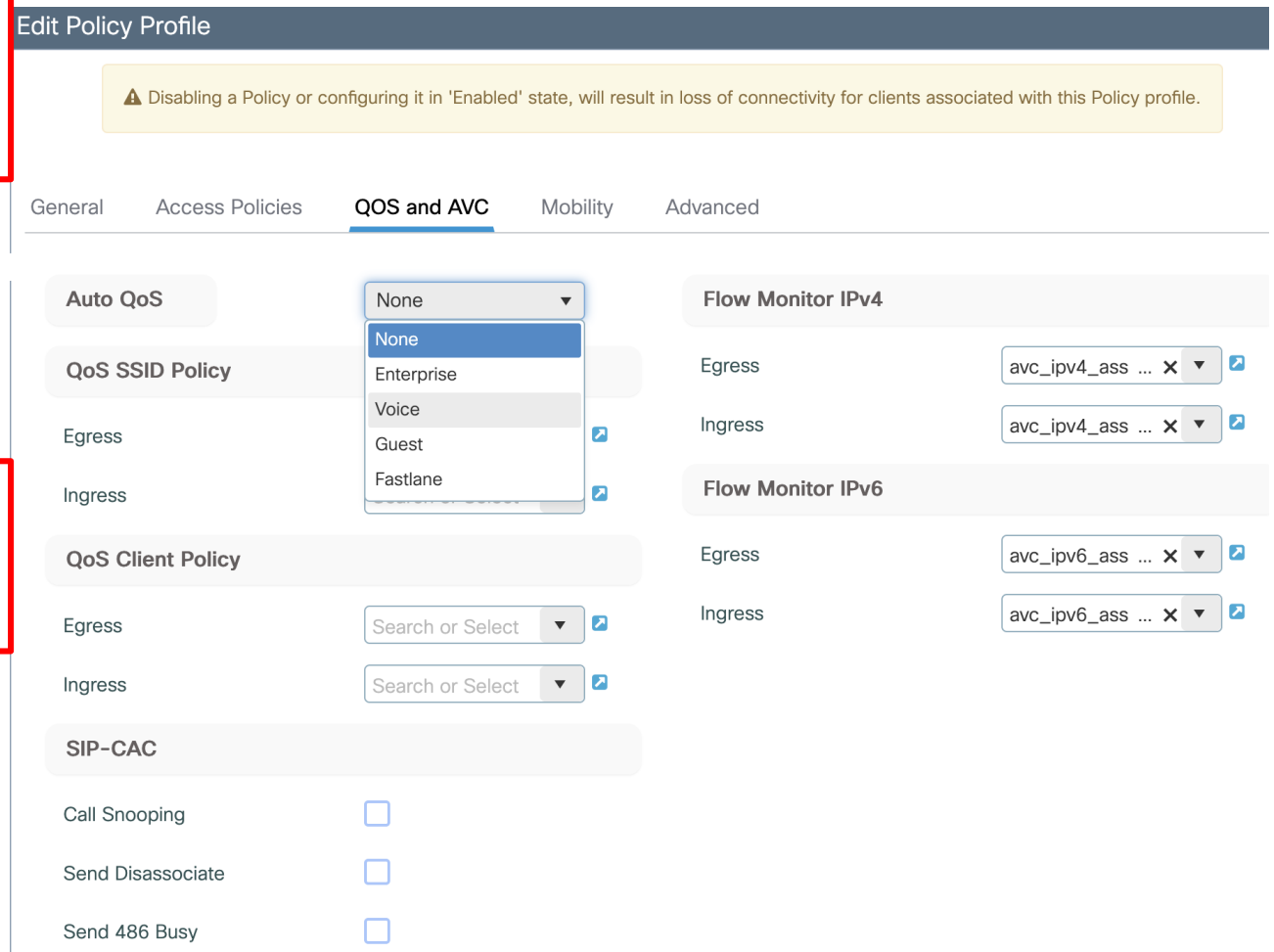
Normally VoIP traffic is unicast (QoS/AVC)
Paging is multicast
- Server send message to clients which Multicast Group to join
- All members join the group and get page from one of the clients

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

QoS, On Prem

- **Voice**: sets the recommended QoS policy to correctly mark and prioritize voice at the SSID level and enables CAC.
- **Guest**: sets the recommended QoS policy at SSID level to mark everything to Best Effort
- **Enterprise**: sets the recommended QoS policy at SSID level to mark VoIP Data, and Signaling, Multimedia, Transaction, Bulk-Data and Scavenger traffic
- **Fastlane**: sets the specific EDCA parameters. Fastlane also sets clients specific policies only for Apple clients.
- **All Above**: queuing is configured on the C9800 egress port for prioritizing voice and CAPWAP traffic

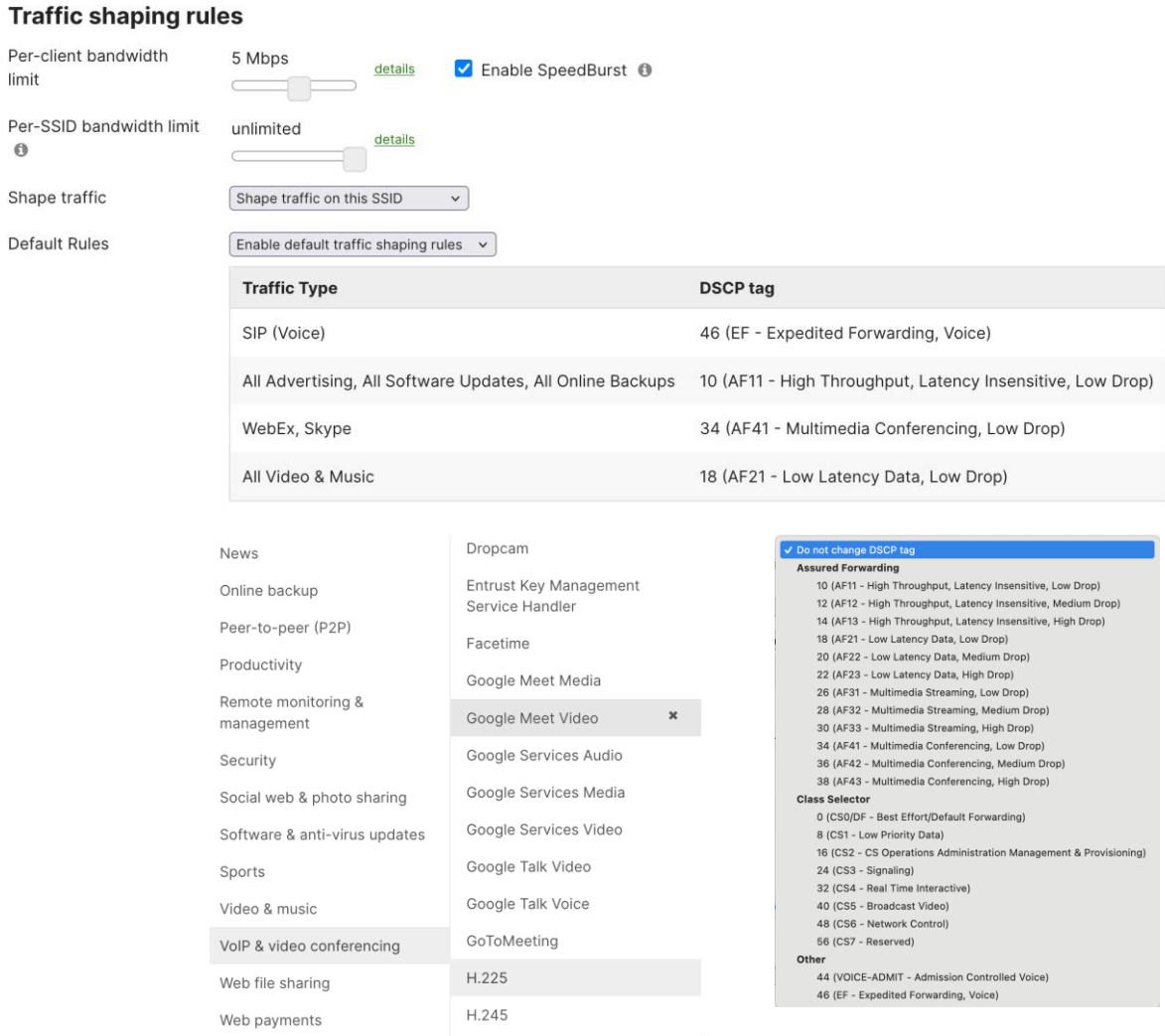
QoS is often an option when configuring the voice device, it needs to be enabled for QoS to work



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

Cloud Based VoIP QoS

- **Per-Client bandwidth**: Set to unlimited or if congestion is an issue limit the client bandwidth (5Mbps) but enable SpeedBurst
- **Per SSID bandwidth limit**: Set to Unlimited
- **Shape Traffic**: Shape traffic on SSID
- **Default Rules**: Typically, use the default setting but if there is a particular application not covered in the default rules there are many customized settings available.



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

Hospital VoIP/Badge Paging

- Design solutions
  - Do the math
    - How many calls per AP
    - Density of phones
    - Remember adding APs is not always a simple matter
    - 5GHz (or 6GHz if available) only.
  - Enable 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.

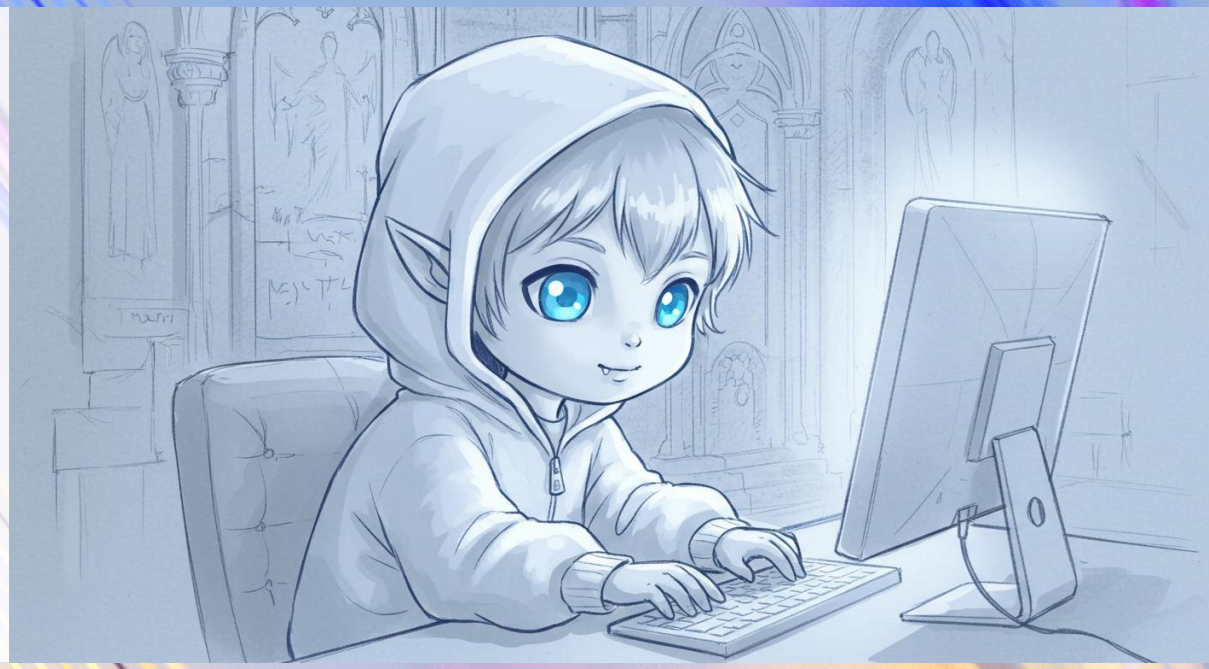
© 2025 Cisco and/or its affiliates. All rights reserved.

Large Venue

- 6GHz Adoption
- Tuning/Timers
- Design

6GHz

How do I use it in my design



The Rules Have Changed: Details



FCC 6GHz Q&A Document

FCC Indoor AP Guidelines

- The introduction of 1200MHz of spectrum at 6GHz that is currently used for licensed applications.
- Two classes of service
  - “Low Power Indoors” (LPI – Indoor Only)
  - “Standard Power” (SP – Indoor or Outdoor)
- To ensure there would be no LPI outdoors the **AP must be clearly marked** as indoor or outdoor and support the operation of one **or** the other.
- Clients are LPI, SP, or both.
- SP provides higher power but less spectrum and requires Automatic Frequency Coordination.
- For indoor operation LPI is first option but if external antenna or higher power is required revert to SP

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

6GHz: The Wi-Fi Rules Have Changed

Low Power Indoors (LPI) / Composite APs

- Must be used indoors only
- No weatherized enclosures allowed
- Must be powered via wire – no batteries
- Can't be moved (no "AP on a cart")
- Tx power limitations imposed by FCC
- Can run SP mode, but even then, still cannot be used outdoors

Standard Power (SP) Only APs

- Enclosures / weatherized APs allowed
- Can be indoors or outdoors
- Must talk to AFC / GPS req'd for perimeter APs
- Limited 6GHz spectrum (no UNII-6/UNII-8)
- Limited @ 30 degrees above horizon

For this discussion clients can have one of 3 certifications (5 available)

- 6XD – LPI Only
- 6FX – SP Only
- 6CD – Dual mode

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

6GHz: The Wi-Fi Rules Have Changed



In 6GHz – LPI vs SP: FCC Rules

Low Power Indoors (LPI) / Composite APs

- Must be used indoors only
- No weatherized enclosures allowed
- Must be powered via wire – no batteries
- Can't be moved (no "AP on a cart")
- Tx power limitations imposed by FCC
- Can run SP mode, but even then, still cannot be used outdoors

LPI / Composite AP Examples:

9166 (omni)
9166D1 (directional)
9164 (omni)
9162 (omni)
9136 (omni / WLC-only)
MR57 (omni / Meraki-only)
9176 (omni)
9176D1 (directional)
9178 (omni)
9172I/H (omni)

Standard Power (SP) Only APs

- Enclosures / weatherized APs allowed
- Can be indoors or outdoors
- Must talk to AFC / GPS req'd for perimeter APs
- Limited 6GHz spectrum (no UNII-6/UNII-8)
- Limited @ 30 degrees above horizon
- Client behavior – LPI-only clients cannot join SP APs

SP-Only – Outdoor-Capable - AP Examples:

9163E (outdoors / weatherized)
IW9167I, E, EH-STA (omni or directional / outdoors / WLC-only)
IW9165E/D

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

Low Power Indoor (LPI) Mode: Details



- "Integrated" (FCC) / "Permanently attached" (Cisco docs) antenna
- Limited to indoor operation (and marked as such)
- Required contention-based protocol
- Not weather resistant
  - Furthermore the use of a weather resistant enclosure is prohibited.
- AP PSD "Max" is 5dBm/MHz – 18dBm@20MHz
- Client "Max" is -1dBm/MHz
- Mesh/Extender devices can operate with same conditions as AP.

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

Standard Power (SP) Mode: Details



- Requires Automated Frequency Coordination (AFC)
  - Note: this comes as a part of the AP licensing for On-Prem or Cloud
  - Requires deterministic location with accuracy (>95% Confidence) reported (some GPS location)
- May have external antenna.
- Maximum EIRP above a 30-degree elevation angle limited to 21 dBm for outdoor units.
- Permanently fixed client devices can be registered with AFC and transmit same power level (and restrictions) as AP.
- Hot Spots not allowed.
- The only vehicular traffic allowed is commercial aircraft over 10K ft.

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

Things to note about 6GHz

- Typically, 1:1 overlay if existing APs at power level 3 or higher.
- 6GHz Mandates WPA 3 which include PMF mandatory.
- 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.

OR

- What about site survey with no battery powered operation?

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

9176D1 Wi-Fi 7 Indoor Access Point

Cisco® Catalyst® 9176D1-x

Directional, Tri-Radio with 12 Spatial Streams!



Penta-Radio Architecture

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

Directional antenna architecture

- 2.4+5 GHz: 6 dBi gain (70x70 deg), 6 GHz: 8 dBi (60x60)*
- Same X,Y as CW9176I – 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

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

6GHz Outdoor Options



IW9167E/I

IW9167E-STA



IW9165E/D



9163E

6GHz Outdoors/SP

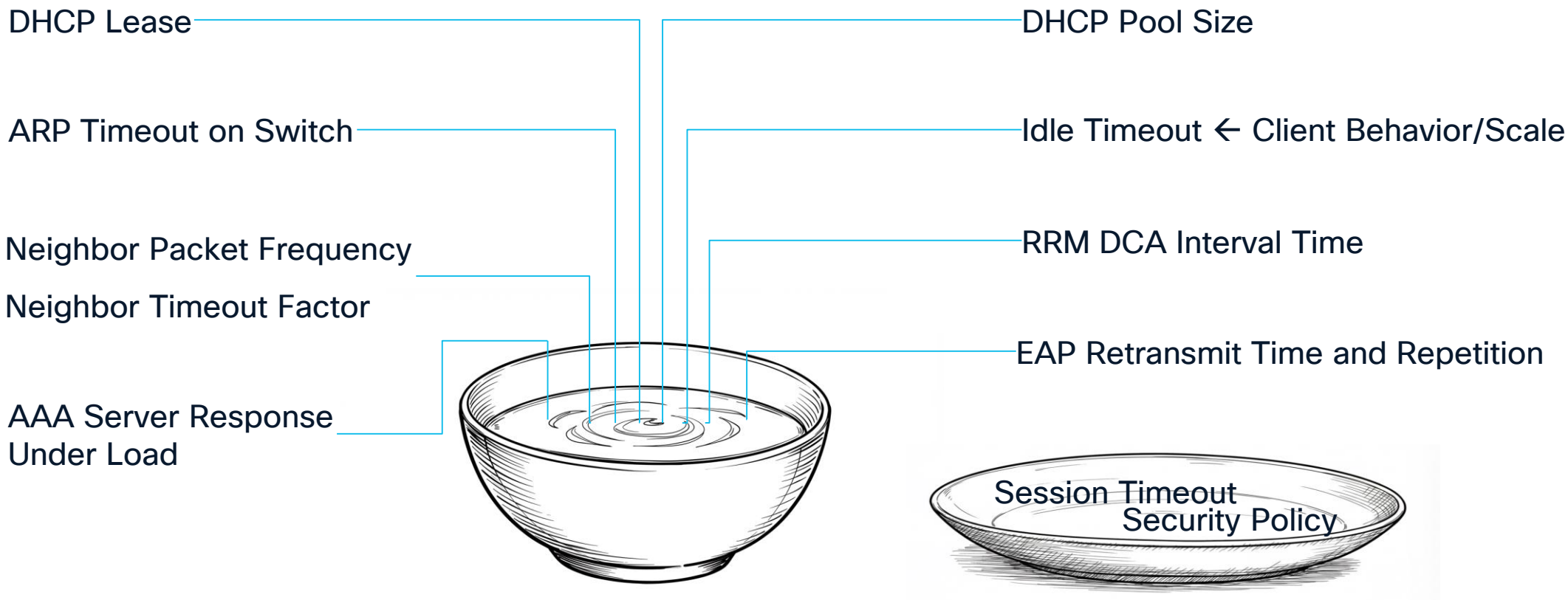
1. Must meet FCC Standard Power Requirements
    1. Must comply with AFC
    2. GPS/GNSS
2. Must be only Outdoor/SP (reconfigurable is not acceptable)
3. Not Mobile
4. Can use external antennas
5. Can (should be) weatherized

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

Timers
How do they interact?



Timer soup



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

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		
	EAPOL-Key retries	0-4 (x)	2	4	0		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
	Identity Request Timeout	0-120 (sec)	30	5	30		
	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	172800	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	15-100000 (sec)	300	35	300-3600		High density closer to 300, lower density closer to 3600 (prevent Client exhaustion)
	Idle Threshold	0-4294(MB)	0				

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

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						Disabled for Passive Clients
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)				
	Neighbor Packet Freq	60-3600 (s)	180 (s) *				* Default is 600 s for 6GHz band
	Reporting Interval	60-3600 (s)	180 (s)				
	Neighbor Timeout Factor	5-60(x)	20 (x)				Hold NDP for Neighbor Timeout Factor x Neighbor packet frequency
	DCA Interval	10 min -24 Hrs	10 (min)				

How do VLAN Groups work Cloud and On Prem

- VLANs are defined and put into a group
  - Must be defined in controller or dashboard
  - Should be less than 32 VLANs per group (both Cloud & O-prem)
  - VLANs are indexed 0 – (VLAN_Total-1)
- When I client joins the client will be provided a VLAN
  - VLANs are marked as dirty if:
    - 3 Clients do not get an IP address (IP Address Learn timeout of 120 Sec [not configurable])
    - Client must complete the timeout period. A client cannot stop and reinitiate the association before the IP Address timer expires and it count as a failure.
  - Client MAC address is “Hashed” to determine the VLAN index assigned on OP and round robin on C.

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

VLAN Group Hash

- So, what does “Hash” mean? How do I know what VLAN should be assigned.
  - The MAC address is broken into 6 octets (0-5)
  - Octet 2 and 4 are grouped (G1), and Octet 3 and 5 are grouped (G2)
  - The VLAN ID chosen is (G1 xor G2) Mode N
  - N= Number of VLANs in Group
  - VLANs are indexed starting with lowest VLAN ID =0 and Highest N-1

Example:



4 VLANs in VLAN group (N = 4)

MAC = a0 b0 c0 d0 e0 f0

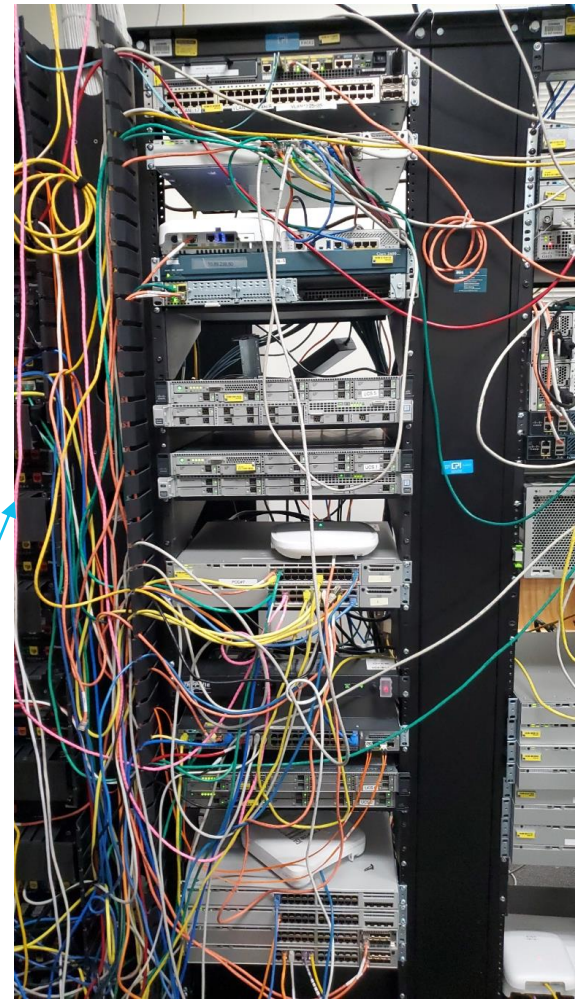
VLAN ID = [(0xc0e0) **xor** (0xd0f0)] **Mod** 4 = 0

The lowest VLAN is selected

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

Architecture/scale example for events center (LPV)

- 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!!

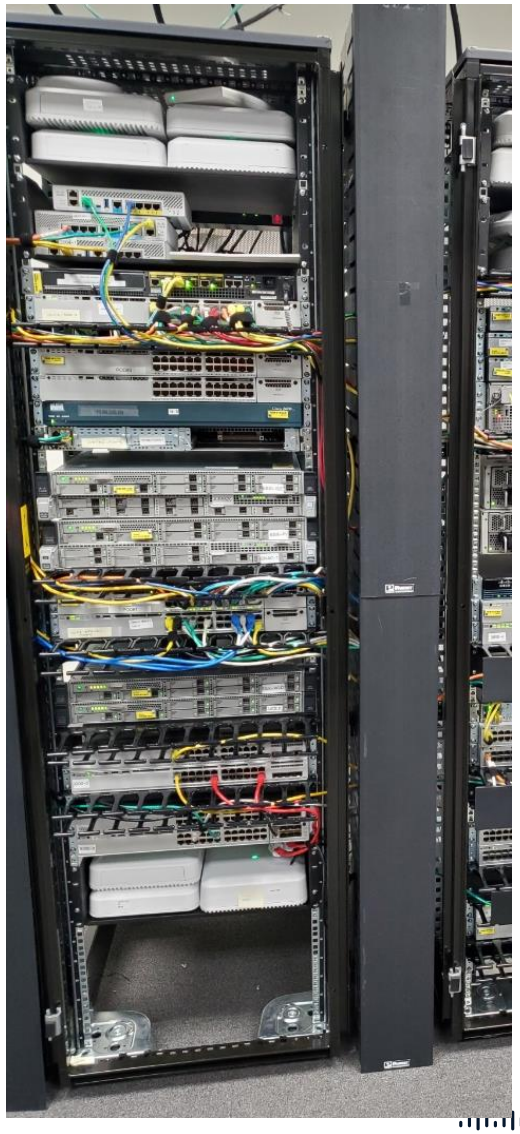
© 2025 Cisco and/or its affiliates. All rights reserved.

Design
Legacy bands and 6GHz

Architecture/scale example for events center
Design considerations (PLAN!)

REFERENCE

- Where are the L3 roaming boundaries?
- Dot1x authentication type and rates
- 15K concurrent subscribers (AAA/WLC/DHCP/Switch)
  - CAM table on core switch…multiple controllers…Multiple hops to GW?
  - Subnet sizes/VLAN Groups
- Enable Proxy ARP to minimize broadcast/unicast traffic
- Capacity requirements
- Timer settings

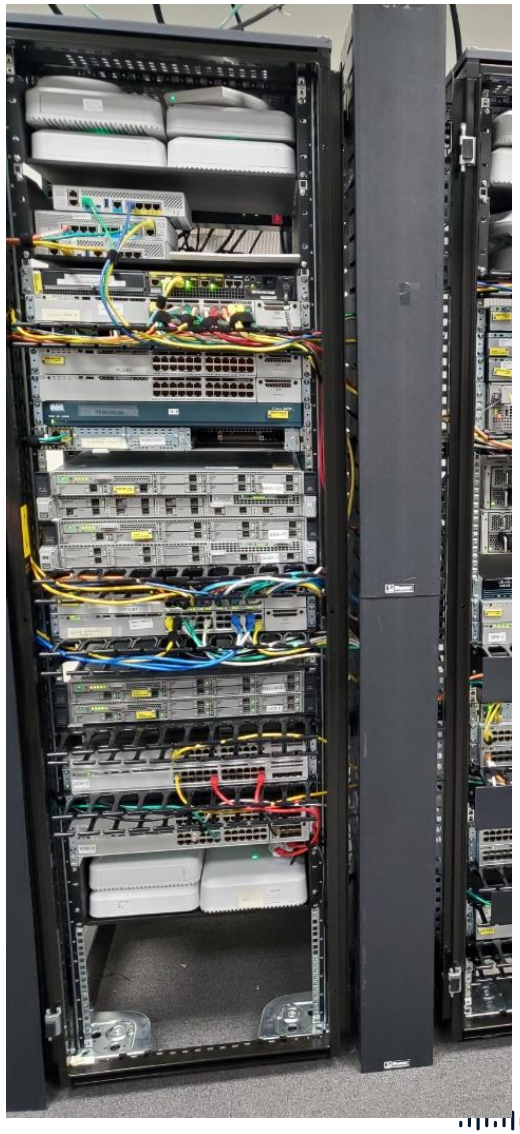


© 2025 Cisco and/or its affiliates. All rights reserved.

Architecture/scale example for events center
Design considerations (PLAN!)



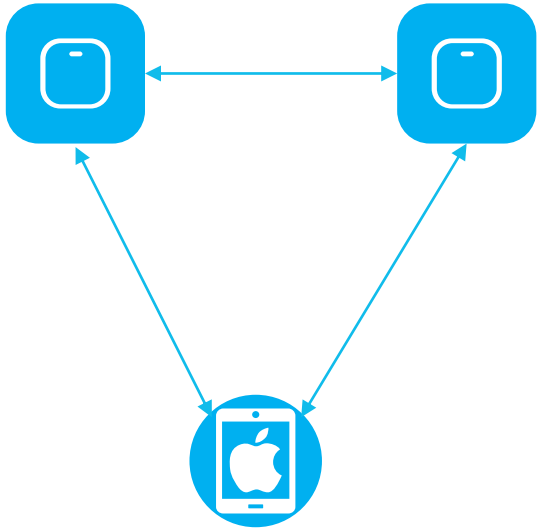
- Where are the L3 roaming boundaries?
- Dot1x authentication rates (75-150 Auth/sec per node depending on types)
- MAB (400+ Auth/sec per node depending on type)
- 15K concurrent subscribers (AAA/WLC/DHCP/Switch)
  - CAM table on core switch...are there multiple controllers? Multiple hops to GW?
  - 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.



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

General design guidelines

- Three things to watch
  - AP Downlink
  - Client Uplink
  - AP Neighbors
- It’s all about SNR and time
  - Directional antennas
  - Increase basic rates, decrease SSID count
  - RX SOP can be your friend
  - Use of 11v & 11k action frames are good but do take airtime/CPU
  - Use 11r for Personal or Enterprise SSIDs





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

High Density RF Design

- You cannot compensate for poor RF design!
- It's about more what do the APs not hear.
- Find APs with highest client count
  - Adjust TPC for more even distribution
  - Band Select and Load balancing are secondary effects
- Find APs with consistent High CU (RX/TX)
- The 9104s make sure you understand orientation and side lobes.

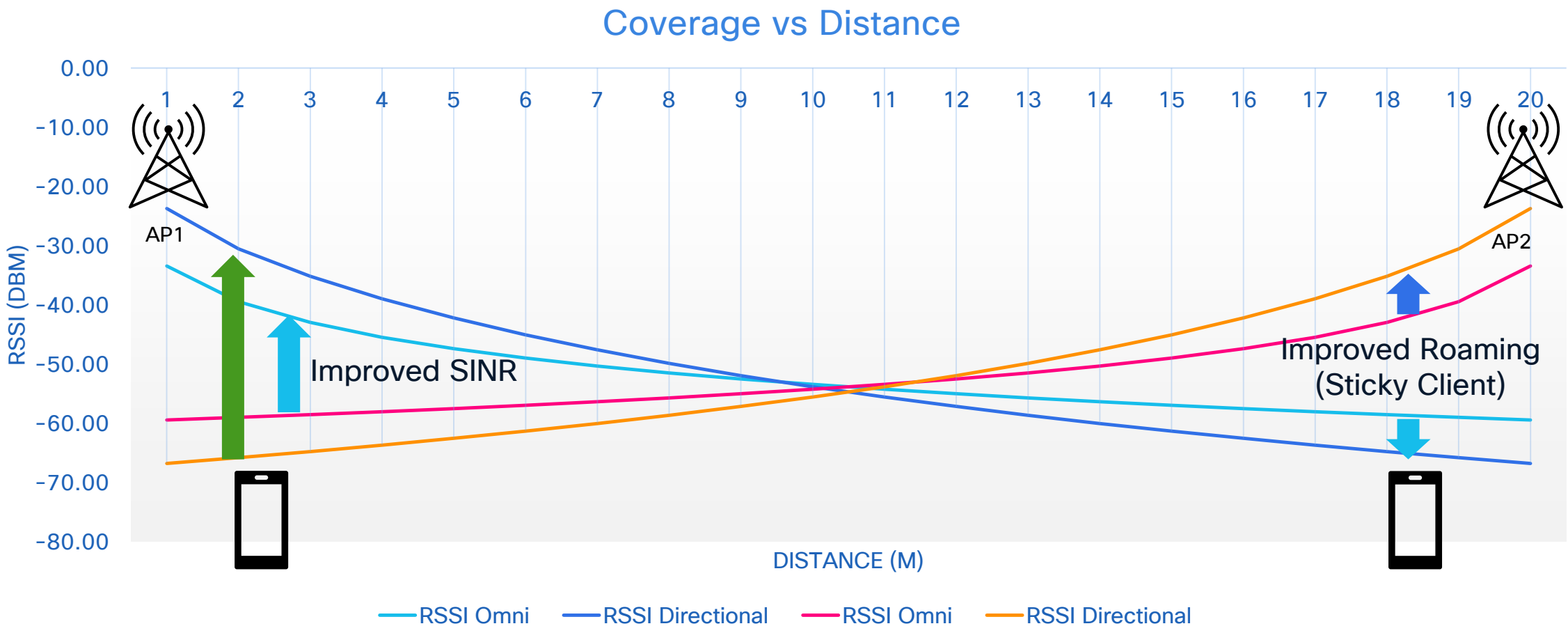




For more details attend: BRKEWN-2087

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

Why directional antennas



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

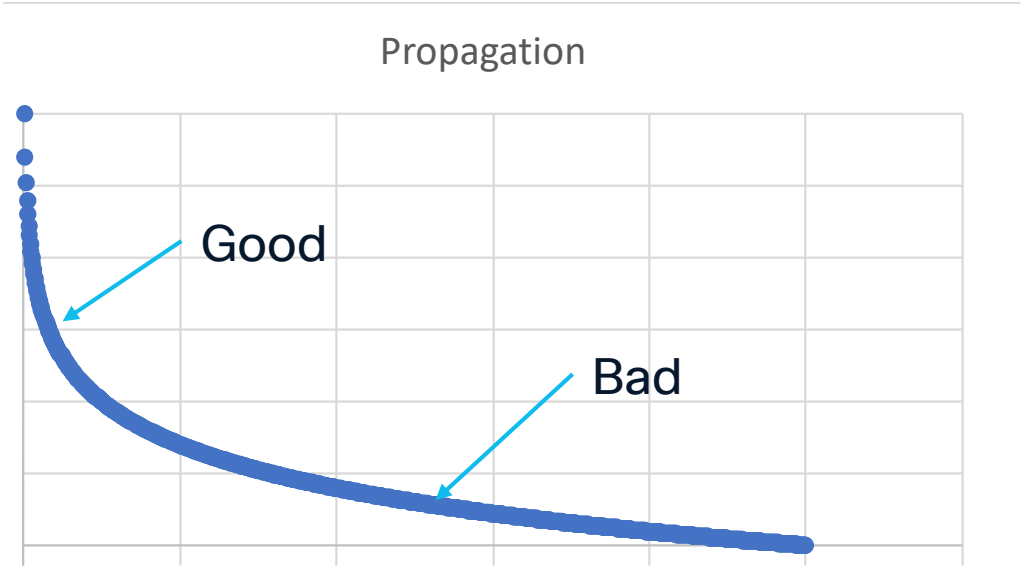
Things that make design challenging

- 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

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

Designing for location

- For RSSI based location what is desirable is a small change in distance is a big change in RSSI
- Need 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.



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

Predictive vs Measured

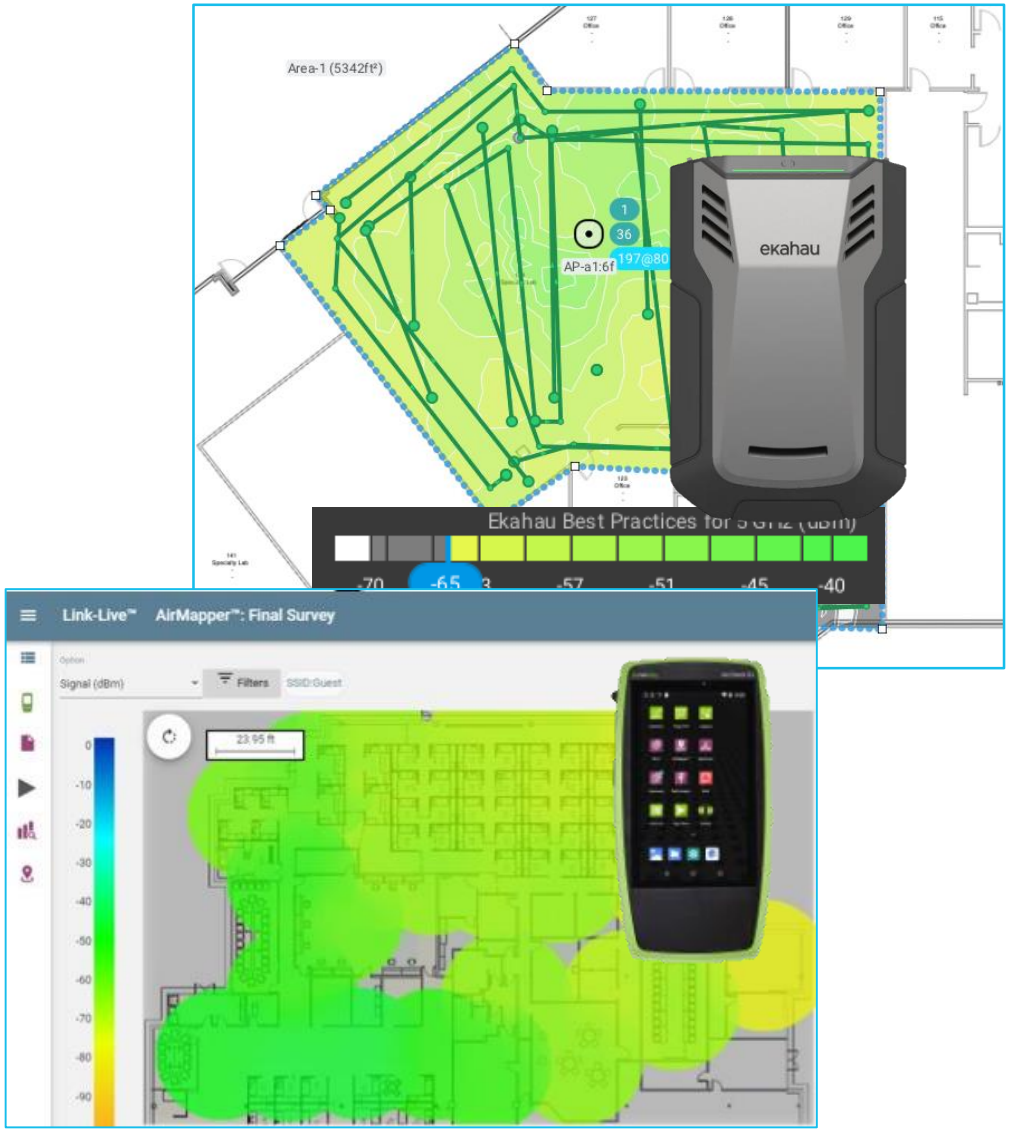
When is good enough, good enough?

A Measured Site Survey is an actual measurement of the RF Coverage in each space

Ekahau SideKick, Hamina Oscium Nomad, and NetAlly have Instruments specifically for measuring Wi-Fi

Predictive Surveys often good enough

- Garbage in, garbage out
- Bound predictive with measurements



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

Authentication in high density

- Simple is better
- We want clients on the network not probing
- Addition of EAP based authentication should be carefully reviewed and well tested.
- Use of OWE transition mode does not drive 6GHz adoption.

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

Large Venue

- 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.

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

Large Public Venue Design

- What is top of mind when addressing RF design?
- Should TPS and DCA be used?
- Should 11K and 11V be enabled?
- Predictive or measured?
- ARP proxy, policing and passive client, good or bad?
- What is the best method of authentication?
- What are the biggest concerns on the wired side?
- What should be done about high probe counts?
- What is “tuning”?
- What do I need to know about deploying 6GHz indoors/outdoors

For more details attend: BRKEWN-2087

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

What about MU-MIMO in High Density

- MU-MIMO requires something call ”Sounding” or Channel State Information (CSI) which effectively uses air time to determine the optimum setting for MIMO.
  - Attempt to decorrelate the signal from multiple users.
  - Requires clients that support MU-MIMO
- This can be very inefficient for small packets...but good news...
  - The radio has additional logic to determine when to attempt MU-MIMO
    - Minimum packet size to use MU-MIMO
    - Minimum signal conditions for MU_MIMO
    - Worst case you are back to SU-MIMO (this wasn’t always the case).

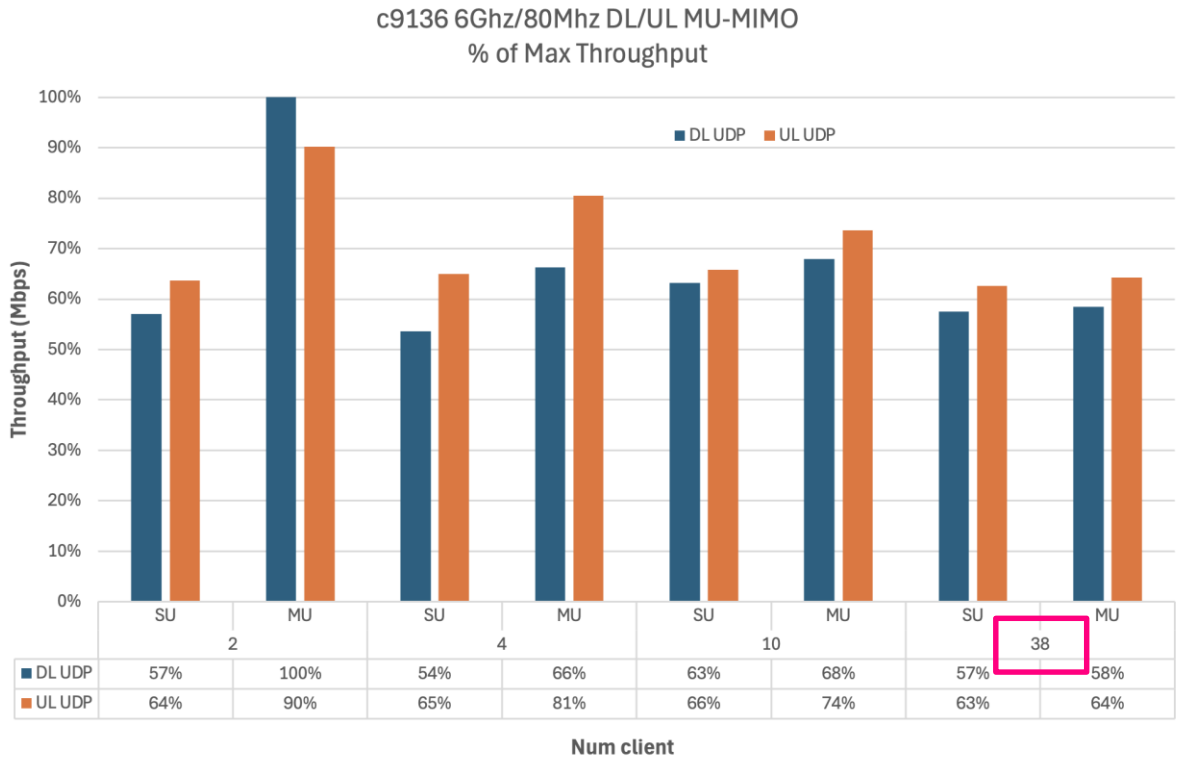


© 2025 Cisco and/or its affiliates. All rights reserved.

What about MU-MIMO in High Density

REFERENCE

- MU-MIMO requires something call ”Sounding” or Channel State Information (CSI) which effectively uses air time to determine the optimum setting for MIMO.
  - Attempt to decorrelate the signal from multiple users allowing multiple users to transmit at the same time.
  - Requires clients that support MU-MIMO
  - SU-MIMO works similarly but only benefits on user at a time.
  - The CSI exchange has multiple considerations
    - It occupies the channel during the transmission sequence.
    - The CSI may return a signature this is not well decorrelated…then multiple signals interfere with each other.
  - Net-net use of MU-MIMO can degrade based on the number of connected clients.
- This can be very inefficient for small packets…but good news…
  - The radio has additional logic to determine when to attempt MU-MIMO
    - Minimum packet size to use MU-MIMO
    - Minimum signal conditions for MU_MIMO
    - Worst case you are back to SU-MIMO (this wasn’t always the case).



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

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

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

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

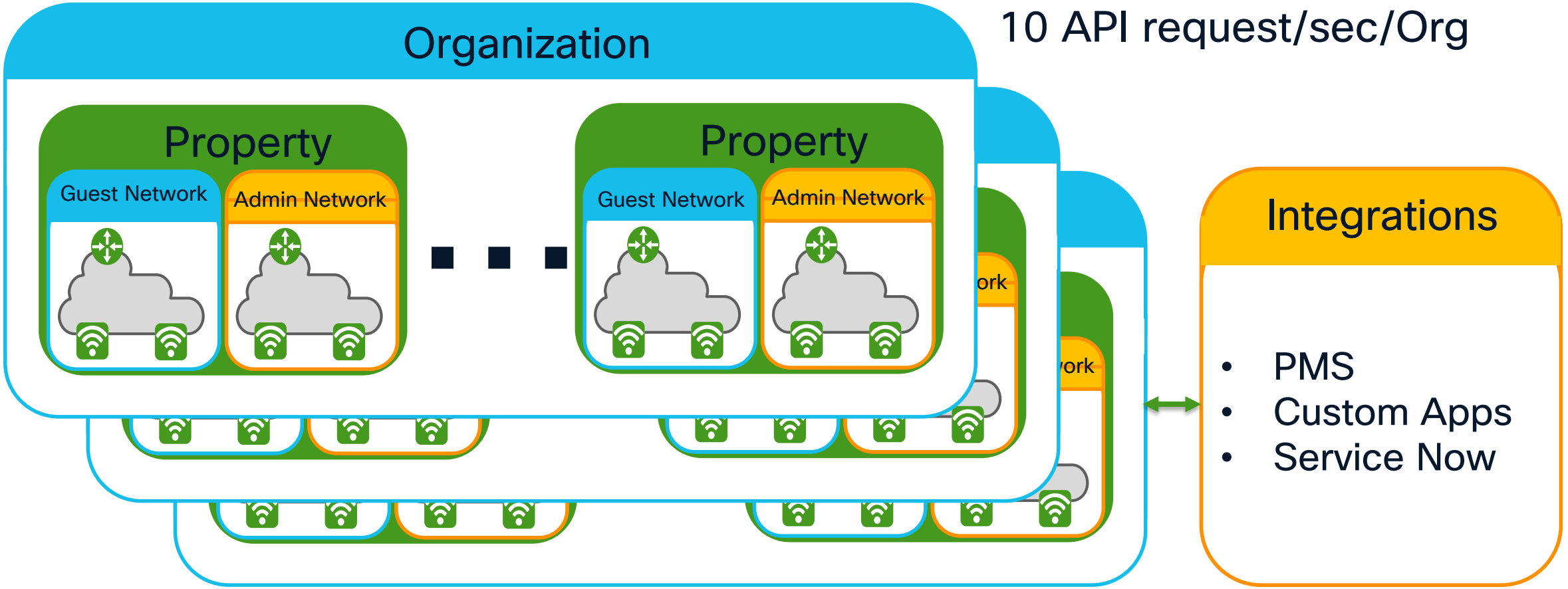
© 2025 Cisco and/or its affiliates. All rights reserved.

Event Center (Requirements)

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

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

How to scale cloud horizontally



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

Example Hilton/IHG



Worldwide Scale:

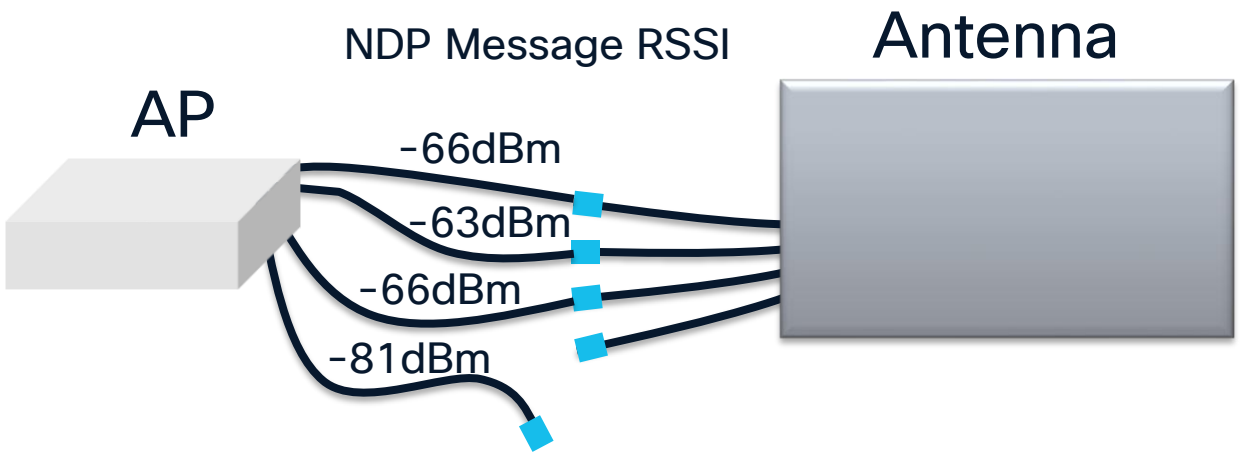
- 1 New property every 36 hours
- 44 Organizations (align with countries and logical divisions)
- 16000 Networks (two per hotel, Admin and Guest)
- 1.2M APs
- 30M clients

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.

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

Broken Antenna



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

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 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

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

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
```

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

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
  - Option 43 Generator for Global Use APs

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

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

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

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
- Wi-Fi 7 and the Growing Future of Wireless Design Guide: https://www.cisco.com/c/en/us/products/collateral/networking/wireless/wifi7-future-of-wireless-dg.html#DesigningConsiderationsforWiFi7

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

Cisco Unplugged

A recurring live series to keep you in tune with the world of Wi-Fi

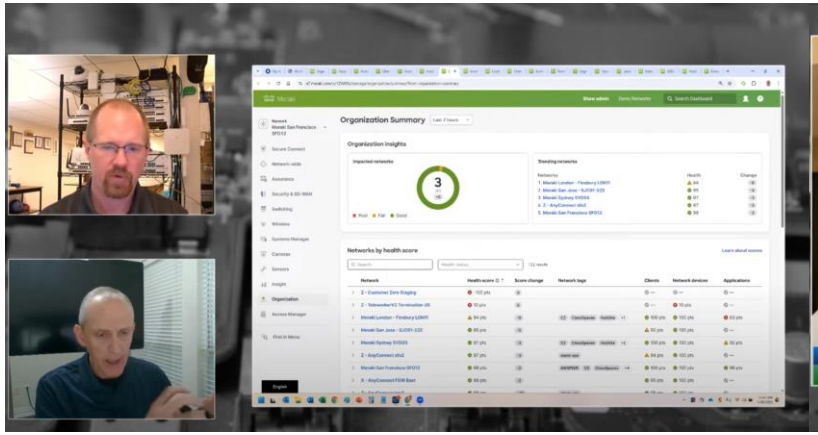
youtube.com/@getunplugged

Over 58,000 views to date, with over 1600 subscribers!













Suggestions for future episodes?
Send your ideas to getunplugged@cisco.com

Unplugged

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



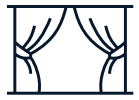
Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

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

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting



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



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

Contact me at: aldumdei@cisco.com

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

Thank you

cisco Live !


CISCO