Catalyst Meets Meraki in Wi-Fi 7: Real-World Implementation, Troubleshooting, and Features of Wi-Fi 7

Akash Malkood
Sr. Customer Delivery Engineering Technical Leader, TAC

BRKEWN-2141

Cisco Webex App

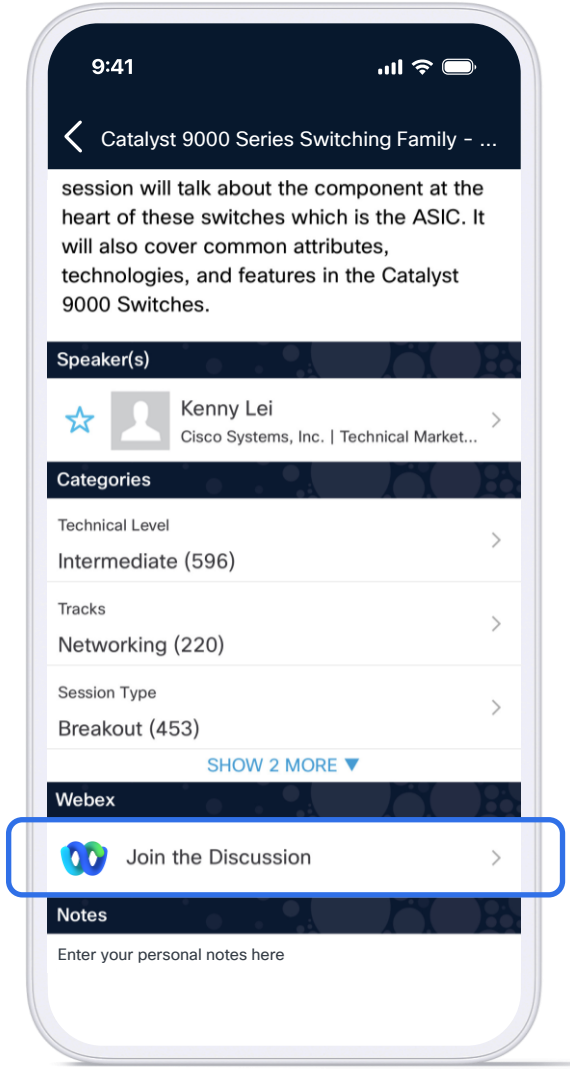
Questions?

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

How

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

Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKEWN-2141**

Agenda

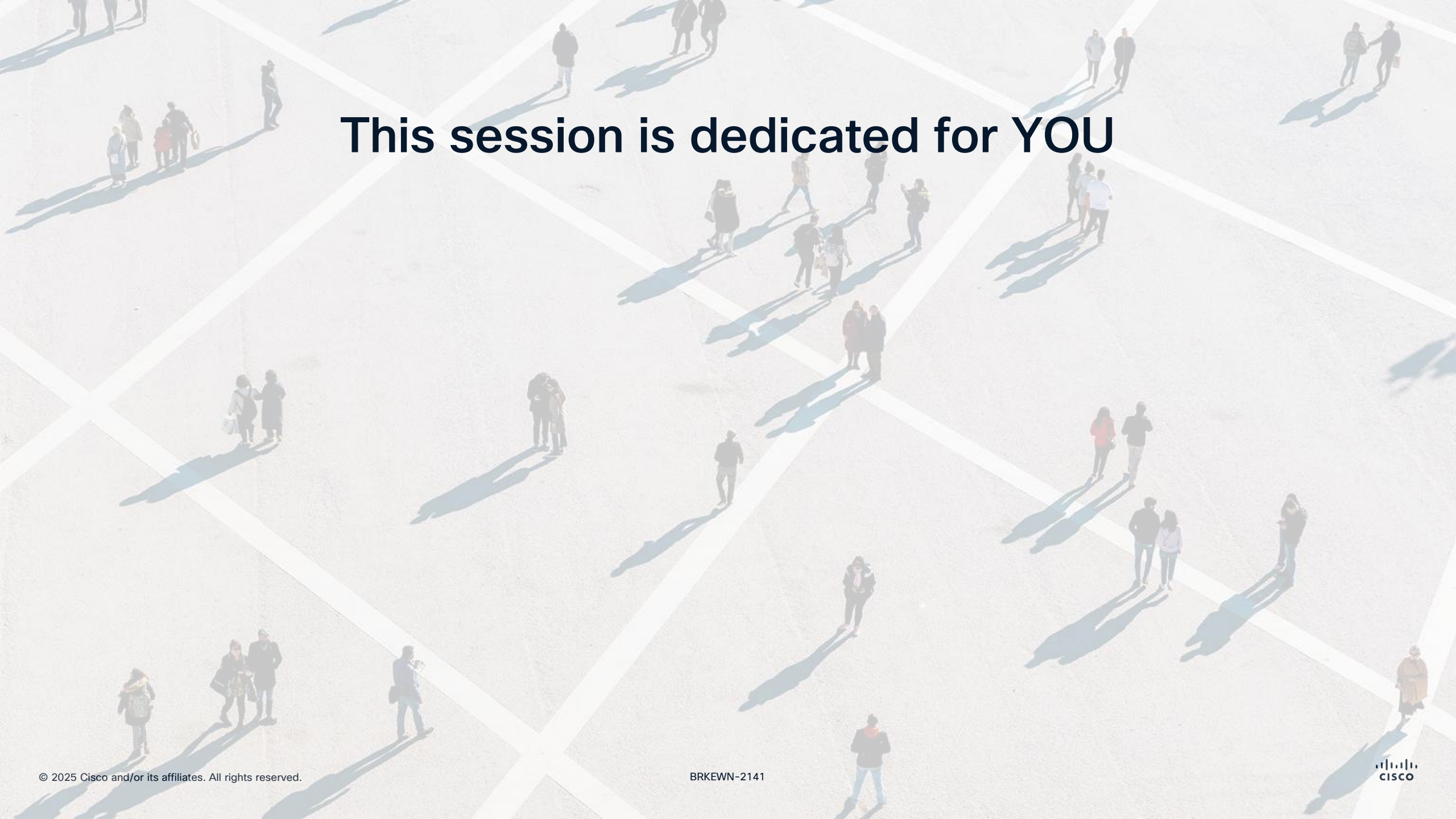
01 Wi-Fi 7 refresher and Cisco's offer

02 How do we onboard the GUAP?

03 Where is my MLD?

04 .11be RRM

05 Art of Isolating issues!



This session is dedicated for YOU

About Akash...

Wi-Fi 7 Refresher and Cisco's offer

Wi-Fi 7 Refresher

Cisco Wi-Fi 7 AP Portfolio

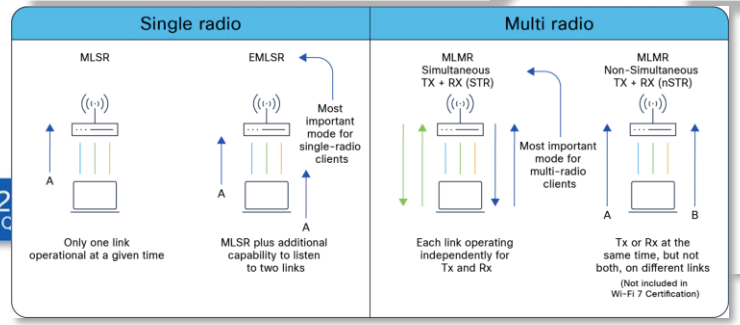
Technical Highlights – Wi-Fi 7

Performance & Efficiency

- 4096-QAM (4K-QAM) → ~20 % higher data rate vs Wi-Fi 6 (needs ~40 dB SNR)
- 320 MHz Channel Width → doubles spectral capacity (6 GHz band)
- Multi-RU OFDMA → flexible resource allocation; higher efficiency in dense traffic

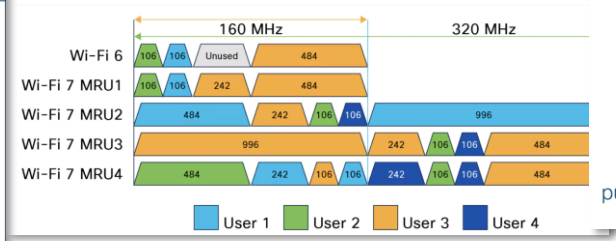
Multi-Link Operation (MLO)

- 2.4GHz + 5GHz or 5 GHz + 6 GHz, multi-band aggregation
- 2 Methods : STR (Simultaneous TX/RX) and EMLSR (shared-radio mode)



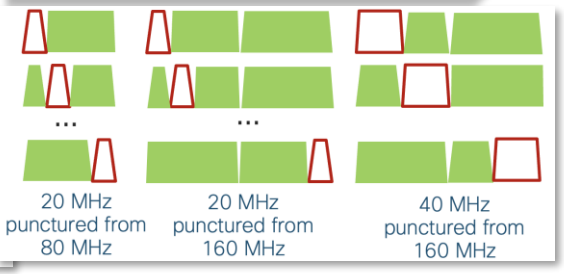
MAC / QoS Improvements

- Enhanced Scheduling → smarter airtime use
- Lower Latency → target < 2 ms with multi-link coordination
- Improved Power Management → Multi-Link Doze & TWT for mobiles

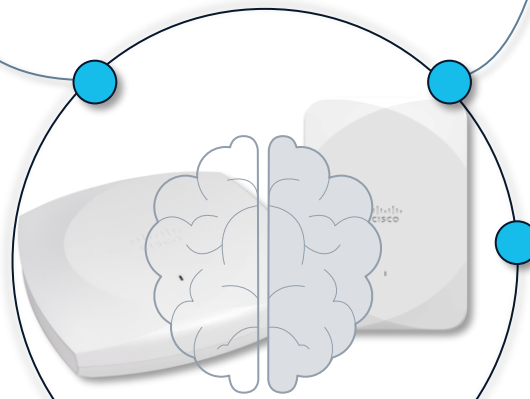


RF & Spectrum Enhancements

- Preamble / RF Puncturing → skip noisy 20 MHz segments, keep wide channel usable
- 6 GHz Operation → 1.2 GHz of clean spectrum (US), low interference environment
- Backward Compatibility → coexists with Wi-Fi 6 and 5 clients



Cisco Wireless CW9172I & CW9172H



Omni-Directional Antenna

2.4 GHz Serving Radio 2x2:2SS

5 GHz Serving Radio 2x2:2SS*

6 GHz Serving Radio 2x2:2SS

Tri-band scanning Radio

2.4 GHz IoT Radio (BLE)

IoT Capabilities

2.4 GHz IoT/BLE

App Hosting on 9172I only.

Built-in USB Port

4.5W of output power

CW9172H: Wall Plate AP

3x 1Gbps LAN port (1x POE out)

1x Passthrough port

CW9172I:

1 x 2.5Gbps

CleanAir Pro

Global Use AP

CleanAir Pro

CW9172I – 17.15.2b

CW9172H – 17.17.1

802.3af/at/bt or DC jack

Cisco Wireless CW9176I & D Access Point

-I is Omni-Directional Antenna

-D is Directional Antenna

2.4 GHz Serving Radio 4x4:4SS*

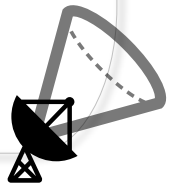
5 GHz Serving Radio 4x4:4SS

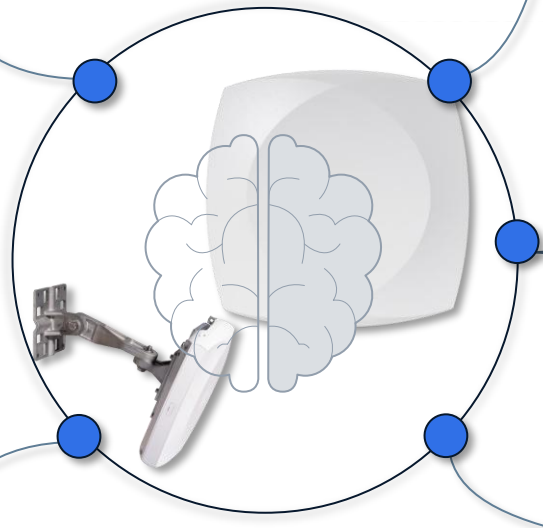
6 GHz Serving Radio 4x4:4SS

Tri-band scanning Radio

XoR Rdio

2.4 GHz IoT Radio





IoT Capabilities

2.4 GHz IoT/BLE, UWB, App Hosting

Built-in USB Port

9W of output power

1 x 10 Gig Ethernet

CleanAir Pro

Global Use AP

Built-in UWB & GPS/GNSS

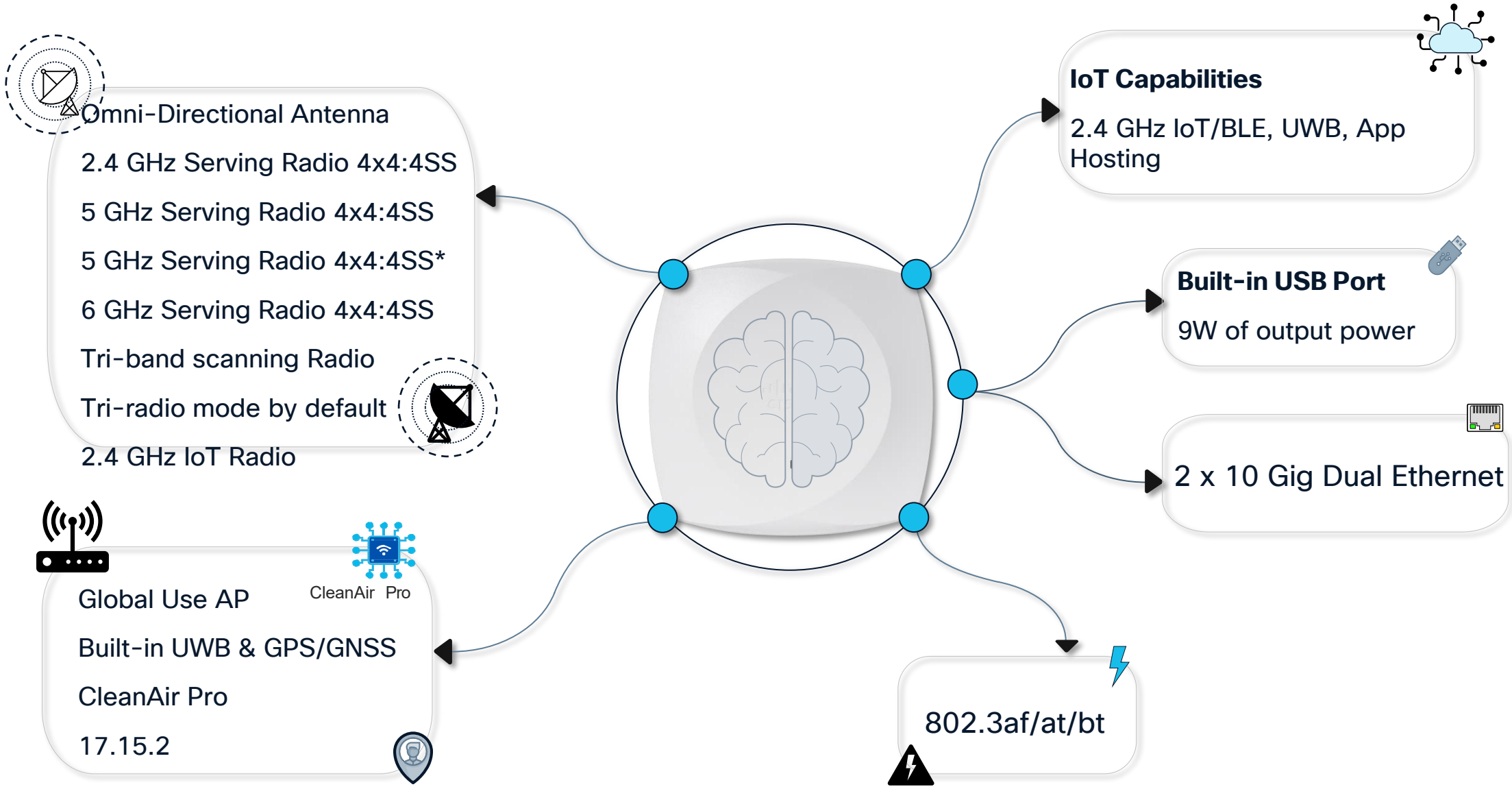
CleanAir Pro

17.15.2

802.3af/at/bt

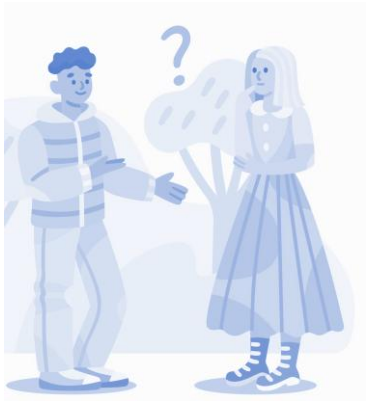
cisco

Cisco Wireless CW9178 Access Point



What is GUAP?

Regulatory Domain?



What about licensing?

How do I onboard the GUAP?

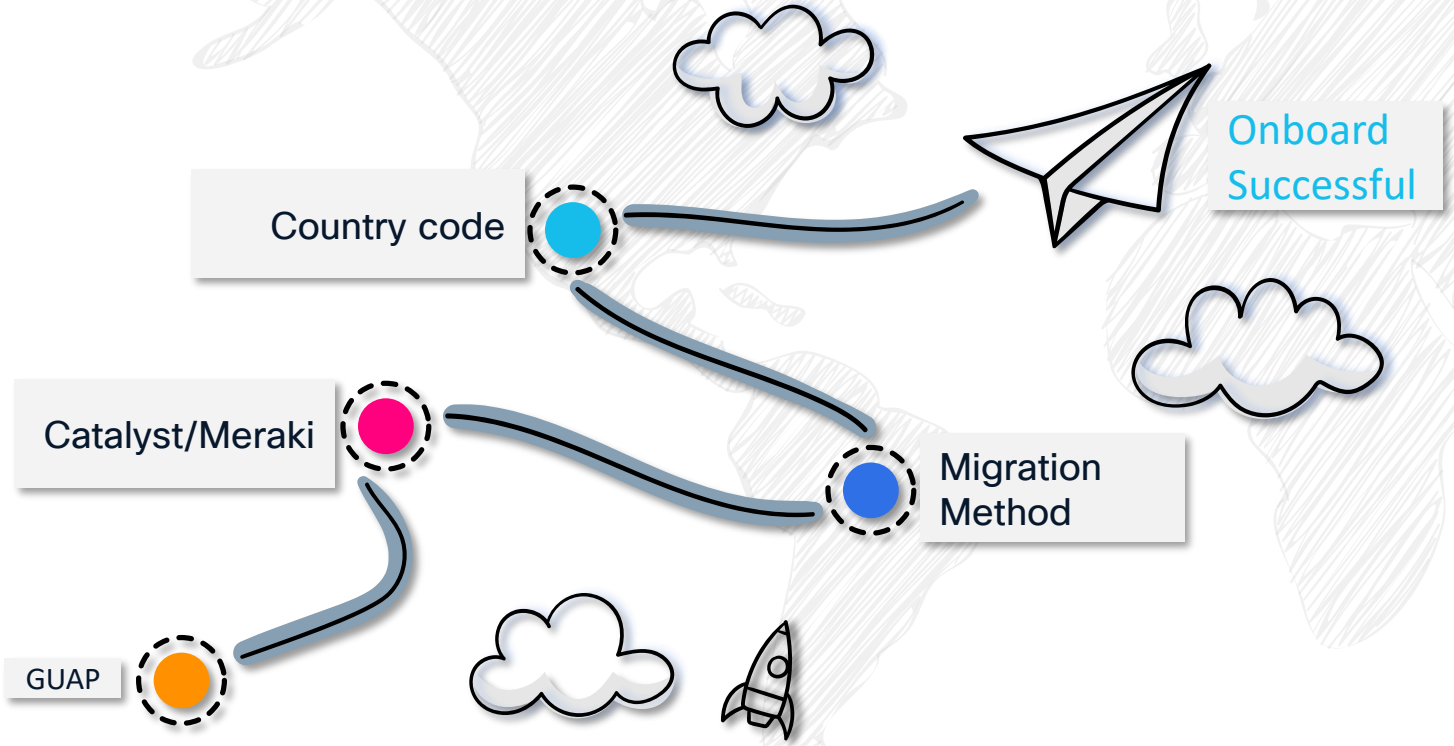
What is GUAP?

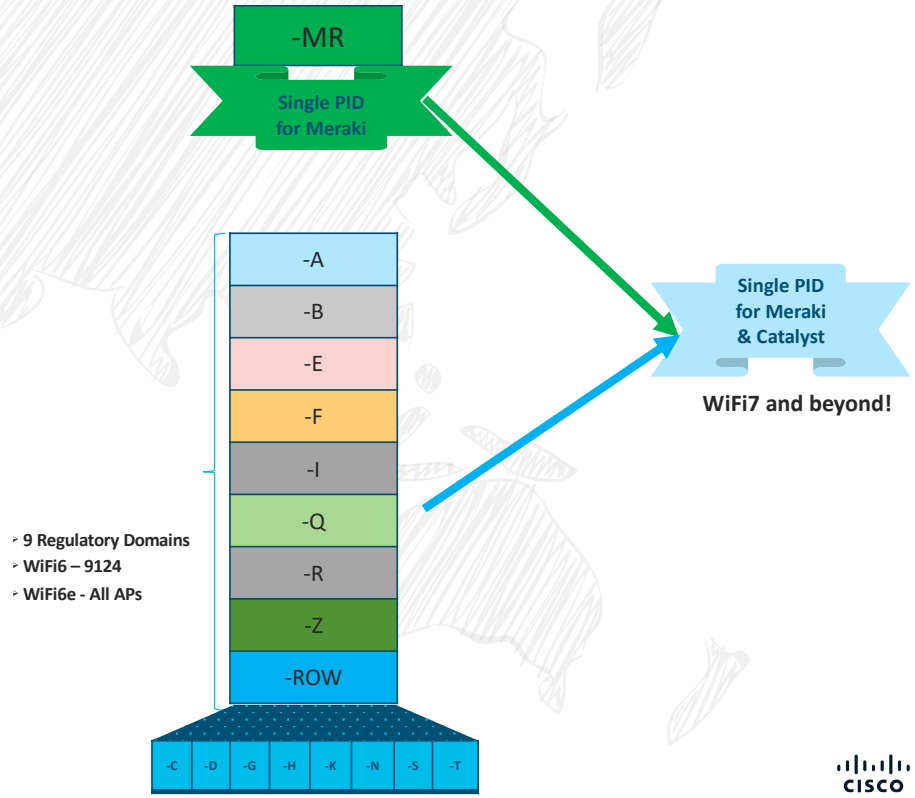
Your Global Use AP(GUAP) is a world traveler with a single passport who needs three things to work anywhere

- A destination choice (Meraki Cloud or Catalyst WLC mode).
- A visa (regulatory country code).
- A local address to check in (WLC join).

What it means?

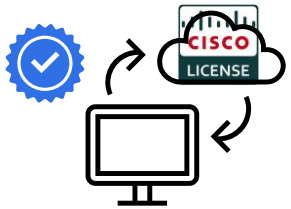
- Single SKU worldwide for Wi-Fi 7 APs
- Day-0: All APs boot to a initial OS, then choose Meraki or migrate to Catalyst.

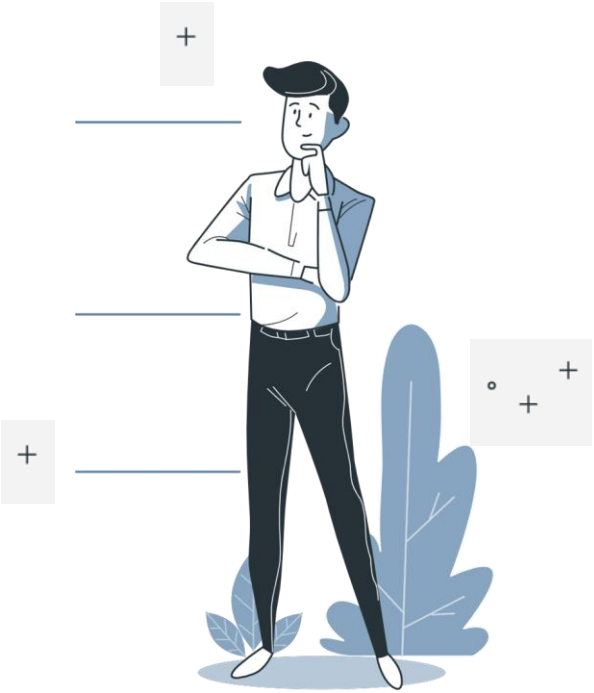




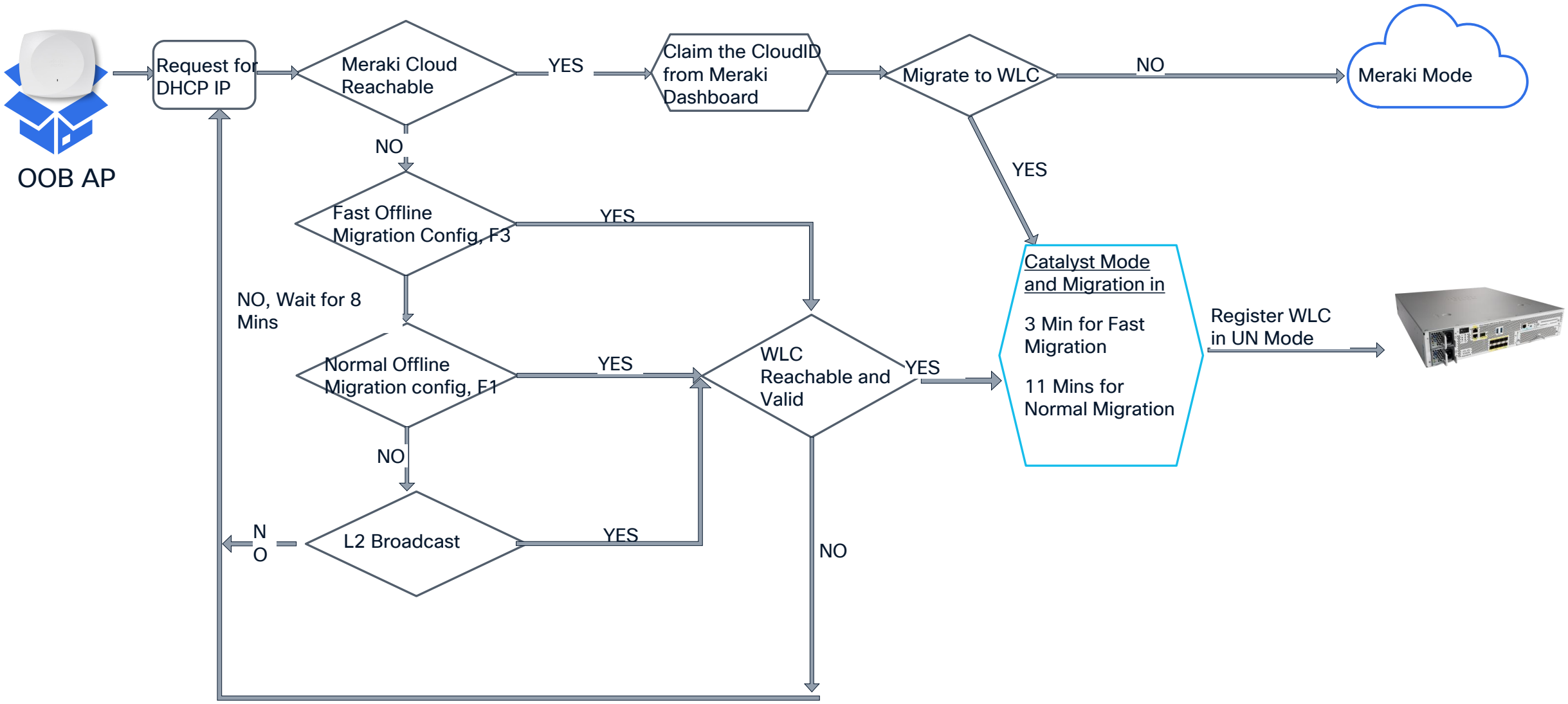
Checklist to onboard a Wi-Fi7

- ✓ Wi-Fi 7 APs?
- ✓ Meraki Account/ GPS/ Hardcoded country code AP
- ✓ 9800 WLC
- ✓ Unified Licenses





OOB Mode of Operation

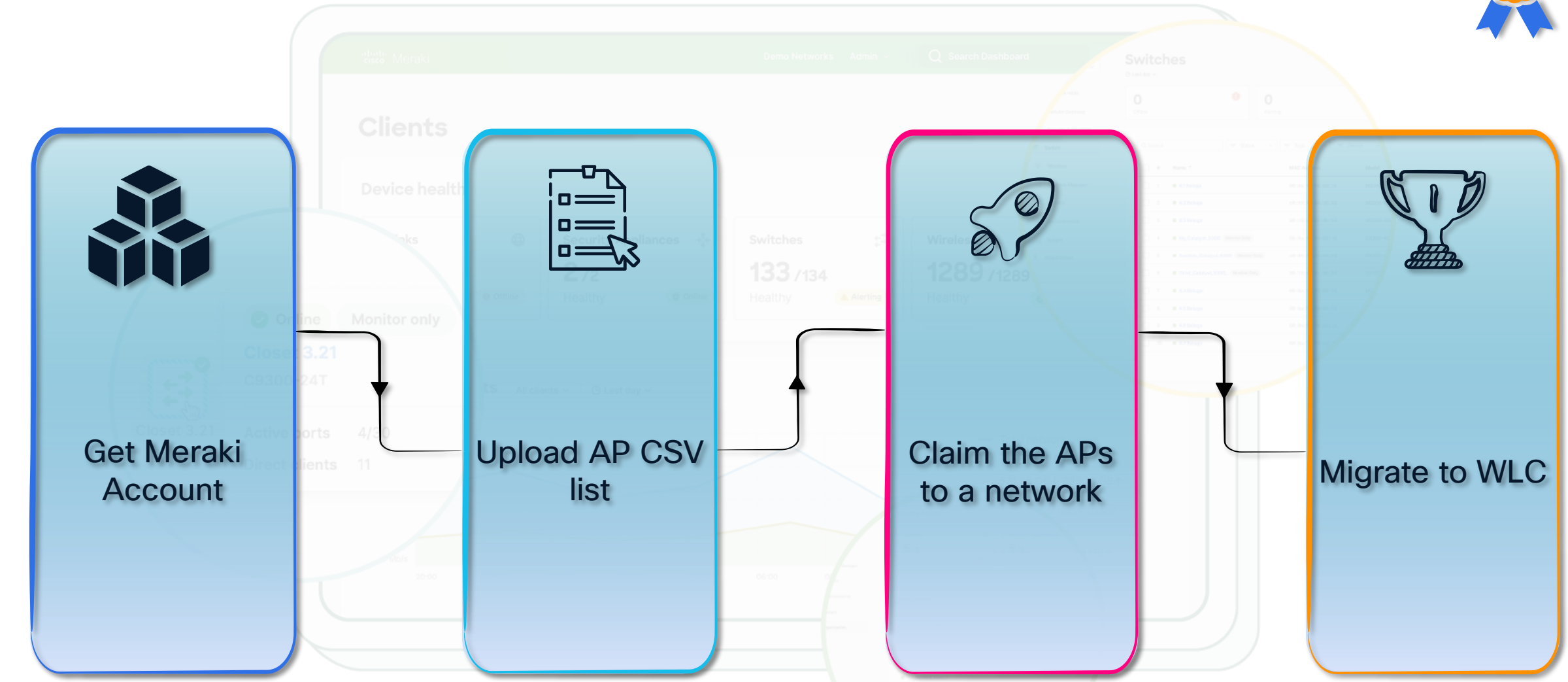


OOB Mode of Operation

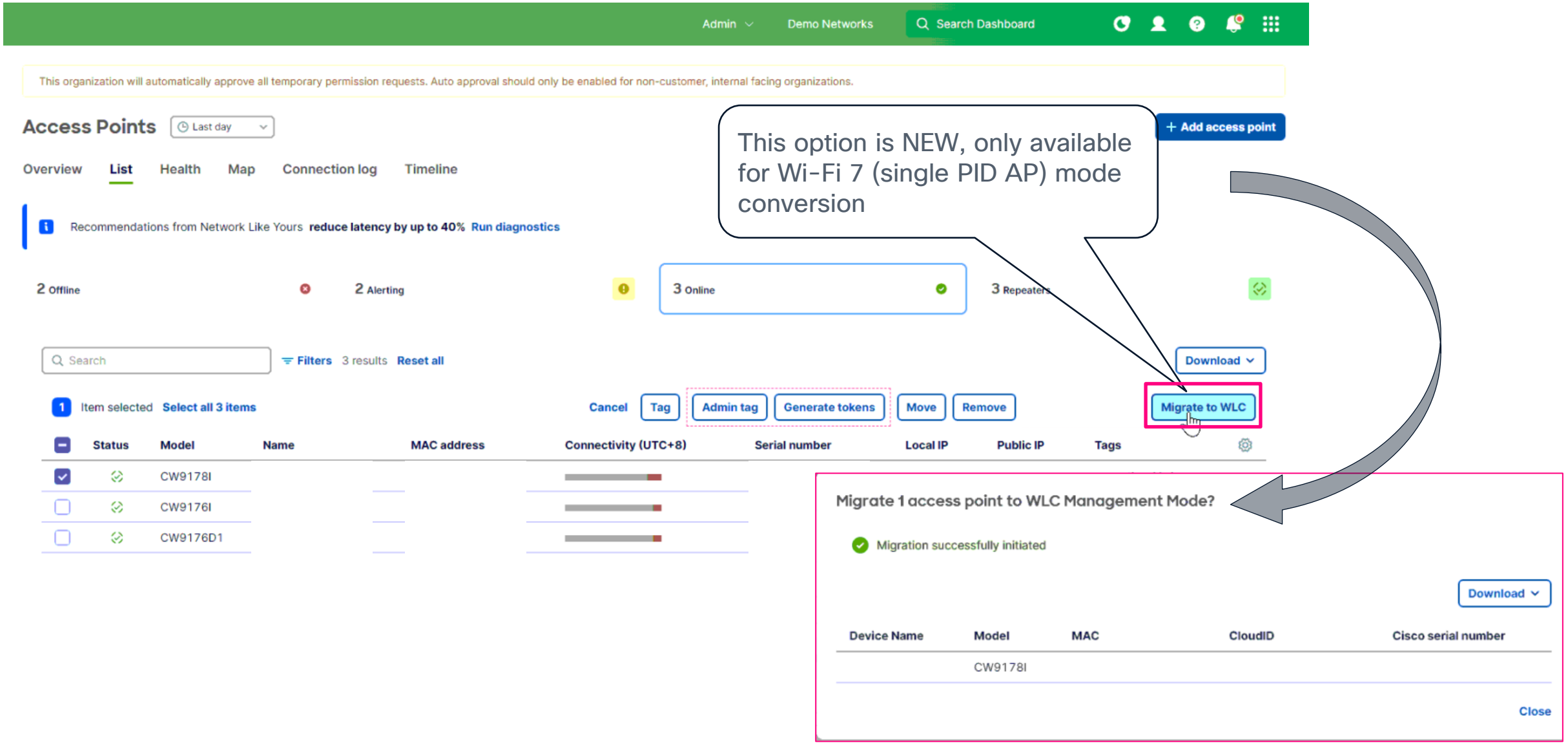
```
<Meraki> offline-migration-info
| [2000-01-01 00:00:26.640] AP in day0 - offline migration
| [2000-01-01 00:01:24.369] [init] start offline migration detection
| [2000-01-01 00:02:26.465] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:02:31.470] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2000-01-01 00:02:31.470] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2000-01-01 00:02:31.470] [fast-offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:02:31.470] [fast-offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:02:31.470] [fast-offline-migration] waiting for 7min before taking any migration decision
| [2000-01-01 00:03:33.531] [fast-offline-migration] waiting for 5min before taking any migration decision
| [2000-01-01 00:04:35.590] [fast-offline-migration] waiting for 4min before taking any migration decision
| [2000-01-01 00:05:37.648] [fast-offline-migration] waiting for 3min before taking any migration decision
| [2000-01-01 00:06:39.707] [fast-offline-migration] waiting for 2min before taking any migration decision
| [2000-01-01 00:07:41.765] [fast-offline-migration] waiting for 1min before taking any migration decision
| [2000-01-01 00:08:43.824] [fast-offline-migration] waiting for 0min before taking any migration decision
| [2000-01-01 00:09:35.874] [offline-migration] forcing DHCP renew
| [2000-01-01 00:09:35.874] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:09:40.879] [offline-migration] migration decision
| [2000-01-01 00:09:40.879] [offline-migration][v4] no WLC IP in DHCP option 43
| [2000-01-01 00:09:40.879] [offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:09:40.879] [offline-migration][v6] no WLC IP in DHCP option 52
| [2000-01-01 00:09:40.879] [offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:09:45.899] [offline-migration][v4][capwap-l2] 0 WLC(s) detected (unsupported)
| [2000-01-01 00:09:50.920] [offline-migration][v6][capwap-l2] 0 WLC(s) detected (unsupported)
| [2000-01-01 00:09:50.920] [offline-migration] no migration & not claimed => restart detection
| [2000-01-01 00:09:55.924] [init] start offline migration detection
```

Meraki Dashboard

Meraki Dashboard operations for Catalyst use cases

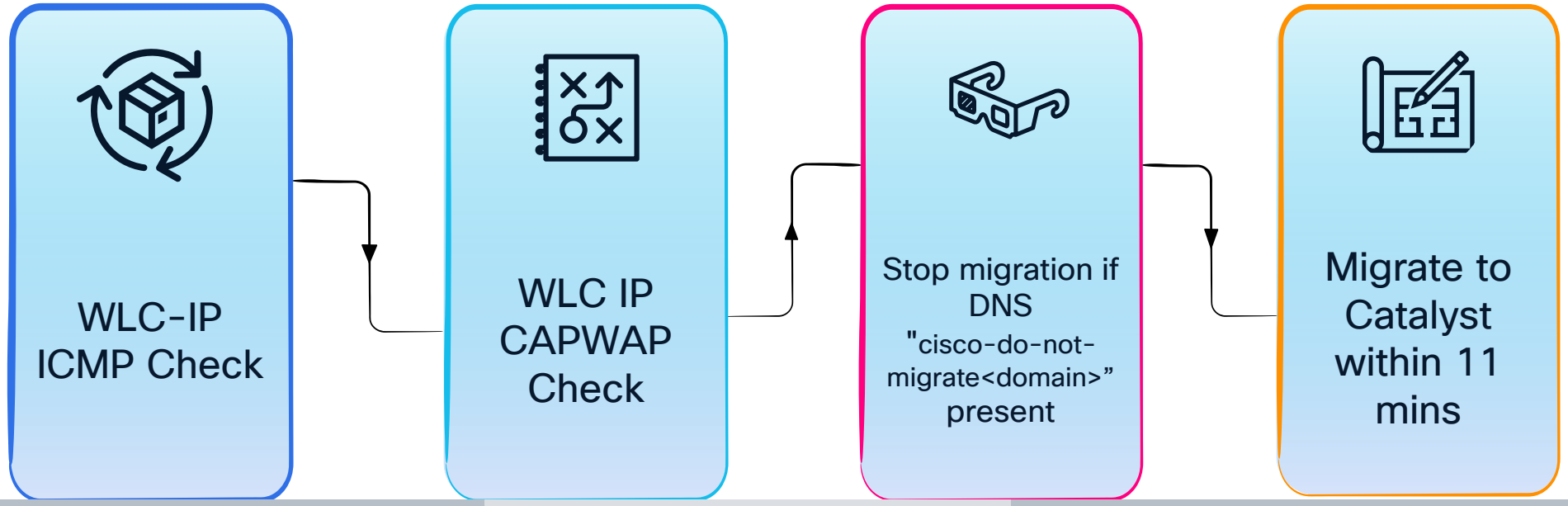


Meraki Dashboard operations for Catalyst use cases



Normal Offline Migration

Normal Offline Migration to Catalyst using DHCPv4 Option 43 and DNSv4



Prevent Migration using WLC config command "no capwap discovery onboarding"

DHCPv4 Option 43 – F1 Format
F1 <size> <IP array>
Example
WLC IP address: 200.1.0.100
ip dhcp pool vlan200
option 43 hex F105c8010064

DNS IPv4 Option – cisco-capwap
cisco-capwap-controller.<domain> is resolve
Example:
ip dns server
ip host cisco-capwap-controller.cisco.com 200.1.0.100

Normal offline Migration to Catalyst using DNS/DHCPv4 Option 43 (F1)

AP Console log – DHCPv4

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:01.252] AP in day0 - offline migration
| [2000-01-01 00:01:54.26 ] [init] start offline migration detection
| [2000-01-01 00:03:02.682] [fast-offline-migration] waiting for 7min
before taking any migration decision
| [2000-01-01 00:04:04.756] [fast-offline-migration] waiting for 5min
before taking any migration decision
| [2000-01-01 00:05:06.829] [fast-offline-migration] waiting for 4min
before taking any migration decision
| [2000-01-01 00:06:08.901] [fast-offline-migration] waiting for 3min
before taking any migration decision
| [2000-01-01 00:07:10.975] [fast-offline-migration] waiting for 2min
before taking any migration decision
| [2000-01-01 00:08:13.51 ] [fast-offline-migration] waiting for 1min
before taking any migration decision
| [2000-01-01 00:09:15.125] [fast-offline-migration] waiting for 0min
before taking any migration decision
| [2000-01-01 00:10:06.186] [offline-migration] forcing DHCP renew
| [2000-01-01 00:10:06.186] [offline-migration] forcing DHCPv6 INFORMATI(
REQUEST
| [2000-01-01 00:10:12.193] [offline-migration] migration decision
| [2000-01-01 00:10:12.193] [offline-migration][v4] WLC IP present in DH(
option 43
| [2000-01-01 00:10:12.215] [offline-migration][v4][capwap] DHCP: WLC
200.1.0.100 is valid - version 17.15.2.33
| [2000-01-01 00:10:12.215] [offline-migration][DHCP][IPv4] migrate to
Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
```

AP Console log – DNS

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:01.528] AP in day0 - offline migration
| [2000-01-01 00:01:50.166] [init] start offline migration detection
| [2000-01-01 00:02:57.328] [fast-offline-migration] waiting for 7min
before taking any migration decision
| [2000-01-01 00:03:59.458] [fast-offline-migration] waiting for 5min
before taking any migration decision
| [2000-01-01 00:05:01.556] [fast-offline-migration] waiting for 4min
before taking any migration decision
| [2000-01-01 00:06:03.656] [fast-offline-migration] waiting for 3min
before taking any migration decision
| [2000-01-01 00:07:05.760] [fast-offline-migration] waiting for 2min
before taking any migration decision
| [2000-01-01 00:08:07.863] [fast-offline-migration] waiting for 1min
before taking any migration decision
| [2000-01-01 00:09:09.966] [fast-offline-migration] waiting for 0min
before taking any migration decision
| [2000-01-01 00:10:02.52 ] [offline-migration] forcing DHCP renew
| [2000-01-01 00:10:07.68 ] [offline-migration] migration decision
| [2000-01-01 00:10:07.69 ] [offline-migration][v4] no WLC IP in DHCP
option 43
| [2000-01-01 00:10:07.71 ] [offline-migration][v4] WLC IP resolved by
DNS: 200.1.0.100
| [2000-01-01 00:10:07.99 ] [offline-migration][v4][capwap] DNS: WLC
200.1.0.100 is valid - version 17.15.2.33
| [2000-01-01 00:10:07.99 ] [offline-migration][DNS][IPv4] migrate to
Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
```

Normal offline Migration to Catalyst using DNS/DHCPv4 Option 43 (F1)

AP Console log – DHCPv4

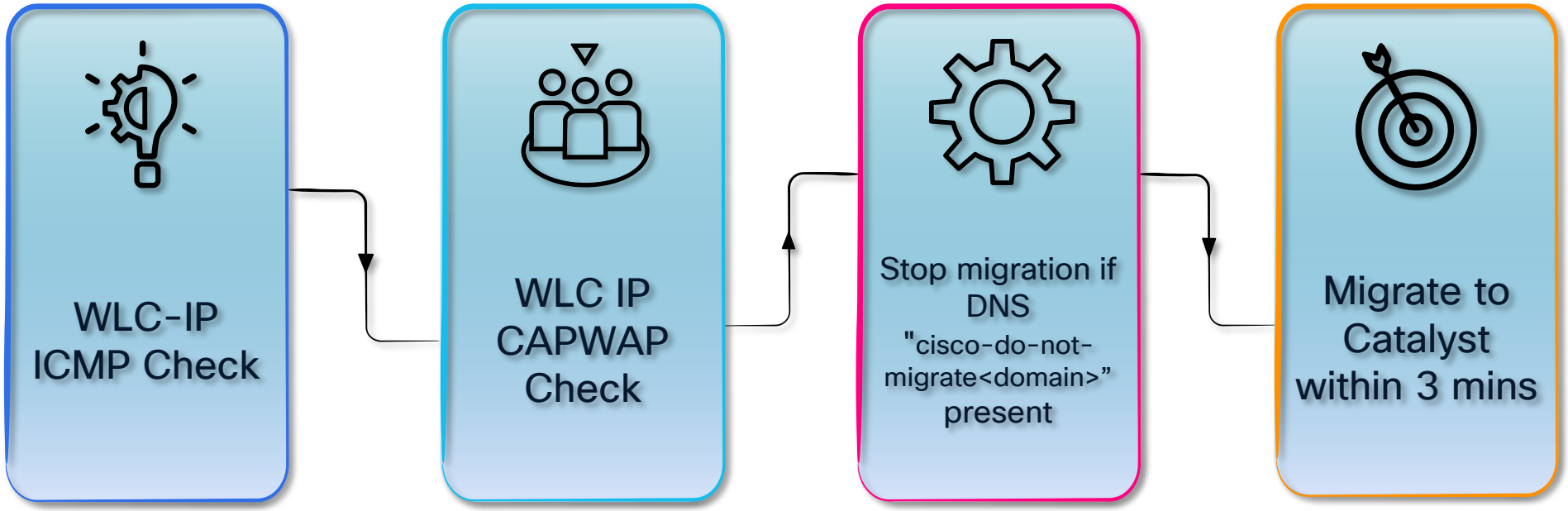
```
<Meraki> offline-migration-info
| [2000-01-01 00:07:10.975] [fast-offline-migration] waiting for 2min
before taking any migration decision
| [2000-01-01 00:08:13.51 ] [fast-offline-migration] waiting for 1min
before taking any migration decision
| [2000-01-01 00:09:15.125] [fast-offline-migration] waiting for 0min
before taking any migration decision
| [2000-01-01 00:10:12.193] [offline-migration][v4] WLC IP present in DHCP option 43
| [2000-01-01 00:10:12.215] [offline-migration][v4][capwap] DHCP: WLC 200.1.0.100 is valid -
version 17.15.2.33
| [2000-01-01 00:10:12.215] [offline-migration][DHCP][IPv4] migrate to Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
```

AP Console log – DNS

```
<Meraki> offline-migration-info
| [2000-01-01 00:07:05.760] [fast-offline-migration] waiting for 2min
before taking any migration decision
| [2000-01-01 00:08:07.863] [fast-offline-migration] waiting for 1min
before taking any migration decision
| [2000-01-01 00:09:09.966] [fast-offline-migration] waiting for 0min
before taking any migration decision
| [2000-01-01 00:10:07.71 ] [offline-migration][v4] WLC IP resolved by DNS: 200.1.0.100
| [2000-01-01 00:10:07.99 ] [offline-migration][v4][capwap] DNS: WLC 200.1.0.100 is valid -
version 17.15.2.33
| [2000-01-01 00:10:07.99 ] [offline-migration][DNS][IPv4] migrate to Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
```

Fast Offline Migration

Fast offline Migration to Catalyst using DNS – DHCPv4 Option 43



Reachability checks ICMP and CAPWAP Discovery

DHCPv4 Option 43 – F3 Format
F3<size><IP array>ModeValue=<1/2>
Meraki: Mode=1
Catalyst: Mode=2
Example
WLC IP address: 200.1.0.100
option 43 hex F305c801006402

DNS Format:
cisco-automigrate.<domain>
Resolved WLC IP is ICMP Reachable.
Example:
ip dns server
ip host cisco-automigrate.cisco.com 200.1.0.100

Fast offline Migration to Catalyst using DHCPv4 Option 43

AP Console log – Running MR OS – F3 [with ICMP reachability]

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:01.574] AP in day0 - offline migration
| [2000-01-01 00:01:56.399] [init] start offline migration detection
| [2000-01-01 00:02:58.578] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:03:03.590] [fast-offline-migration][v4][icmp] DHCP: WLC 200.1.0.100 is reachable
| [2000-01-01 00:03:03.590] [fast-offline-migration][DHCP][IPv4] migrate to Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

AP Console log – Running MR OS – F3 [ICMP Block]

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:01.204] AP in day0 - offline migration
| [2000-01-01 00:01:54.332] [init] start offline migration detection
| [2000-01-01 00:02:57.972] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:03:07.983] [fast-offline-migration][v4][icmp] DHCP: WLC 200.1.0.100 is unreachable
| [2000-01-01 00:03:08.1  ] [fast-offline-migration][v4][capwap] DHCP: WLC 200.1.0.100 is valid - version 17.15.2.33
| [2000-01-01 00:03:08.1  ] [fast-offline-migration][DHCP][IPv4] migrate to Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

Fast offline Migration to Catalyst using DHCPv4 Option 43

AP Console log – Running MR OS – F3 [with ICMP reachability]

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:01.574] AP in day0 - offline migration

 | [2000-01-01 00:03:03.590] [fast-offline-migration][v4][icmp] DHCP: WLC 200.1.0.100 is reachable
 | [2000-01-01 00:03:03.590] [fast-offline-migration][DHCP][IPv4] migrate to Catalyst

Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

AP Console log – Running MR OS – F3 [ICMP Block]

```
<Meraki> offline-migration-info

 | [2000-01-01 00:03:07.983] [fast-offline-migration][v4][icmp] DHCP: WLC 200.1.0.100 is unreachable
 | [2000-01-01 00:03:08.1  ] [fast-offline-migration][v4][capwap] DHCP: WLC 200.1.0.100 is valid - version
 17.15.2.33
 | [2000-01-01 00:03:08.1  ] [fast-offline-migration][DHCP][IPv4] migrate to Catalyst

Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

Fast offline Migration to Catalyst using DNS – DHCPv4

AP Console log – Running MR OS [with ICMP reachability]

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:00.998] AP in day0 - offline migration
| [2000-01-01 00:01:47.351] [init] start offline migration detection
| [2000-01-01 00:02:52.993] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:02:57.999] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2000-01-01 00:02:57.999] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][v4][icmp] DNS automigrate: WLC 200.1.0.100 is reachable
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][DNS][IPv4] migrate to Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

AP Console log – Running MR OS [ICMP Block]

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:00.998] AP in day0 - offline migration
| [2000-01-01 00:01:47.351] [init] start offline migration detection
| [2000-01-01 00:02:52.993] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:02:57.999] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2000-01-01 00:02:57.999] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2000-01-01 00:03:03.5  ] [fast-offline-migration][v4][icmp] DNS automigrate: WLC 200.1.0.100 is unreachable
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][v4][capwap] DNS automigrate: WLC 200.1.0.100 is valid - version 17.15.2.20
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][DNS][IPv4] migrate to Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

Fast offline Migration to Catalyst using DNS – DHCPv4

AP Console log – Running MR OS [with ICMP reachability]

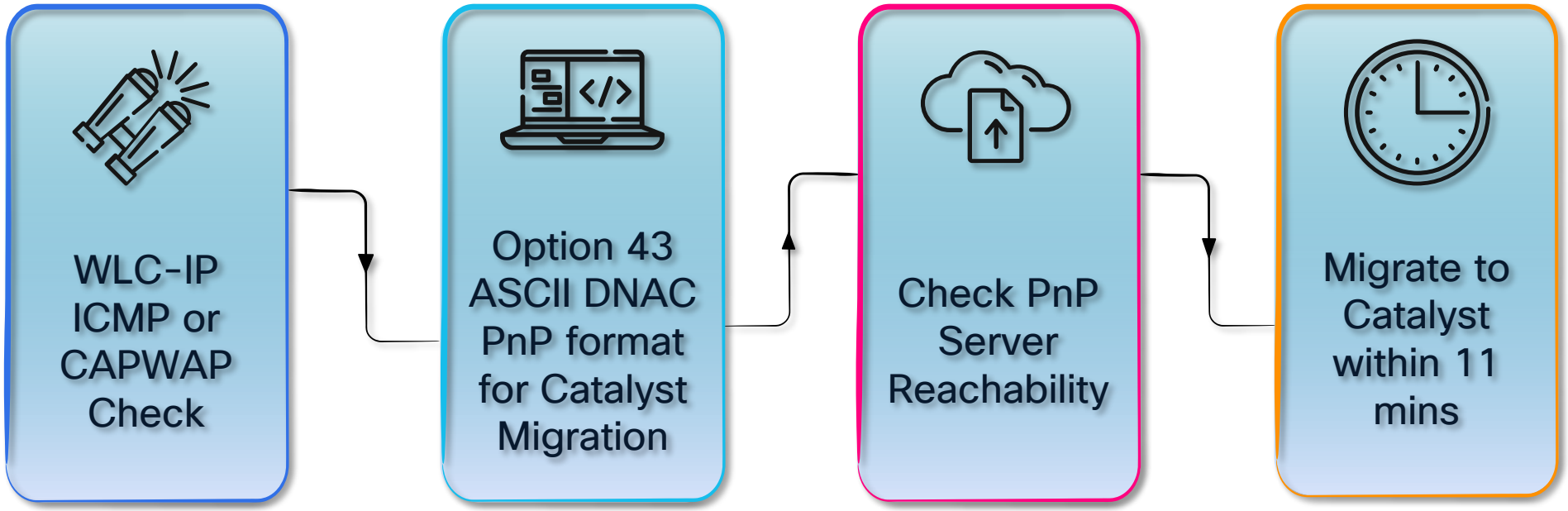
```
<Meraki> offline-migration-info
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][v4][icmp] DNS automigrate: WLC 200.1.0.100 is reachable
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][DNS][IPv4] migrate to Catalyst
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

AP Console log – Running MR OS [ICMP Block]

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:00.998] AP in day0 - offline migration
| [2000-01-01 00:03:03.5  ] [fast-offline-migration][v4][icmp] DNS automigrate: WLC 200.1.0.100 is
unreachable
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][v4][capwap] DNS automigrate: WLC 200.1.0.100 is valid -
version 17.15.2.20
| [2000-01-01 00:03:03.22 ] [fast-offline-migration][DNS][IPv4] migrate to Catalyst
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

Cisco PnP Server

Normal offline Migration to Catalyst using DNAC PnP server



Note:
"capwap-discovery onboard unicast" is default configuration on AP join Profile.

Use "no capwap-discovery onboarding" to prevent discovery responses from the WLC

DHCPv4 Option 43 – PnP Format
F2 <size> <IP array>

Example
ip dhcp pool vlan200
network 200.1.0.0 255.255.0.0
default-router 200.1.0.1
option 43 ascii 5A1N;B2;K4;I200.1.0.75;J80

Normal offline Migration to Catalyst using DNS – DHCPv4

AP Console log – Running Meraki OS

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:01.252] AP in day0 - offline migration
| [2000-01-01 00:01:54.26 ] [init] start offline migration detection
| [2000-01-01 00:02:57.676] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:03:02.682] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2000-01-01 00:03:02.682] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2000-01-01 00:03:02.682] [fast-offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:03:02.682] [fast-offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:03:02.682] [fast-offline-migration] waiting for 7min before taking any migration decision
| [2000-01-01 00:04:04.756] [fast-offline-migration] waiting for 5min before taking any migration decision
| [2000-01-01 00:05:06.829] [fast-offline-migration] waiting for 4min before taking any migration decision
| [2000-01-01 00:06:08.901] [fast-offline-migration] waiting for 3min before taking any migration decision
| [2000-01-01 00:07:10.975] [fast-offline-migration] waiting for 2min before taking any migration decision
| [2000-01-01 00:08:13.51 ] [fast-offline-migration] waiting for 1min before taking any migration decision
| [2000-01-01 00:09:15.125] [fast-offline-migration] waiting for 0min before taking any migration decision
| [2000-01-01 00:10:06.186] [offline-migration] forcing DHCP renew
| [2000-01-01 00:10:06.186] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:10:12.193] [offline-migration] migration decision
| [2000-01-01 00:10:12.193] [offline-migration][v4] WLC IP present in DHCP option 43 (ciscopnp): 200.1.0.75
| [2000-01-01 00:10:12.195] [offline-migration][v4][icmp] DHCP: WLC 200.1.0.75 is alive
| [2000-01-01 00:10:12.215] [offline-migration][DHCP][IPv4] migrate to Catalyst
<Meraki> meraki_watchdog: Signal TERM, exiting loop
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

Normal offline Migration to Catalyst using DNS – DHCPv4

AP Console log – Running Meraki OS

```
<Meraki> offline-migration-info
| [2000-01-01 00:01:01.252] AP in day0 - offline migration
| [2000-01-01 00:01:54.26 ] [init] start offline migration detection
| [2000-01-01 00:02:57.676] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:03:02.682] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2000-01-01 00:03:02.682] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2000-01-01 00:03:02.682] [fast-offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:03:02.682] [fast-offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:03:02.682] [fast-offline-migration] waiting for 7min before taking any migration decision
| [2000-01-01 00:04:04.756] [fast-offline-migration] waiting for 5min before taking any migration decision
| [2000-01-01 00:05:06.829] [fast-offline-migration] waiting for 4min before taking any migration decision
| [2000-01-01 00:06:08.901] [fast-offline-migration] waiting for 3min before taking any migration decision
| [2000-01-01 00:07:10.975] [fast-offline-migration] waiting for 2min before taking any migration decision
| [2000-01-01 00:08:13.51 ] [fast-offline-migration] waiting for 1min before taking any migration decision
| [2000-01-01 00:09:15.125] [fast-offline-migration] waiting for 0min before taking any migration decision
| [2000-01-01 00:10:06.186] [offline-migration] forcing DHCP renew
| [2000-01-01 00:10:06.186] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:10:12.193] [offline-migration] migration decision
| [2000-01-01 00:10:12.193] [offline-migration][v4] WLC IP present in DHCP option 43 (ciscopnp): 200.1.0.75
| [2000-01-01 00:10:12.195] [offline-migration][v4][icmp] DHCP: WLC 200.1.0.75 is alive
| [2000-01-01 00:10:12.215] [offline-migration][DHCP][IPv4] migrate to Catalyst

Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
```

Prevent Offline Migration

Prevent Offline Migration to Catalyst using DNS – DHCPv4

“cisco-do-not-automigrate” to prevent migraton

DHCPv4 DNS – “cisco-automigrate”
Format:
cisco-capwap-controller.<domain> is resolved
cisco-do-not-automigrate.<domain> to prevent migration

Example:

```
ip dns server
ip host cisco-capwap-controller.cisco.com 200.1.0.100
ip host cisco-do-not-automigrate.cisco.com 200.1.0.100
```

AP Console log – Running Meraki OS

```
| [2000-01-01 00:15:28.69 ] [fast-offline-migration] waiting for 3min before taking any migration decision
| [2000-01-01 00:16:30.140] [fast-offline-migration] waiting for 2min before taking any migration decision
| [2000-01-01 00:17:32.211] [fast-offline-migration] waiting for 1min before taking any migration decision
| [2000-01-01 00:18:34.282] [fast-offline-migration] waiting for 0min before taking any migration decision
| [2000-01-01 00:19:26.342] [offline-migration] forcing DHCP renew
| [2000-01-01 00:19:26.342] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:19:31.347] [offline-migration] migration decision
| [2000-01-01 00:19:31.347] [offline-migration][v4] no WLC IP in DHCP option 43
| [2000-01-01 00:19:31.349] [offline-migration][v4] WLC IP resolved by DNS: 200.1.0.100
| [2000-01-01 00:19:31.349] [offline-migration][v4] do-not-automigrate resolved, no migration allowed
| [2000-01-01 00:19:31.349] [offline-migration] no migration & not claimed => restart detection
```

Prevent Offline Migration to Catalyst using DNS – DHCPv4

"cisco-do-not-automigrate" to prevent migraton

DHCPv4 DNS – "cisco-automigrate"
Format:
cisco-capwap-controller.<domain> is resolved
cisco-do-not-automigrate.<domain> to prevent migration

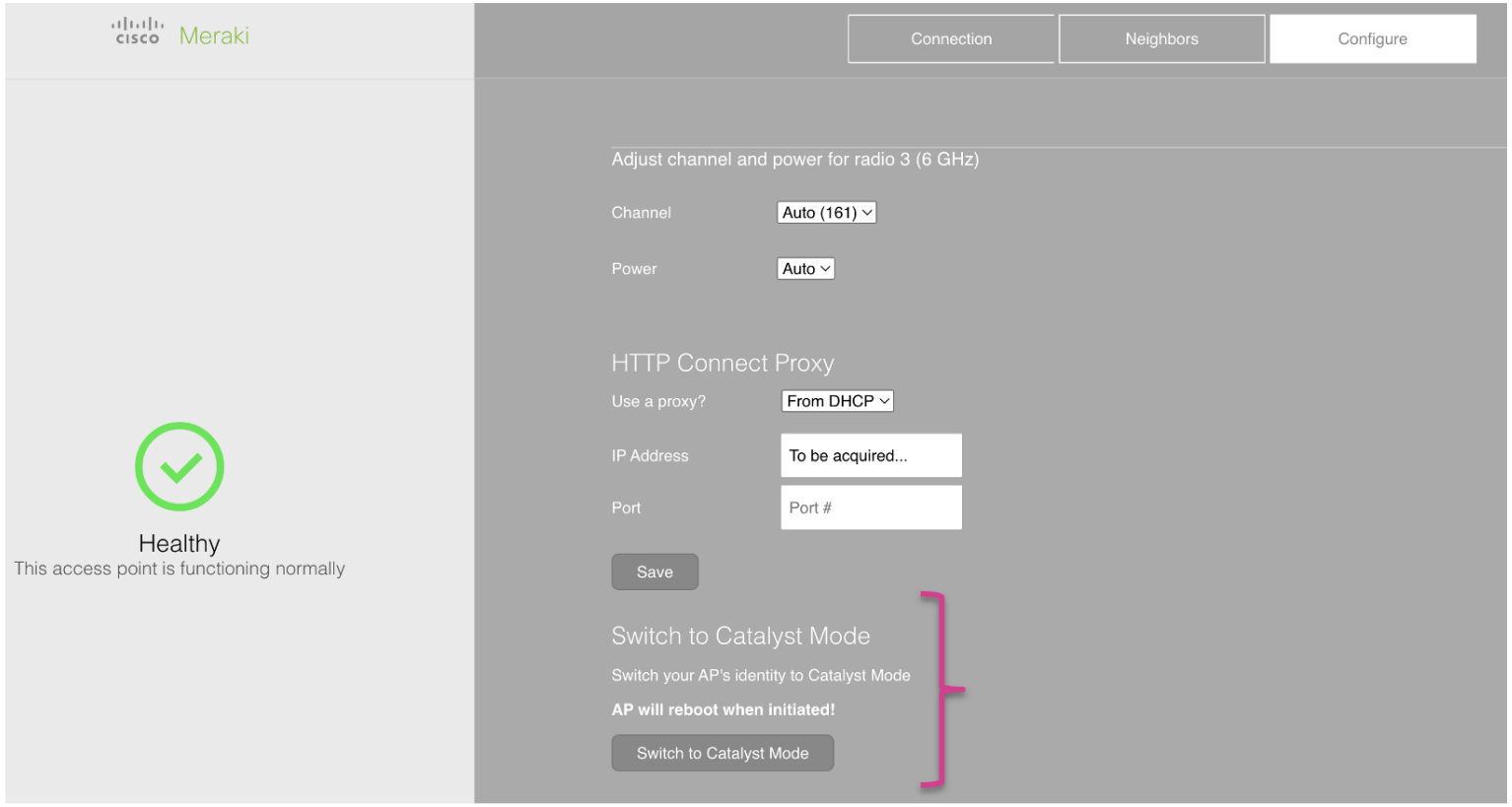
Example:
ip dns server
ip host cisco-capwap-controller.cisco.com 200.1.0.100
ip host cisco-do-not-automigrate.cisco.com 200.1.0.100

AP Console log – Running Meraki OS

```
| [2000-01-01 00:15:28.69 ] [fast-offline-migration] waiting for 3min before taking any migration decision
| [2000-01-01 00:16:30.140] [fast-offline-migration] waiting for 2min before taking any migration decision
| [2000-01-01 00:17:32.211] [fast-offline-migration] waiting for 1min before taking any migration decision
| [2000-01-01 00:18:34.282] [fast-offline-migration] waiting for 0min before taking any migration decision
| [2000-01-01 00:19:26.342] [offline-migration] forcing DHCP renew
| [2000-01-01 00:19:31.347] [offline-migration][v4] no WLC IP in DHCP option 43
| [2000-01-01 00:19:31.349] [offline-migration][v4] WLC IP resolved by DNS: 200.1.0.100
| [2000-01-01 00:19:31.349] [offline-migration][v4] do-not-automigrate resolved, no migration allowed
| [2000-01-01 00:19:31.349] [offline-migration] no migration & not claimed => restart detection
```

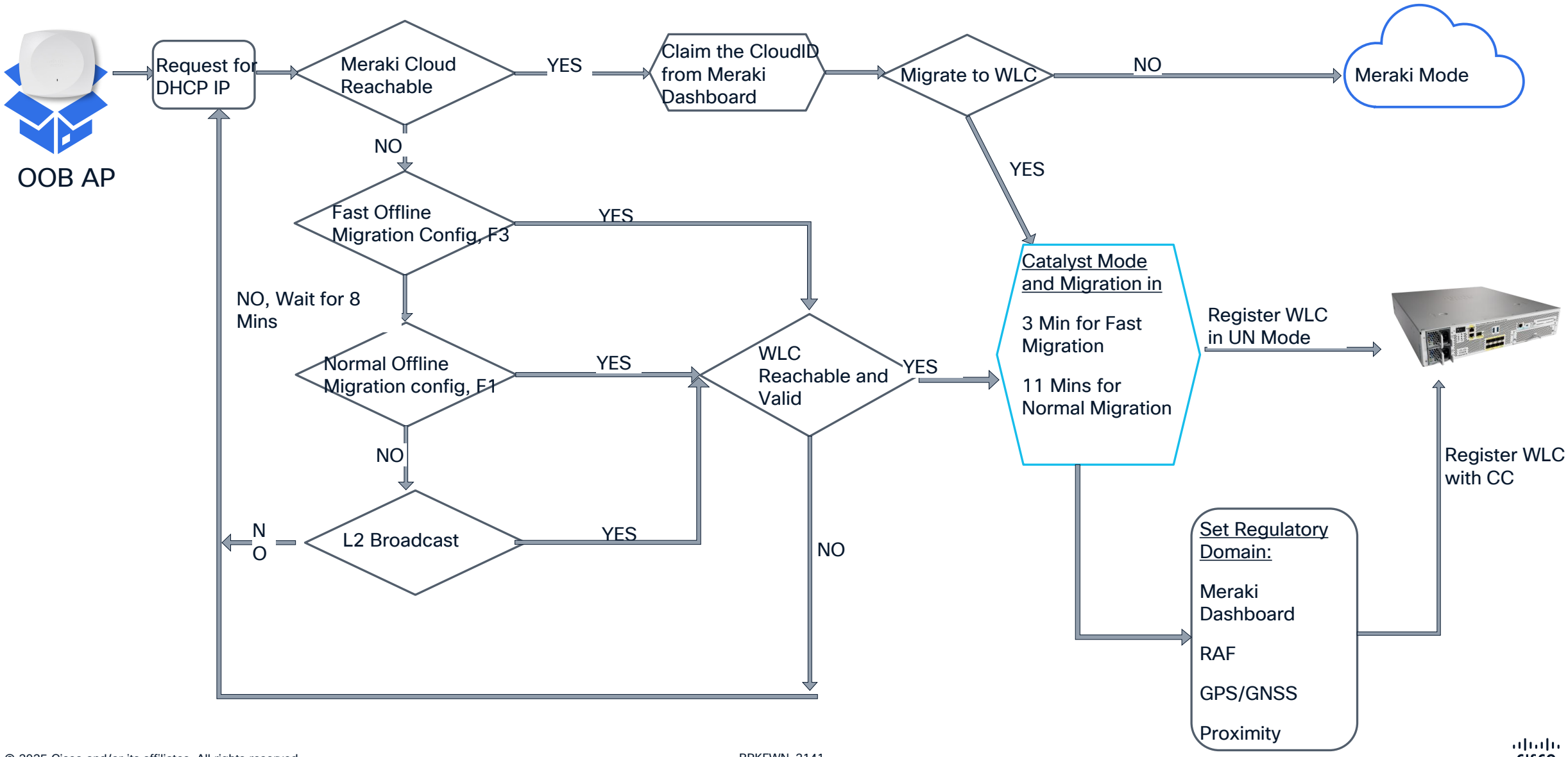
Local Status Page Migration to Catalyst (POC Scenario)

- Post fast offline migration, AP will broadcast default SSIDs – Meraki or Meraki-XXXX
- Connect to Meraki SSID
- Access the AP Local page at 10.128.128.126 with credentials Username: CloudID, Password: <blank>
- In the configure tab, click on ‘Switch to Catalyst Mode’

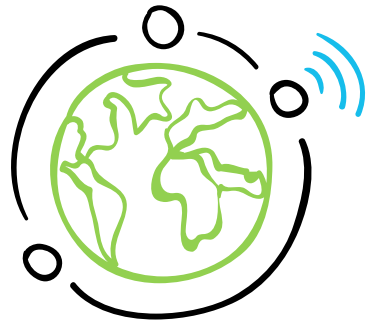


Configure Country Code

OOB Mode of Operation



World-Wide Mode – 2.4G Radio is Up



- AP will operate in World-Wide Mode (2.4G radio only) until Country Code is Resolved.
- AP will send the Proximity/GPS/Regulator Activation File request to WLC for every 1 min

```
AP8C88.814F.0710#sh ip int br
Interface              IP-Address      Method   Status                  Protocol      Speed      Duplex
*wired0                200.1.25.59     DHCP     up                      up            10000      full
wired1                 n/a             n/a      down                    down          n/a        n/a
auxiliary-client       unassigned      unset    up                      up            n/a        n/a
wifi0                  n/a             n/a      up                      up            n/a        n/a
wifi1                  n/a             n/a      administatively down    down          n/a        n/a
wifi2                  n/a             n/a      administatively down    down          n/a        n/a
wifi3                  n/a             n/a      administatively down    down          n/a        n/a

AP8C88.814F.0710#[*06/28/2025 04:03:35.9970] Sending proximity_request payload
[*06/28/2025 04:03:35.9984] SinglePID Proximity resolution: Country Code not available
[*06/28/2025 04:03:36.0015] SinglePID Regulatory Blob resolution: Country Code not available
[*06/28/2025 04:04:33.9956] Sending proximity_request payload
[*06/28/2025 04:04:33.9975] SinglePID Proximity resolution: Country Code not available
[*06/28/2025 04:04:34.0002] SinglePID Regulatory Blob resolution: Country Code not available
[*06/28/2025 04:05:30.0197] Sending proximity_request payload
[*06/28/2025 04:05:30.0229] SinglePID Proximity resolution: Country Code not available
```

Regulatory Activation File (RAF)

Country Code Determination – Regulatory Activation File

```
AP8C88.814F.F570#[*12/16/2024 04:24:55.0118] Sending proximity_request
payload
[*12/16/2024 04:24:55.0135] SinglePID Proximity resolution: Country Code not
available
[*12/16/2024 04:24:55.0163] SinglePID Regulatory Blob resolution: Country
Code not available
[*12/16/2024 04:25:56.2508]
[*12/16/2024 04:25:56.2508]
[*12/16/2024 04:25:56.2508] Country Code US resolved through Regulatory Blob
[*12/16/2024 04:25:56.2508]
[*12/16/2024 04:25:56.2508]
[*12/16/2024 04:25:56.3064] AP Rebooting: Reset Reason - Country Code Changed
         Stopping DHCPv6 client...
[  OK  ] Stopped Cisco image/firmware updater service.
         Stopping Cisco image/firmware updater service...
         Stopping Cisco Power Daemon...
[  OK  ] Stopped target Timers.
```

Resolved the Country Code via Regulatory Activation File

Fastest compared of all the methods

Solution with Bulk APs, with no Cisco AP and restriction to GPS.

Country Code Determination – Regulatory Activation File

```
AP8C88.814F.F570#[*12/16/2024 04:24:55.0118] Sending proximity_request
payload
[*12/16/2024 04:24:55.0135] SinglePID Proximity resolution: Country Code not
ava
[*1
Cod
[*1  [*12/16/2024 04:25:56.2508] Country Code US resolved through Regulatory Blob
[*1  [*12/16/2024 04:25:56.2508]
[*1  [*12/16/2024 04:25:56.2508]
[*1  [*12/16/2024 04:25:56.3064] AP Rebooting: Reset Reason - Country Code Changed
[*1
[*1

[  OK  ] Stopped Cisco image/firmware updater service.
         Stopping Cisco image/firmware updater service...
         Stopping Cisco Power Daemon...
[  OK  ] Stopped target Timers.
```

Resolved the Country Code via Regulatory Activation File

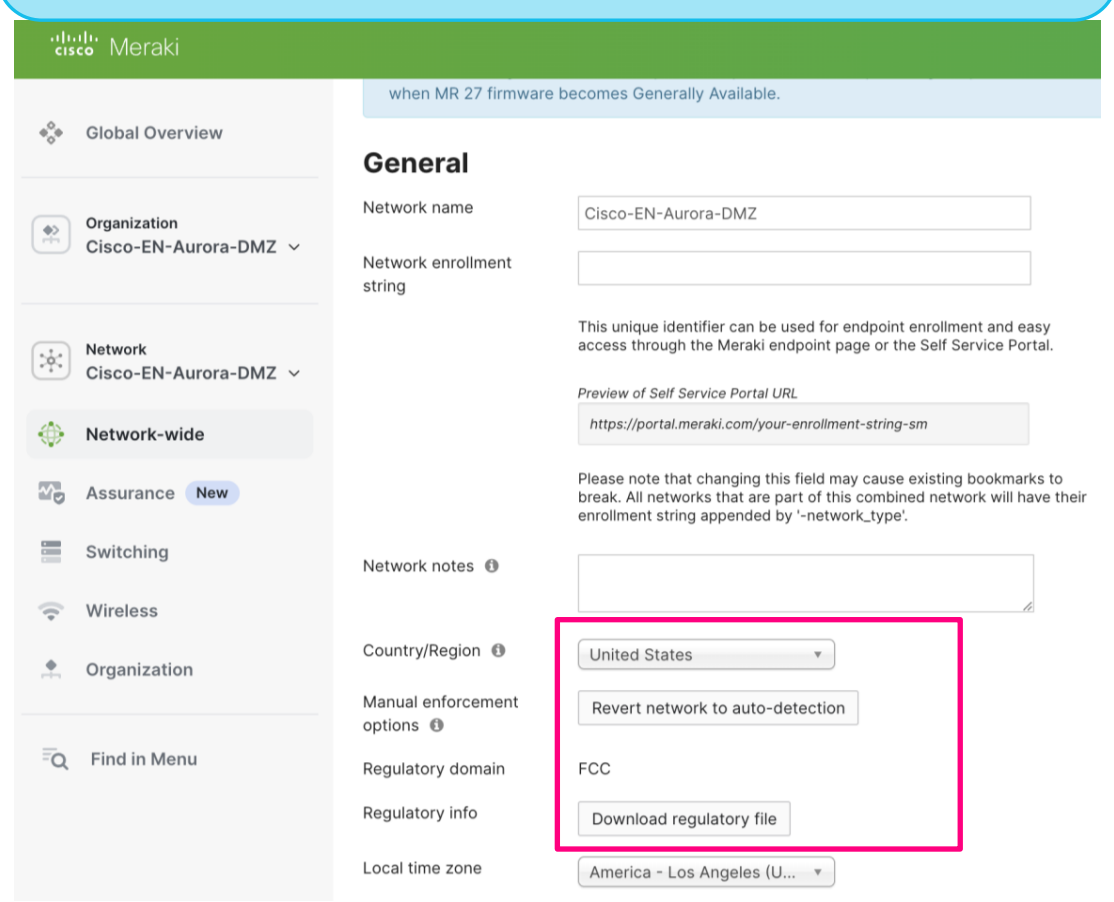
Solution with Bulk APs, with no Cisco AP and restriction to GPS.

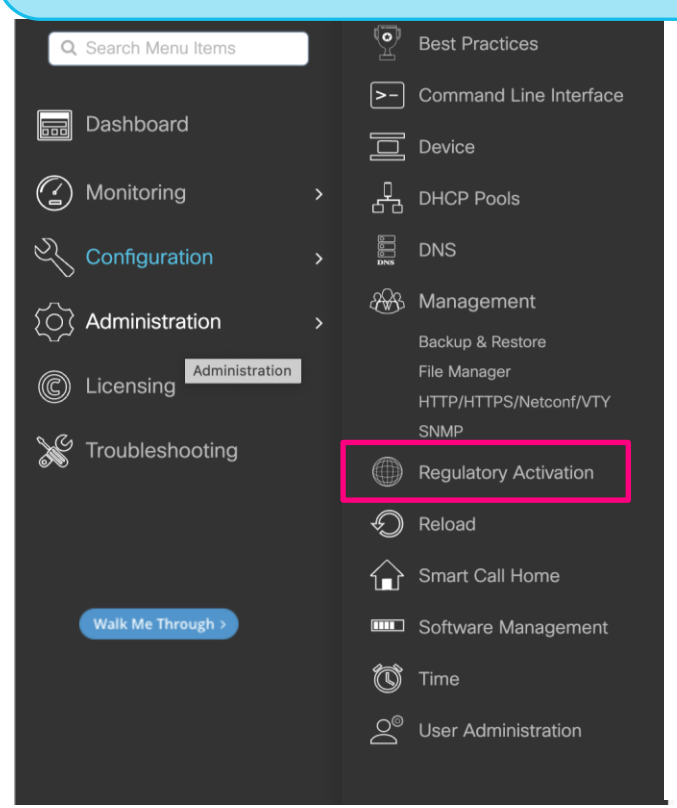
cisco

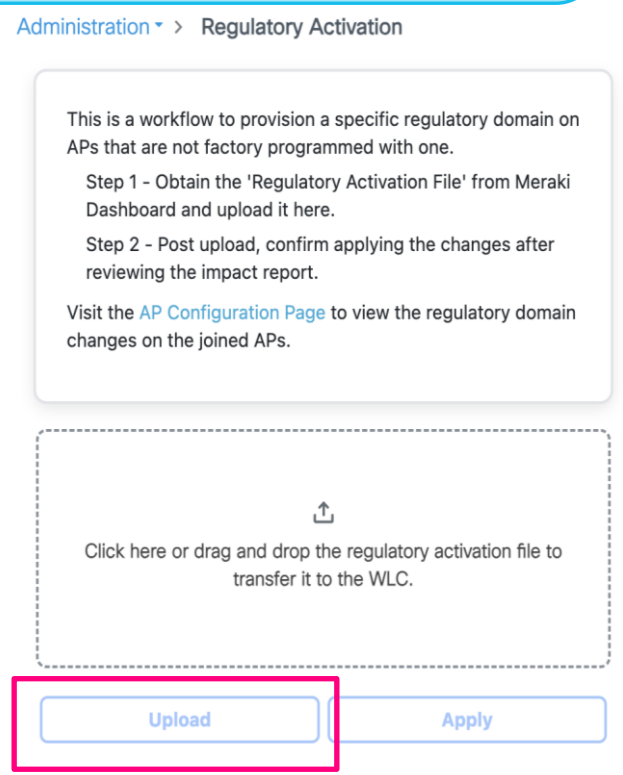
Country Code Determination – Regulatory Activation File (RAF)

Download the RAF from Dashboard
Network Wide -> General -> Click Download Regulatory File Button
Regulatory File should be per Network Level

Administration-> Regulatory Activation
Upload the RAF and Apply to activate and store the data.
Recommended : Activate the RAF before powering ON AP



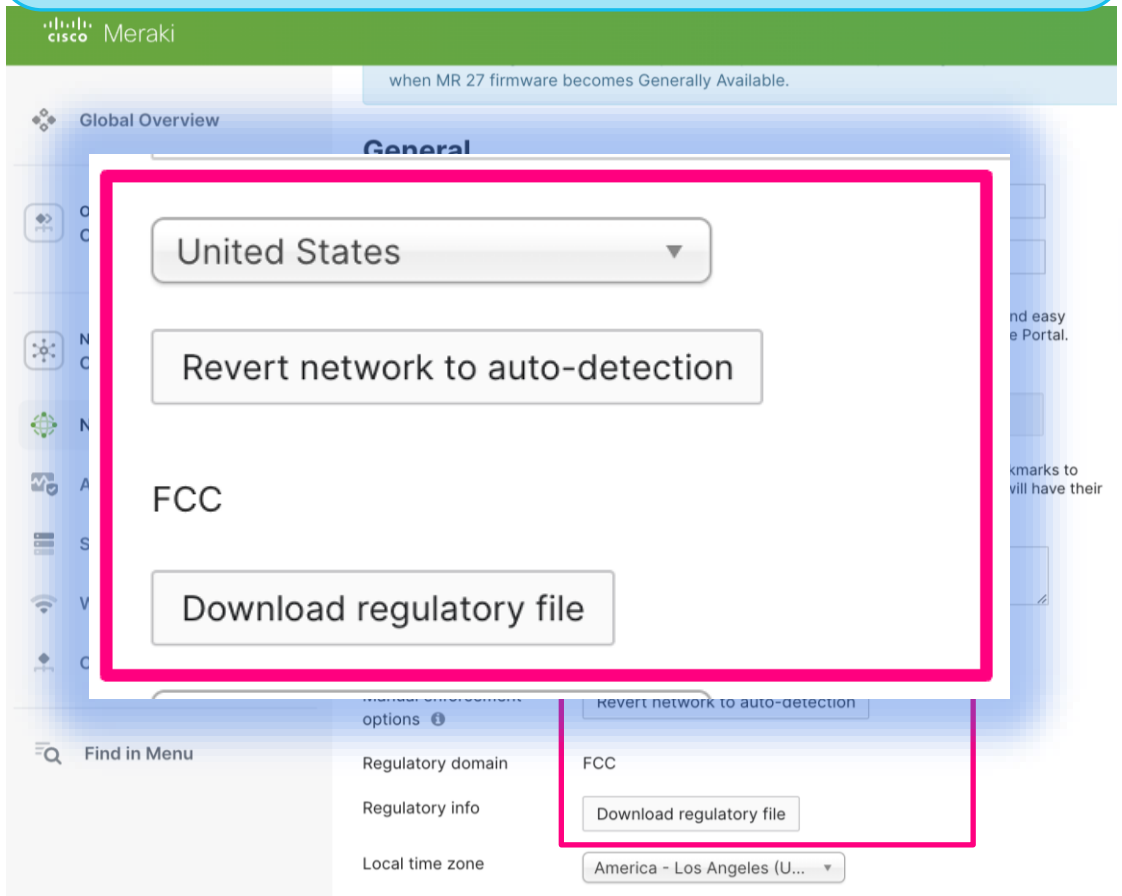


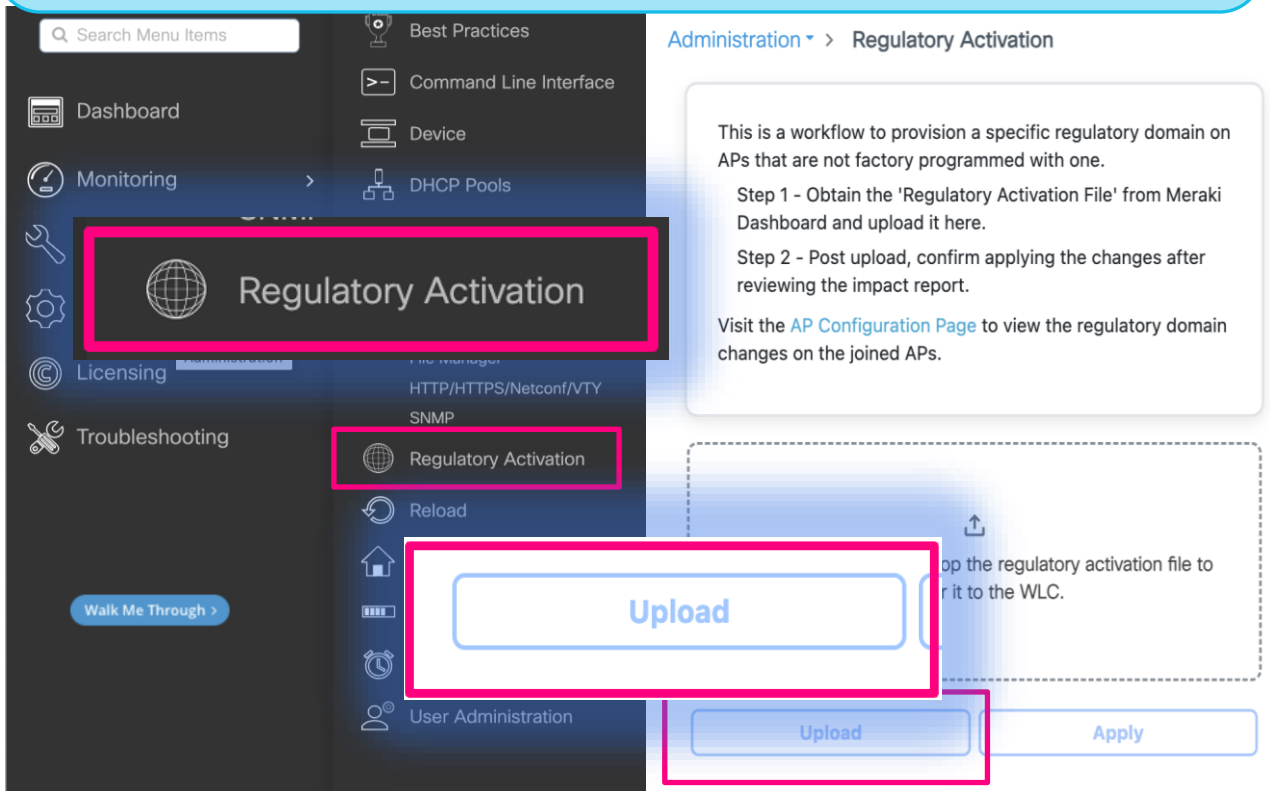


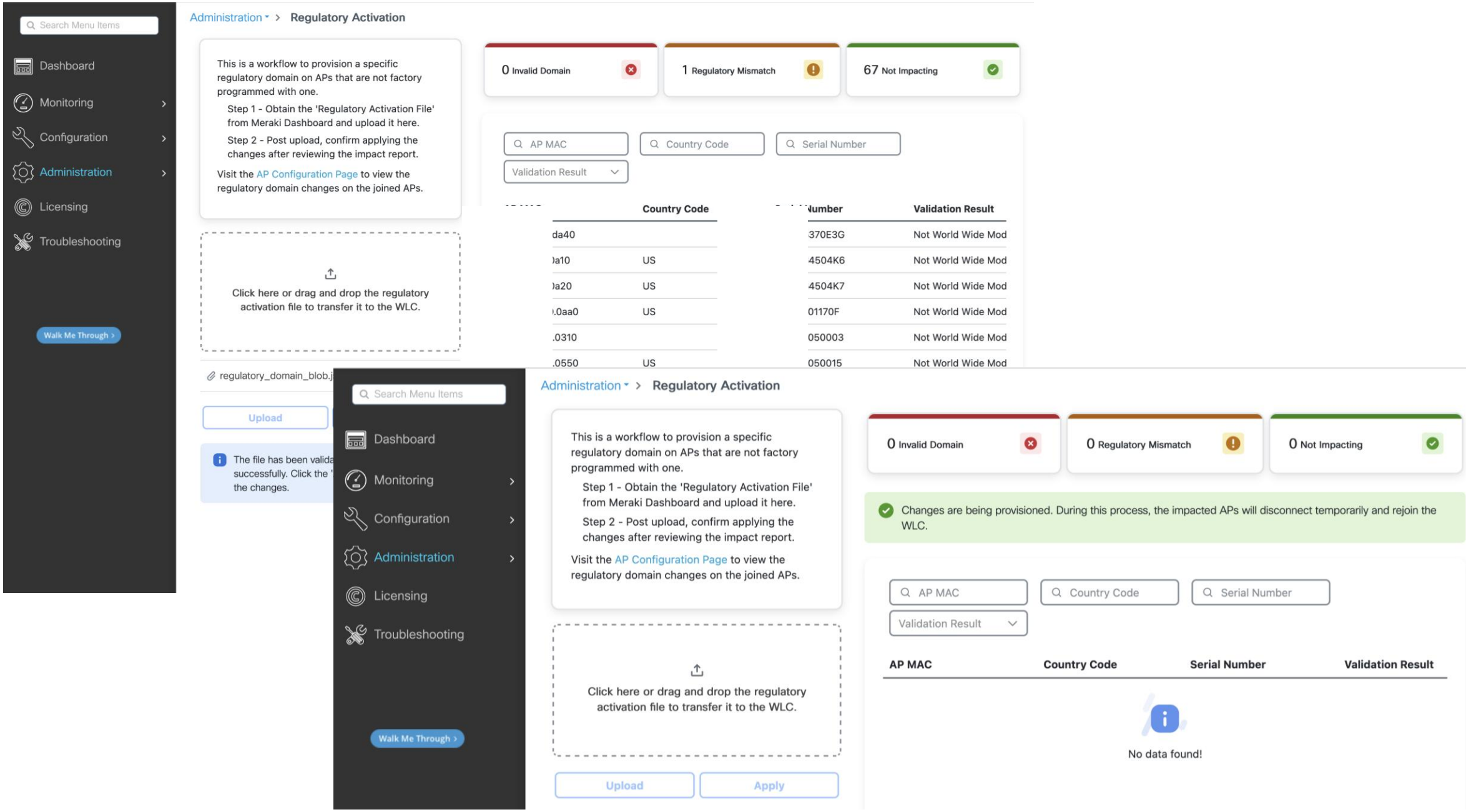
Country Code Determination – Regulatory Activation File (RAF)

Download the RAF from Dashboard
Network Wide -> General -> Click Download Regulatory File Button
Regulatory File should be per Network Level

Administration-> Regulatory Activation
Upload the RAF and Apply to activate and store the data.
Recommended : Activate the RAF before powering ON AP







Proximity

Country Code Determination – Proximity

Resolve 80% of Catalyst customers in Cloud Not Ready deployments

APs and Neighbor APs must join the same controller. No site-tag limitation

Country codes are discovered through the NDP messages.

AP relocation to a different country

1. Clear country code from AP and WLC
2. Learn the new country
3. Join the AP to same or new controller with new country code
4. Move the AP to desired site-tag with right country

```
AP8C88.814F.0710#[*12/16/2024 00:00:53.2402] Sending proximity_request payload
[*12/16/2024 00:00:53.2425] SinglePID Regulatory Blob resolution: Country Code not
available
AP8C88.814F.0710#[*12/16/2024 00:01:51.2612] Sending proximity_request payload
[*12/16/2024 00:01:51.2632] SinglePID Regulatory Blob resolution: Country Code not
available
[*12/16/2024 00:02:51.2840] Sending proximity_request payload
[*12/16/2024 00:02:51.2855] Country Code US resolved through Proximity
[*12/16/2024 00:02:51.3427] AP Rebooting: Reset Reason - Country Code Changed
[  OK  ] Stopped Cisco FIPS QCA radio POST.
         Stopping Cisco FIPS QCA radio POST...
         Stopping Cisco Power Daemon...
```

Country Code Determination – Proximity

Resolve 80% of Catalyst customers in Cloud Not Ready deployments

```
AP8C88.814F.0710#[*12/16/2024 00:00:53.2402] Sending proximity_request payload
[*12/16/2024 00:00:53.2425] SinglePID Regulatory Blob resolution: Country Code not available
AP8C88.814F.0710#[*12/16/2024 00:01:51.2612] Sending proximity_request payload
[*12/16/2024 00:01:51.2632] SinglePID Regulatory Blob resolution: Country Code not available
```

```
[*12/16/2024 00:02:51.2840] Sending proximity_request payload
[*12/16/2024 00:02:51.2855] Country Code US resolved through Proximity
[*12/16/2024 00:02:51.3427] AP Rebooting: Reset Reason - Country Code Changed
```

through the NDP messages.

AP relocation to a different country

1. Clear country code from AP and WLC
2. Learn the new country
3. Join the AP to same or new controller with new country code
4. Move the AP to desired site-tag with right country

GNSS/GPS

Country Code Determination – GPS

AP will send the Geo-Cordinates [Longtitude, Latitude] to WLC

WLC will find the Country Code based on Geo-Coordinates.

WLC will send the Country Code to AP.

AP will skip the Country Code if its < 5KM from the Border of neighbor countries.

```
--More-- [*04/25/2024 13:39:36.7956] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:40:39.8161] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:41:42.7987] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:42:45.5004] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:43:43.7937] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:44:26.9084] GPS/GNSS signal acquired
[*04/25/2024 13:44:26.9345] Country Code US resolved through GPS/GNSS
[*04/25/2024 13:44:26.9779] AP Rebooting: Reset Reason - Country Code Changed
         Stopping Cisco rtd service...
[  OK  ] Stopped target Timers.
         Stopping Cisco Power Daemon...
[  OK  ] Stopped Pine scan auxiliary radio tuning service.
         Stopping Pine scan auxiliary radio tuning service...
[  OK  ] Removed slice system-sshd\x2dkeygen.slice.
         Stopping Ranging Daemon Service...
```

Country Code Determination – GPS

AP will send the Geo-Cordinates [Longtitude, Latitude] to WLC

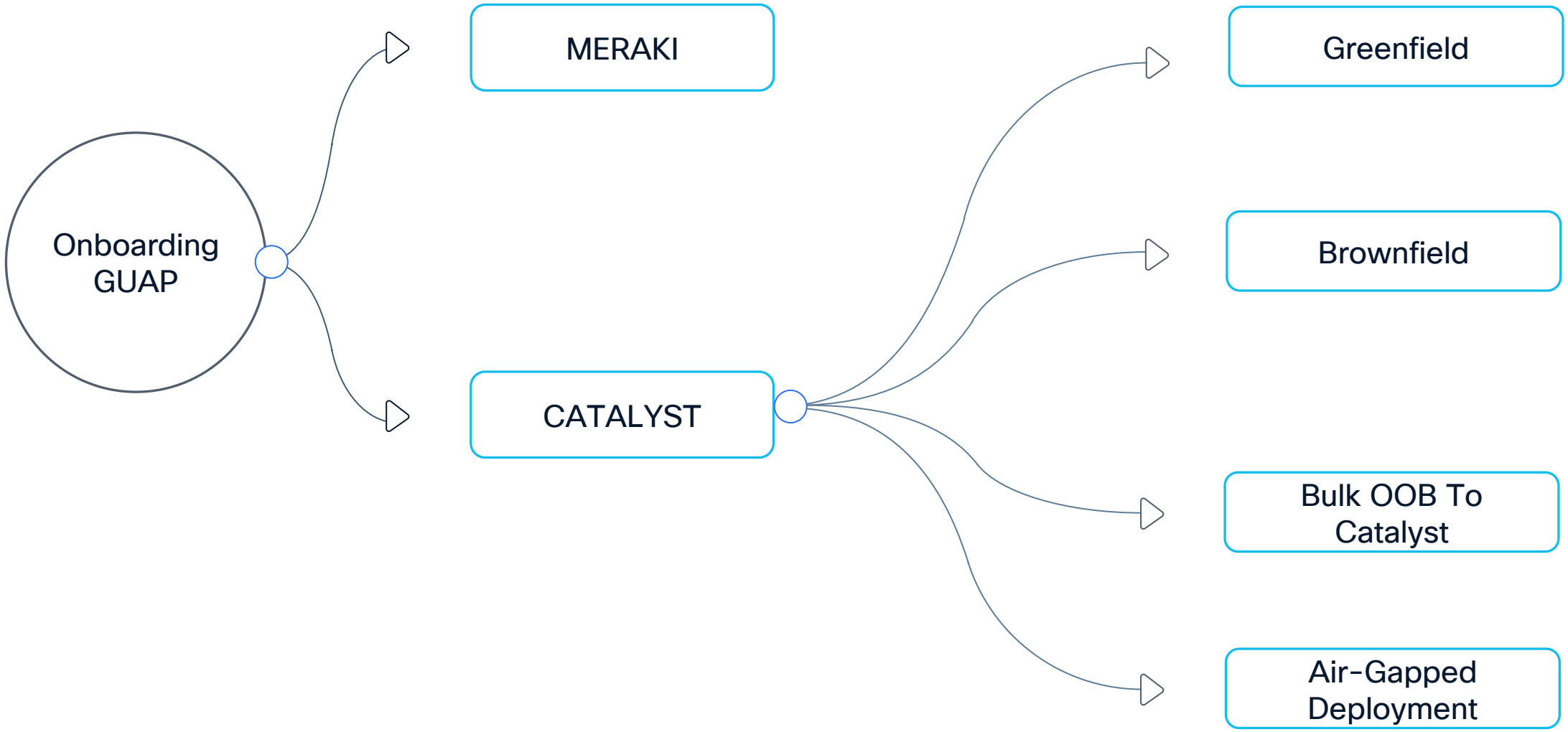
WLC will find the Country Code based on Geo-Coordinates.

AP will skip the Country Code if its < 5KM from the Border of neighbor countries.

```
--More-- [*04/25/2024 13:39:36.7956] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:40:39.8161] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:41:42.7987] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:42:45.5004] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:43:43.7937] SinglePID Proximity resolution: Country Code not
available
[*04/25/2024 13:44:26.9084] GPS/GNSS signal acquired
[*04/25/2024 13:44:26.9345] Country Code US resolved through GPS/GNSS
[*04/25/2024 13:44:26.9779] AP Rebooting: Reset Reason - Country Code Changed
```

```
[  OK  ] Removed slice system-sshd\x2dkeygen.slice.
         Stopping Ranging Daemon Service...
```

Onboarding Scenarios



Scenario 1 – Greenfield

Onboarding

Primary: Meraki Dashboard

Backup: Fast offline migration

Regulatory Domain

Primary: Regulatory Activation File (RAF)

Backup: GPS/GNSS

Operations and Planning

WLC IOS-XE ≥ 17.15.3; reachable

RAF uploaded

site-tag country matches target site

OOB AP → Fast Trigger → COS → RAF/CC Applied → Join WLC & Radios Up

Scenario 2 – Brownfield

Onboarding

Primary: Normal Offline migration

Secondary: Fast Offline migration

Regulatory Domain

Primary: Proximity

Backup: RAF

Operations and Planning

Validate existing DHCP/DNS.

Verify Proximity CC resolution.

AP site-tag country matches resolved CC; radios come up.

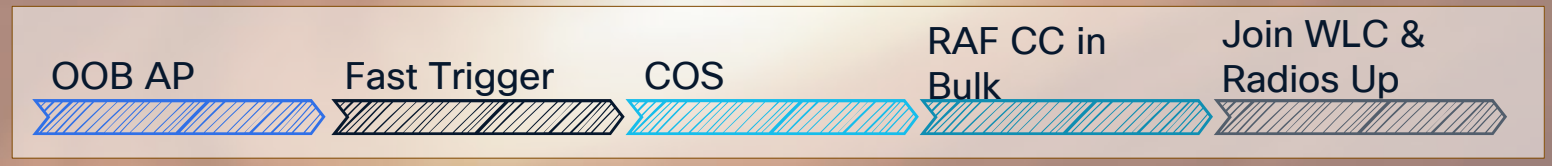
Scenario 3 – Bulk OOB to Catalyst

Onboarding	Regulatory Domain	Operations and Planning
Primary: Meraki Dashboard Secondary: Fast Offline migration	Primary: RAF Backup: Proximity	Batches per building/floor Validate WLC IP AP site-tag country matches resolved CC; radios come up.

OOB Bulk AP → Scaled Fast Trigger → COS → RAF CC in Bulk → Join WLC & Radios Up

Scenario 4: Air-Gapped Deployment

Onboarding	Regulatory Domain	Operations and Planning
Primary: Fast Offline Migration Secondary: Normal Offline migration	Primary: RAF/GPS Backup: Proximity	Based on above scenarios we can decide on the Operations and Planning.



Summary: AP Mode Of Operation Migration

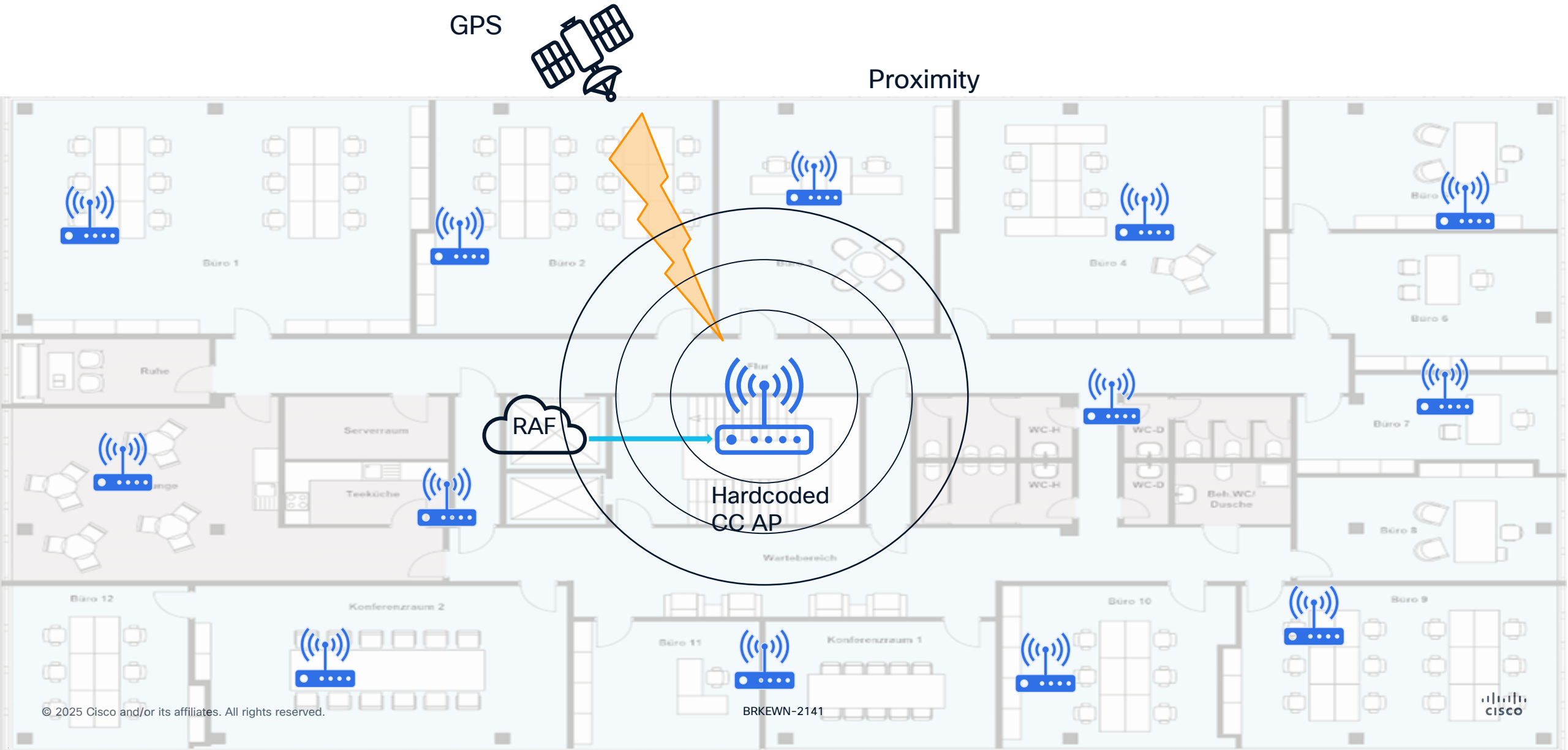
Method	Config Anchor	Speed	Reachability Check	Example	Prevent/Control
Meraki Dashboard Mode Conversion	Claim in Dashboard; set mode	Fast	Cloud reachable and claimed.	Through Dashboard	NA
DHCPv4 F1	option 43 hex F1<size><IP array>	Normal	CAPWAP to 9800WLC ≥ 17.15.	WLC IP 200.1.0.100 F105C8010064.	no capwap-discovery onboarding.
DHCPv4 F3	option 43 hex F3<size><IP array> 02	Fast	ICMP or CAPWAP to at least one 9800WLC IP.	WLC 200.1.0.100 F305C801006402	no capwap-discovery onboarding.
DNS Normal	A/AAAA for cisco-capwap-controller.<domain>	Normal	CAPWAP to resolved IP.	ip host cisco-capwap-controller.cisco.com 200.1.0.100	Publish cisco-do-not-automigrate.<domain>.
DNS Fast	A/AAAA for cisco-automigrate.<domain>	Fast	ICMP (or CAPWAP) to resolved IP.	ip host cisco-automigrate.cisco.com 200.1.0.100	Remove automigrate record.
DNAC PnP ASCII	option 43 ascii ciscopnp string	Normal	ICMP to PnP server.	option 43 ascii 5A1N;B2;K4;I200.1.0.75;J80	no capwap-discovery onboarding
CAPWAP L2 Discovery	L2 broadcast/multicast only	Normal	CAPWAP L2 presence.	capwap-discovery onboarding all.	Keep default (unicast only).

Note: “offline migration” refers to migration without Meraki cloud
Note: “capwap-discovery onboard unicast” is default configuration.
Use “no capwap-discovery onboarding” to prevent discovery responses from the WLC

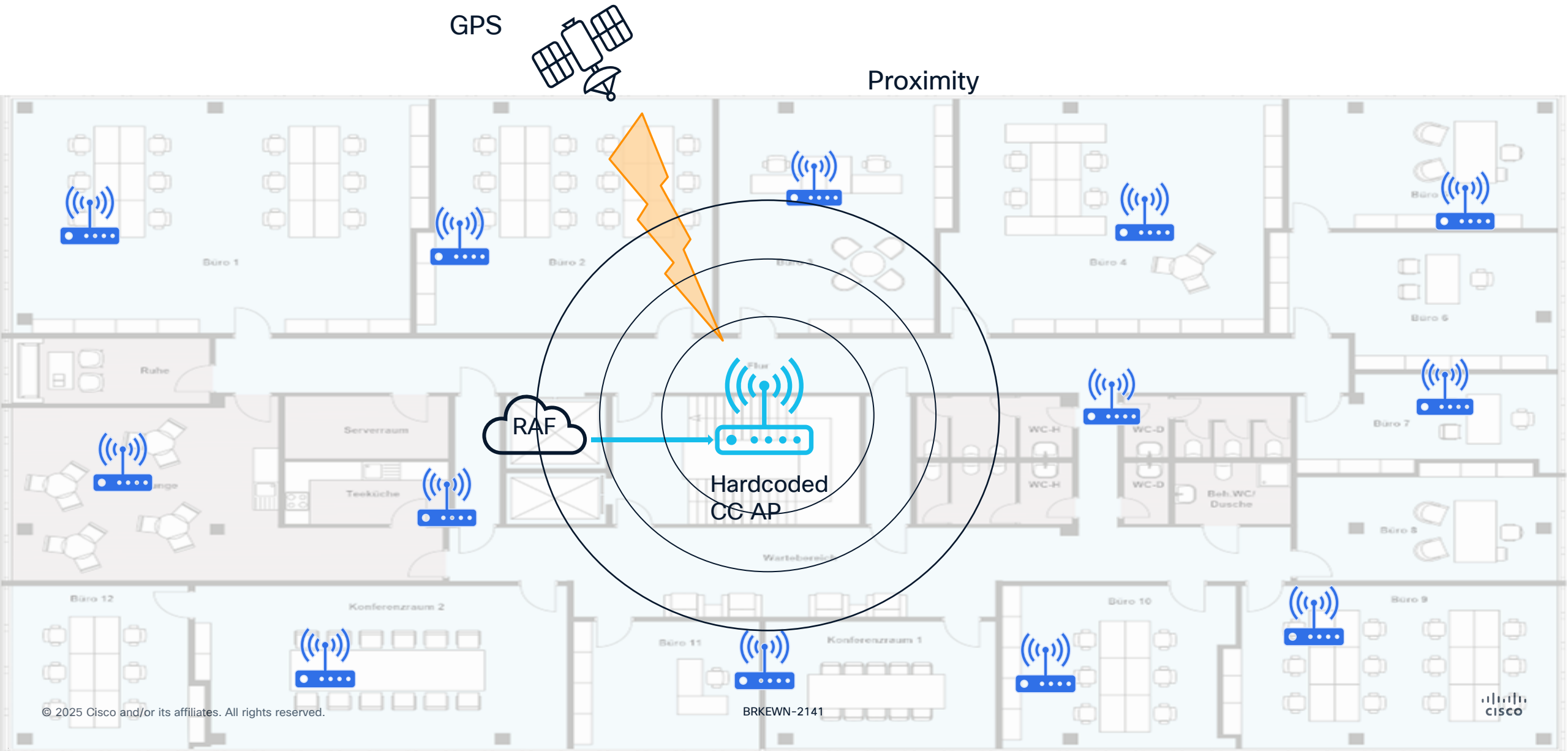
Summary: Regulatory Domain

Method	How Country Is Determined	Best Fit Scenarios	Limitations / Edge Cases	Validation (WLC/AP)
Meraki Cloud (Geo IP)	AP reaches Dashboard; country inferred from Geo IP and stored with device.	Cloud-ready sites; hybrid deployments.	Depends on public IP geolocation accuracy; not applicable in air-gapped sites.	AP:Verify country after mode switch; WLC: show ap name <ap> config general
GPS/GNSS	AP obtains coordinates; WLC maps coordinates to country.	Outdoor/near windows; mobile or temporary sites.	Ignored if < 5 km from national border; indoor/urban can be slow or unavailable.	AP console: “Country Code <XX> resolved through GPS/GNSS”; WLC: show ap name <ap> config general.
Proximity	AP learns country from nearby APs (same WLC) that already have a valid country.	Brownfield/campus with legacy fixed-PID APs or already-resolved GUAPs.	Requires neighbors with valid CC; RF isolation delays resolution.	AP console: “Country Code <XX> resolved through Proximity”; WLC: show ap summary world-wide-mode (should clear).
Regulatory Activation File (RAF)	Signed file mapped per AP MAC → Country; WLC applies to AP.	Greenfield/ air-gapped sites; deterministic rollouts; compliance-driven environments.	Requires pre-staging and MAC mapping; manage lifecycle/audit.	WLC: show ap regulatory activation mac <mac>, show ap regulatory activation all; AP reboot after application.

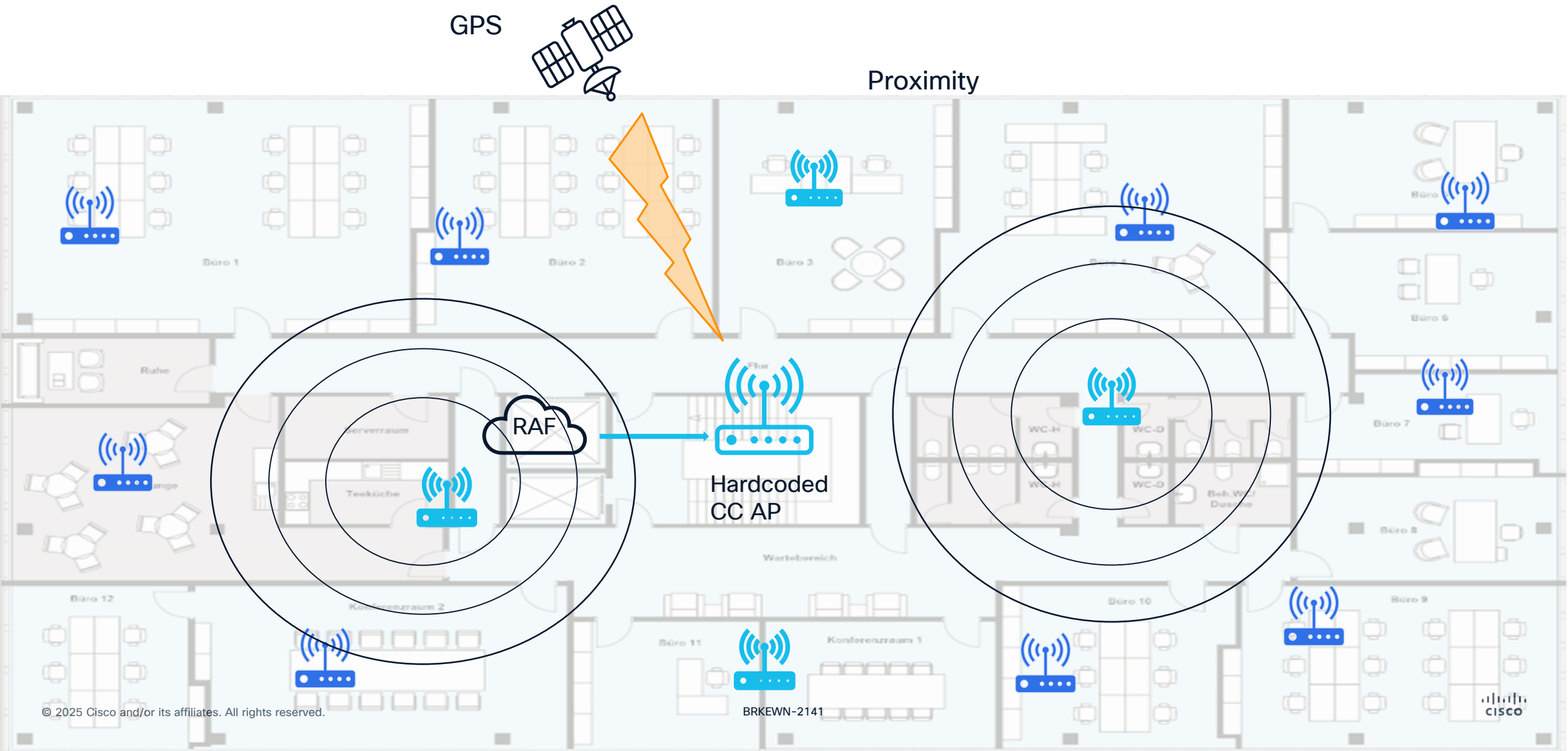
Country Code for Bulk Migration – Best Method



Country Code for Bulk Migration – Best Method

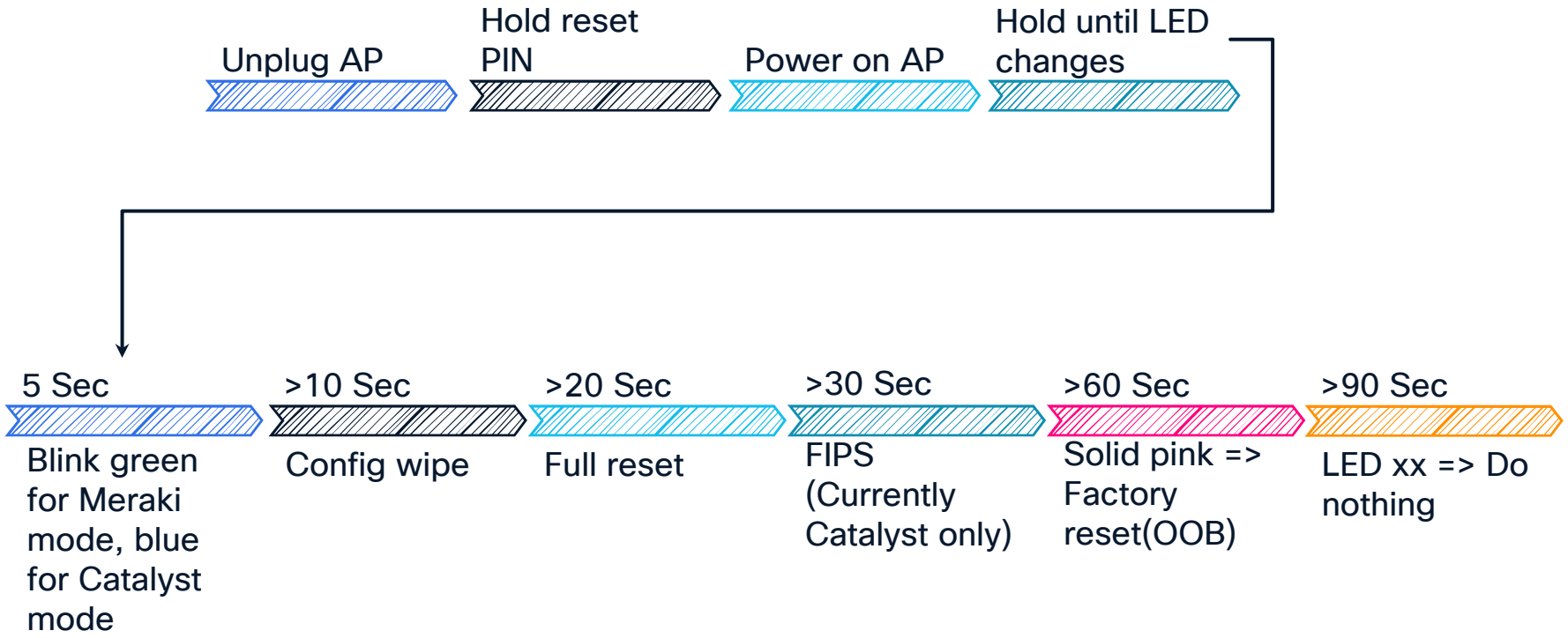


Country Code for Bulk Migration – Best Method



Country Code for Bulk Migration – Best Method

Mode Recovery with Factory Reset

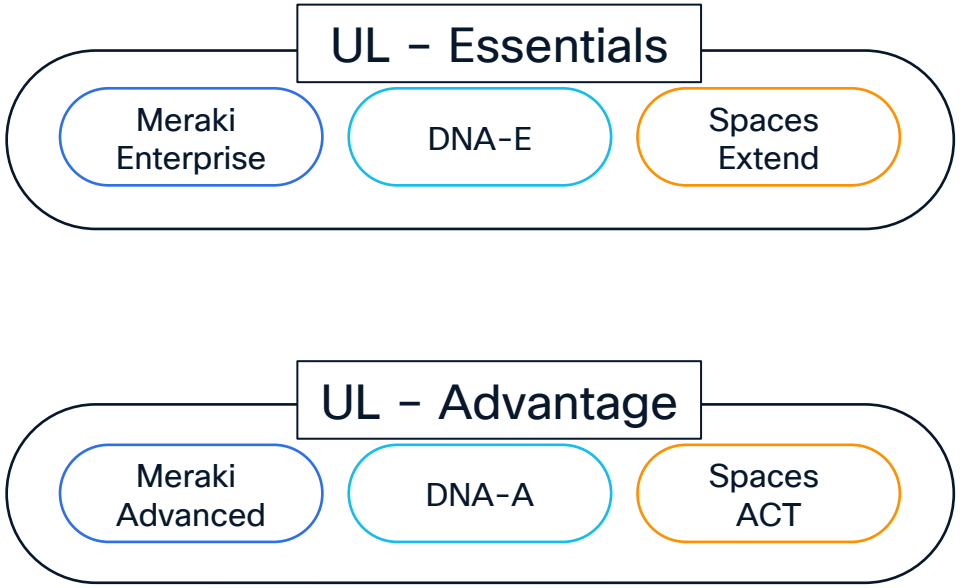



```
Reset button is pressed. Mode = Catalyst
Keep the button pressed for > 10 seconds for config reset
Keep the button pressed for > 20 seconds for full reset
Keep the button pressed for > 30 seconds for FIPS reset
Keep the button pressed for > 60 seconds for deep (factory) reset

Waiting for the button to be released:  7 seconds
```

Unified licensing

- 2 New Licenses
  - LIC-CW-E (Unified License essential)
  - LIC-CW-A (Unified License advantage)
- Benefits of new license-
  - Unified Licensing have Flexibility
    - on-premise, cloud, or hybrid.
    - Adding additional licenses to an existing network.
    - Newly added licenses will automatically inherit the settings of the parent network.

Unified Licensing MVP Launch: Dec 2024



One time set up for non-compliant APs

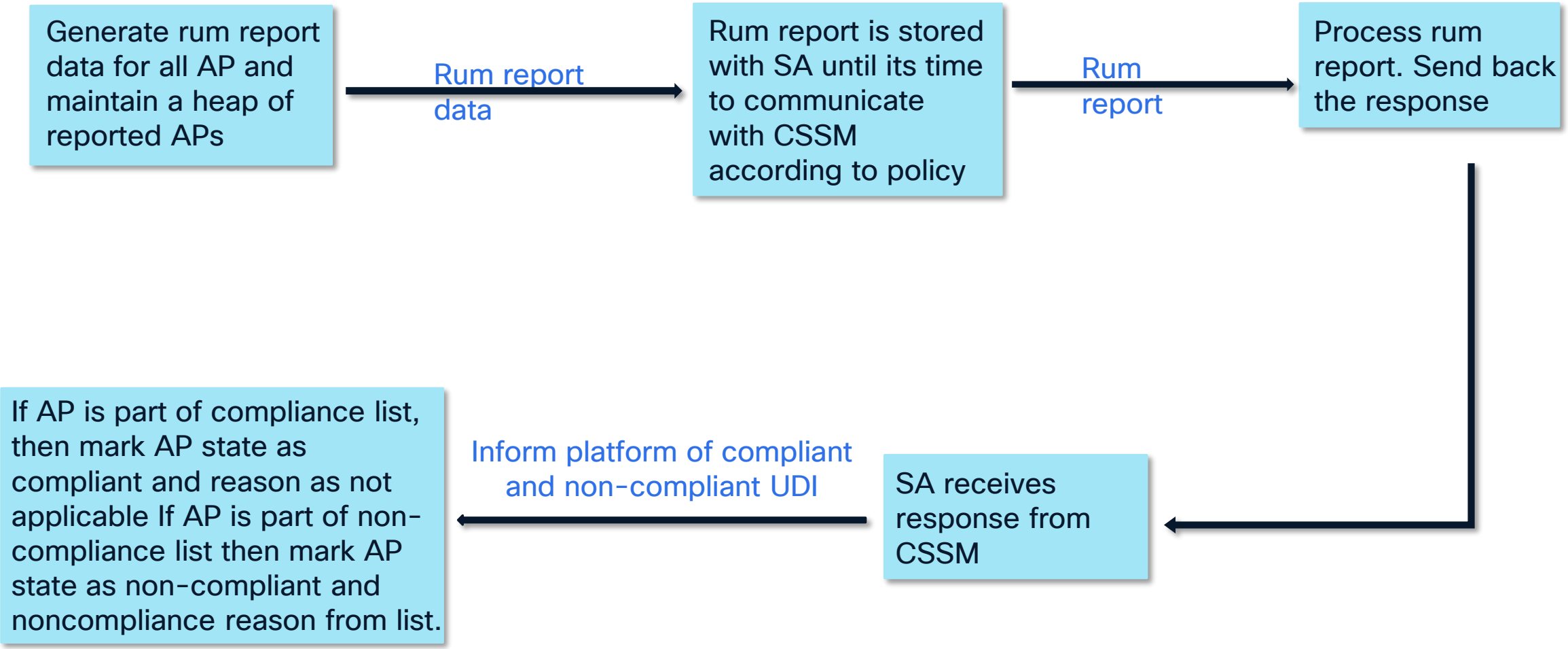
Never Licensed:

- Full device functionality restricted until licensed
- For Cisco Wireless: 2.4GHz only until licensed

License Expiration:

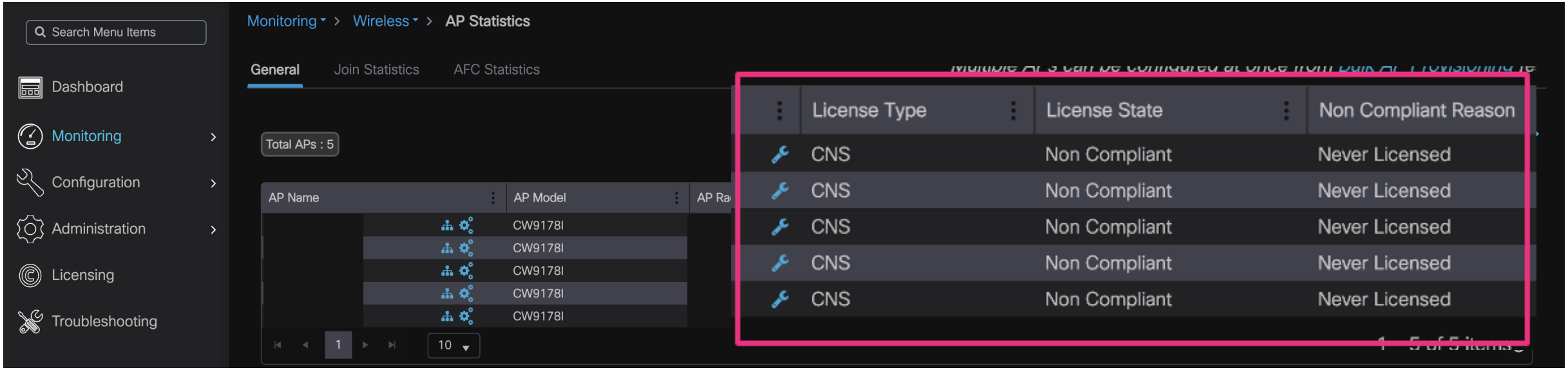
- Devices will continue to pass traffic
- Management and monitoring via Cisco network management platforms will be restricted
- Software updates will be restricted, except for PSIRT and critical bug fixes
- Additional Cisco cloud-based services and features (e.g., Spaces, ISE, TE) included in the management license like add-ons will be restricted
- Access to Cisco Support provided through the subscription will be denied

One time set up for non-compliant APs



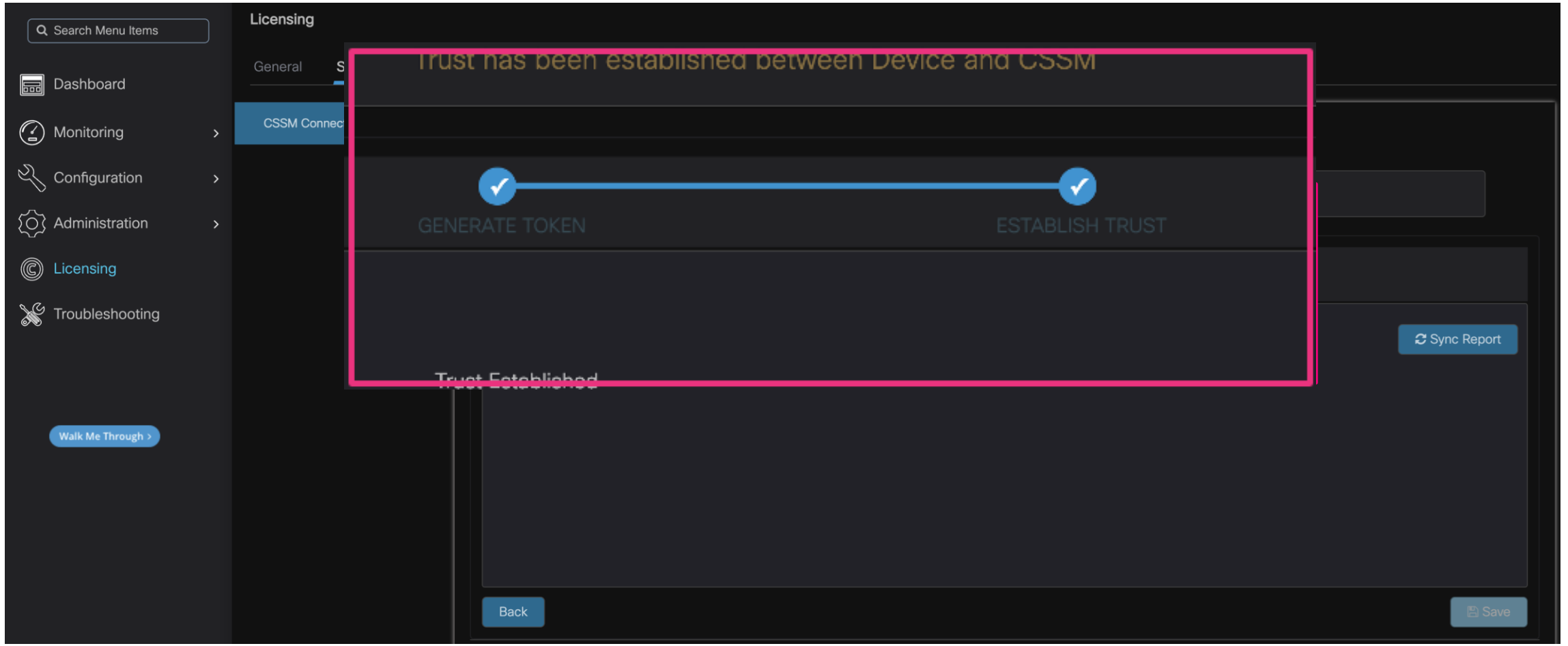
One time set up for non-compliant APs

1



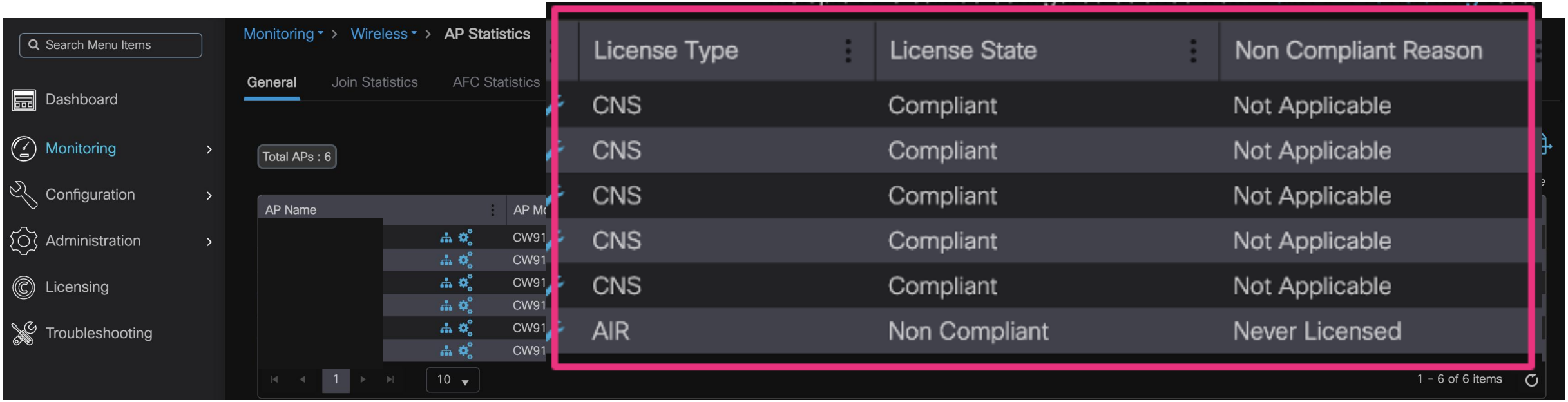
One time set up for non-compliant APs

2



One time set up for non-compliant APs

3



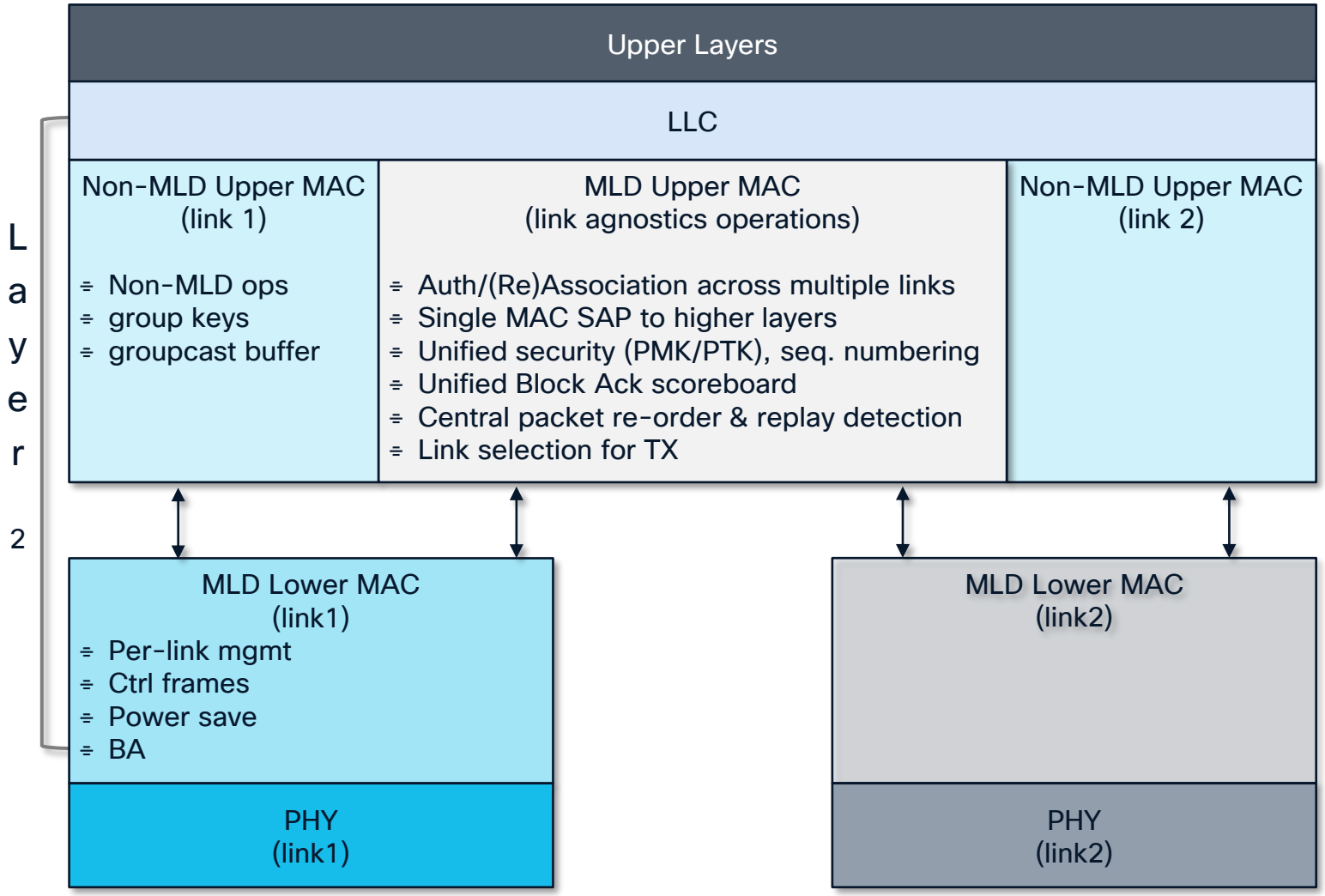
Which is the SSID?

What should I configure?

Is there a change in Client Connection Flow?

Where are my MLD?

Management Changes in .be – MAC Layer



Benefits

- Throughput: Parallel PHY operation in STR mode.
- Reliability: Multi-band/ multi-link path diversity.
- Latency: Steer packets to best-performing link.
- Simplified upper layers: One MAC view regardless of # links.

Initial configuration for Wi-Fi 7

WLAN Config - WLAN should enable all the bands, or atleast 5 and 6 for MLO

Security configs - All the recommended Security Configs for Wi-Fi 7: WPA3/GCMP256, WPA2/AES for 802.1x and OPEN/OWE

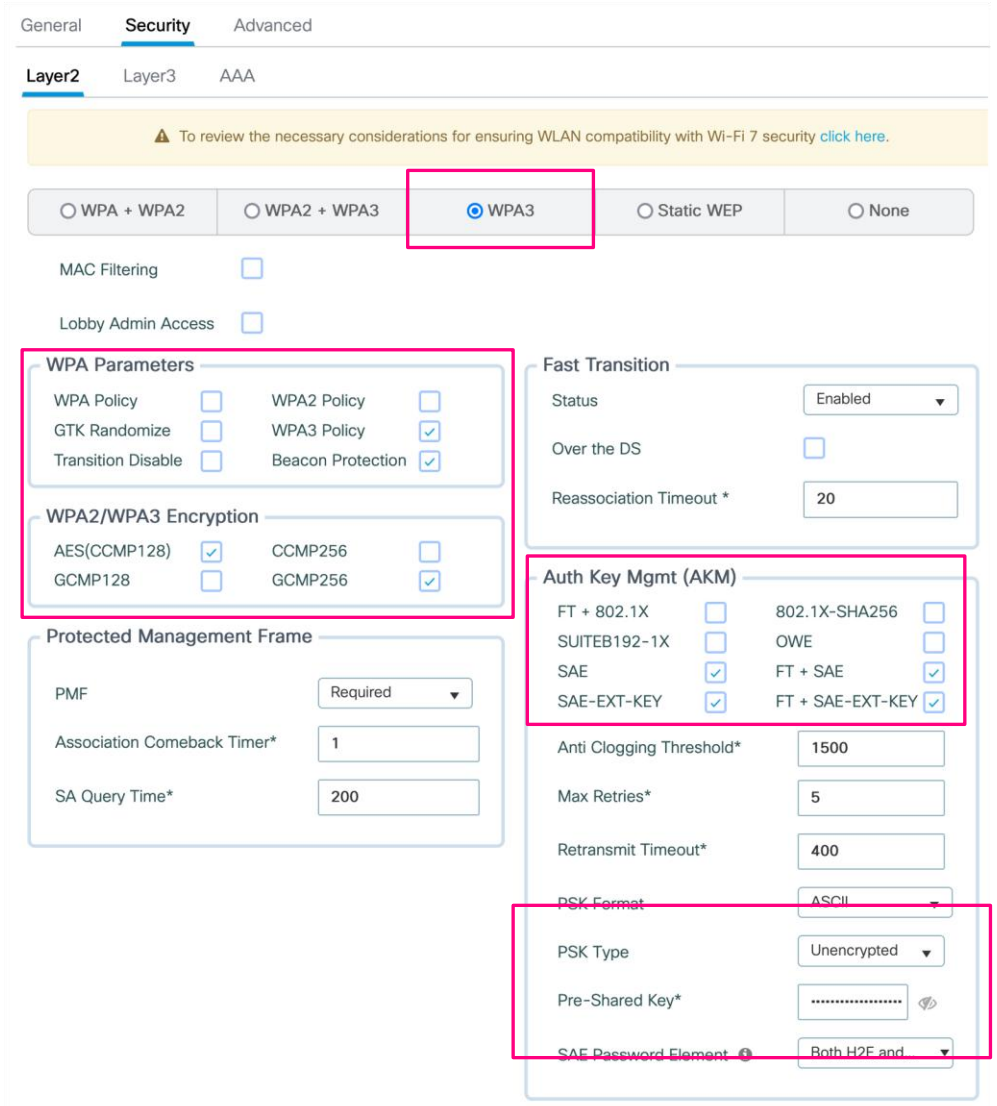
L2 security features for Wi-Fi 7

	Enterprise (802.1X) SSID	Personal (passphrase) SSID	OWE (guest) SSID
WPA2+WPA3 or WPA3	WPA2+WPA3 allowed today	WPA3 only	WPA3 only
Beacon Protection	Mandatory	Mandatory	Mandatory
AES (CCMP 128)	The minimum mandatory today	Allowed (for earlier standards too)	Allowed (for earlier standards too)
GCMP 256	Optional today	Mandatory	Mandatory
PMF Required	Mandatory	Mandatory	Mandatory
Fast Transition	Highly recommended*	Highly recommended**	Disabled
AKMs	• 802.1X (SHA1) for earlier standards • 802.1X-SHA256 mandatory • FT + 802.1X (SHA256) highly recommended*	• SAE for earlier standards • FT + SAE highly recommended** for earlier standards • SAE-EXT-KEY mandatory • FT + SAE-EXT-KEY highly recommended**	OWE (no Transition Mode)

* FT + 802.1X uses SHA256 (although not explicit in the name), which can be used for Wi-Fi 7 along with “plain” 802.1X-SHA256

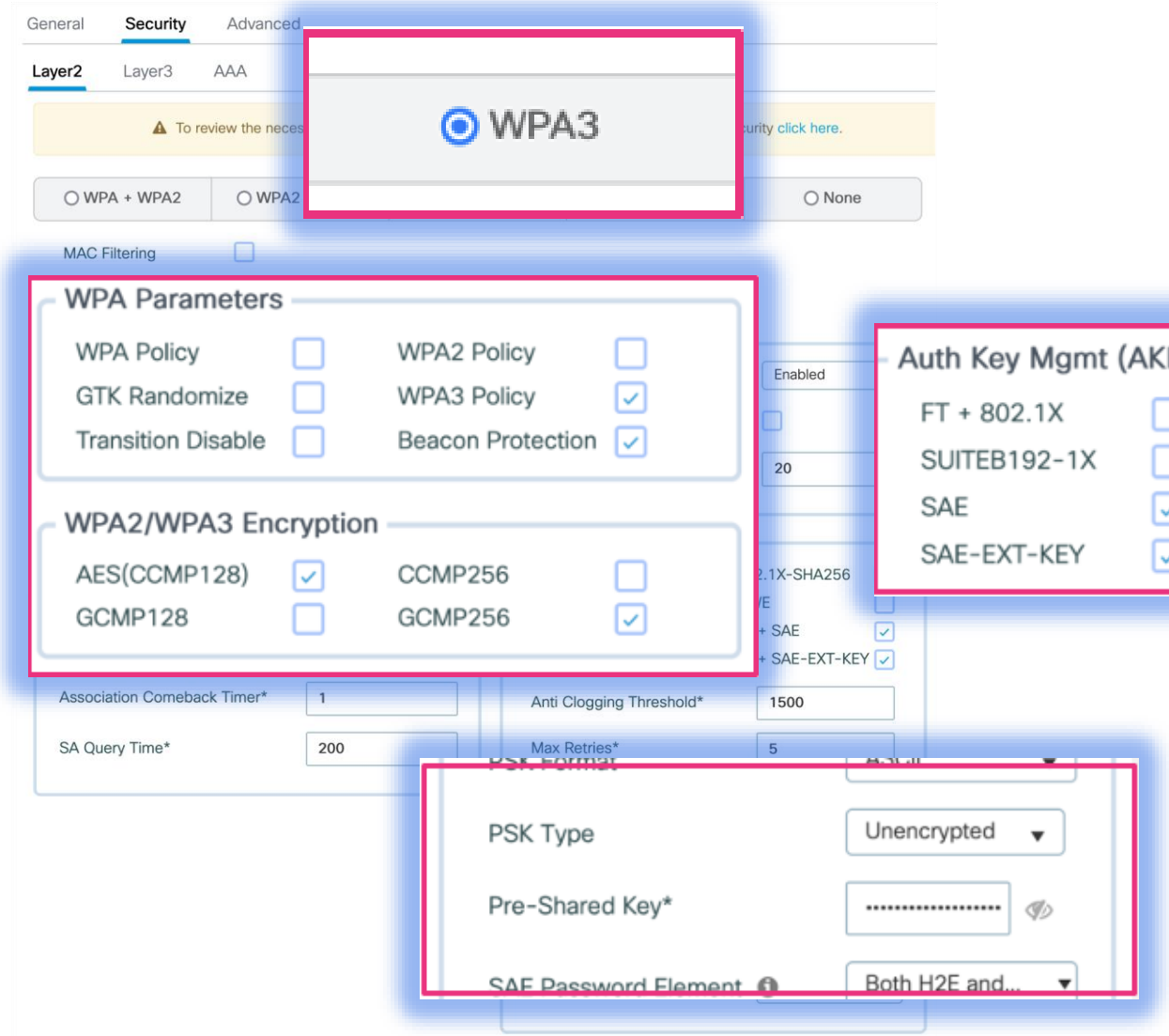
** When using SAE the key derivation process is much longer than with the former PSK.
For being able to speed things up in case of roaming, some clients refuse to associate in the first place if FT is not enabled.

9800 Personal (passphrase) for Wi-Fi 7



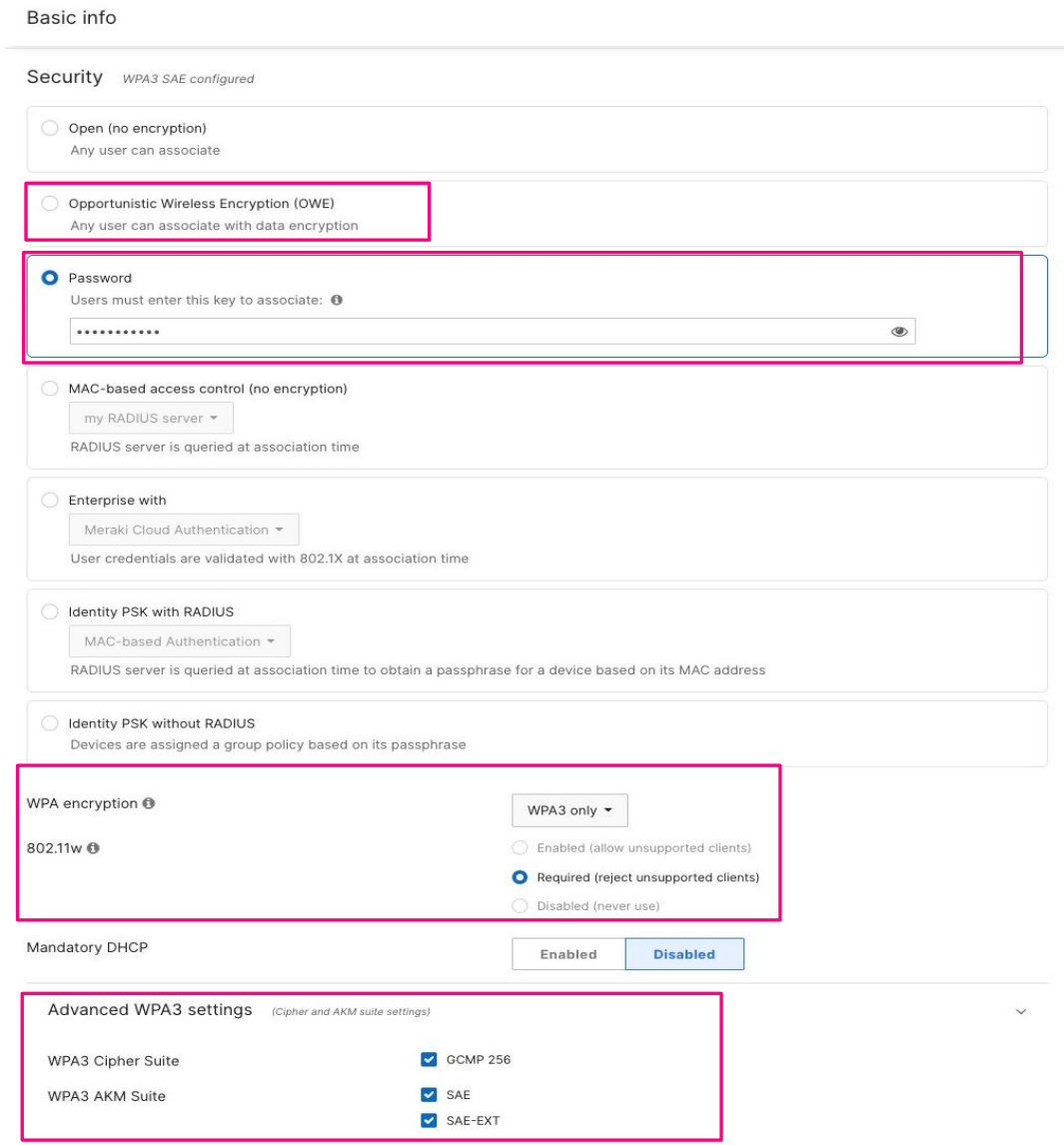
- WPA3 settings:
  - Beacon Protection
  - AES(CCMP128)
  - GCMP256
  - PMF: Required (for Device Analytics too) Fast Transition: Enabled
- AKM:
  - SAE, FT + SAE
  - SAE-EXT-KEY, FT + SAE-EXT-KEY
  - Fast Transition / 802.11r = Enabled
  - No “Adaptive Enabled”, as it would benefit Apple/Samsung endpoints only
  - Over the DS = unchecked
  - Over the Air (OTA) is the technique all endpoints are supporting

9800 Personal (passphrase) for Wi-Fi 7

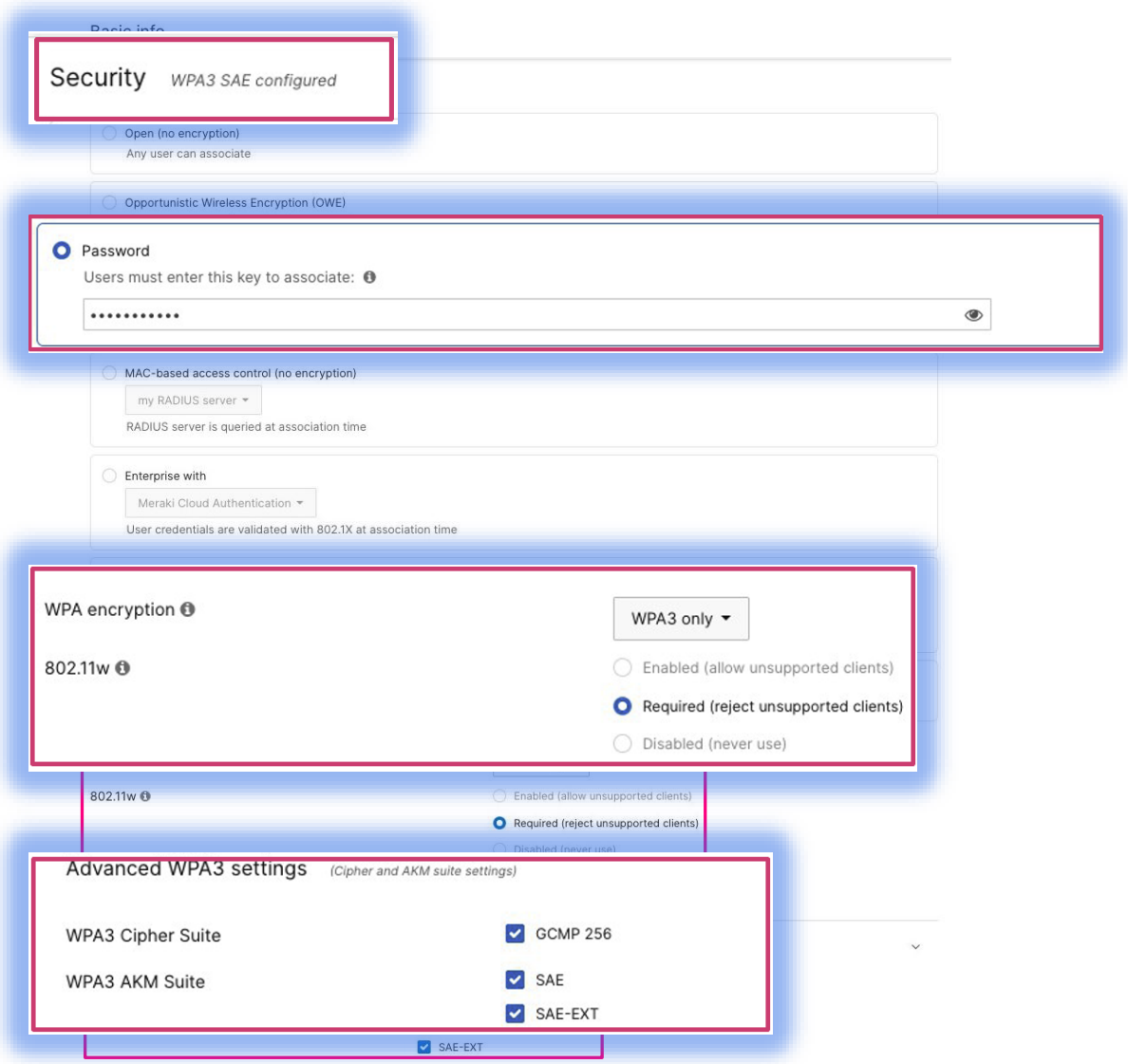


- WPA3 settings:
  - Beacon Protection
  - AES(CCMP128)
  - GCMP256
  - PMF: Required (for Device Analytics too) Fast Enabled
  - SAE
  - KEY, FT + SAE-EXT-KEY
  - Fast Transition / 802.11r = Enabled
  - No “Adaptive Enabled”, as it would benefit Apple/Samsung endpoints only
  - Over the DS = unchecked
  - Over the Air (OTA) is the technique all endpoints are supporting

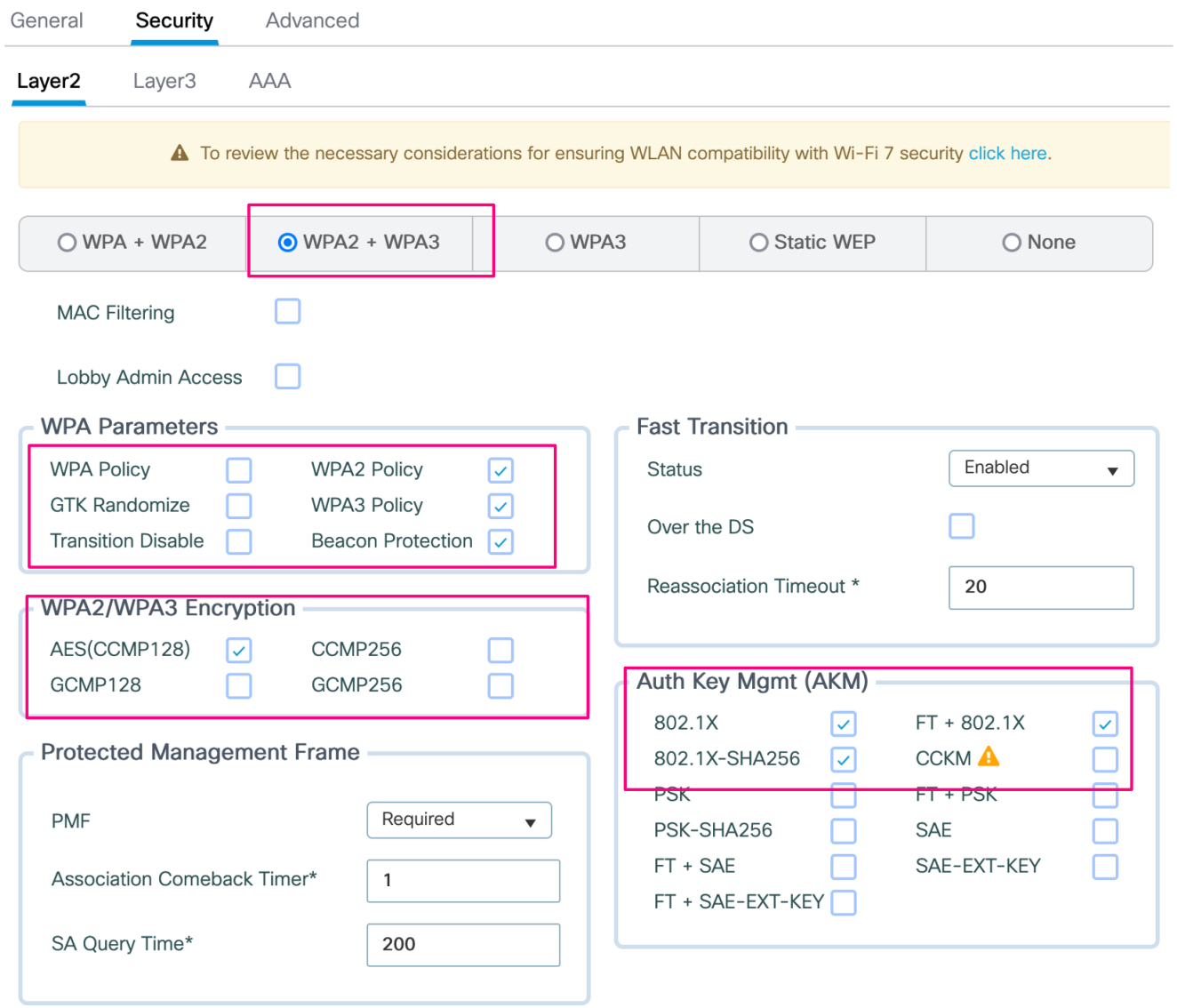
Meraki Personal (passphrase) for Wi-Fi 7



Meraki Personal (passphrase) for Wi-Fi 7

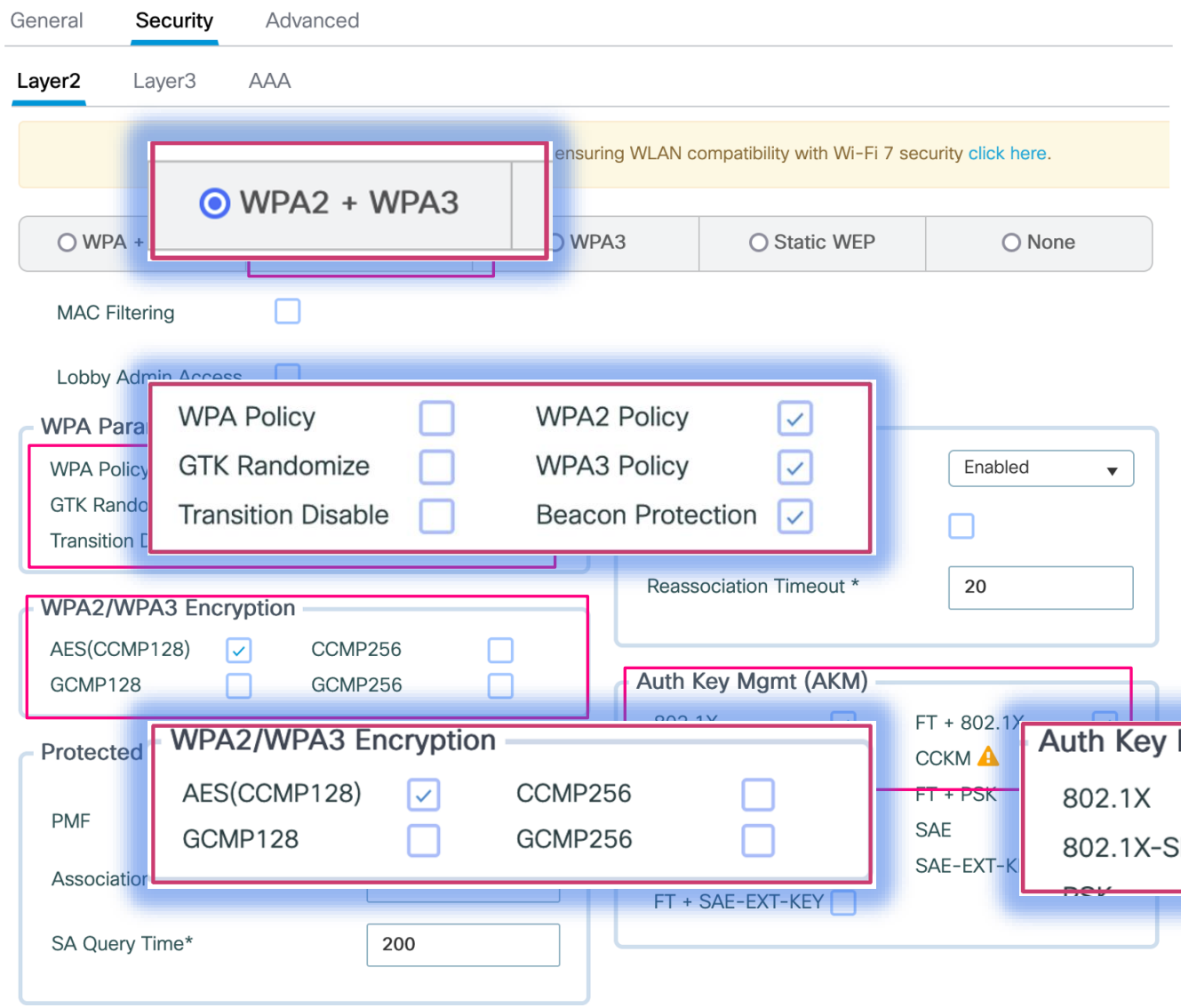


9800 Enterprise (802.1X) for Wi-Fi 7



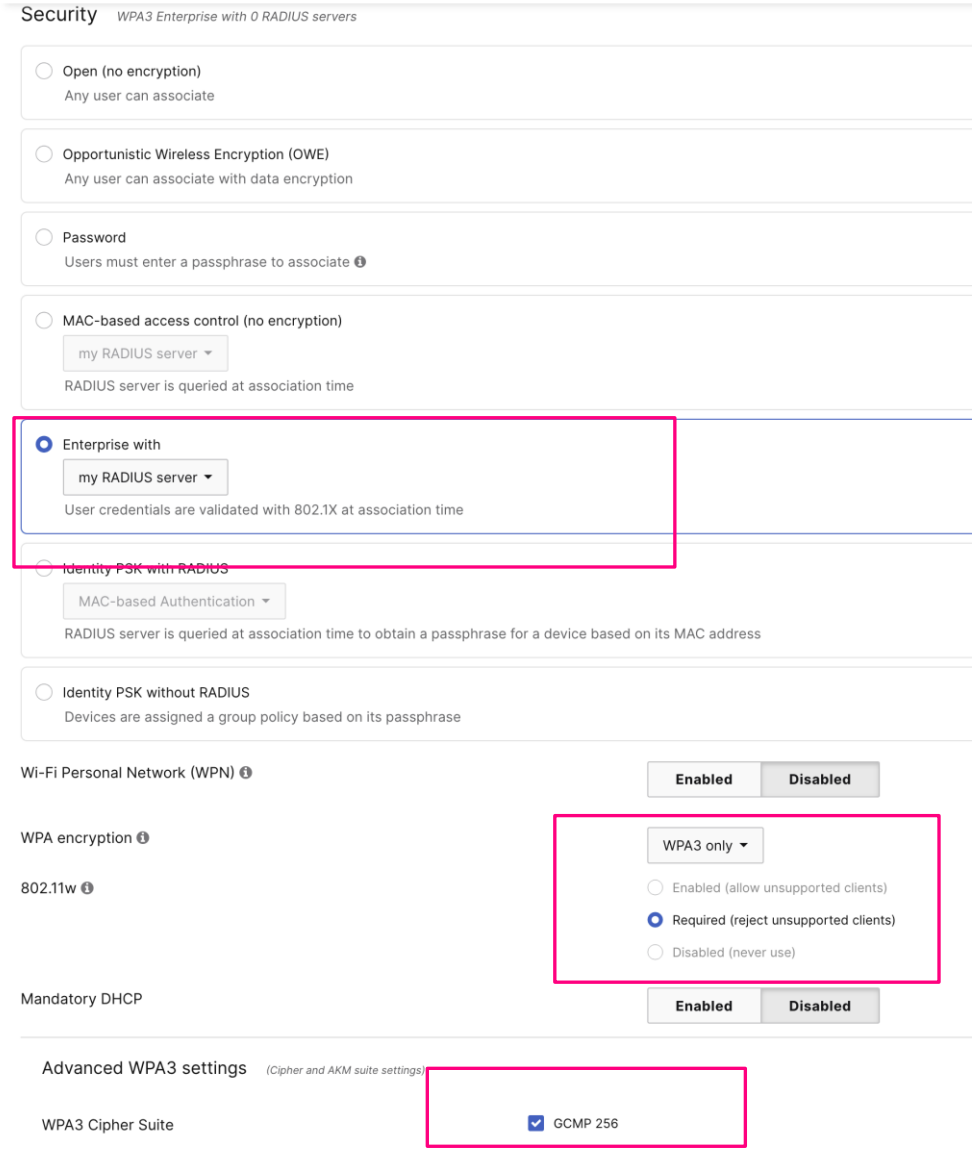
- WPA2/WPA3 settings:
  - Beacon Protection
  - AES(CCMP128)
  - PMF: Required (for Device Analytics too) Fast Transition: Enabled
- AKM:
  - 802.1X
  - FT + 802.1X
  - 802.1X-SHA256
- Fast Transition / 802.11r = Enabled
  - No “Adaptive Enabled”, as it would benefit Apple/Samsung endpoints only
  - Over the DS = unchecked
  - Over the Air (OTA) is the technique all endpoints are supporting

9800 Enterprise (802.1X) for Wi-Fi 7

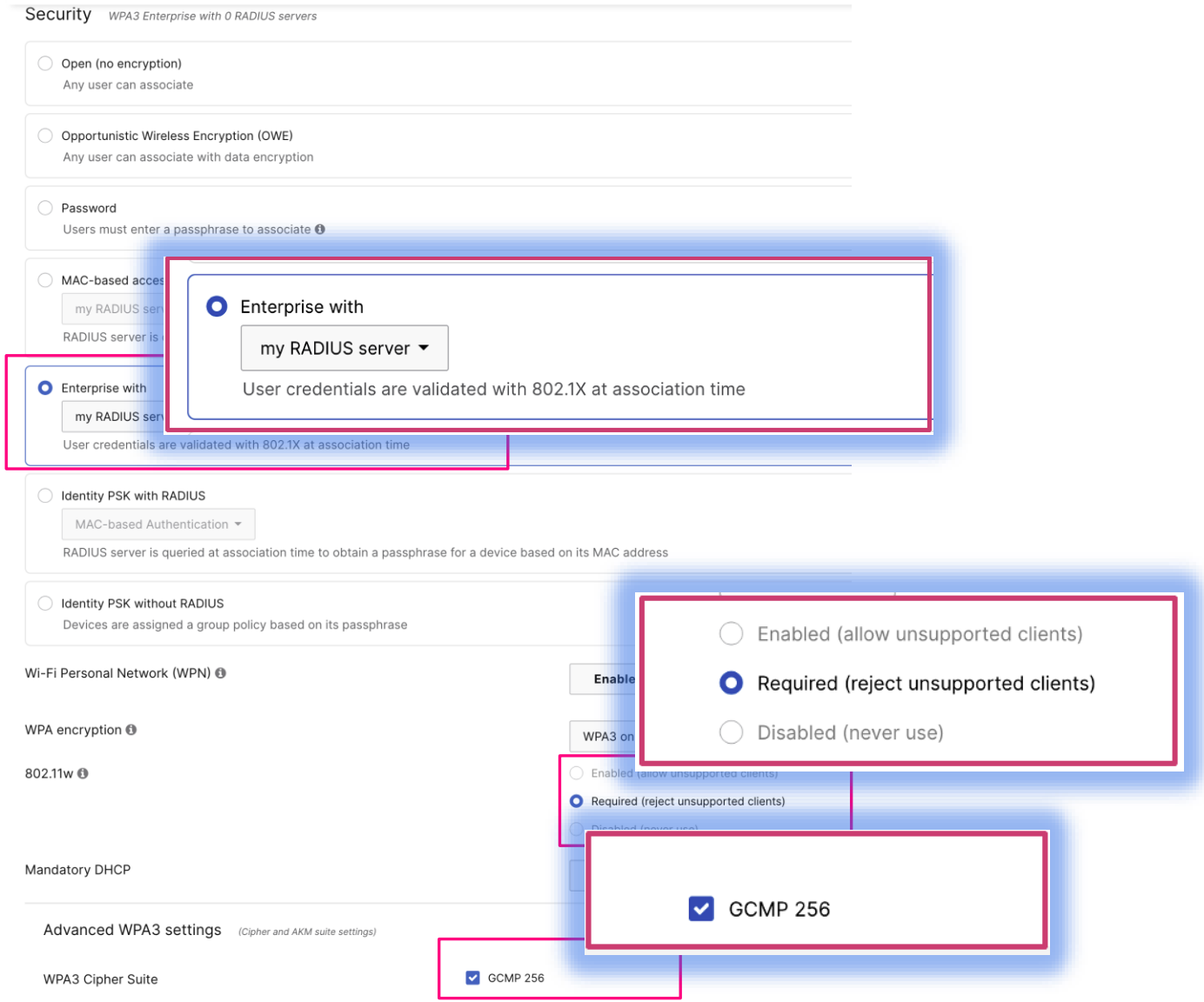


- WPA2/WPA3 settings:
  - Beacon Protection
  - AES(CCMP128)
  - PMF: Required (for Device Analytics too) Fast Transition: Enabled
- AKM:
  - 802.1X
  - FT + 802.1X
  - 802.1X-SHA256
- Fast Transition / 802.11r = Enabled
  - No “Adaptive Enabled”, as it would benefit ints only
  - ked
  - he technique all endpoints are supporting

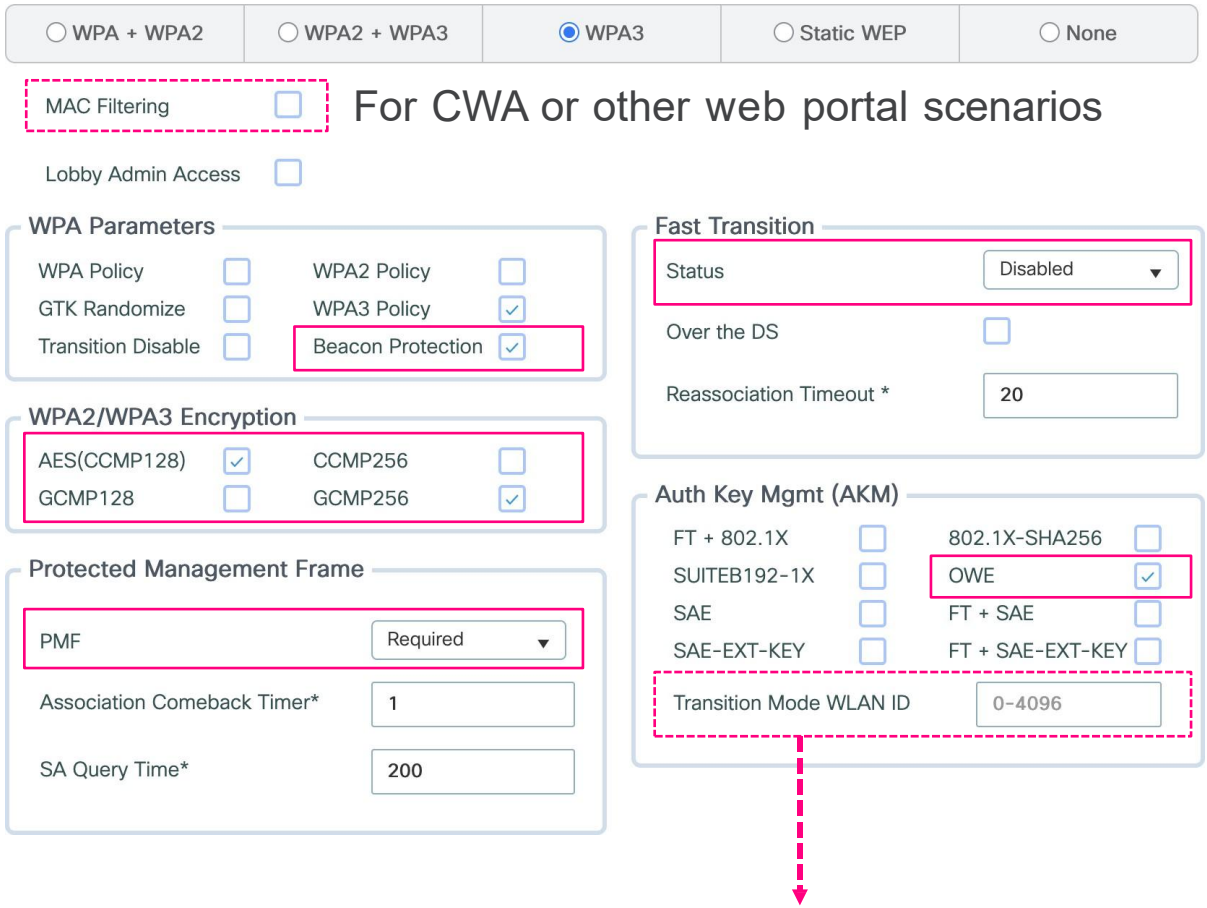
Meraki Enterprise (802.1X) for Wi-Fi 7



Meraki Enterprise (802.1X) for Wi-Fi 7



9800 OWE for Wi-Fi 7

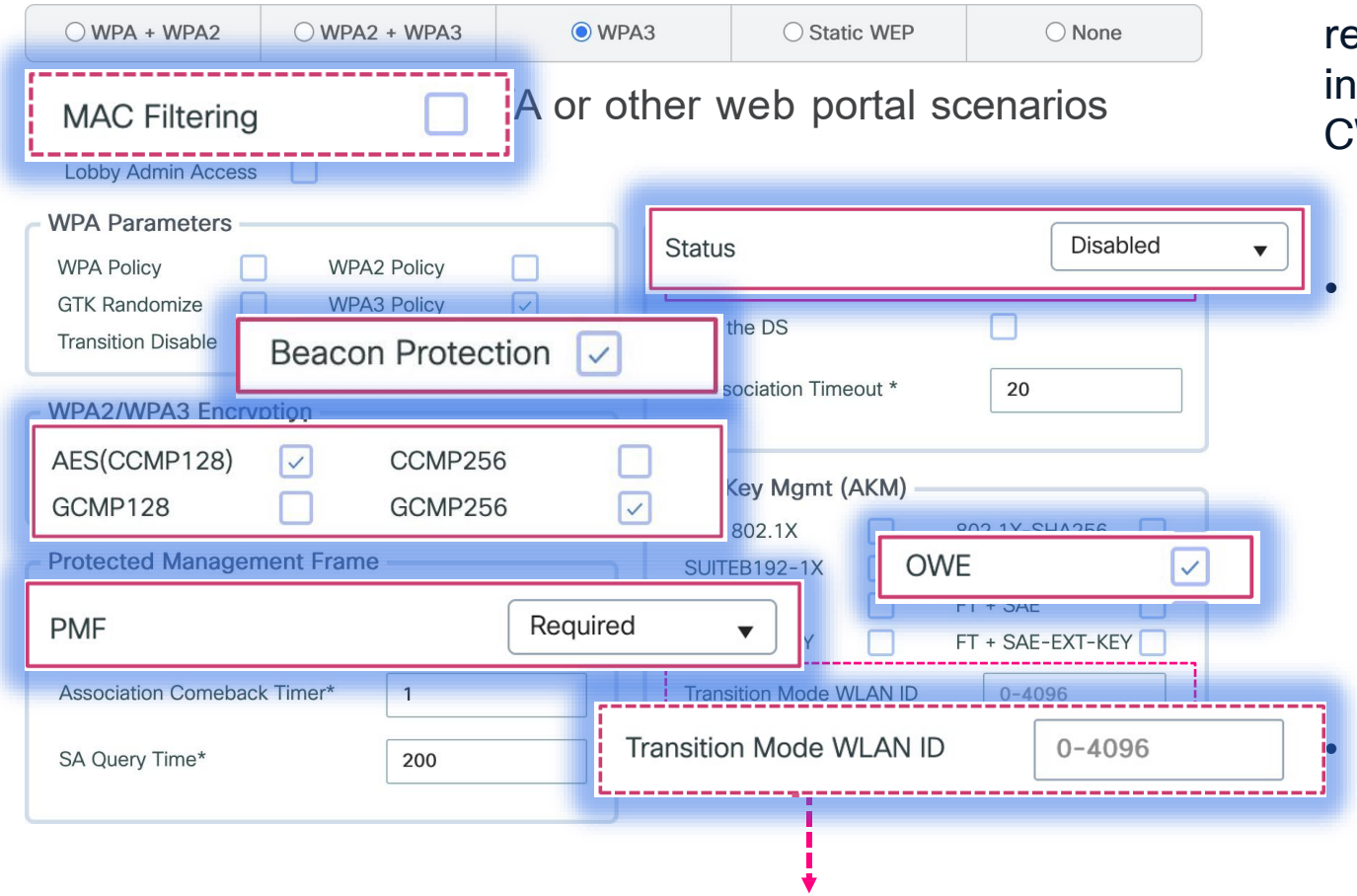


No Transition Mode if we want to keep support for 6 GHz / Wi-Fi 6E / Wi-Fi 7

Note: OWE still supports any type of portal redirection technique, just like other SSIDs (9800's internal web portal, external web portals, LWA, CWA, Spaces, etc.)

- WPA3 settings:
  - Beacon Protection
  - AES(CCMP128)
  - GCMP256
  - PMF: Required
  - Fast Transition: Disabled
- AKM: OWE

9800 OWE for Wi-Fi 7

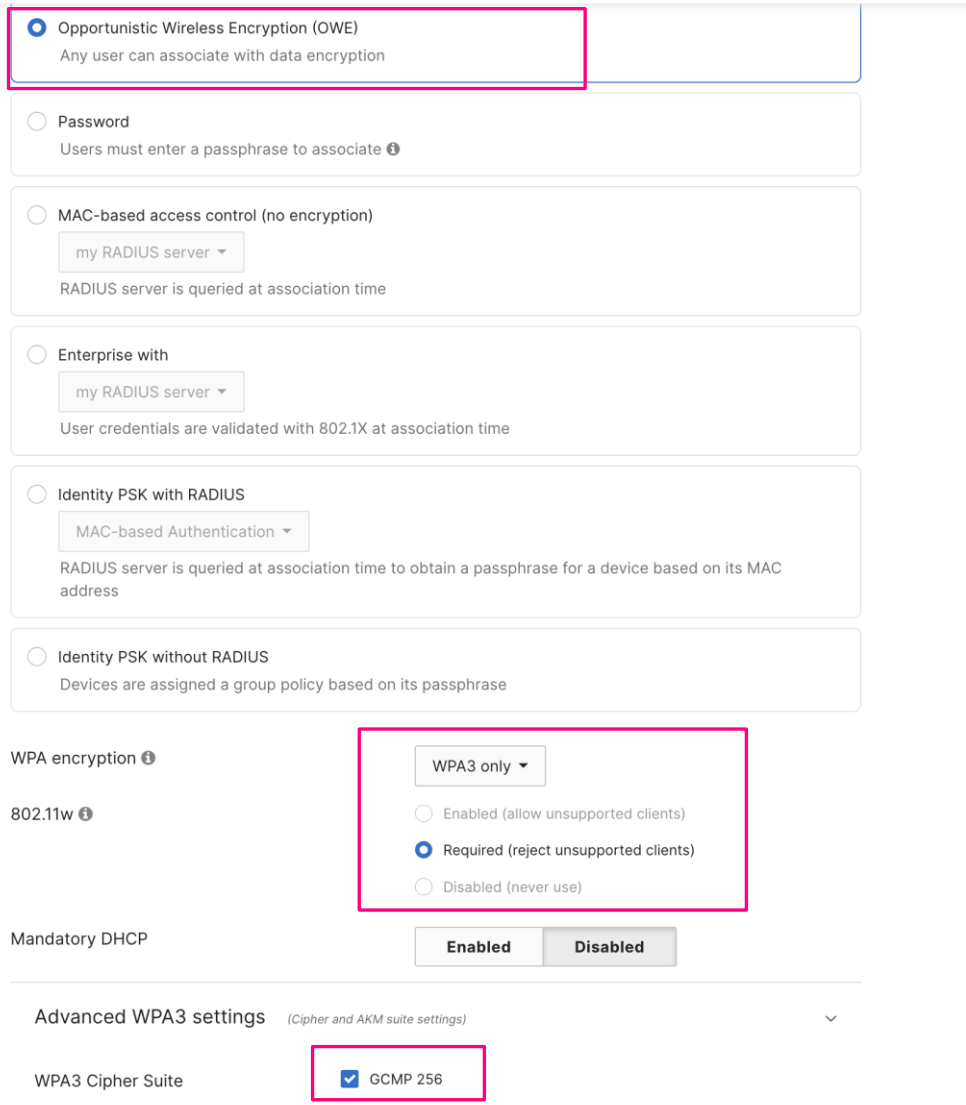


No Transition Mode if we want to keep support for 6 GHz / Wi-Fi 6E / Wi-Fi 7

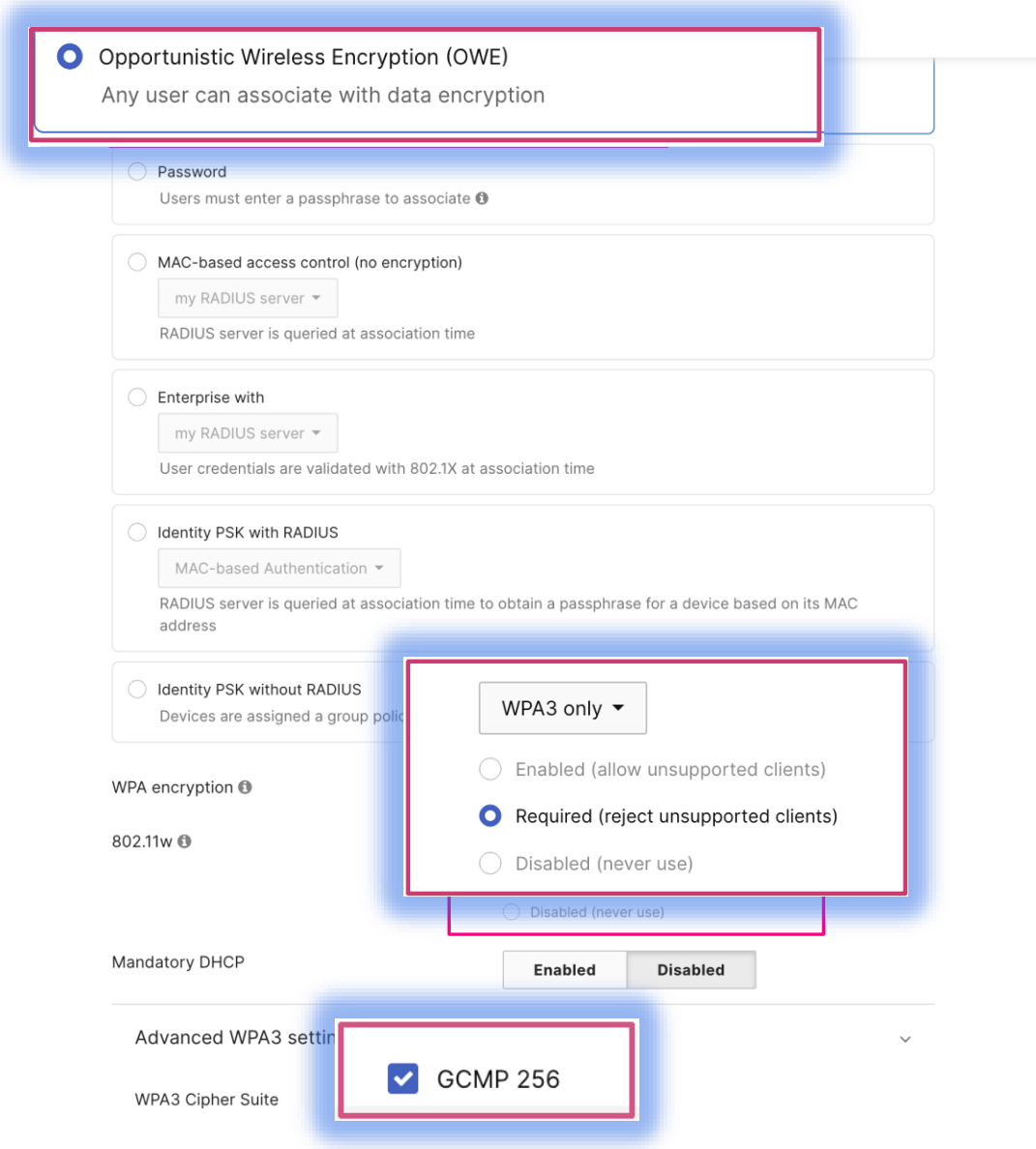
Note: OWE still supports any type of portal redirection technique, just like other SSIDs (9800's internal web portal, external web portals, LWA, CWA, Spaces, etc.)

- WPA3 settings:
  - Beacon Protection
  - AES(CCMP128)
  - GCMP256
  - PMF: Required
  - Fast Transition: Disabled
- AKM: OWE

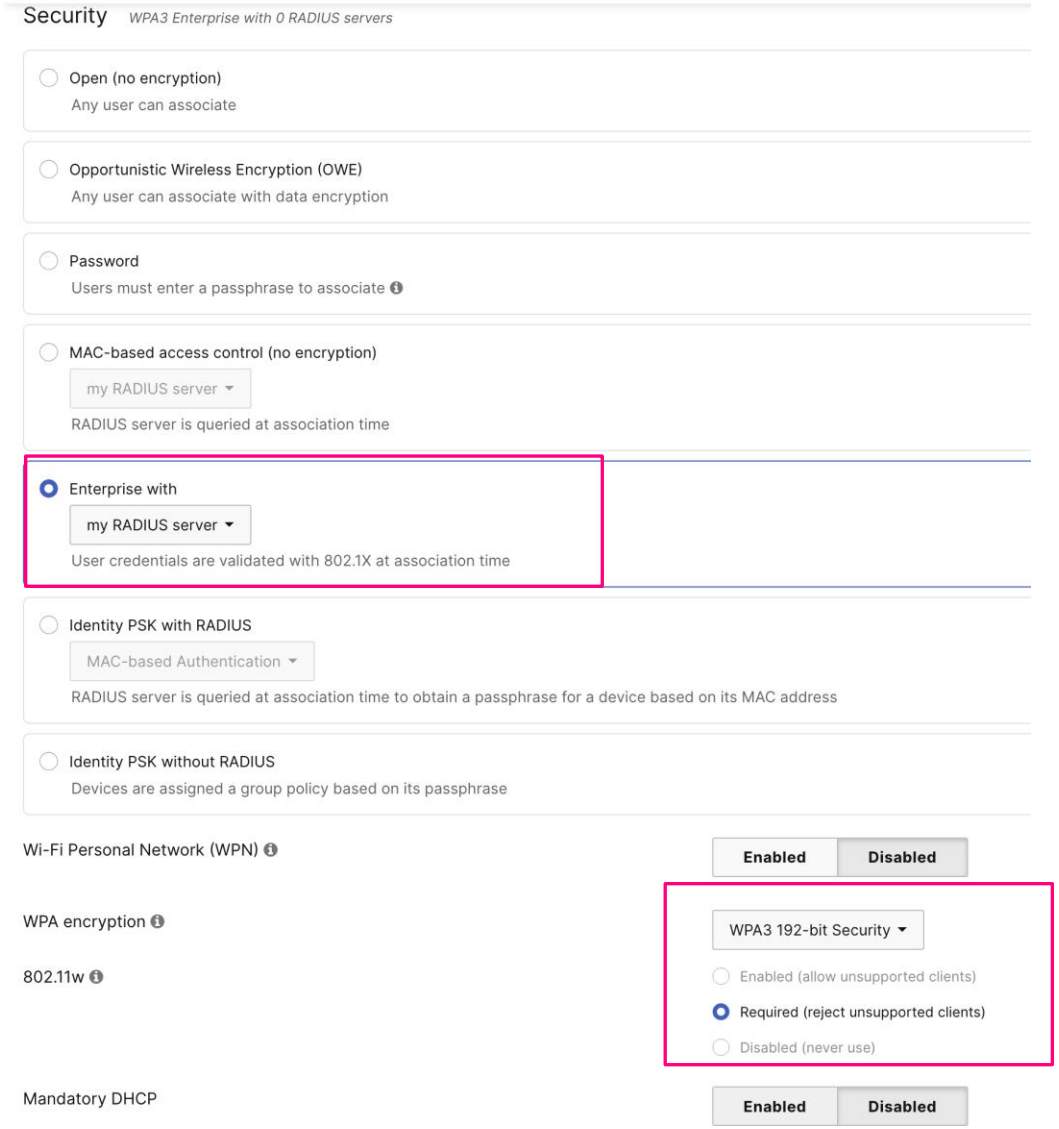
Meraki OWE for Wi-Fi 7



Meraki OWE for Wi-Fi 7



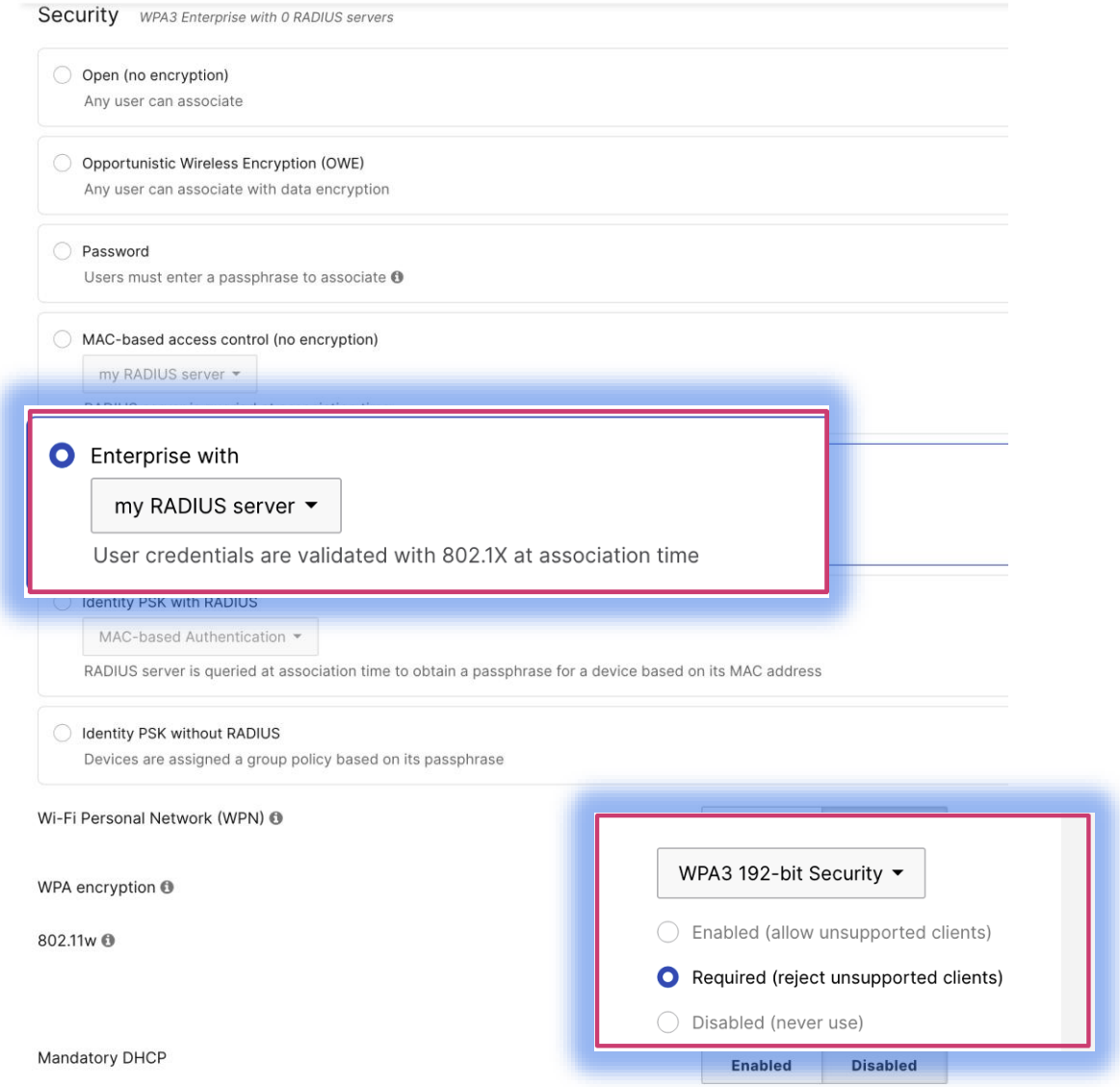
Meraki Enterprise (802.1X) for Wi-Fi 7 – WPA3 192-bit



Note:

- SuiteB – 192 Bit SSID will only be supported on SSIDs #13 – #15.
- This is to ensure that the correct MBSSID grouping is enabled for all types of SSIDs on the network.

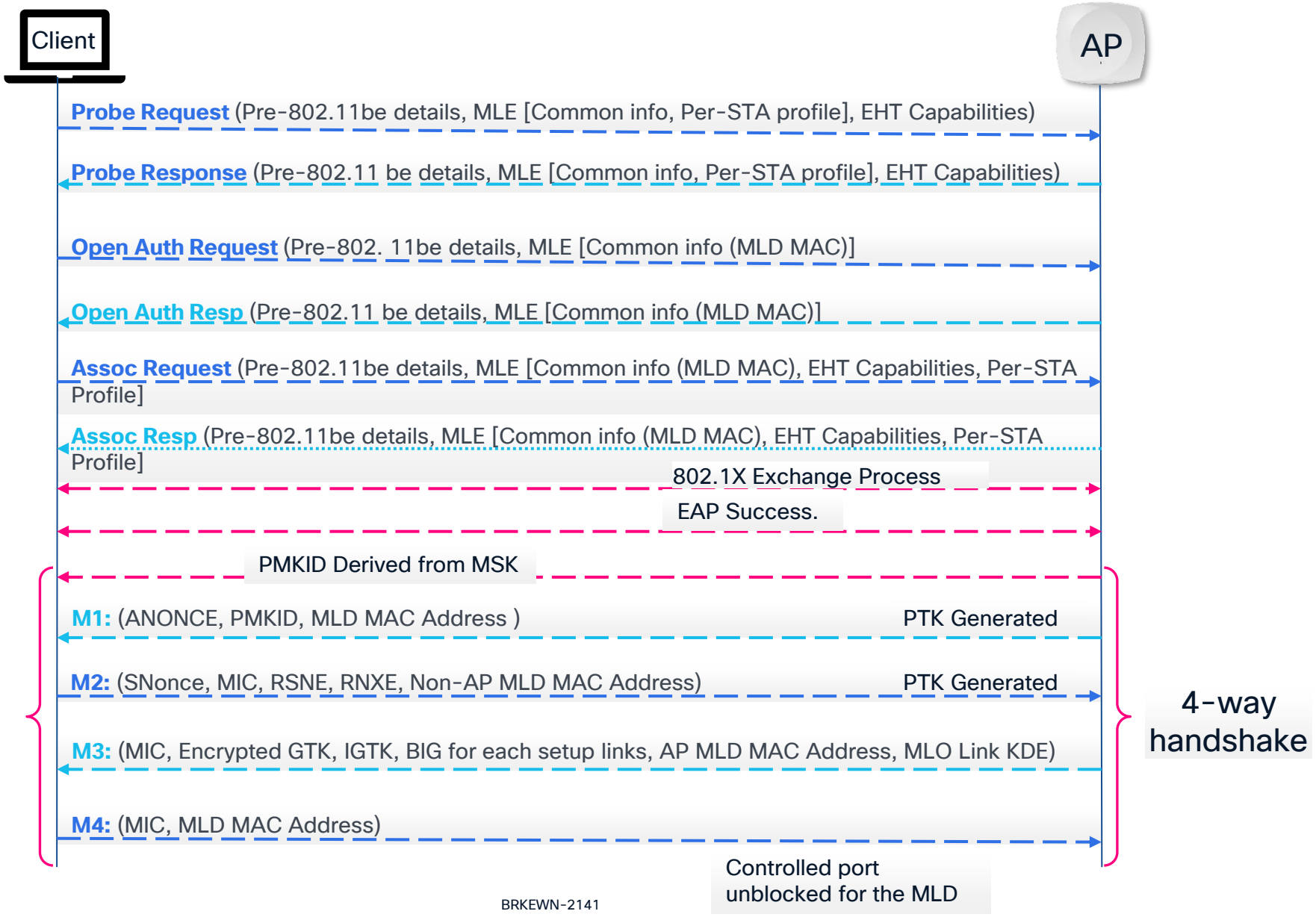
Meraki Enterprise (802.1X) for Wi-Fi 7 – WPA3 192-bit



Note:

- SuiteB – 192 Bit SSID will only be supported on SSIDs #13 – #15.
- This is to ensure that the correct MBSSID grouping is enabled for all types of SSIDs on the network.

MLO – Client connection



No.	Time	Source	Destination	Protocol	Length	Channel	Info
1187163	09:05:35.988097	Microsoft_b4:05:25	Cisco_6a:00:02	802.11	264	1	Probe Request, SN=256, FN=0, Flags=........C, SSID="Ghost"
1187170	09:05:35.991821	Cisco_6a:00:02	Microsoft_b4:05:…	802.11	439	1	Probe Response, SN=3829, FN=0, Flags=........C, BI=100, SSID="Ghost"
1187171	09:05:35.991821	Cisco_6a:00:02	Microsoft_b4:05:…	802.11	439	1	Probe Response, SN=3829, FN=0, Flags=....R...C, BI=100, SSID="Ghost"
1187195	09:05:36.004695	Cisco_6a:00:02	Microsoft_b4:05:…	802.11	96	1	Authentication, SN=3830, FN=0, Flags=........C
1187229	09:05:36.016394	Microsoft_b4:05:25	Cisco_6a:00:02	802.11	261	1	Association Request, SN=258, FN=0, Flags=........C, SSID="Ghost"
1187230	09:05:36.016394	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187274	09:05:36.037190	Cisco_6a:00:02	Microsoft_b4:05:…	802.11	275	1	Association Response, SN=0, FN=0, Flags=........C
1187293	09:05:36.043510	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	109	1	Request, Identity
1187450	09:05:36.101704	Microsoft_b4:05:25	Cisco_6a:00:02	EAPOL	105	1	Start
1187451	09:05:36.101704	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187456	09:05:36.101704	Microsoft_b4:05:25	Cisco_6a:00:02	EAP	116	1	Response, Identity
1187457	09:05:36.101704	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187461	09:05:36.101704	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	109	1	Request, Identity
1187476	09:05:36.103895	Microsoft_b4:05:25	Cisco_6a:00:02	EAP	116	1	Response, Identity
1187477	09:05:36.103895	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187495	09:05:36.116661	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	110	1	Request, TLS EAP (EAP-TLS)
1187503	09:05:36.116661	Microsoft_b4:05:25	Cisco_6a:00:02	EAP	110	1	Response, Legacy Nak (Response Only)
1187504	09:05:36.116661	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187522	09:05:36.126040	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	110	1	Request, Protected EAP (EAP-PEAP)
1187536	09:05:36.133694	Microsoft_b4:05:25	Cisco_6a:00:02	TLSv1.2	541	1	Client Hello
1187537	09:05:36.133694	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187596	09:05:36.163551	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	1116	1	Request, Protected EAP (EAP-PEAP)
1187610	09:05:36.164695	Microsoft_b4:05:25	Cisco_6a:00:02	EAP	110	1	Response, Protected EAP (EAP-PEAP)
1187611	09:05:36.164695	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187624	09:05:36.177234	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	1112	1	Request, Protected EAP (EAP-PEAP)
1187651	09:05:36.182448	Microsoft_b4:05:25	Cisco_6a:00:02	EAP	110	1	Response, Protected EAP (EAP-PEAP)
1187652	09:05:36.182448	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187678	09:05:36.188368	Cisco_6a:00:02	Microsoft_b4:05:…	TLSv1.2	186	1	Server Hello, Certificate, Server Key Exchange, Server Hello Done
1187697	09:05:36.198058	Microsoft_b4:05:25	Cisco_6a:00:02	TLSv1.2	272	1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1187698	09:05:36.198058	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187714	09:05:36.215855	Cisco_6a:00:02	Microsoft_b4:05:…	TLSv1.2	161	1	Change Cipher Spec, Encrypted Handshake Message
1187741	09:05:36.215855	Microsoft_b4:05:25	Cisco_6a:00:02	EAP	110	1	Response, Protected EAP (EAP-PEAP)
1187742	09:05:36.215855	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187763	09:05:36.225750	Cisco_6a:00:02	Microsoft_b4:05:…	TLSv1.2	140	1	Application Data
1187823	09:05:36.256155	Microsoft_b4:05:25	Cisco_6a:00:02	TLSv1.2	147	1	Application Data
1187824	09:05:36.256155	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187841	09:05:36.267231	Microsoft_b4:05:25	Cisco_6a:00:02	TLSv1.2	201	1	Application Data
1187842	09:05:36.267231	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187908	09:05:36.284500	Cisco_6a:00:02	Microsoft_b4:05:…	TLSv1.2	186	1	Application Data
1187924	09:05:36.288219	Microsoft_b4:05:25	Cisco_6a:00:02	TLSv1.2	141	1	Application Data
1187925	09:05:36.288219	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1187952	09:05:36.297200	Cisco_6a:00:02	Microsoft_b4:05:…	TLSv1.2	150	1	Application Data
1187954	09:05:36.297200	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	150	1	Request, Protected EAP (EAP-PEAP)
1187959	09:05:36.300909	Microsoft_b4:05:25	Cisco_6a:00:02	TLSv1.2	150	1	Application Data
1187960	09:05:36.300909	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1188023	09:05:36.327186	Cisco_6a:00:02	Microsoft_b4:05:…	EAP	108	1	Success
1188032	09:05:36.332982	Cisco_6a:00:02	Microsoft_b4:05:…	EAPOL	221	1	Key (Message 1 of 4)
1188045	09:05:36.338095	Microsoft_b4:05:25	Cisco_6a:00:02	EAPOL	223	1	Key (Message 2 of 4)
1188046	09:05:36.338095	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1188051	09:05:36.339004	Cisco_6a:00:02	Microsoft_b4:05:…	EAPOL	319	1	Key (Message 3 of 4)
1188062	09:05:36.346352	Microsoft_b4:05:25	Cisco_6a:00:02	EAPOL	199	1	Key (Message 4 of 4)
1188063	09:05:36.346352	10.106.107.251	Microsoft_b4:05:…	802.11	76	1	Acknowledgement, Flags=........C
1188151	09:05:36.384167	Microsoft_b4:05:25	Broadcast	802.11	120	1	Data, SN=1470, FN=0, Flags=.pm...F.C

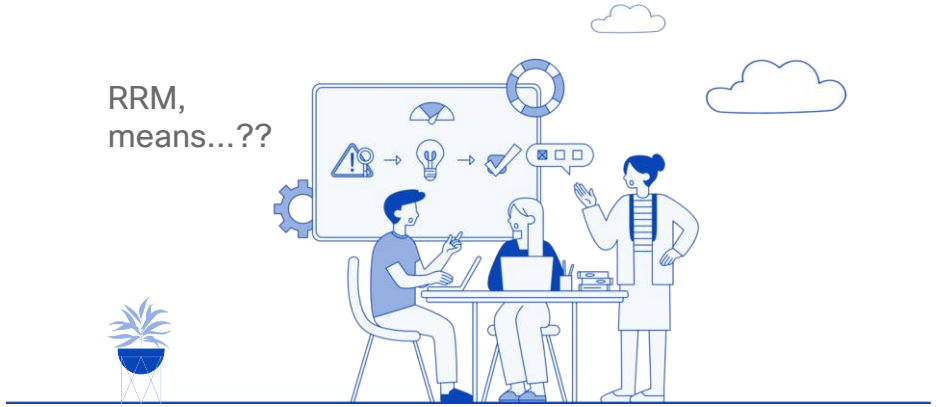
Probe Request/Response

Auth, Assoc Request/Response

EAPOL

4way Handshake

cisco



RRM Configuration

Wi-Fi 7 Initial RRM Configs

Enable .11be data rates

Preamble Puncturing

Channel Bond

For Preamble Puncturing to work the channel bond should be >= 80MHz

Global

General | Coverage | **DCA** | TPC | RF Grouping | Spatial Reuse

Dynamic Channel Assignment Algorithm

Channel Assignment Mode: (•) Automatic ( ) Freeze [Invoke Channel Update Once] ( ) Off

Interval: 10 minutes

Anchortime: 0

Avoid Foreign AP Interference: ☑

Avoid Cisco AP load: ☐

Avoid Non 5 GHz Noise: ☑

Avoid Persistent Non-Wi-Fi Interference: ☐

Zero Wait DFS: ☐

Channel Assignment Leader: WLC (10.106.107.251)

Last Auto Channel Assignment: 33 second(s) ago

DCA Channel Sensitivity: medium

Channel Width: ( ) 20 MHz ( ) 40 MHz ( ) 80 MHz (•) 160 MHz ( ) Best (DBS)

RF Profile

General | 802.11 | **RRM** | Advanced | 802.11ax | 802.11be

General | Coverage | TPC | **DCA**

Dynamic Channel Assignment

Avoid AP Foreign AP Interference: ☑

Zero Wait DFS: ☐

Channel Width: ( ) 20 MHz ( ) 40 MHz ( ) 80 MHz (•) 160 MHz ( ) Best (DBS)

DCA Channels:

☑ 36	☑ 40	☑ 44	☑ 48	☑ 52	☑ 56
☑ 60	☑ 64	☑ 100	☑ 104	☑ 108	☑ 112
☑ 116	☑ 120	☑ 124	☑ 128	☑ 132	☑ 136
☑ 140	☑ 144	☑ 149	☑ 153	☑ 157	☑ 161
☐ 165	☐ 169	☐ 173			

High Speed Roam

Mode Enable: ☐

Neighbor Timeout*: 5

Client Network Preference: Default

Cancel | Update & Apply to Device

Channel Bond

For Preamble Puncturing to work the channel bond should be >= 80MHz

Global

General | Coverage | DCA | TPC | RF Grouping | Spatial Reuse

Dynamic Channel Assignment Algorithm

Channel Assignment Mode: Automatic / Freeze / Off — Invoke Channel Update Once

Interval: 10 minutes

Anchortime: 0

Avoid Foreign AP Interference

Avoid Cisco AP load

Avoid Non 5 GHz Noise

Avoid Persistent Non-Wi-Fi Interference

Zero Wait DFS

Channel Assignment Leader: WLC (10.106.107.251)

Last Auto Channel Assignment: 33 second(s) ago

Channel Width: 20 MHz / 40 MHz / 80 MHz / 160 MHz / Best (DBS)

Channel Width: 20 MHz / 40 MHz / 80 MHz / 160 MHz / Best (DBS)

RF Profile

General | 802.11 | RRM | Advanced | 802.11ax | 802.11be

General | Coverage | TPC | DCA

Dynamic Channel Assignment

Avoid AP Foreign AP Interference

Zero Wait DFS

Channel Width: 20 MHz / 40 MHz / 80 MHz / 160 MHz / Best (DBS)

116 120 124 128 132 136
140 144 149 153 157 161
165 169 173

High Speed Roam

Mode Enable

Neighbor Timeout*: 5

Client Network Preference: Default

Cancel | Update & Apply to Device

Channel Bond

For Preamble Puncturing to work the channel bond should be >= 80MHz

Radio Configs → RF Profiles

5 GHz radio settings

Turn off 5 GHz radio — See band selection above.

Channel width — **Auto** | **Manual**

Manual 5 GHz channel width

Disable auto channel width by manually selecting a channel width for the access points in this profile.

- 20 MHz (28 channels)
  Recommended for High Density deployments and environments expected to encounter DFS events. More unique channels available, reducing chance of interference.
- 40 MHz (14 channels)
  For low to medium density deployments.
- **80 MHz (7 channels)**
  For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.

General | 2.4 GHz | 5 GHz | 6 GHz

Channel width — **Auto** | **Manual**

Manual 6 GHz channel width

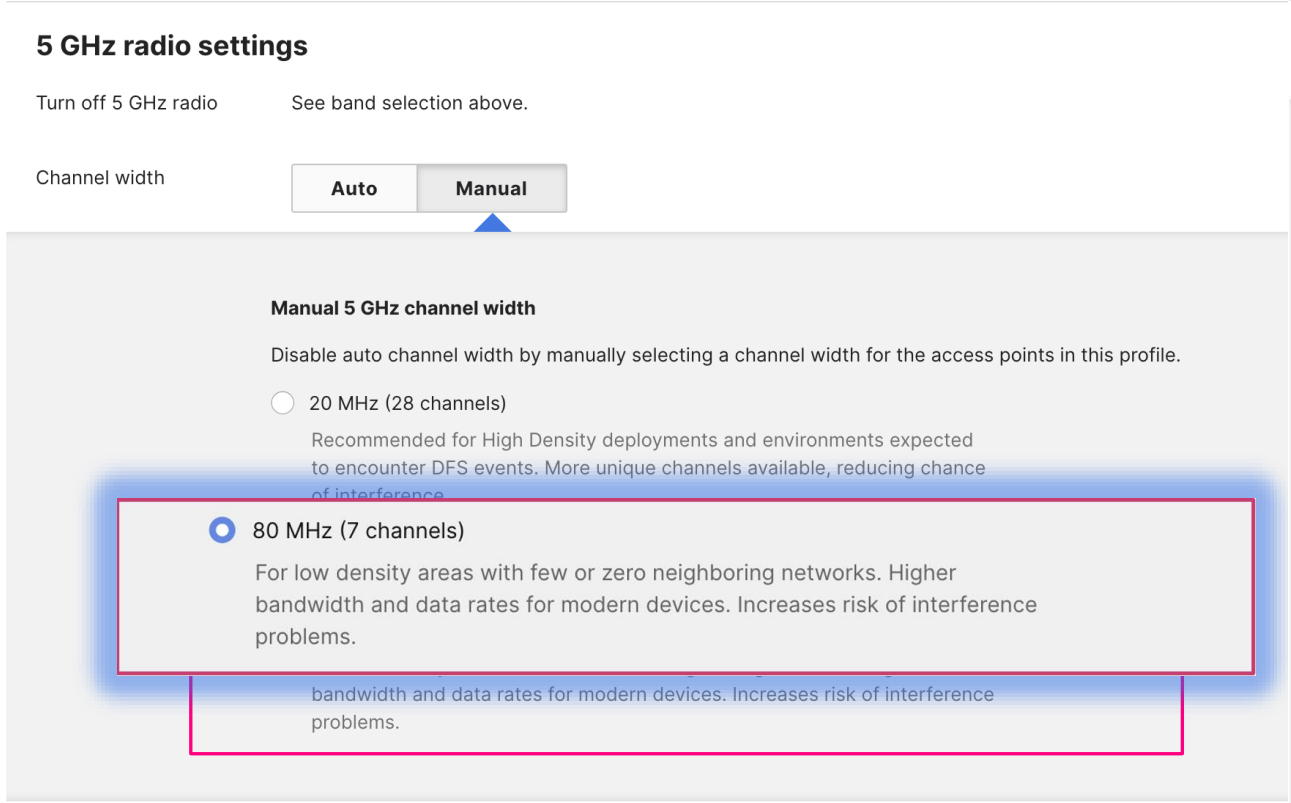
Disable auto channel width by manually selecting a channel width for the access points in this profile.

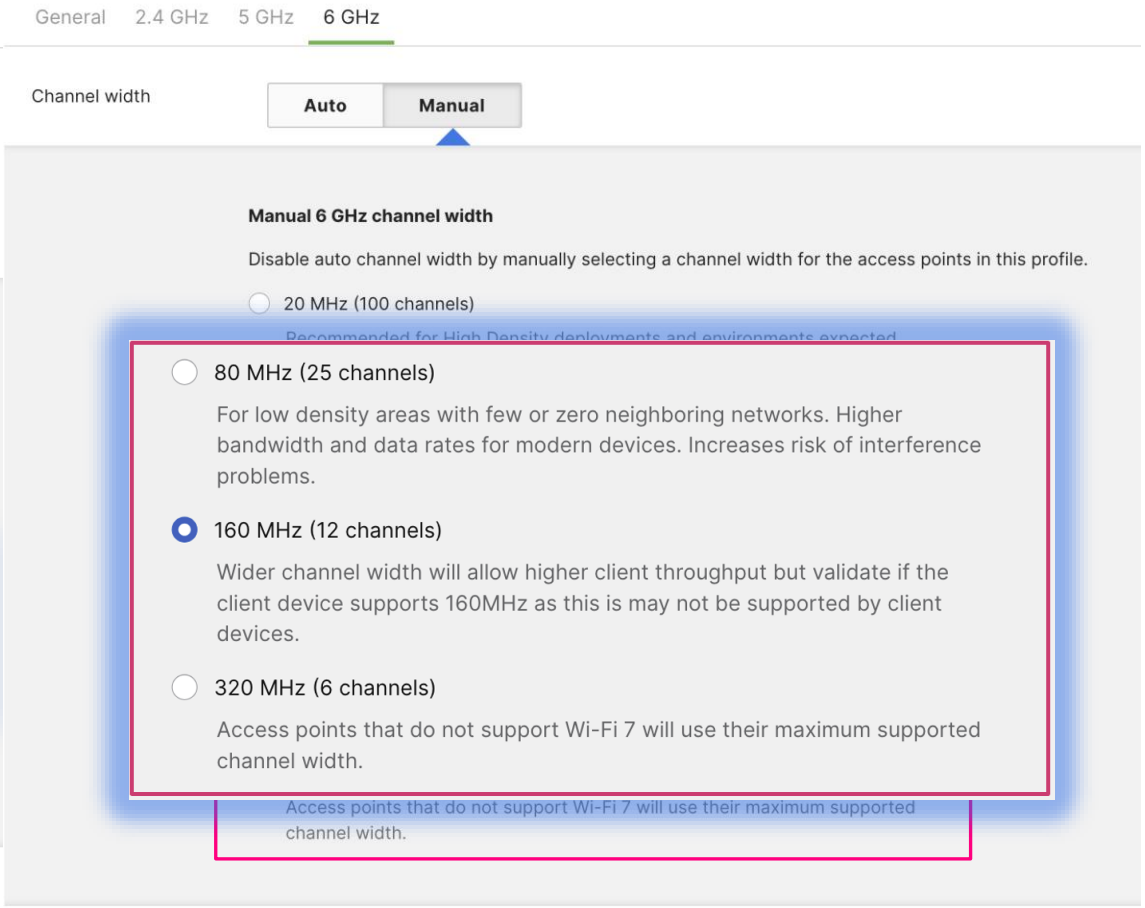
- 20 MHz (100 channels)
  Recommended for High Density deployments and environments expected to encounter DFS events. More unique channels available, reducing chance of interference.
- 40 MHz (50 channels)
  For low to medium density deployments.
- 80 MHz (25 channels)
  For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.
- **160 MHz (12 channels)**
  Wider channel width will allow higher client throughput but validate if the client device supports 160MHz as this is may not be supported by client devices.
- 320 MHz (6 channels)
  Access points that do not support Wi-Fi 7 will use their maximum supported channel width.

Channel Bond

For Preamble Puncturing to work the channel bond should be >= 80MHz

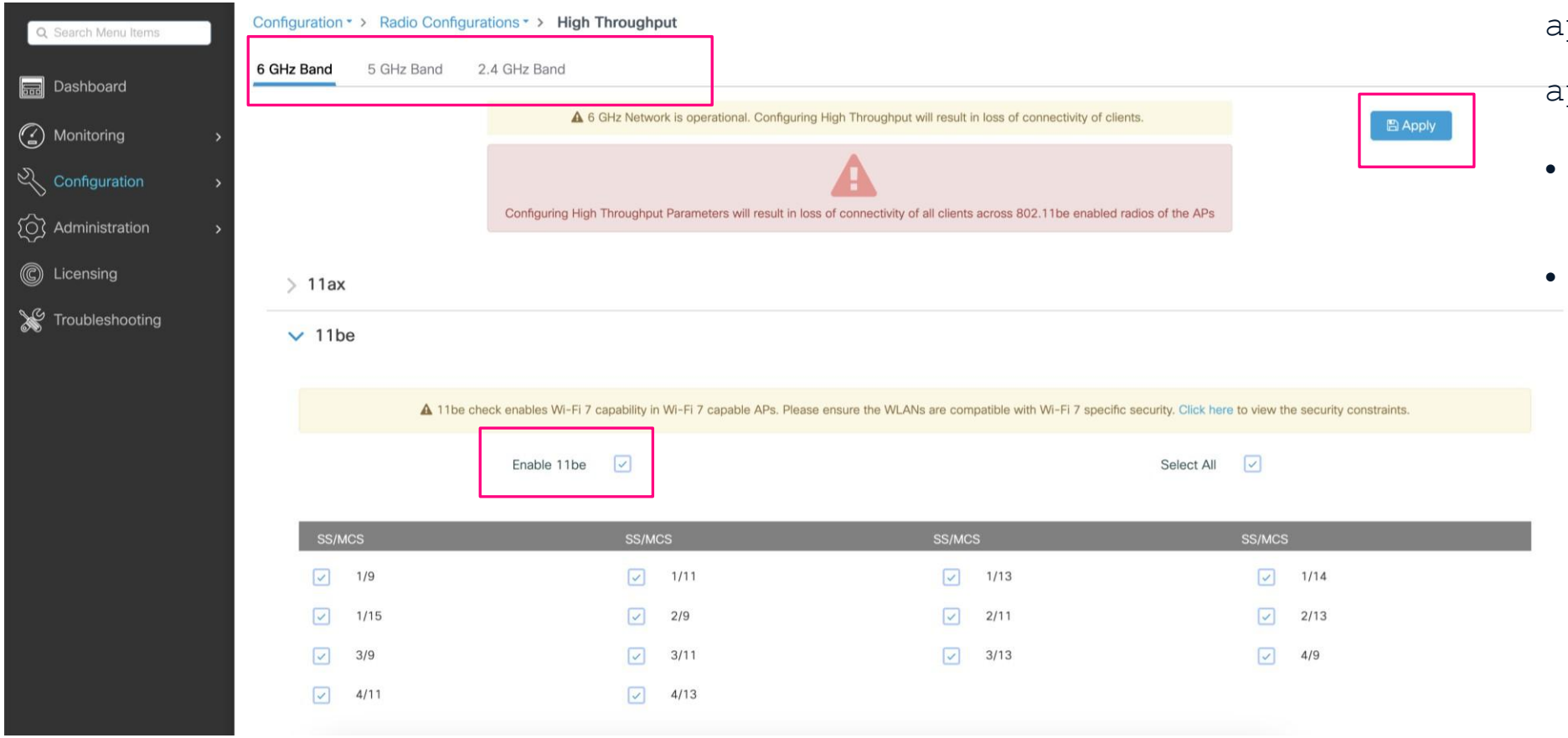
Radio Configs → RF Profiles





802.11be Datarates

Configuration > Radio Configurations > High Throughput > 2.4/5/6 GHz Band

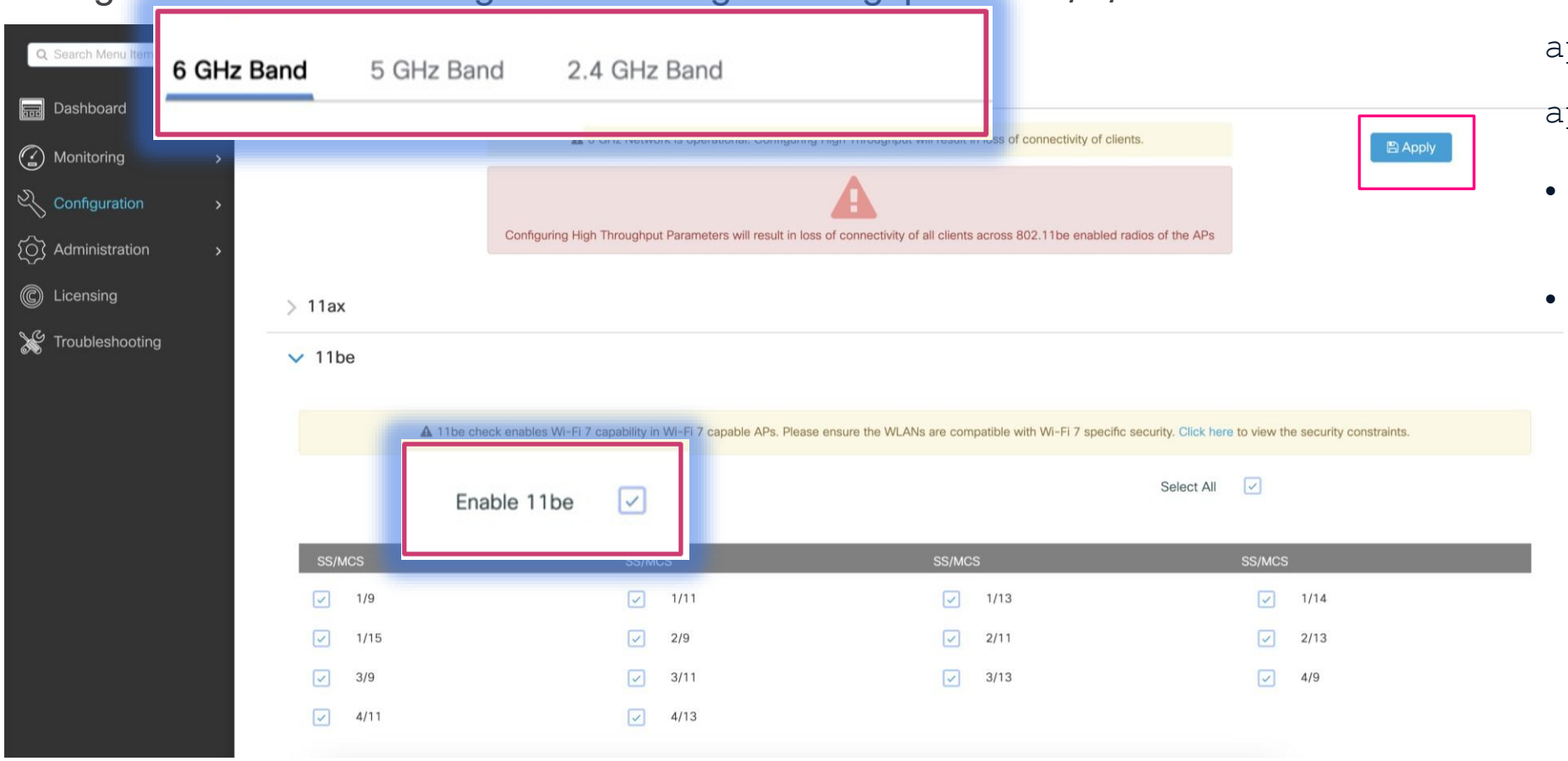



```
ap dot11 24ghz dot11be
ap dot11 5ghz dot11be
ap dot11 6ghz dot11be
```

- 11be support is disabled by default
- Enabling it will cause Wi-Fi 7 capable and enabled radios to reset

802.11be Datarates

Configuration > Radio Configurations > High Throughput > 2.4/5/6 GHz Band



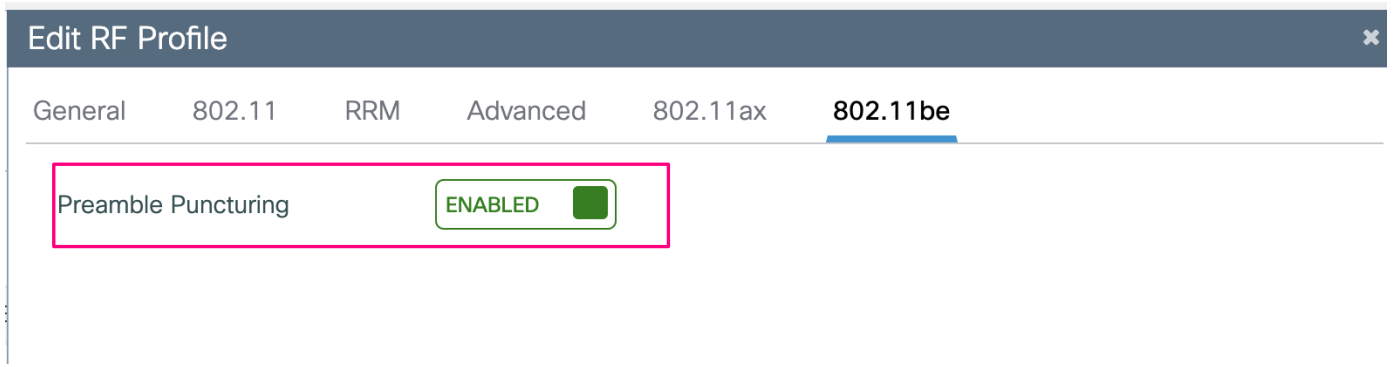

```
ap dot11 24ghz dot11be
ap dot11 5ghz dot11be
ap dot11 6ghz dot11be
```

- 11be support is disabled by default
- Enabling it will cause Wi-Fi 7 capable and enabled radios to reset

Preamble Puncturing

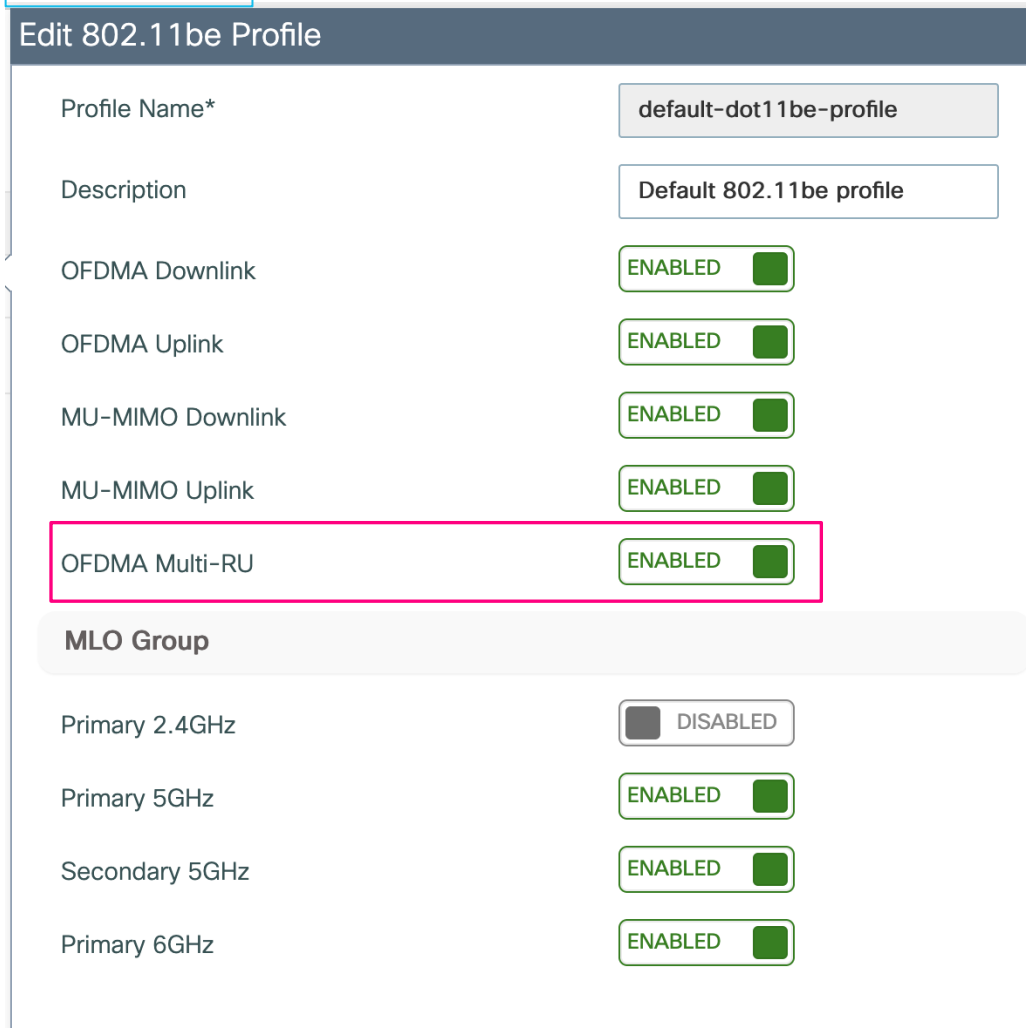
Set the channel bonding <=80Mhz

Configaration>Tags &

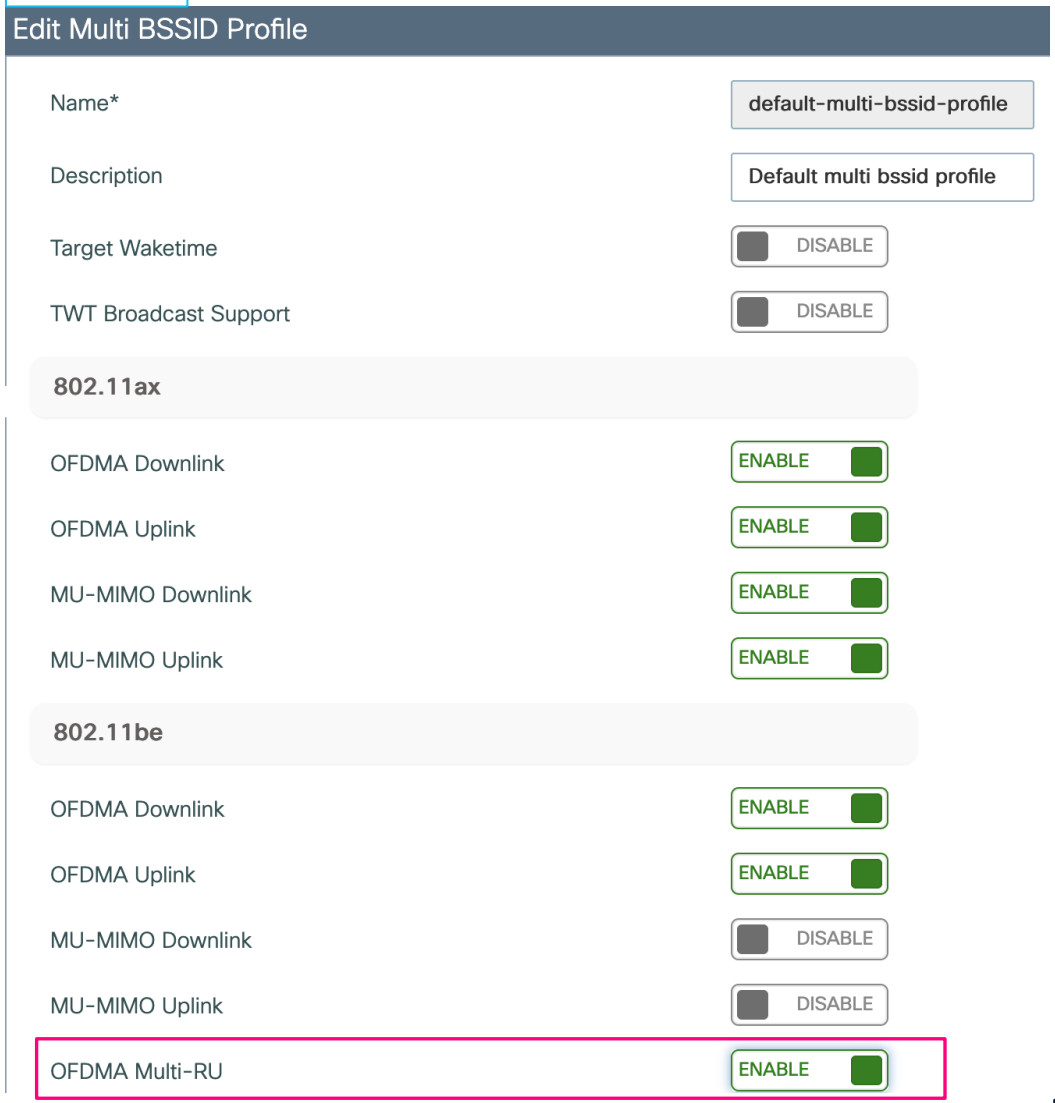


Configure OFDMA Multi RU

2.4/5 GHz Tags & Profiles>802.11be>default-dot11be-profile

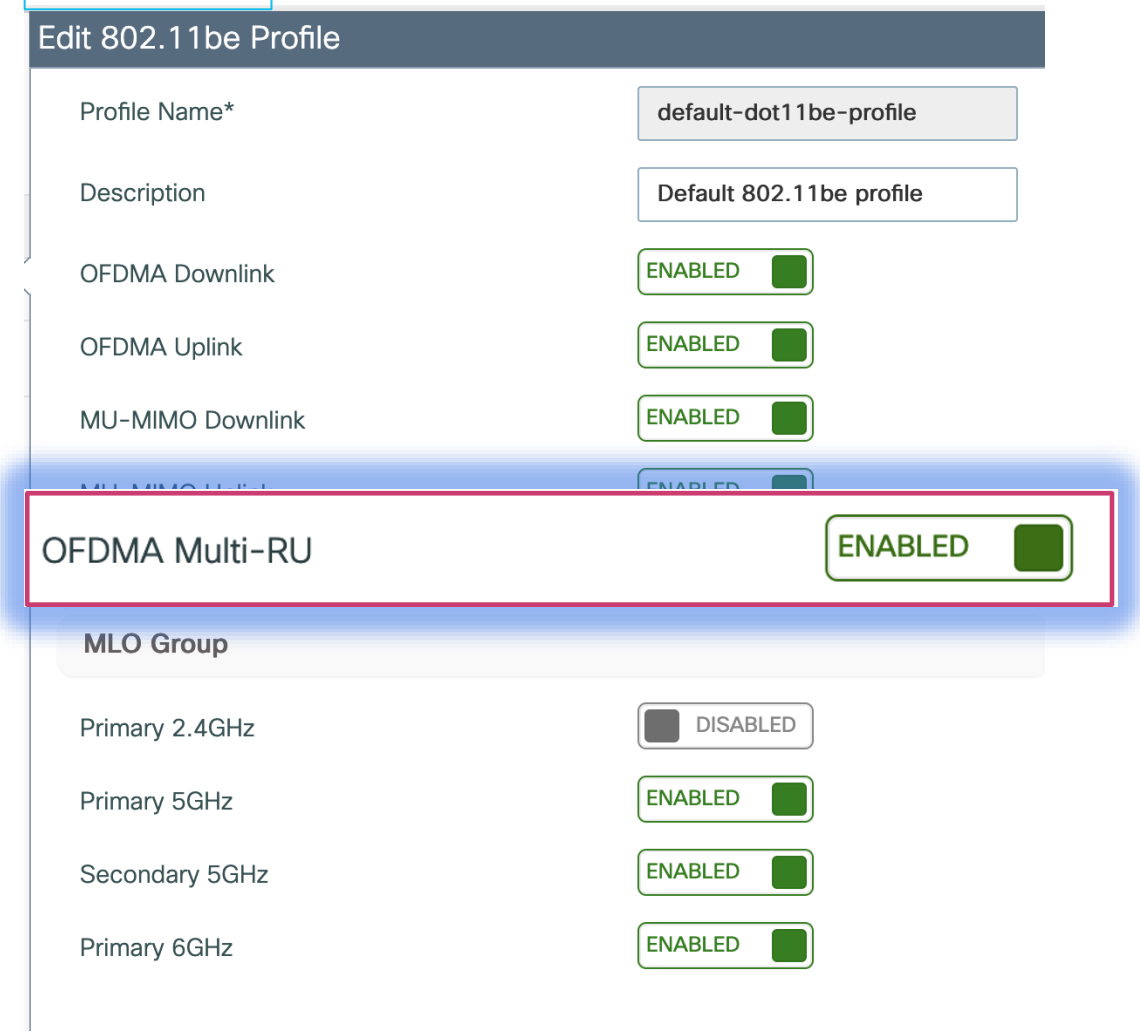


6 GHz Tags & Profiles >Multi BSSID>OFDMA Multi-RU



Configure OFDMA Multi RU

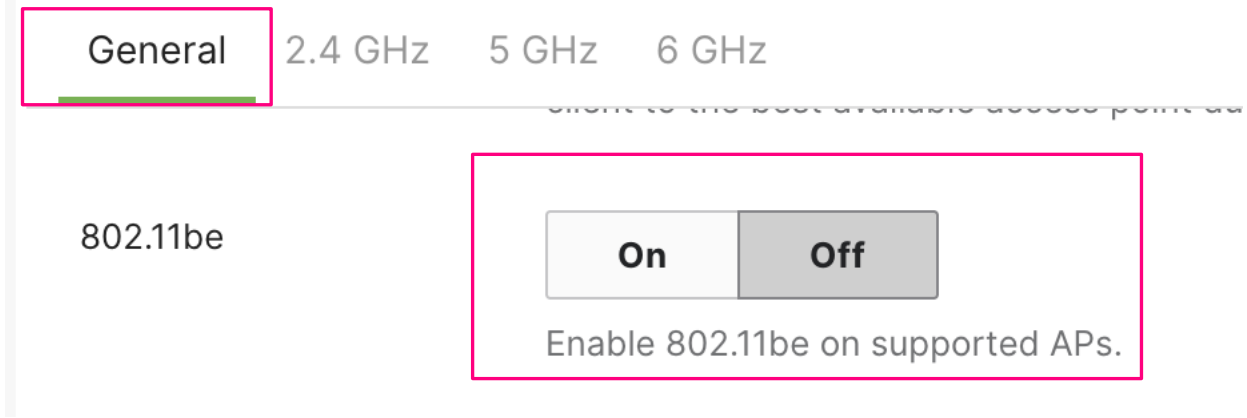
2.4/5 GHz Tags & Profiles>802.11be>default-dot11be-profile



6 GHz Tags & Profiles >Multi BSSID>OFDMA Multi-RU

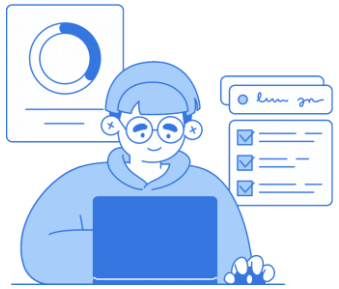
Meraki: Enable 802.11be

Wireless>Radio Setting>RF Profile>General



After enabling 802.11be, Meraki cloud will enable Preamble puncturing and OFDMA Multi RU.

What commands to run?



How is this Working?

Let’s escalate!!

Looks like its not Join..

Art of Isolating issues!

AP Level Troubleshooting

AP Join Troubleshooting – Without AP Console or SSH

Check LED status

GUAP		
Pattern	Color	Meaning / Status
Solid Orange / Amber	🟠	AP booting up (Day 0 Mode)
Rainbow (cycling colors)	🌈	AP discovering mode (deciding Meraki or Catalyst)
Blinking Blue	🔵✨	Software upgrade or image migration in progress
Solid Green	🟢	AP joined WLC successfully, no clients
Solid Blue	🔵	AP connected to Meraki Cloud, clients active
Blinking Orange	🟠✨	Unable to determine mode (no Cloud or WLC found)
Red (steady)	🔴	Hardware or image fault
Blinking Green	🟢✨	Site Survey / Local mode (for testing)
Off (configured)	⚫	LED disabled via configuration

MERAKI		
LED Color / Pattern	**Visual**	**Meaning / Status**
Solid Orange	🟠	AP booting up
Rainbow (cycling colors)	🌈	AP initializing / scanning channels
Blinking Blue	🔵✨	Firmware upgrade in progress
Solid Green	🟢	AP online, healthy, no clients connected
Solid Blue	🔵	AP online with clients connected
Blinking Orange	🟠✨	AP cannot reach Meraki Cloud
Blinking Green	🟢✨	Site Survey Mode
Solid Orange (post boot)	🟠	Hardware or image fault
Off (Run Dark)	⚫	LED intentionally disabled

AP Join Troubleshooting – Without AP Console or SSH

- Check if the AP has received the DHCP IP.
- Connectivity to Meraki cloud

Test	Command	Expected Result
DNS	nslookup dashboard.meraki.com	Should resolve to a valid IP
Ping	ping dashboard.meraki.com	Should reply
Port test	telnet dashboard.meraki.com 443	Should connect
AP local test	In Local Status Page → “Ping Dashboard”	Should succeed

- Check if the Migration option are correctly configured
  - Fast/Normal migration of DHCP option 43
  - DNS
  - AP Join Profile set to no-unicast

Offline Migration Method	Example Command / Configuration
Fast Offline Migration (DHCP Option 43)	WLC 200.1.0.100
	F305C801006402
Normal Offline Migration (DHCP Option 43)	WLC IP 200.1.0.100
	F105C8010064
Fast Offline Migration (DNS)	cisco-automigrate.<domain>
Normal Offline Migration (DNS)	cisco-capwap-controller.<domain>
PnP Offline Migration	5A1N;B2;K4;I200.1.0.75;J80

AP Join Troubleshooting – Without AP Console or SSH

Show commands on WLC – AP join

```
CLWLC#show ap summary
Number of APs: 12

CC = Country Code
RD = Regulatory Domain

AP Name                          Slots AP Model           Ethernet MAC   Radio MAC      CC   RD   IP Address                                State        Location
-------------------------------------------------------------------------------------------------------------------------------------------------------------
9176_1                           3     CW9176I            cc6e.2a67.d840 9056.715f.eee0 US   -B   10.107.70.73                              Registered   default
location
9178_2                           4     CW9178I            8c88.814f.0050 ecf4.0cb3.cae0 US   -B   10.107.70.36                              Registered   AP2
9176D_1                          3     CW9176D1           cc6e.2a3c.ca70 ecf4.0cbd.bce0 US   -UN  10.107.70.49                              Registered   default
location
9178_1                           4     CW9178I            8c88.814f.0240 ecf4.0cc7.1b60 US   -B   10.107.70.173                             Registered   AP1
```

```
WLC#show wireless stats ap join summary
Number of APs: 18
Base MAC        Ethernet MAC    AP Name                          IP Address                                Status      Last Failure Phase    Last Disconnect Reason
-------------------------------------------------------------------------------------------------------------------------------------------------------------
4891.d5f3.c890  4891.d5ee.7a94  AP-BCP-2ndFloor                   10.107.70.183                             Not Joined  Run                   Heart beat timer expiry
5017.ff05.f010  c08c.60be.0aa8  APc08c.60be.0aa8                 10.107.70.165                             Not Joined  Join                  Unsupported ap
6cd6.e362.92d0  4891.d5ef.e0ac  9136_3                           10.107.70.185                             Not Joined  Run                   DTLS close alert from
peer
ecf4.0cb3.cae0  8c88.814f.0050  9178_2                           10.107.70.36                              Joined      Run                   Max Retransmission to AP
ecf4.0cbd.bce0  cc6e.2a3c.ca70  9176D_1                          10.107.70.49                              Joined      Run                   Tag modified
```

AP Join Troubleshooting – Without AP Console or SSH

Show commands on WLC – AP join

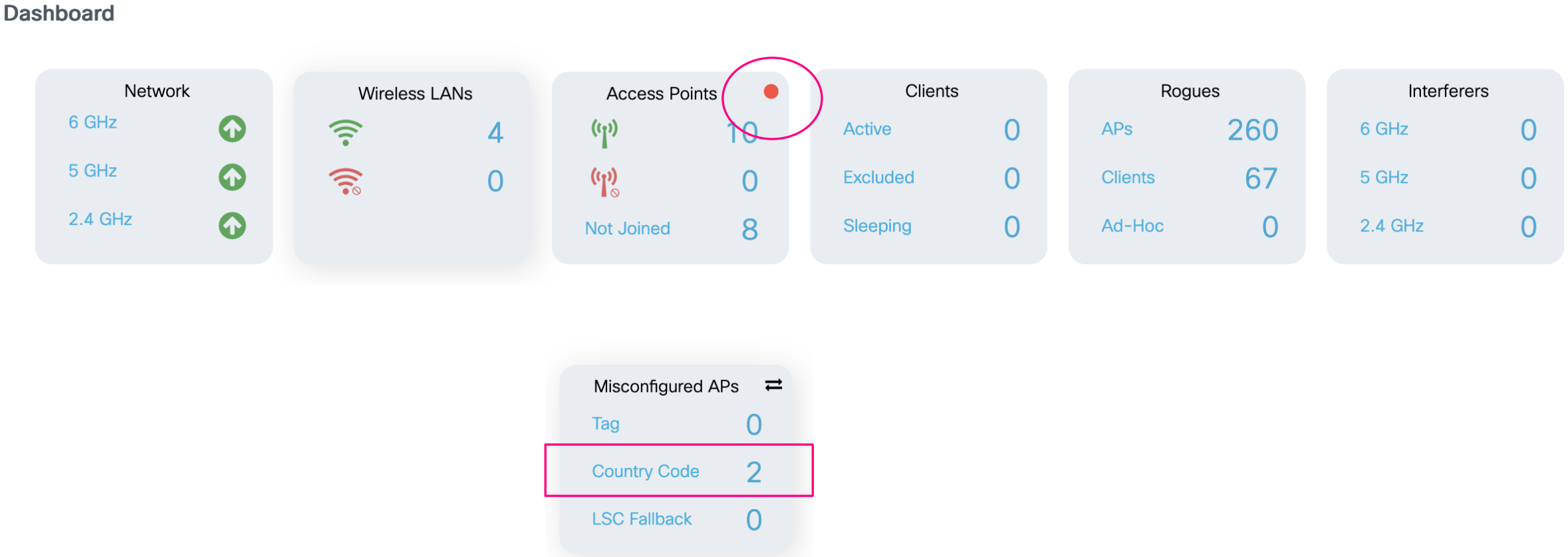
```
WLC#show logging

*Sep  1 13:12:56.599: %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1 R0/4: wncd: AP Event: AP Name:
APc08c.60be.0aa8 Mac: 5017.ff05.f010 Session-IP: 10.107.70.165[57515] 10.107.70.171[5246] Disjoined Unsupported ap
```

RA Traces:

```
2025/10/03 07:51:16.956084341 {wncd_x_R0-0}{1}: [errmsg] [18256]: (note): %CW_LIC-5-AP_NON_COMPLIANT_STATE: R0/0:
wncd: AP with mac address ecf4.0cb3.cae0 has moved to non-compliant state
2025/10/03 07:51:16.956184295 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [18256]: (note): MAC: ecf4.0cb3.cae0  Join
processing complete. AP in joined state
2025/10/03 07:51:18.321715124 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [18256]: (note): MAC: ecf4.0cb3.cae0  Received
CAPWAP change state event request
2025/10/03 07:51:18.323193932 {wncd_x_R0-0}{1}: [apmgr-db] [18256]: (note): MAC: ecf4.0cb3.cae0  Process country
code request : Proximity based country resolution : 4, Longitude : , Latitude : , Country source : 2
2025/10/03 07:51:20.387125001 {wncd_x_R0-0}{1}: [apmgr-db] [18256]: (note): MAC: ecf4.0cb3.cae0  Ack received for
most config payload
```

AP Join Troubleshooting - Without the AP Console or SSH

Check the number of APs unable to set the country from the 9800 Dashboard.

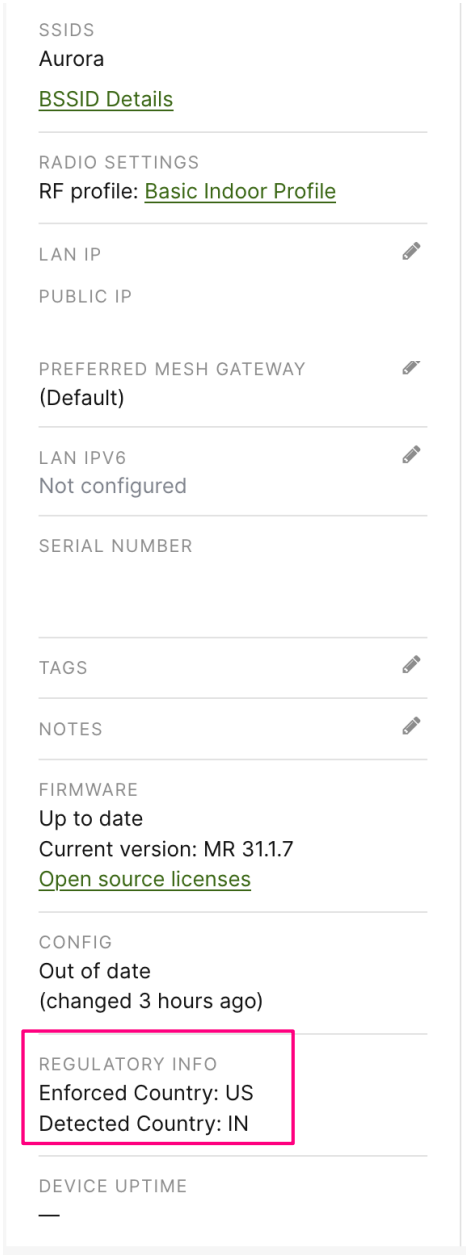


AP Join Troubleshooting – Without the AP Console or SSH

Show commands on WLC – AP join

```
WLC#show ap name 9178_1 config general | i Country
Country Code                                    : Multiple Countries : AU,DZ,US
Regulatory Domain Allowed by Country            : 802.11bg:-AE^   802.11a:-ABEINZ^   802.11 6GHz:-BZ
AP Country Code                                 : US  - United States
Country Code Resolution Method                       : Regulatory Activation File

WLC#show ap name 9172_1 config general | i Country
Country Code                                    : Multiple Countries : AU,DZ,US
Regulatory Domain Allowed by Country            : 802.11bg:-AE^   802.11a:-ABEINZ^   802.11 6GHz:-BZ
AP Country Code                                 : US  - United States
Country Code Resolution Method                         : Proximity

WLC#show ap name 9176_1 config general | inc Country
Country Code                                    : US
Regulatory Domain Allowed by Country            : 802.11bg:-A 802.11a:-AB 802.11 6GHz:-B
AP Country Code                                 : US  - United States
Country Code Resolution Method                         : GPS


WLC#show ap regulatory activation all
Regulatory Activation file Meta-data
-----------------------------------
Date Created     : 2024-12-04T15:48:09Z
Created By       : xxxx@cisco.com/SSO
Device count     : 15
Organization Id  :

AP MAC              Serial Number      Country code
-----------------------------------------------------
0c7b.c8aa.c122                           US
8c88.814f.0050       WNT2841000J         US
8c88.814f.0240       WNT2841007G         US
9818.88bd.0e3e                           US
```

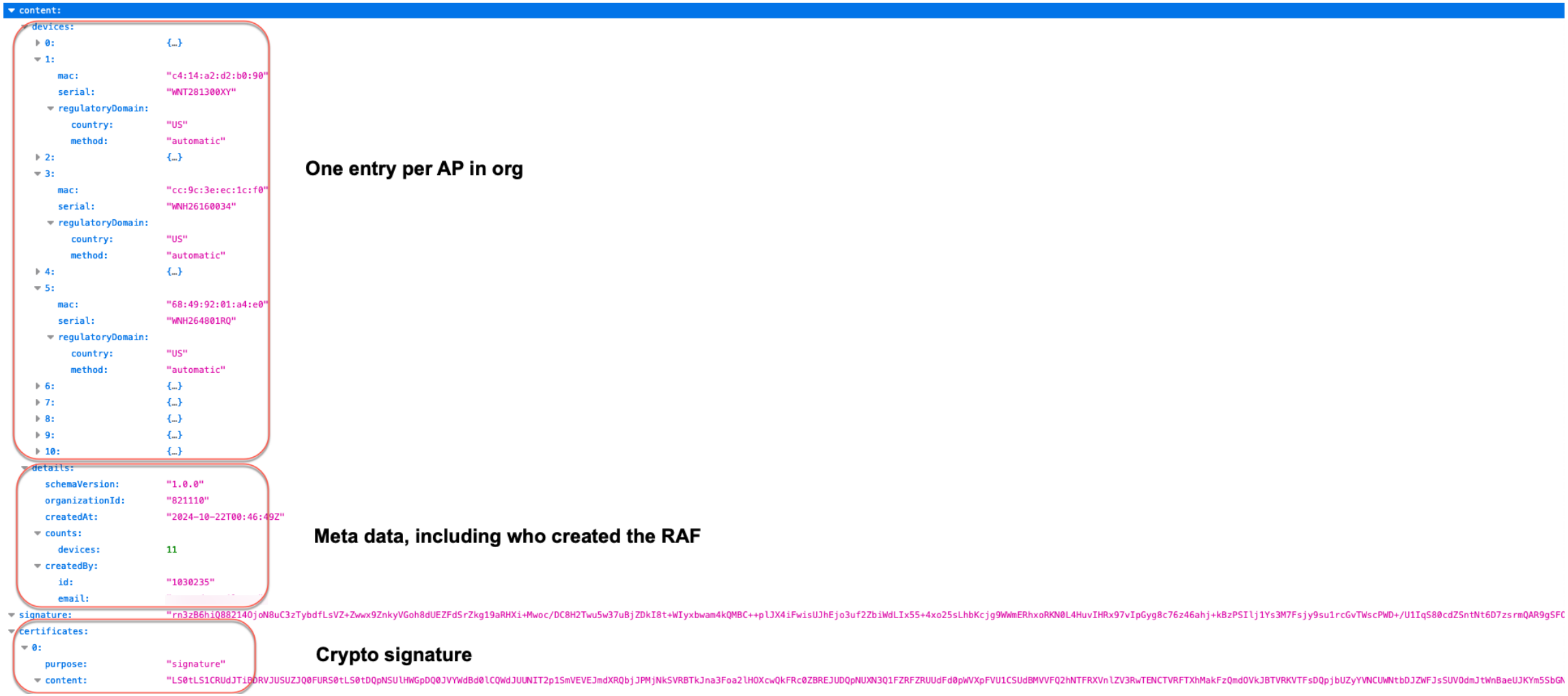
AP Join Troubleshooting – Without the AP Console or SSH



AP Join Troubleshooting – RAF File

RAF file contains information for all networks that the current user has write permission to.

This will generate a JSON file.



One entry per AP in org

Meta data, including who created the RAF

Crypto signature

AP Join Troubleshooting – With AP Console or SSH

MR OS Boot Console

```
<Meraki> offline-migration-info
| [2000-01-01 00:00:26.640] AP in day0 - offline migration
| [2000-01-01 00:01:24.369] [init] start offline migration detection
| [2000-01-01 00:02:26.465] [fast-offline-migration-delay] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:02:31.470] [fast-offline-migration][v4] no fast offline migration by DHCP
| [2000-01-01 00:02:31.470] [fast-offline-migration][v6] no fast offline migration by DHCP
| [2000-01-01 00:02:31.470] [fast-offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:02:31.470] [fast-offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:02:31.470] [fast-offline-migration] waiting for 7min before taking any migration decision
| [2000-01-01 00:03:33.531] [fast-offline-migration] waiting for 5min before taking any migration decision
| [2000-01-01 00:04:35.590] [fast-offline-migration] waiting for 4min before taking any migration decision
| [2000-01-01 00:05:37.648] [fast-offline-migration] waiting for 3min before taking any migration decision
| [2000-01-01 00:06:39.707] [fast-offline-migration] waiting for 2min before taking any migration decision
| [2000-01-01 00:07:41.765] [fast-offline-migration] waiting for 1min before taking any migration decision
| [2000-01-01 00:08:43.824] [fast-offline-migration] waiting for 0min before taking any migration decision
| [2000-01-01 00:09:35.874] [offline-migration] forcing DHCP renew
| [2000-01-01 00:09:35.874] [offline-migration] forcing DHCPv6 INFORMATION REQUEST
| [2000-01-01 00:09:40.879] [offline-migration] migration decision
| [2000-01-01 00:09:40.879] [offline-migration][v4] no WLC IP in DHCP option 43
| [2000-01-01 00:09:40.879] [offline-migration][v4] missing DNS config (server and/or domain)
| [2000-01-01 00:09:40.879] [offline-migration][v6] no WLC IP in DHCP option 52
| [2000-01-01 00:09:40.879] [offline-migration][v6] missing DNS config (server and/or domain)
| [2000-01-01 00:09:45.899] [offline-migration][v4][capwap-l2] 0 WLC(s) detected (unsupported)
| [2000-01-01 00:09:50.920] [offline-migration][v6][capwap-l2] 0 WLC(s) detected (unsupported)
| [2000-01-01 00:09:50.920] [offline-migration] no migration & not claimed => restart detection
| [2000-01-01 00:09:55.924] [init] start offline migration detection
```

AP Join Troubleshooting – With AP Console or SSH

GPS/GNSS

```
9178_2#show  gnss info
GnssState: Started
ExternalAntenna: false
Fix: No-Fix ValidFix: false Time: 2025-10-06 11:19:33
Latitude: 0 Longitude: 0
HorAcc: 3530033.6 hDOP: 99
Uncertainty Ellipse:
 Major axis: 3530033.6 Minor axis: 3530033.6 Orientation: 0
Altitude MSL: -12 HAE: 0 VertAcc: 160000
NumSat: 0 RangeRes: 0 GpGstRms: 0
pDOP: 140 hDOP: 99 vDOP: 99 nDOP: 99 eDOP: 99 gDOP: 0 tDOP: 0
LastFixTime:
SatelliteCount: 0
GNSS_PostProcessor: N/A
CiscoGNSS: N/A
Last Location Acquired: N/A
```

Client Troubleshooting

Adaptors on Windows – Qualcomm

```
C:\Users\Wirel>netsh wlan show interface
There are 2 interfaces on the system:
    Name                   : WiFi
    Description            : Qualcomm(R) FastConnect(TM) 7800 Mobile Connectivity System
    GUID                   : aaf94e2f-fc88-46b5-bc45-482e278ecc93
     Physical address      : c4:cb:76:b1:05:25
    Interface type         : Primary
    State                  : connected
    SSID                   : Workoholic
    MLD AP BSSID           : f2:d8:05:6a:00:10
          LinkID: 1, Local: c6:cb:76:b1:05:25, AP: f0:d8:05:65:01:0f, RSSI: -65, Channel: 124, Band: 5 GHz, BW: 20
          LinkID: 0, Local: d6:cb:76:b1:05:25, AP: f0:d8:05:65:01:00, RSSI: -52, Channel: 1, Band: 2.4 GHz, BW: 20
    Connected Akm-cipher   : [ akm = 00-0f-ac:24, cipher =  00-0f-ac:09 ]
    Network type           : Infrastructure
    Radio type             : 802.11be
    Authentication         : WPA3-Personal  (H2E)
    Cipher                 : GCMP-256
    Connection mode        : Profile
    Receive rate (Mbps)    : 344.2
    Transmit rate (Mbps)   : 344.2
    Signal                 : 96%
    Profile                : Workoholic
    QoS MSCS Configured          : 0
    QoS Map Configured           : 0
    QoS Map Allowed by Policy    : 0
```

Adaptors on Windows – Intel

```
C:\Users\Wirel>netsh wlan show interface
There is 1 interface on the system:
    Name                   : Wi-Fi
    Description            : Intel(R) Wi-Fi 7 BE201 320MHz
    GUID                   : bc5ea7c2-c888-4ff8-aaaf-26f56304ac2f
    Physical address       : ec:4c:8c:71:f3:04
    Interface type         : Primary
    State                  : connected
    SSID                   : Workoholic
    MLD AP BSSID           : f2:d8:05:6a:00:10
          LinkID: 1, Local: ee:4c:8c:71:f3:07, AP: f0:d8:05:6b:00:0f, RSSI: -64, Channel: 124, Band: 5 GHz, BW: 0
          LinkID: 0, Local: ee:4c:8c:71:f3:08, AP: f0:d8:05:6b:00:00, RSSI: -57, Channel: 1, Band: 2.4 GHz, BW: 0
    Connected Akm-cipher   : [ akm = 00-0f-ac:24, cipher =  00-0f-ac:09 ]
    Network type           : Infrastructure
    Radio type             : 802.11be
    Authentication         : WPA3-Personal  (H2E)
    Cipher                 : GCMP-256
    Connection mode        : Profile
    Receive rate (Mbps)    : 258
    Transmit rate (Mbps)   : 258
    Signal                 : 81%
    Profile                : Workoholic
    QoS MSCS Configured          : 0
    QoS Map Configured           : 0
    QoS Map Allowed by Policy    : 0
```

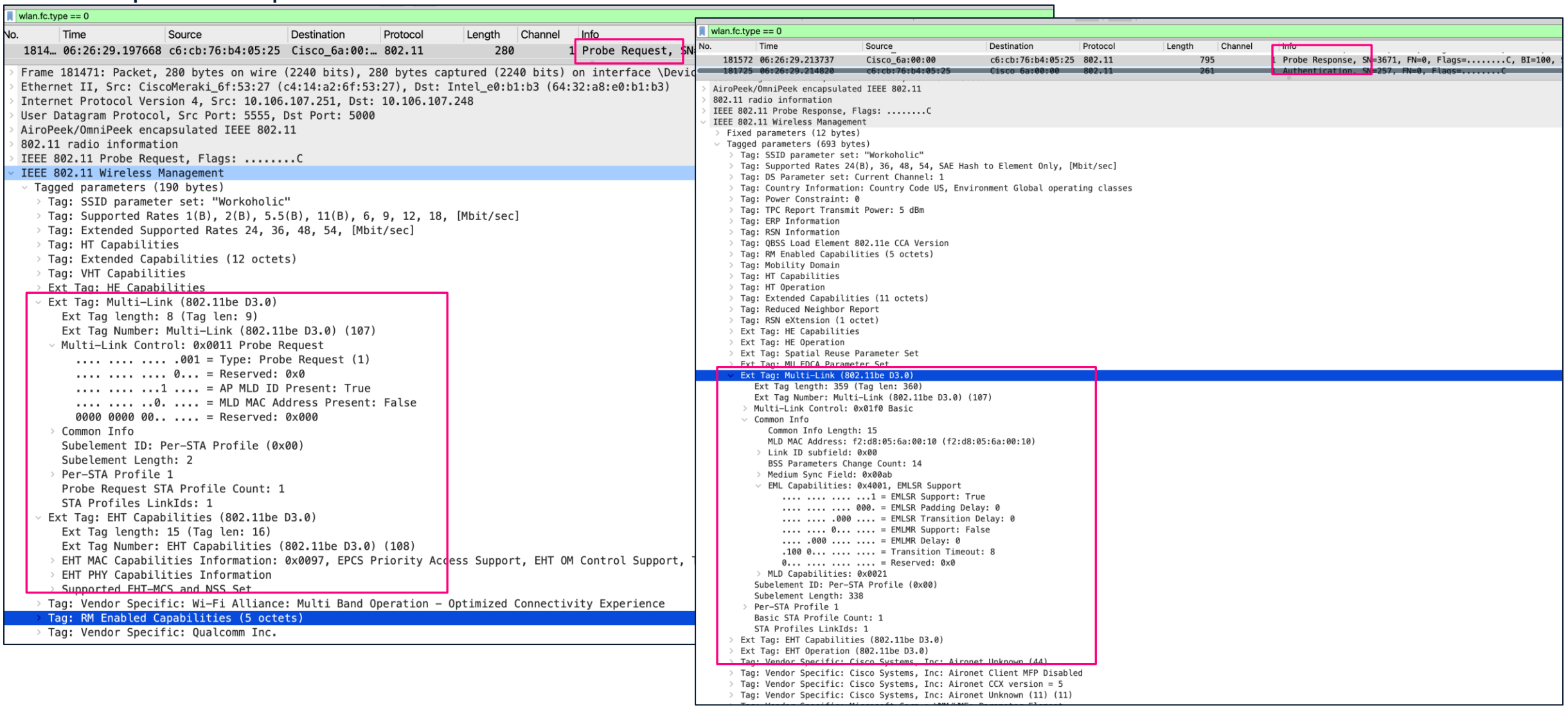
OTA Packet Flow

WPA3, SAE

179989	06:26:29.197668	c6:cb:76:b4:05:25	Cisco_6a:00:00	802.11	280	1	Probe Request, SN=256, FN=0, Flags=........C, SSID="Workoholic"
180089	06:26:29.213737	Cisco_6a:00:00	c6:cb:76:b4:05:25	802.11	795	1	Probe Response, SN=3671, FN=0, Flags=........C, BI=100, SSID="Workoholic"
180242	06:26:29.214820	c6:cb:76:b4:05:25	Cisco_6a:00:00	802.11	261	1	Authentication, SN=257, FN=0, Flags=........C
180359	06:26:29.231379	Cisco_6a:00:00	c6:cb:76:b4:05:25	802.11	110	1	Authentication, SN=3672, FN=0, Flags=........C
180485	06:26:29.249068	c6:cb:76:b4:05:25	Cisco_6a:00:00	802.11	218	1	Authentication, SN=258, FN=0, Flags=........C
180629	06:26:29.257503	Cisco_6a:00:00	c6:cb:76:b4:05:25	802.11	213	1	Authentication, SN=3673, FN=0, Flags=........C
180720	06:26:29.260664	c6:cb:76:b4:05:25	Cisco_6a:00:00	802.11	142	1	Authentication, SN=259, FN=0, Flags=........C
180774	06:26:29.274199	Cisco_6a:00:00	c6:cb:76:b4:05:25	802.11	142	1	Authentication, SN=3674, FN=0, Flags=........C
180992	06:26:29.282759	c6:cb:76:b4:05:25	Cisco_6a:00:00	802.11	415	1	Association Request, SN=260, FN=0, Flags=........C, SSID="Workoholic"
181230	06:26:29.321601	Cisco_6a:00:00	c6:cb:76:b4:05:25	802.11	487	1	Association Response, SN=0, FN=0, Flags=........C
181299	06:26:29.325566	Cisco_6a:00:00	c6:cb:76:b4:05:25	EAPOL	233	1	Key (Message 1 of 4)
181667	06:26:29.348685	c6:cb:76:b4:05:25	Cisco_6a:00:00	EAPOL	290	1	Key (Message 2 of 4)
181755	06:26:29.356857	Cisco_6a:00:00	c6:cb:76:b4:05:25	EAPOL	527	1	Key (Message 3 of 4)
182109	06:26:29.392803	c6:cb:76:b4:05:25	Cisco_6a:00:00	EAPOL	250	1	Key (Message 4 of 4)

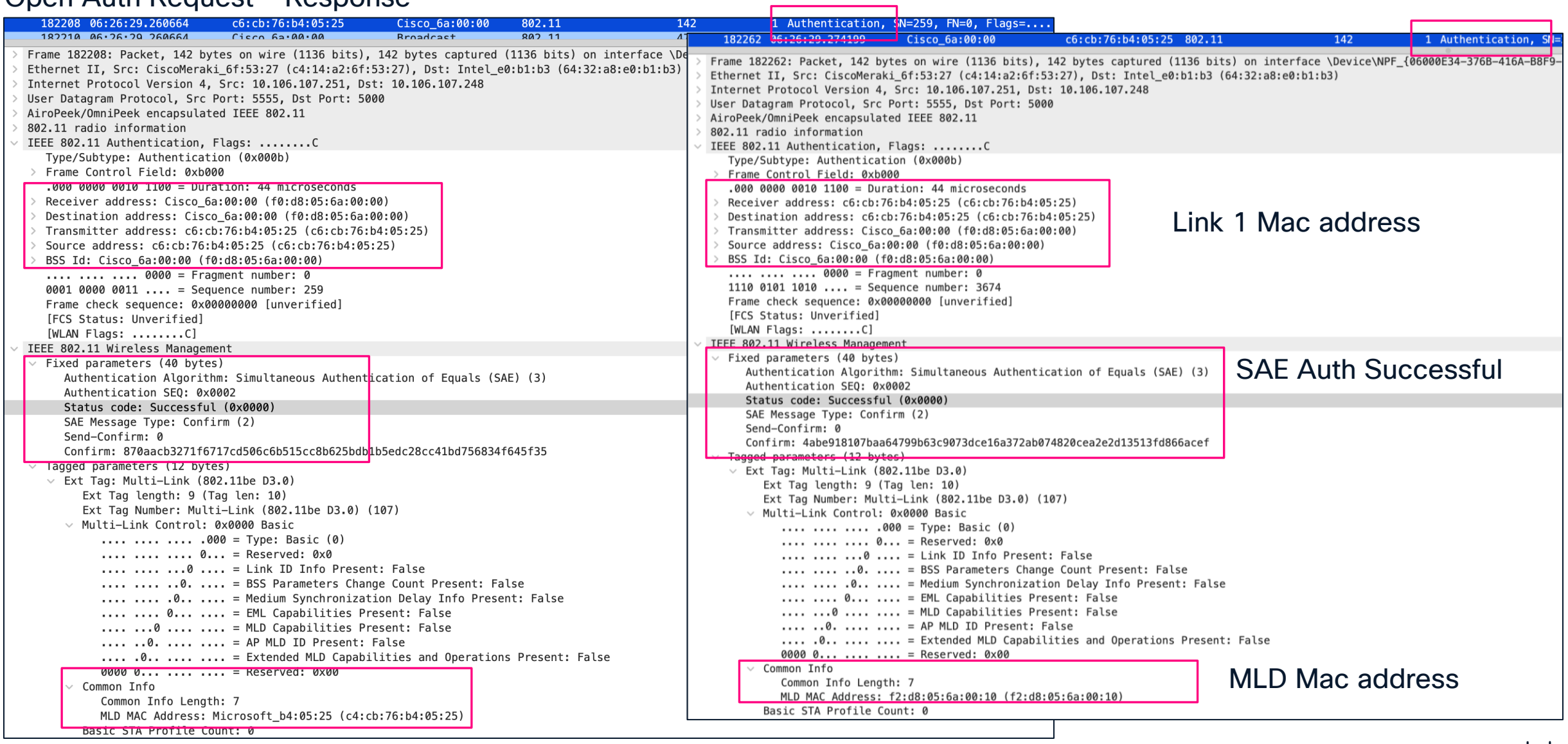
OTA Packet Flow

Prode Request - Response



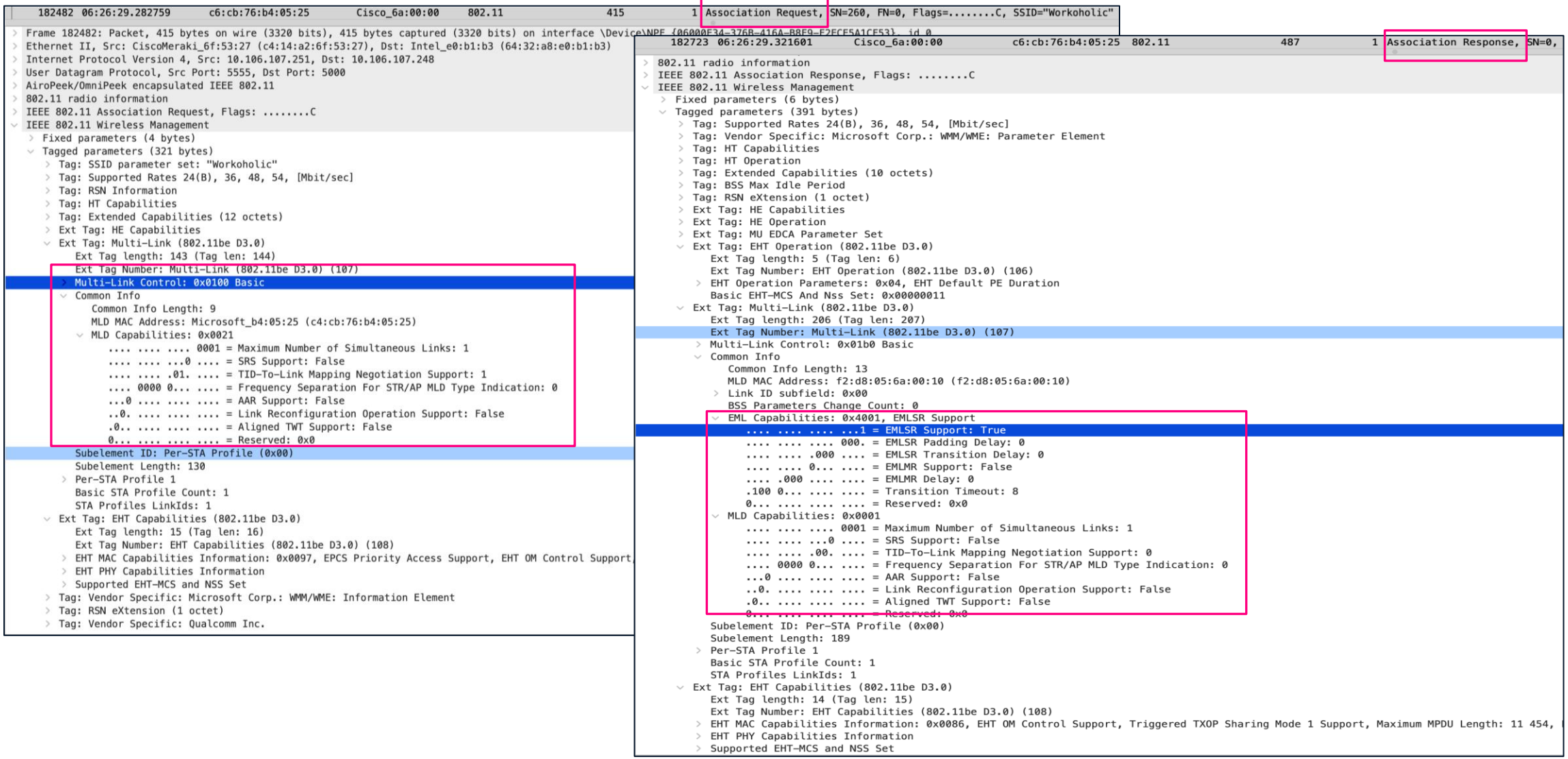
OTA Packet Flow

Open Auth Request - Response



OTA Packet Flow

Association Request - Response



Wi-Fi 7 Client Detail with MLO - 9800

Example: MLMR-STR

360 View | General | QOS Statistics | ATF Statistics | Mobility History | Call Statistics

Client Properties | AP Properties | Security Information | Client Statistics | QOS Properties | EoGRE

Counters and RF

Client Stats	Band : 2.4 GHz	Band : 5 GHz
AP Slot	AP Slot 0	AP Slot 1
Station Link MAC Address	c6cb.76b4.0525	d6cb.76b4.0525
BSSID	f0d8.056a.0000	f0d8.056a.000f
Number of Bytes Received from Client	6574023	154299
Number of Bytes Sent to Client	828990	24483
Number of Packets Received from Client	64271	1527
Number of Packets Sent to Client	4156	112
Number of Data Retries	1	0
Number of RTS Retries	0	0
Number of Tx Total Dropped Packets	0	0
Number of Duplicate Received Packets	0	0
Number of Decrypt Failed Packets	0	0
Number of Mic Failured Packets	0	0
Number of Mic Missing Packets	0	0
Number of Policy Errors	0	0
Radio Signal Strength Indicator	-49 dBm	-52 dBm
Signal to Noise Ratio	49 dB	44 dB
Last Statistics Update	10/13/2025 10:00:22	10/13/2025 06:39:19

IP - Zone ID Mapping

IP Address	Zone-Id
10.106.107.245	0x00000000

360 View | General | QOS Statistics | ATF Statistics | Mobility History

Client Properties | AP Properties | Security Information | Client Statistics

VRF Name	N/A
Central NAT	DISABLED
11v DMS Capable	No
QoS Map Capable	No
FlexConnect Data Switching	N/A
FlexConnect DHCP Status	N/A
FlexConnect Authentication	N/A
Number of links dropped due to downsizing	0
Client Scan Report Time	Timer not running
Max Client Protocol Capability	Wi-Fi 7 (802.11be)
Wi-Fi to Cellular Steering	Not implemented
Cellular Capability	N/A
Regular ASR support	DISABLED
L3 Access	DISABLED
Client Gateway IPv4 Address	10.106.107.249
Enhanced Multi Link	None
STR Capable	Yes
No. of associated links	2
Band	2.4 GHz, 5 GHz
No. of Known links	2
Confidence Level	0

Mobility

Move Count	0
Role	Local
Roam Type	None
Complete Timestamp	10/13/2025 06:29:22 IST

Device Classification

Wi-Fi 7 Client Detail with MLO - 9800

Example: EMLSR

360 View | General | QOS Statistics | ATF Statistics | Mobility History | Call Statistics

Client Properties | AP Properties | Security Information | Client Statistics | QOS Properties

Counters and RF

Client Stats	Band : 2.4 GHz	Band : 5 GHz
AP Slot	AP Slot 0	AP Slot 1
Station Link MAC Address	ee4c.8c71.f307	ee4c.8c71.f308
BSSID	f0d8.056a.0000	f0d8.056a.000f
Number of Bytes Received from Client	7235404	197577
Number of Bytes Sent to Client	12318567098	202575
Number of Packets Received from Client	58621	1678
Number of Packets Sent to Client	18418702	623
Number of Data Retries	698181	8
Number of RTS Retries	0	0
Number of Tx Total Dropped Packets	0	0
Number of Duplicate Received Packets	0	0
Number of Decrypt Failed Packets	0	0
Number of Mic Failured Packets	0	0
Number of Mic Missing Packets	0	0
Number of Policy Errors	0	0
Radio Signal Strength Indicator	-53 dBm	-42 dBm
Signal to Noise Ratio	45 dB	54 dB
Last Statistics Update	10/13/2025 10:01:52	10/13/2025 09:36:21

IP - Zone ID Mapping

IP Address	Zone-Id
10.106.107.254	0x00000000
fe80::91c4:2271:4aa6:5596	0x8000033a

360 View | General | QOS Statistics | ATF Statistics | Mobility History | Call St

Client Properties | AP Properties | Security Information | Client Statistics | QOS

Central NAT	DISABLED
11v DMS Capable	No
QoS Map Capable	No
FlexConnect Data Switching	N/A
FlexConnect DHCP Status	N/A
FlexConnect Authentication	N/A
Number of links dropped due to downsizing	0
Client Scan Report Time	Timer not running
Max Client Protocol Capability	Wi-Fi 7 (802.11be)
Wi-Fi to Cellular Steering	Not implemented
Cellular Capability	N/A
Regular ASR support	DISABLED
L3 Access	DISABLED
Client Gateway IPv4 Address	10.106.107.249
Enhanced Multi Link	EMLSR
STR Capable	No
No. of associated links	2
Band	2.4 GHz, 5 GHz
No. of Known links	2
Confidence Level	0

Mobility

Move Count	0
Role	Local
Roam Type	None
Complete Timestamp	10/13/2025 05:46:12 IST

Device Classification

Device Name	Unknown Device

Wi-Fi 7 Client details on Meraki Cloud

CLIENTS

Pixel-8-Pro

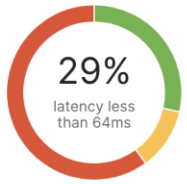
Overview Connections Performance Ro

Status	associated since Oct 8 20:41
Location Status	unknown
SSID	Aurora
Access point	cc:6e:2a:3c:e9:d0
Splash	N/A
Link 0 Signal	43dB (channel 44, 5 GHz)
Link 1 Signal	44dB (channel 157, 5 GHz)
Device type, OS	Google
Capable Wi-Fi standards	802.11be - 2.4, 5, and 6 GHz details
Tools	history packet capture disconnect client
Notes	

Current client connection

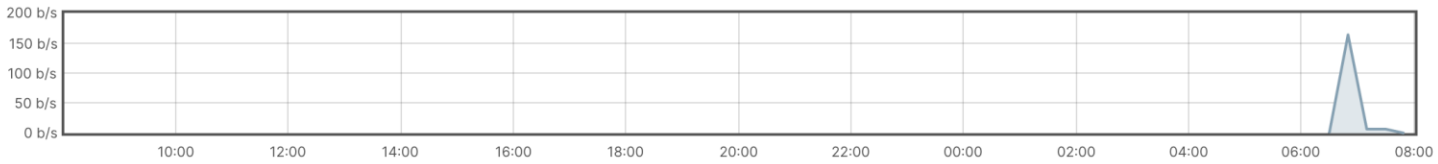
Health for the last 2 hours

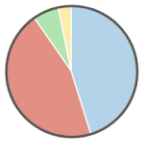
No wireless connectivity data in the selected time period



Usage for the last day

26 KB (↓ None, ↑ 26 KB) Applications





Policy

Device policy: normal
Bandwidth: unlimited
Layer 3 firewall: 0 rules
Layer 7 firewall: 0 rules
Traffic shaping: 0 rules
show details »

Network

IPv4 address: 10.161.102.145
MAC address: 5c:33:7b:ec:84:4d
Link 0 MAC address: 5e:33:7b:ec:84:4f
Link 1 MAC address: 5e:33:7b:ec:84:4e

Ping

Loss rate: –
Average latency: –

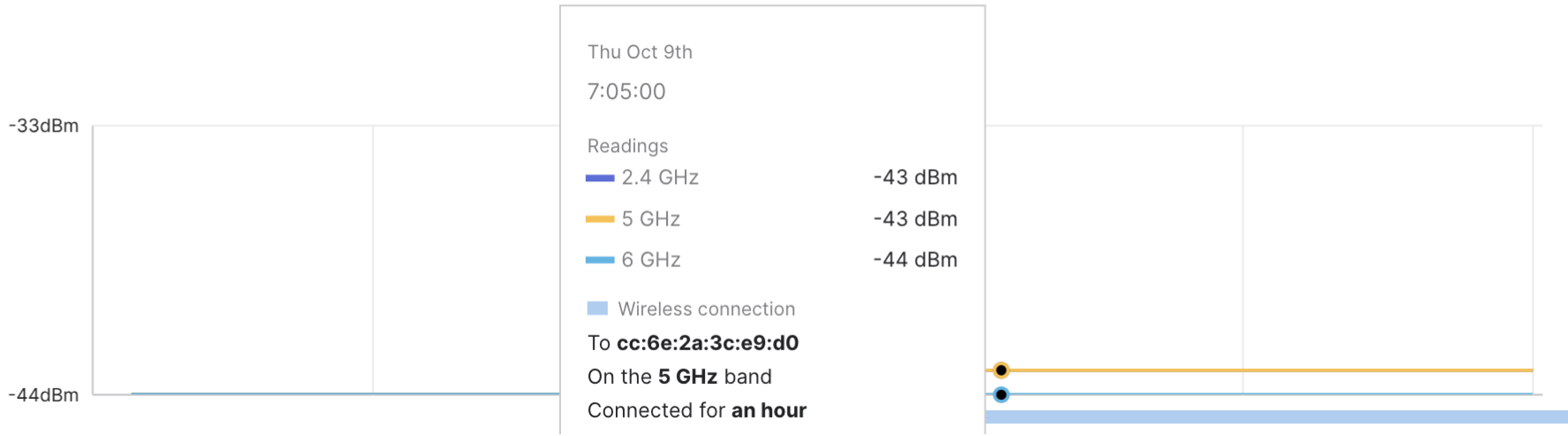
Wi-Fi 7 Client details on Meraki Cloud

Signal quality

in RSSI

2.4 GHz
100% Signal quality > -67dBm

5 GHz
100% Signal quality > -67dBm

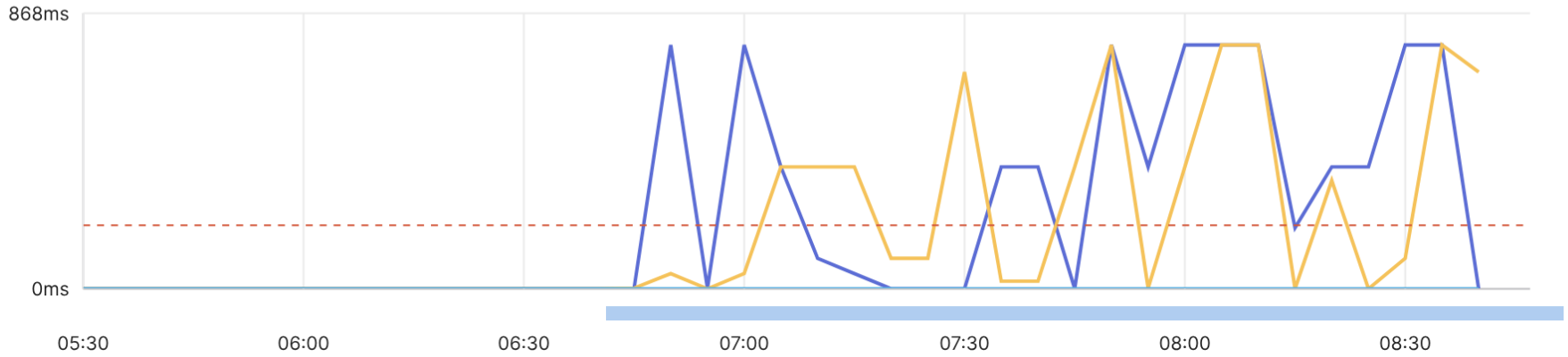


Average wireless latency

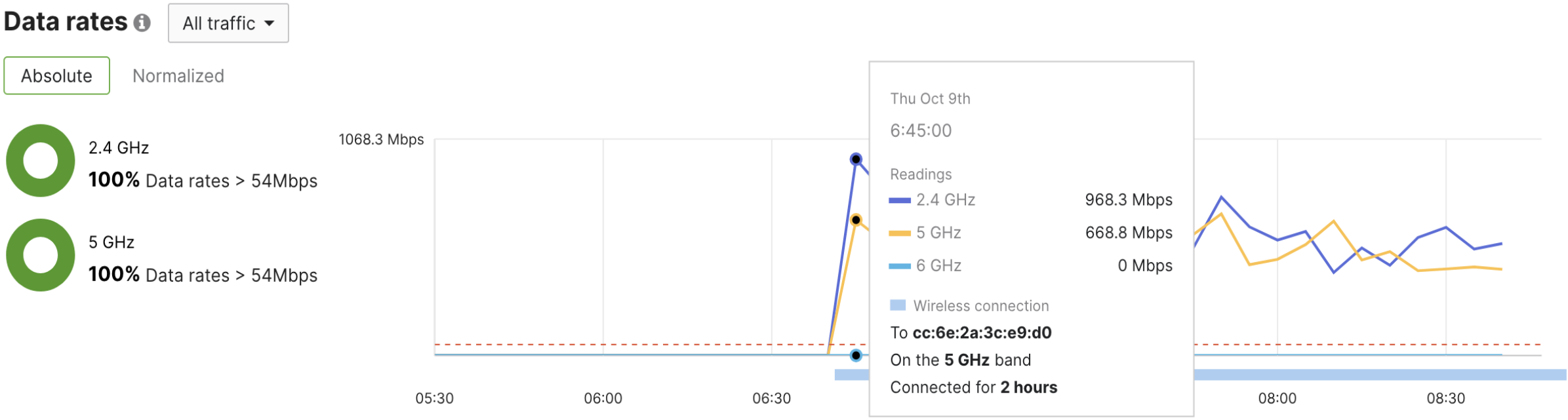
All traffic | Slowest APs

2.4 GHz
22% Wireless latency < 200ms

5 GHz
43% Wireless latency < 200ms



Wi-Fi 7 Client details on Meraki Cloud



Intelligent Capture

No.	Time	Source	Destination	Protocol	Length	Info
3034	2.347122	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1383, FN=0, Flags=....., BI=100, SSID="Aurora"
3038	2.347636	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1383, FN=0, Flags=....R..., BI=100, SSID="Aurora"
3042	2.348152	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1383, FN=0, Flags=....R..., BI=100, SSID="Aurora"
3046	2.348695	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1383, FN=0, Flags=....R..., BI=100, SSID="Aurora"
3130	2.369074	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1384, FN=0, Flags=....., BI=100, SSID="Aurora"
3134	2.369635	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1384, FN=0, Flags=....R..., BI=100, SSID="Aurora"
3138	2.370158	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1384, FN=0, Flags=....R..., BI=100, SSID="Aurora"
3139	2.370676	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1384, FN=0, Flags=....R..., BI=100, SSID="Aurora"
3142	2.371384	c2:6e:3a:3c:e9:d0	Broadcast	802.11	564	Beacon frame, SN=281, FN=0, Flags=....., BI=100, SSID="Aurora"
3144	2.371367	c2:6e:2a:3c:e9:d0	Broadcast	802.11	538	Beacon frame, SN=258, FN=0, Flags=....., BI=100, SSID="Aurora"
3208	2.387392	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1385, FN=0, Flags=....., BI=100, SSID="Aurora"
3211	2.387904	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1385, FN=0, Flags=....R..., BI=100, SSID="Aurora"
3213	2.388448	c2:6e:3a:3c:e9:d0	c2:42:a8:57:4d:92	802.11	534	Probe Response, SN=1385, FN=0, Flags=....R..., BI=100, SSID="Aurora"

```
▼ IEEE 802.11 Wireless Management
  ▼ Tagged parameters (454 bytes)
    ▶ Tag: VHT Operation
    ▶ Tag: Tx Power Envelope
    ▶ Tag: Reduced Neighbor Report
    ▶ Ext Tag: HE Capabilities
    ▶ Ext Tag: HE Operation
```

```
0000  00 00 30 00 6f 08 00 40   ea c2 bf 88 02 00 00 00   ..0.o..@  ........
0010  00 18 64 14 40 01 00 00   00 00 00 03 7f 00 10 00   ..d.@...  ........
0020  ca 3d 02 00 00 00 00 00   00 00 00 00 74 89 20 30   .=......  ....t. 0
0030  80 00 00 00 ff ff ff ff   ff ff c2 6e 2a 3c e9 d0   ........  ...n*<..
0040  c2 6e 2a 3c e9 d0 b0 0e   38 00 00 00 00 00 00 00   .n*<....  8.......
0050  64 00 11 15 00 06 41 75   72 6f 72 61 01 07 12 98   d.....Au  rora....
0060  24 b0 48 60 6c 05 04 00   01 00 00 07 1c 55 53 04   $.H`l...  .....US.
```

Event Logs

Event log for access points

Oct 8 23:29:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.1X	PMKSA cache match	radio: 0, vap: 3, group: , attr:
Oct 8 23:29:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.11	802.11 association	channel: 44, rssi: 53, band: 5
Oct 8 23:23:26	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.11	802.11 disassociation	client has left AP
Oct 8 23:23:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA authentication	
Oct 8 23:23:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA authentication	
Oct 8 23:23:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.1X	PMKSA cache match	radio: 0, vap: 3, group: , attr:
Oct 8 23:23:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.11	802.11 association	channel: 44, rssi: 54, band: 5
Oct 8 23:17:26	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.11	802.11 disassociation	client has left AP
Oct 8 23:17:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA authentication	
Oct 8 23:17:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA authentication	
Oct 8 23:17:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.1X	PMKSA cache match	radio: 0, vap: 3, group: , attr:
Oct 8 23:17:09	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.11	802.11 association	channel: 44, rssi: 54, band: 5
Oct 8 23:11:12	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.11	802.11 disassociation	client has left AP
Oct 8 23:11:12	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA deauthentication	radio: 1, vap: 3, client_mac: F4:52:93:2D:99:CB « hide is_mld true assoc_mac 36:4D:DF:72:15:56
Oct 8 23:11:12	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA deauthentication	radio: 0, vap: 3, client_mac: F4:52:93:2D:99:CB « hide is_mld true assoc_mac 36:4D:DF:72:15:56
Oct 8 23:10:52	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA authentication	
Oct 8 23:10:52	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	WPA	WPA authentication	
Oct 8 23:10:52	cc:6e:2a:3c:e9:d0	Aurora	f4:52:93:2d:99:cb	802.1X	PMKSA cache match	radio: 0, vap: 3, group: , attr:

30 total

Unified Licensing Commands

- Default License state of AP after join
  - show ap summary license
  - show ap name <AP Name> config general
    - License Type
    - License State
    - Non-Compliance Reason
- License consumption and RUM reports
  - show license rum id all
  - show license summary
  - license smart sync all
- Show commands to refer the AP list for added, bulk, deleted, no-change and summary
  - show license cw entities added
  - show license cw entities summary
- show license tech support
- show license history message import compliance

Akash's Take on Wi-Fi 7

Feature	Theory	Practical Reality
4096-QAM (4K-QAM)	12 bits/symbol, +20% throughput vs 1024-QAM; needs ~40 dB SNR.	Works only close to AP (~5–10 m LOS); falls back to 1024-/256-QAM with distance.
320 MHz channel bonding	Doubles bandwidth (vs 160 MHz).	Usable mainly in 6 GHz band; rare in dense or DFS-limited areas.
Multi-Link Operation (MLO)	Combines 5 + 6 GHz links for speed & low latency.	Adopted in premium clients for complete MLO functionality. As clients are limited in which mode they support.
Lower Latency (EHT MAC changes)	Multi-Link redundancy + TID-to-Link Mapping can cut latency to <2 ms in theory.	Typically, 10–20% improvement; depends on load and interference.
6 GHz Operation	Up to 1.2 GHz clean spectrum	Region-dependent; regulatory limits affect channel width and power.

Why Wi-Fi 7

Future-Proof Investment

- Wi-Fi 6/6E & 7 ready
- Scalable hardware
- Long-term stability
- Evolving device ecosystem

Smart Spaces & AI Integration

- Smarter scheduling
- Improved OFDMA / MU-MIMO
- Cleaner RF design
- High-density efficiency

Better Performance Today

- Clean spectrum
- Multi-Link Operation (MLO)
- Low latency, high reliability
- AR/VR, gaming, high-throughput

Enterprise-Grade Features

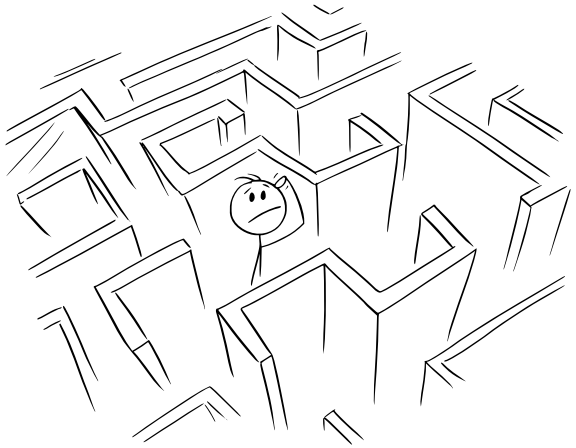
- IoT & automation
- Real-time analytics
- Smart offices & cities
- Massive device handling

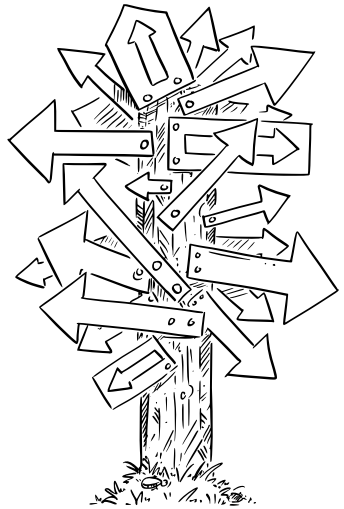
6 GHz & Multi-Link Ready

- Mission-critical reliability
- Ultra-low latency
- TWT, WPA3, enhanced scheduling
- Healthcare, finance, campus

Q&A

How can I help you today?





Thank you

Complete your session evaluations

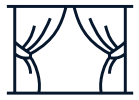
Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

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

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

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

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

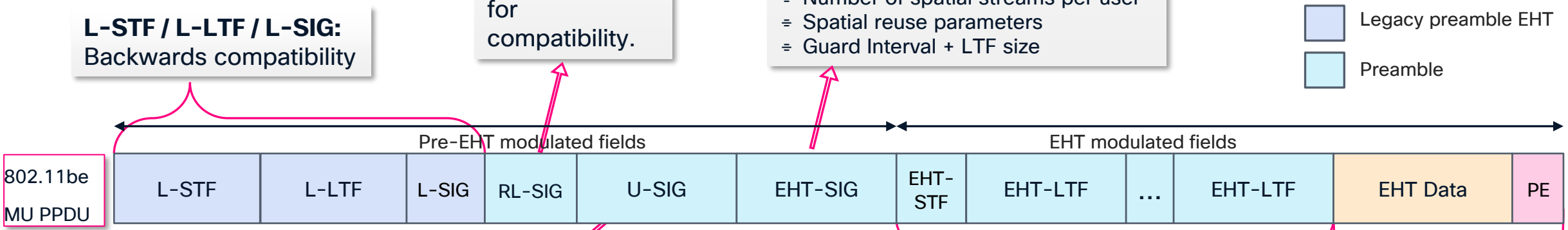

CISCO

Management Changes in .be – PPDU Layer

L-STF / L-LTF / L-SIG:
Backwards compatibility

RL-SIG:
Repeats legacy rate/length info for compatibility.

EHT-SIG: Carries specific per-user parameters:
- RU allocation (OFDMA)
- STA ID
- MCS & coding rate (e.g., 4096-QAM MCS12/13)
- Number of spatial streams per user
- Spatial reuse parameters
- Guard Interval + LTF size



U-SIG (Universal Signal field):
Introduces PHY Version Identifier so future standards after 802.11be can be auto-detected.

EHT-STF & EHT-LTF: Synchronization and MIMO channel estimation:
- EHT-LTF types: 1×, 2×, 4× symbol duration depending on GI requirements.
- Number of EHT-LTF symbols increases with spatial streams.

Data Field & Packet Extension:
The actual payload (MAC frames), modulated per-user according to MCS.
Packet Extension keeps transmit power continuity for CCA purposes.