

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

CISCO Live !

Akash Malkood
Sr. Customer Delivery Engineering Technical Leader, TAC

Cisco Webex App

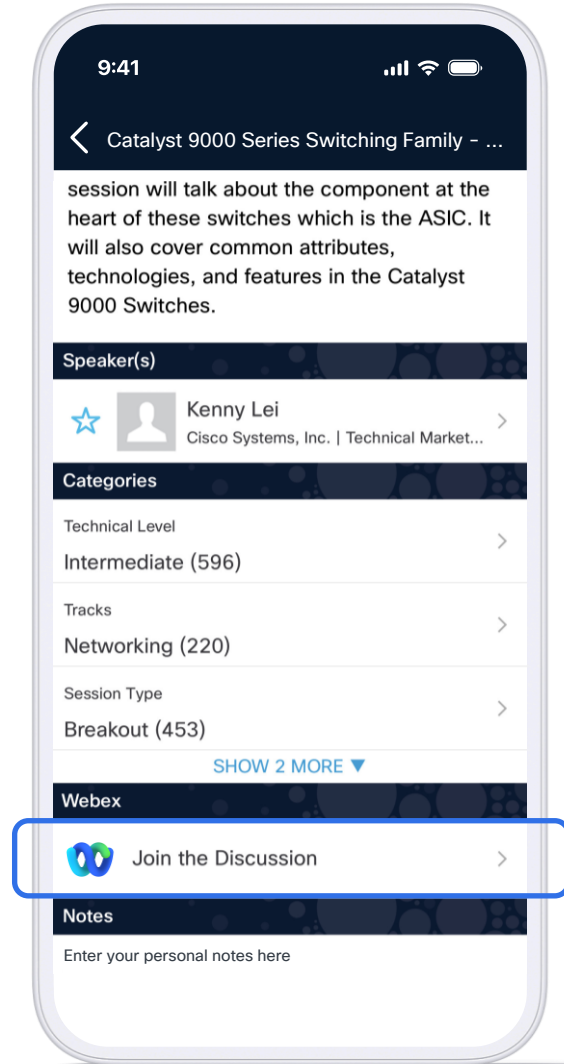
Questions?

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://cislive.ciscoevents.com/cislivebot/#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)

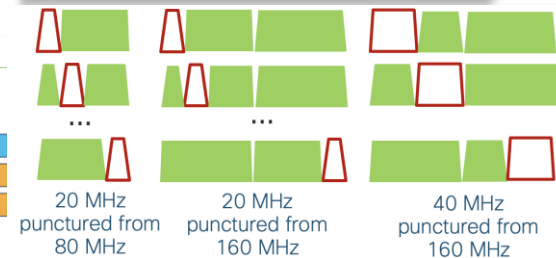
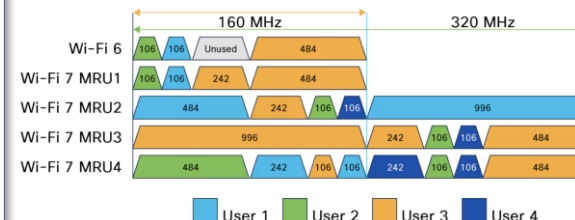
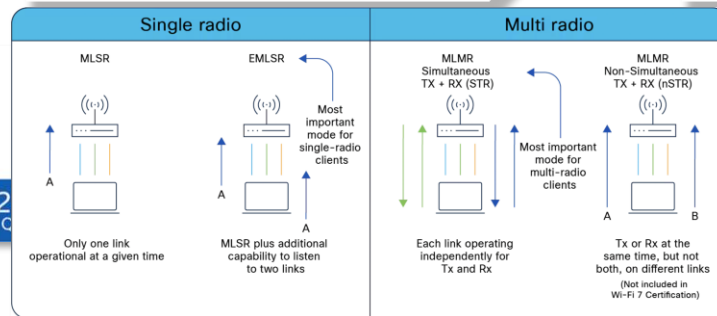
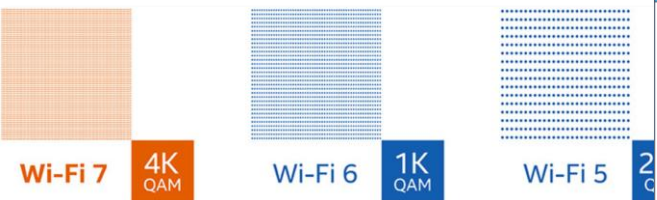
- **2.4GHz + 5GHz or 5 GHz + 6 GHz**, multi-band aggregation
- **2 Methods** : STR (Simultaneous TX/RX) and EMLSR (shared-radio mode)

🧬 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



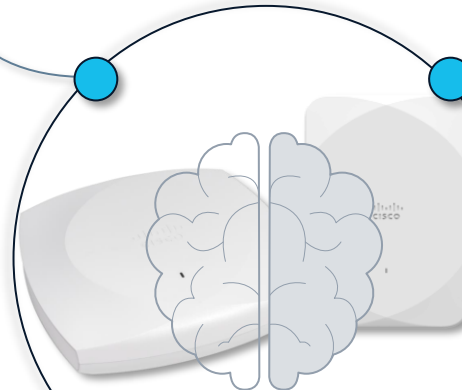
- Omni-Directional Antenna
- 2.4 GHz Serving Radio 2x2:2SS
- 5 GHz Serving Radio 2x2:2SS*
- 6 GHz Serving Radio 2x2:2SS
- Tri-band scanning Radio
- 2.4 GHz IoT Radio (BLE)



CleanAir Pro



- Global Use AP
- CleanAir Pro
- CW9172I - 17.15.2b
- CW9172H - 17.17.1



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

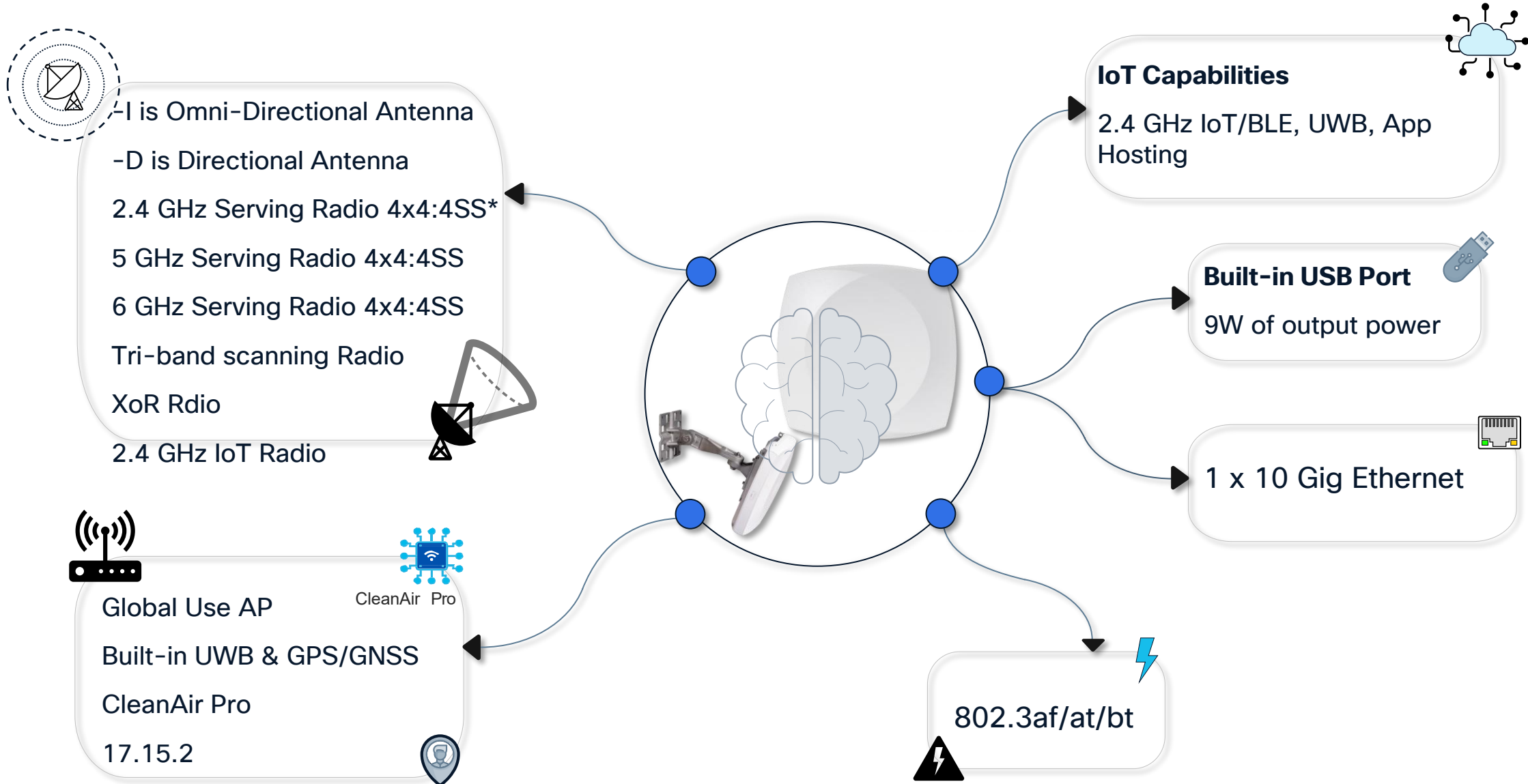
CW9172I:

- 1 x 2.5Gbps

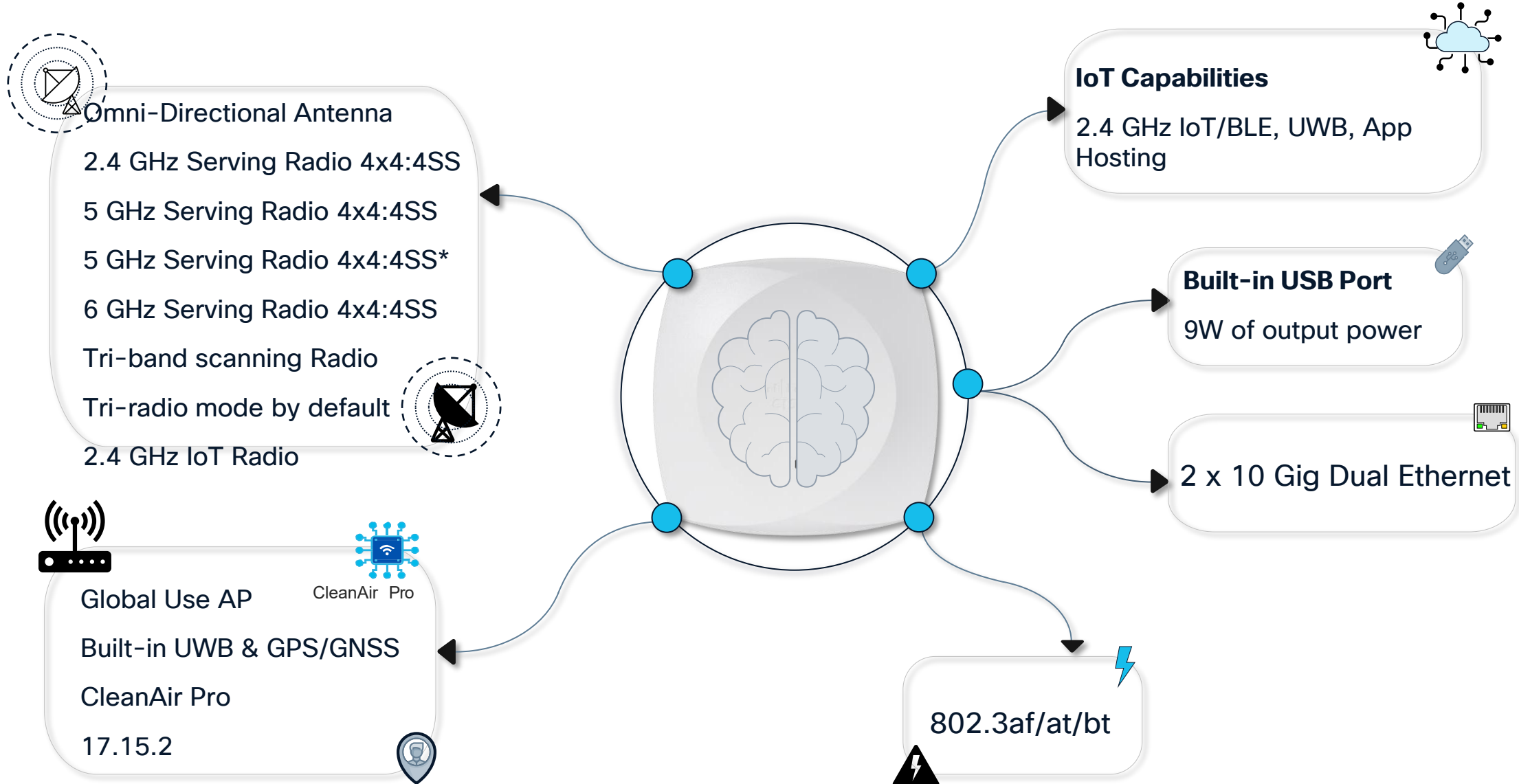
802.3af/at/bt or DC jack



Cisco Wireless CW9176I & D Access Point



Cisco Wireless CW9178 Access Point





What is GUAP?



Regulatory Domain?



What about licensing?

How do I onboard the GUAP?

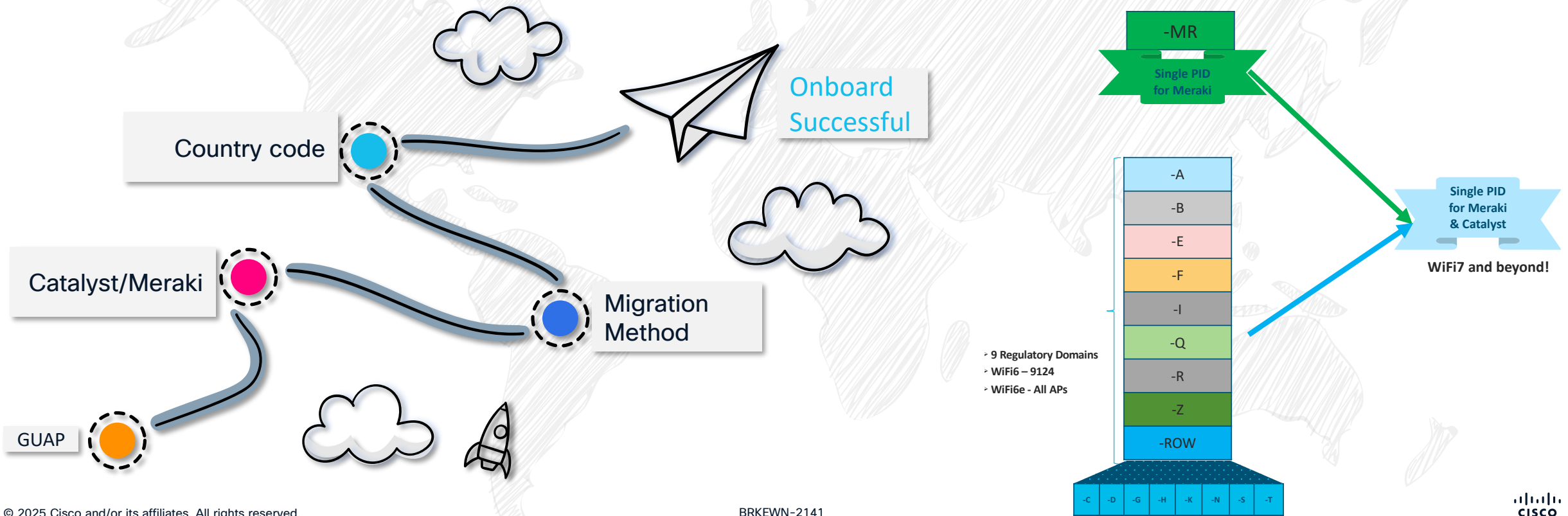
What is GUAP?

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?



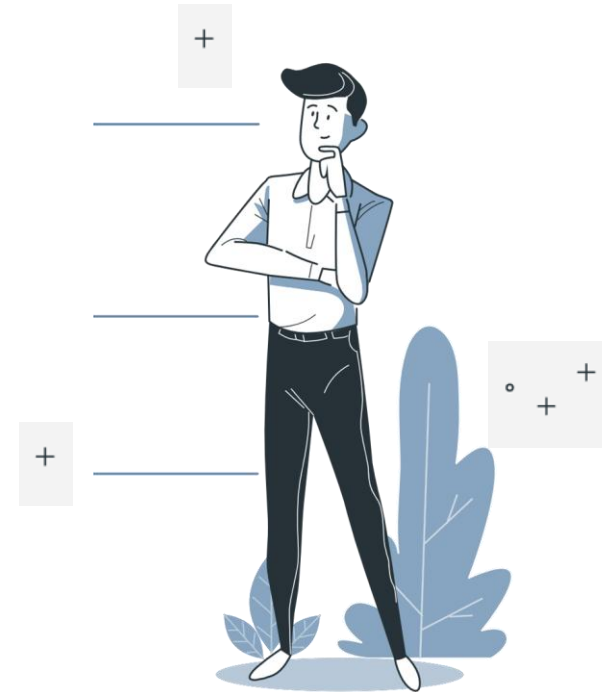
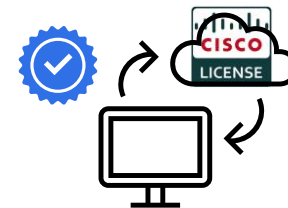
✓ Meraki Account/ GPS/ Hardcoded country code AP



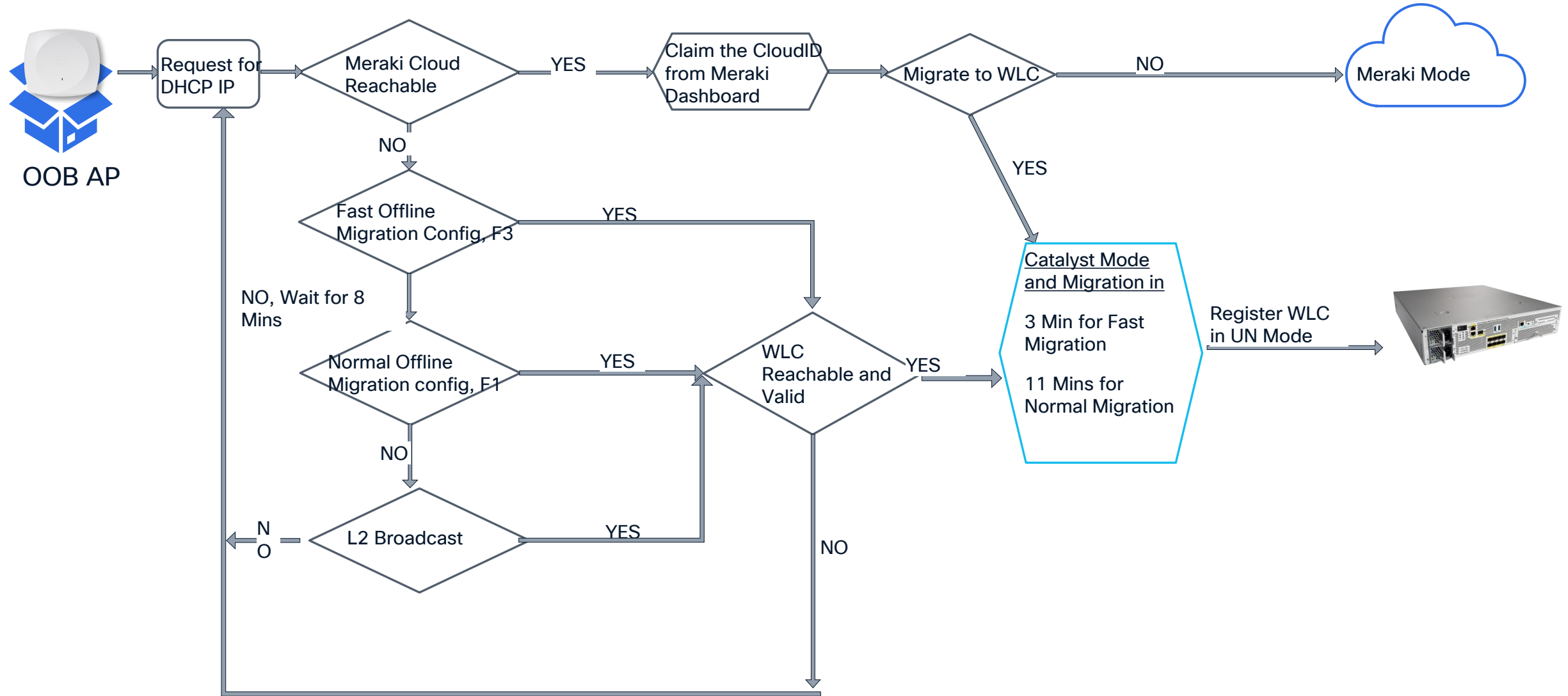
✓ 9800 WLC



✓ Unified Licenses



OOB Mode of Operation

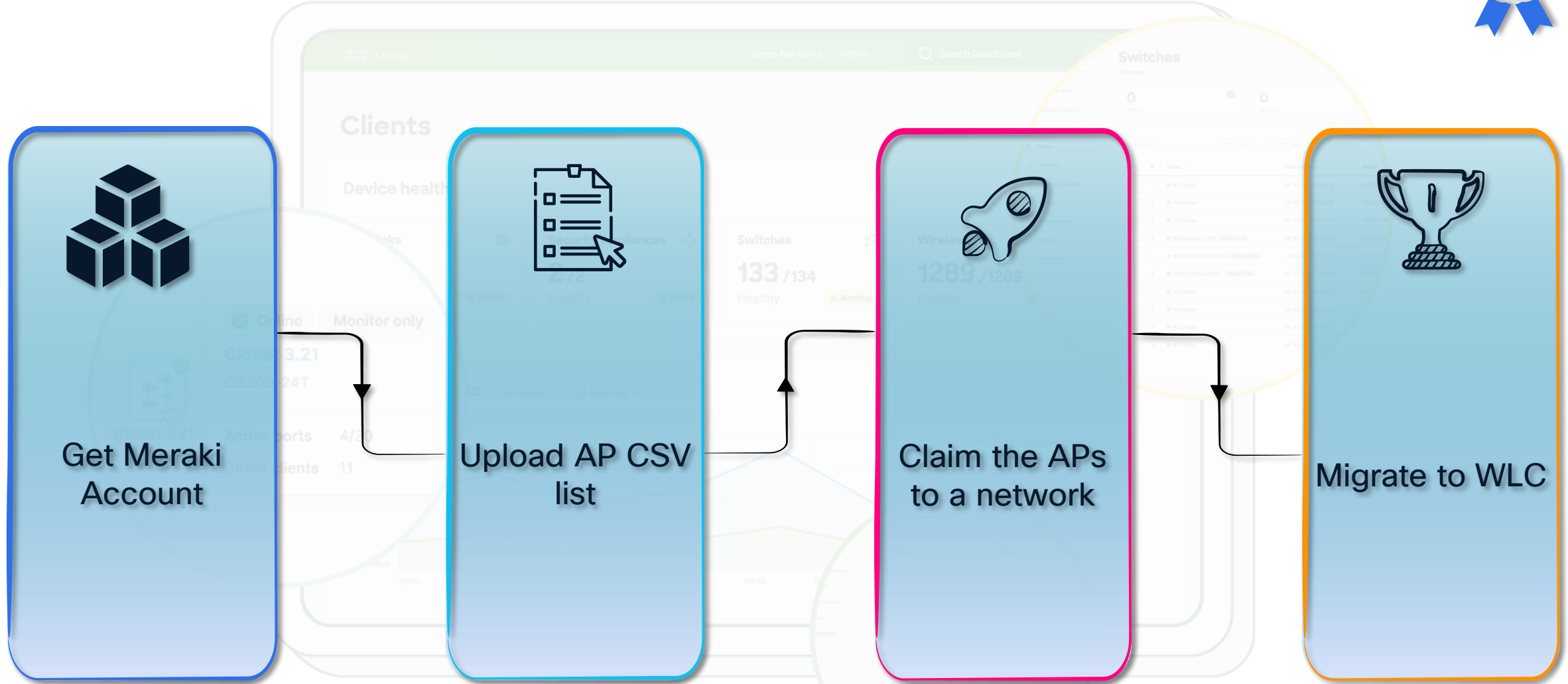


OoB Mode of Operation

```
<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

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

Access Points

Last day ▾

+ Add access point

Overview List Health Map Connection log Timeline


 Recommendations from Network Like Yours **reduce latency by up to 40%** [Run diagnostics](#)


2 Offline

 2 Alerting

 3 Online








3 Repeaters

 Filters 3 results [Reset all](#)

 1 Item selected [Select all 3 items](#)


Cancel

▾

	Status	Model	Name	MAC address	Connectivity (UTC+8)	Serial number	Local IP	Public IP	Tags	
<input checked="" type="checkbox"/>		CW9178I								
<input type="checkbox"/>		CW9176I								
<input type="checkbox"/>		CW9176D1								

This option is NEW, only available for Wi-Fi 7 (single PID AP) mode conversion

Migrate 1 access point to WLC Management Mode?

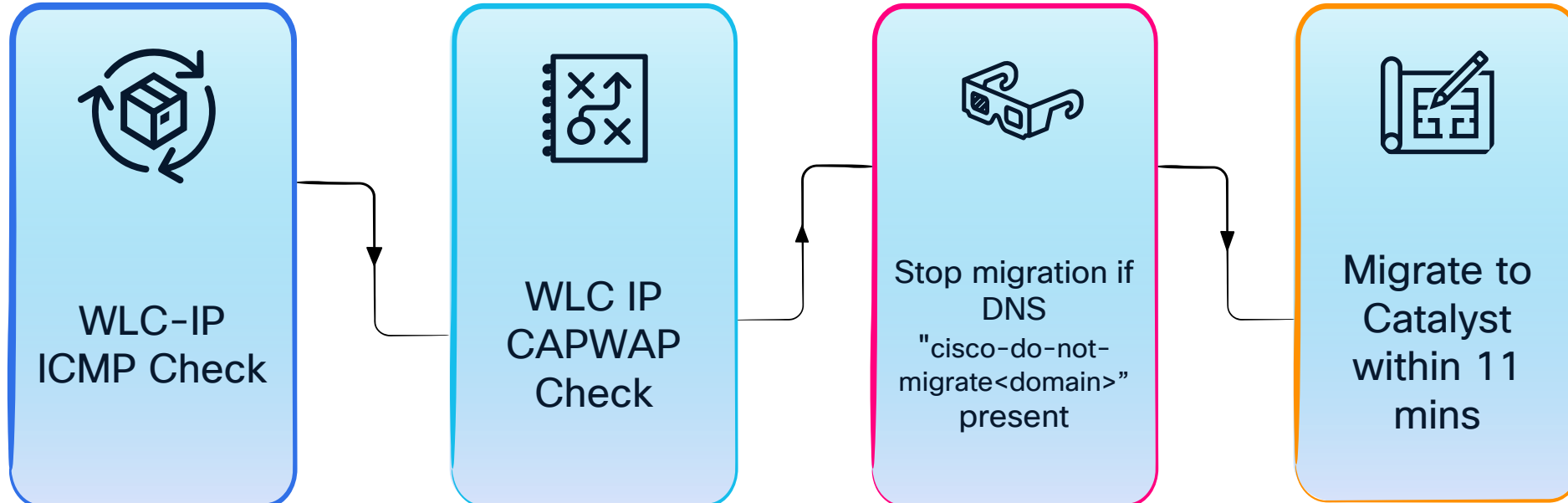
 Migration successfully initiated

▾

Device Name	Model	MAC	CloudID	Cisco serial number
	CW9178I			

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 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 00:01:01.528] 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)

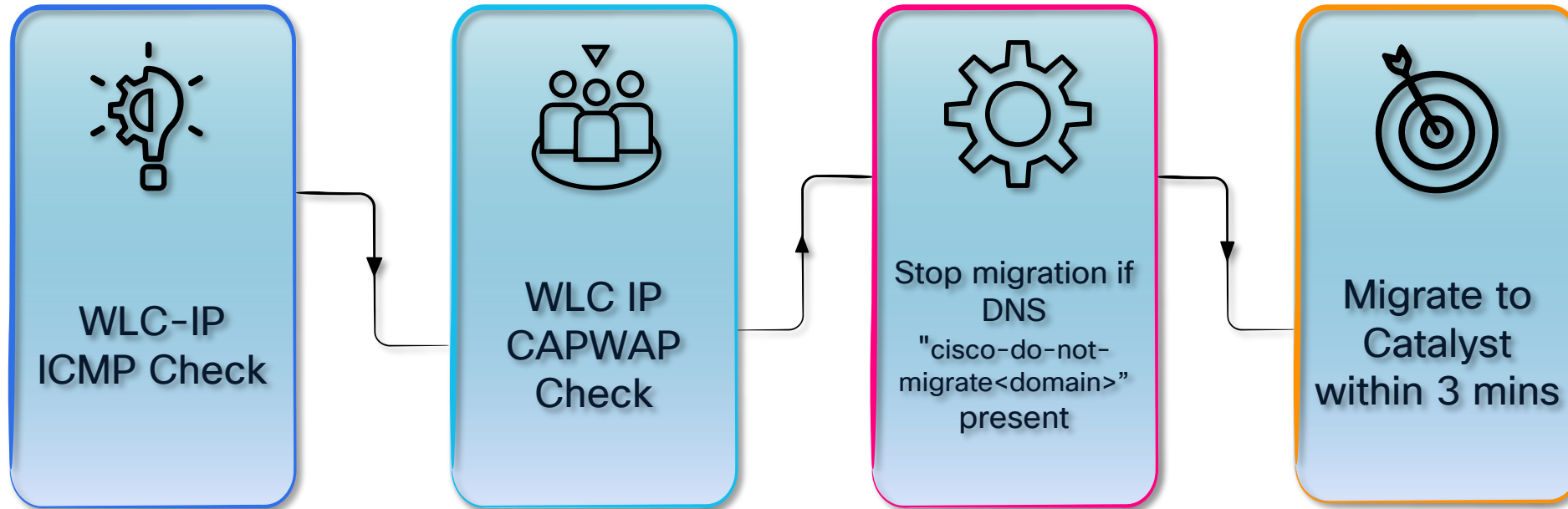
AP Console log - DHCPv4

AP Console log - DNS

```
<Meraki> offline-migration-info
| [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
| [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 00:10:07.71 ] [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
```

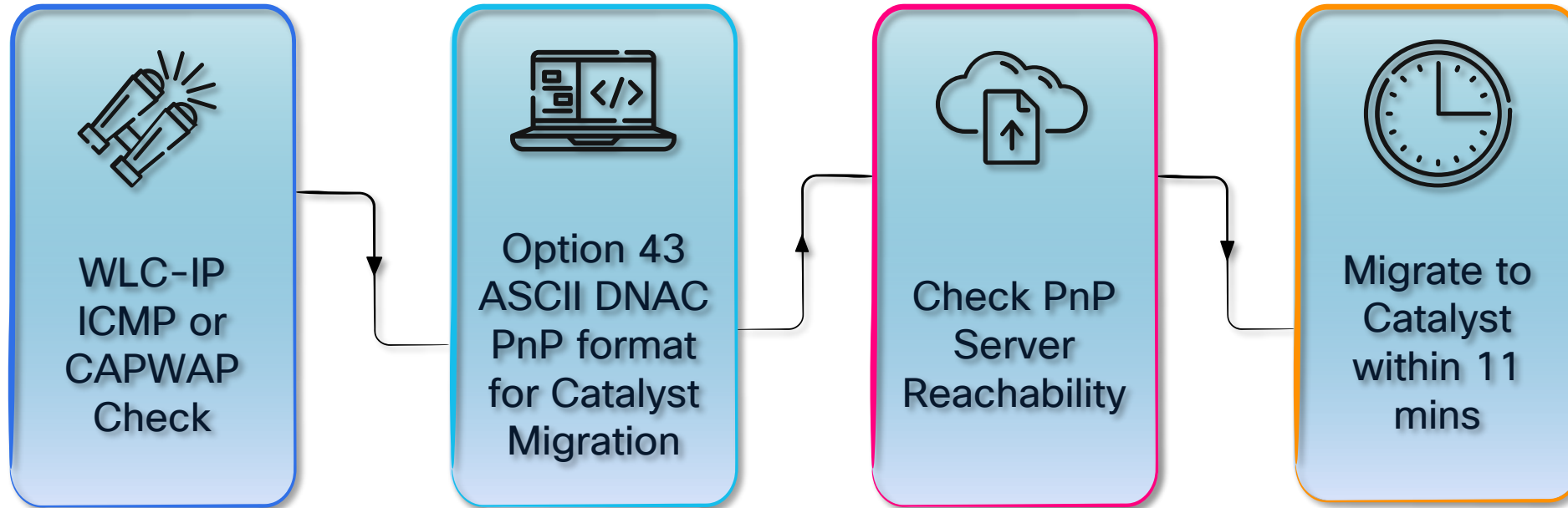
```
| [2000-01-01 00:01:47.251] [init] start offline migration detection
```

```
| [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
```

```
The system is going down NOW!  
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 migration

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 migration

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
```

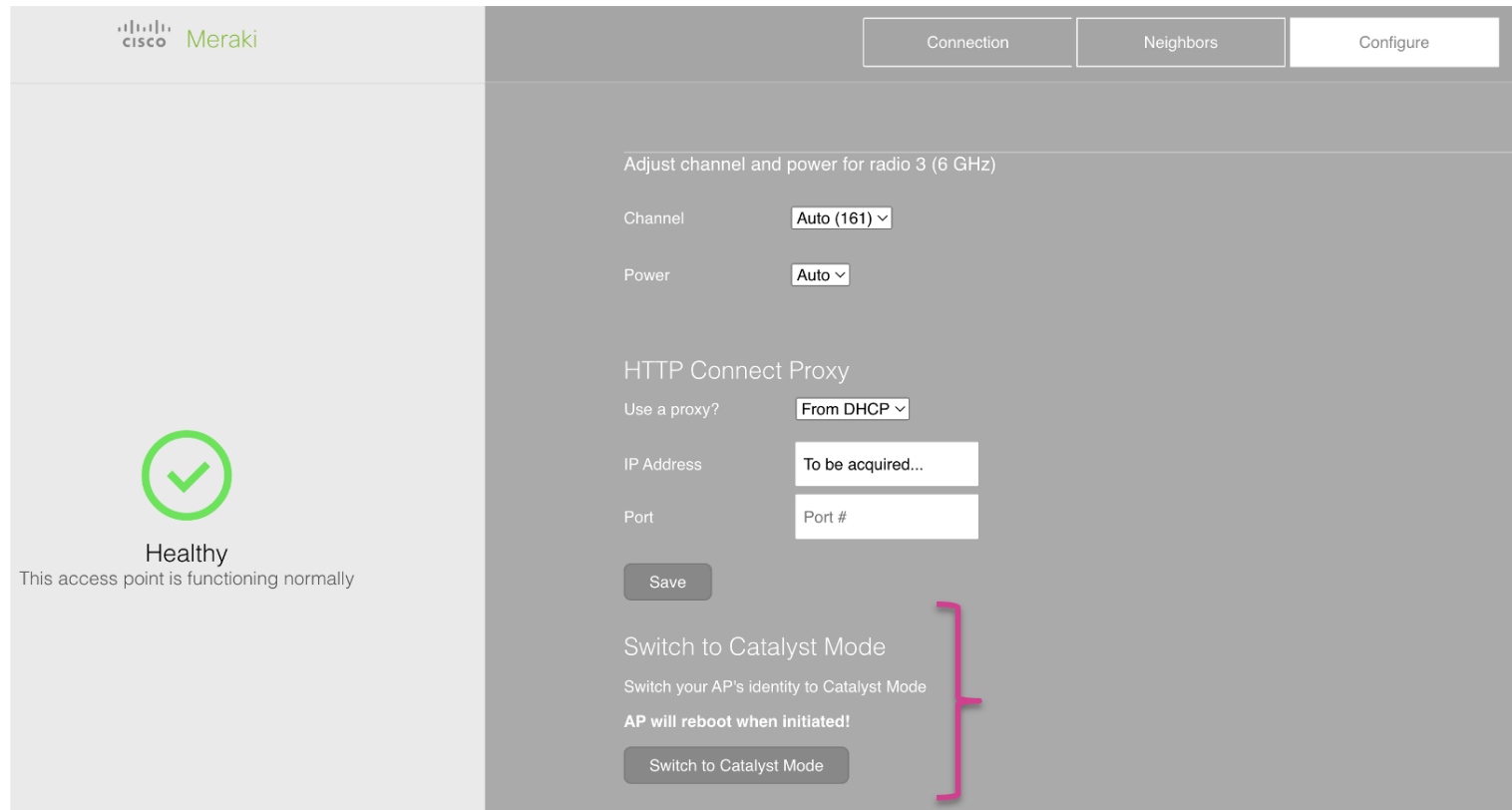
AP Console log - Running Meraki OS

```
[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)

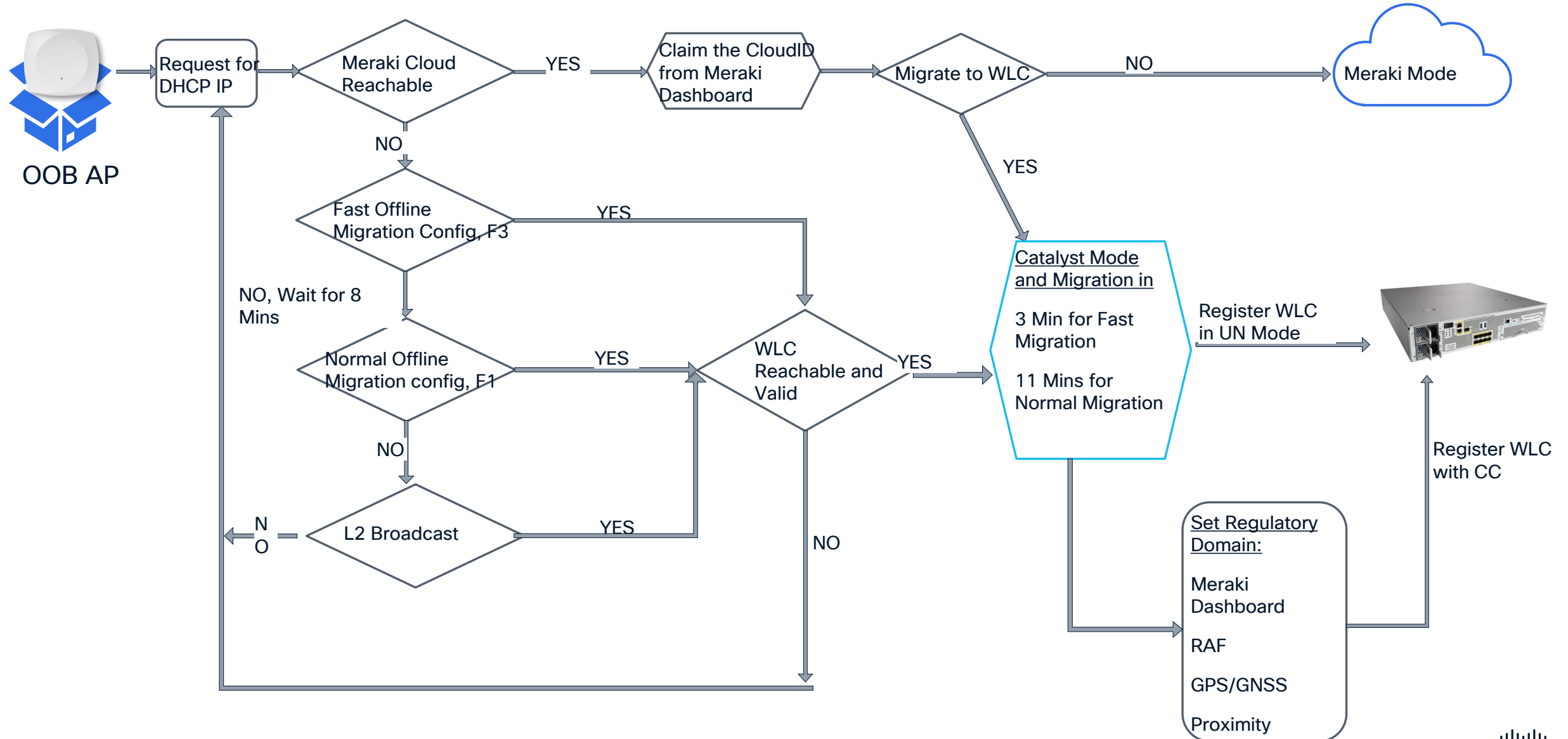
- Post fast offline migration, AP will broadcast default SSIDs – Meraki or Meraki-XXXX
- Connect to Meraki SSID
- Access the AP Local page at 10.128.128.126 with credentials Username: CloudID, Password: <blank>
- In the configure tab, click on ‘Switch to Catalyst Mode’



The screenshot shows the Meraki AP Local Status Page. On the left, a green checkmark icon is displayed above the text "Healthy" and "This access point is functioning normally". On the right, the "Configure" tab is active, showing settings for radio 3 (6 GHz). The "Channel" is set to "Auto (161)" and "Power" is set to "Auto". Under the "HTTP Connect Proxy" section, "Use a proxy?" is set to "From DHCP", "IP Address" is "To be acquired...", and "Port" is "Port #". A "Save" button is located below these settings. At the bottom, there is a "Switch to Catalyst Mode" button, which is highlighted with a pink bracket. Below this button, the text "Switch your AP's identity to Catalyst Mode" and "AP will reboot when initiated!" is displayed.

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 04:25:56.3064] 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



Resolved the Country Code via
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.
```



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

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

when MR 27 firmware becomes Generally Available.

General

Network name: Cisco-EN-Aurora-DMZ

Network enrollment string: [Empty]

This unique identifier can be used for endpoint enrollment and easy access through the Meraki endpoint page or the Self Service Portal.

Preview of Self Service Portal URL: <https://portal.meraki.com/your-enrollment-string-sm>

Please note that changing this field may cause existing bookmarks to break. All networks that are part of this combined network will have their enrollment string appended by '-network_type'.

Network notes: [Empty]

Country/Region: **United States**

Manual enforcement options: [Revert network to auto-detection]

Regulatory domain: FCC

Regulatory info: [Download regulatory file]

Local time zone: America - Los Angeles (U...)

Administration > Regulatory Activation

This is a workflow to provision a specific regulatory domain on APs that are not factory programmed with one.

Step 1 - Obtain the 'Regulatory Activation File' from Meraki Dashboard and upload it here.

Step 2 - Post upload, confirm applying the changes after reviewing the impact report.

Visit the [AP Configuration Page](#) to view the regulatory domain changes on the joined APs.

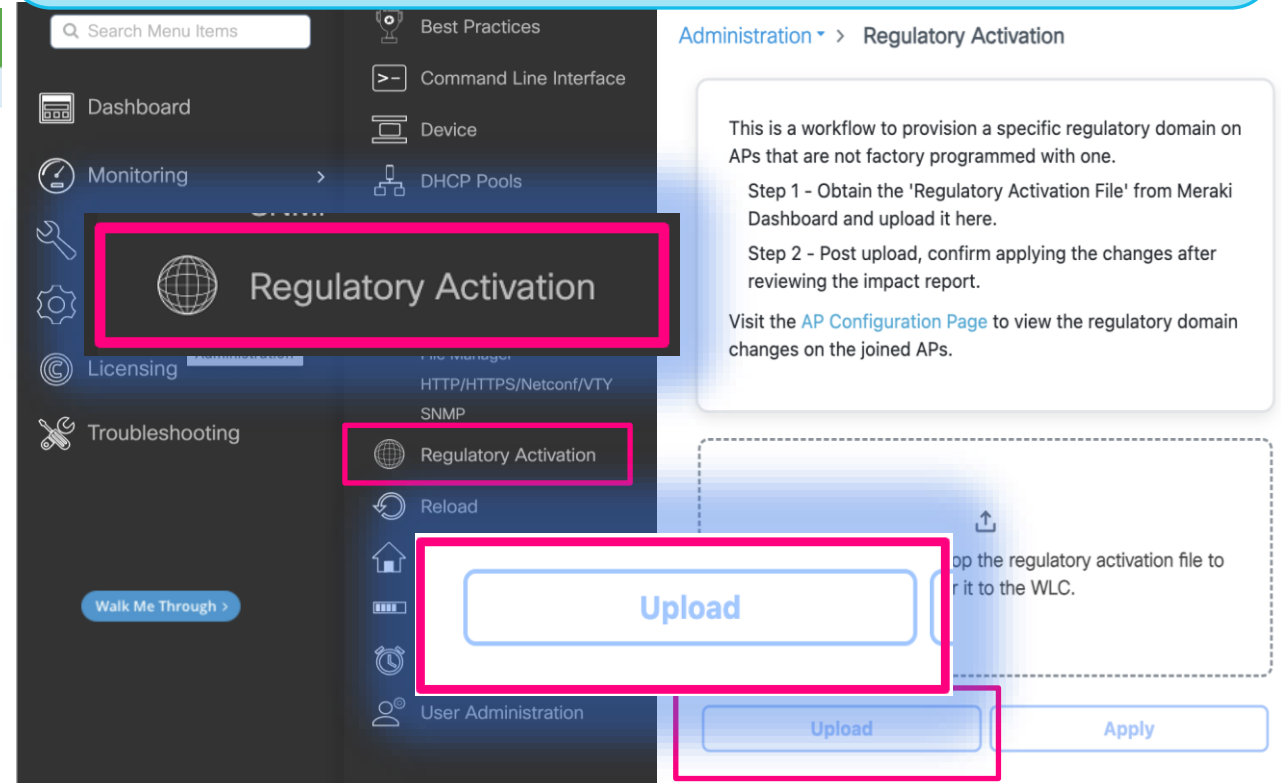
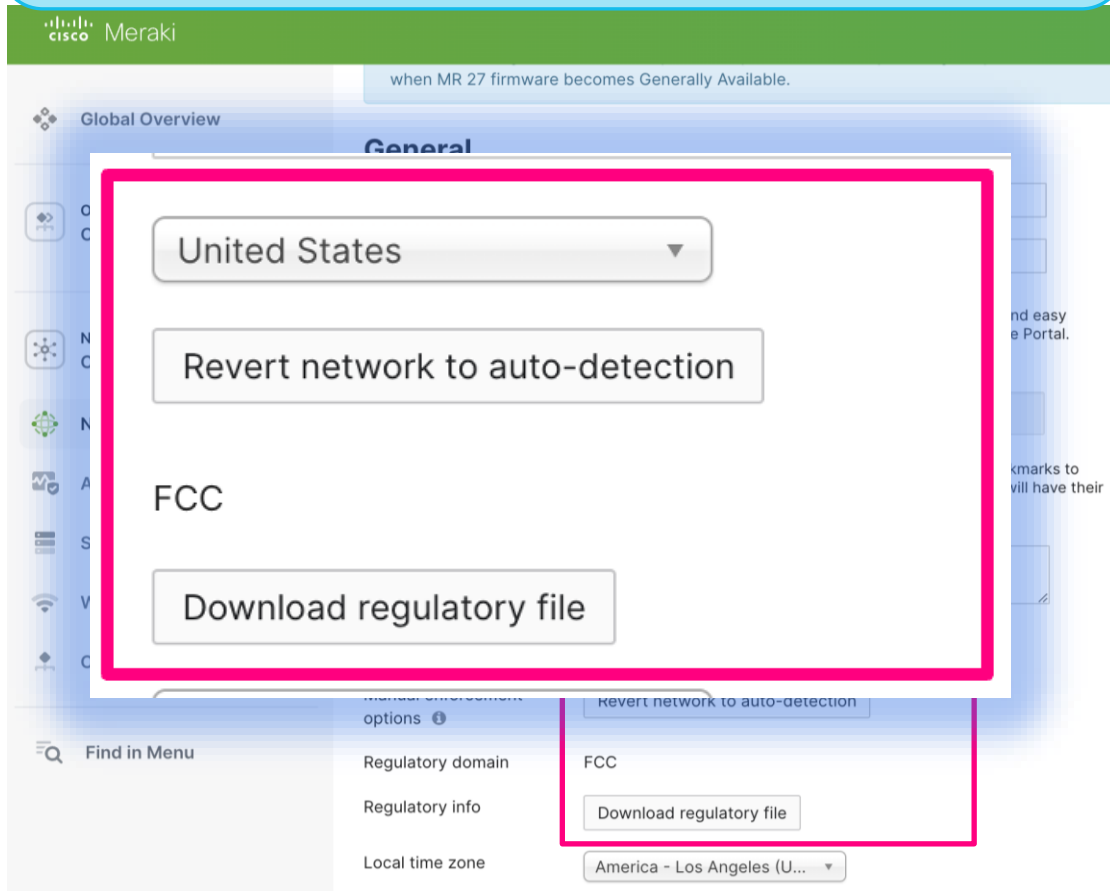
Click here or drag and drop the regulatory activation file to transfer it to the WLC.

Upload **Apply**

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



Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Walk Me Through >

Administration > Regulatory Activation

This is a workflow to provision a specific regulatory domain on APs that are not factory programmed with one.

Step 1 - Obtain the 'Regulatory Activation File' from Meraki Dashboard and upload it here.

Step 2 - Post upload, confirm applying the changes after reviewing the impact report.

Visit the [AP Configuration Page](#) to view the regulatory domain changes on the joined APs.

Click here or drag and drop the regulatory activation file to transfer it to the WLC.

regulatory_domain_blob.j

Upload

The file has been validated successfully. Click the changes.

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Walk Me Through >

0 Invalid Domain ✖ 1 Regulatory Mismatch ! 67 Not Impacting ✔

AP MAC Country Code Serial Number

Validation Result

AP MAC	Country Code	Serial Number	Validation Result
da40		370E3G	Not World Wide Mod
1a10	US	4504K6	Not World Wide Mod
1a20	US	4504K7	Not World Wide Mod
10aa0	US	01170F	Not World Wide Mod
.0310		050003	Not World Wide Mod
.0550	US	050015	Not World Wide Mod

Administration > Regulatory Activation

This is a workflow to provision a specific regulatory domain on APs that are not factory programmed with one.

Step 1 - Obtain the 'Regulatory Activation File' from Meraki Dashboard and upload it here.

Step 2 - Post upload, confirm applying the changes after reviewing the impact report.

Visit the [AP Configuration Page](#) to view the regulatory domain changes on the joined APs.

Click here or drag and drop the regulatory activation file to transfer it to the WLC.

Upload Apply

0 Invalid Domain ✖ 0 Regulatory Mismatch ! 0 Not Impacting ✔

Changes are being provisioned. During this process, the impacted APs will disconnect temporarily and rejoin the WLC.

AP MAC Country Code Serial Number

Validation Result

AP MAC	Country Code	Serial Number	Validation Result
--------	--------------	---------------	-------------------

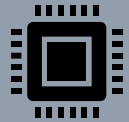
No data found!

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-Coordinates [Longitude, 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-Coordinates [Longitude, Latitude] to WLC

```
--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
```



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



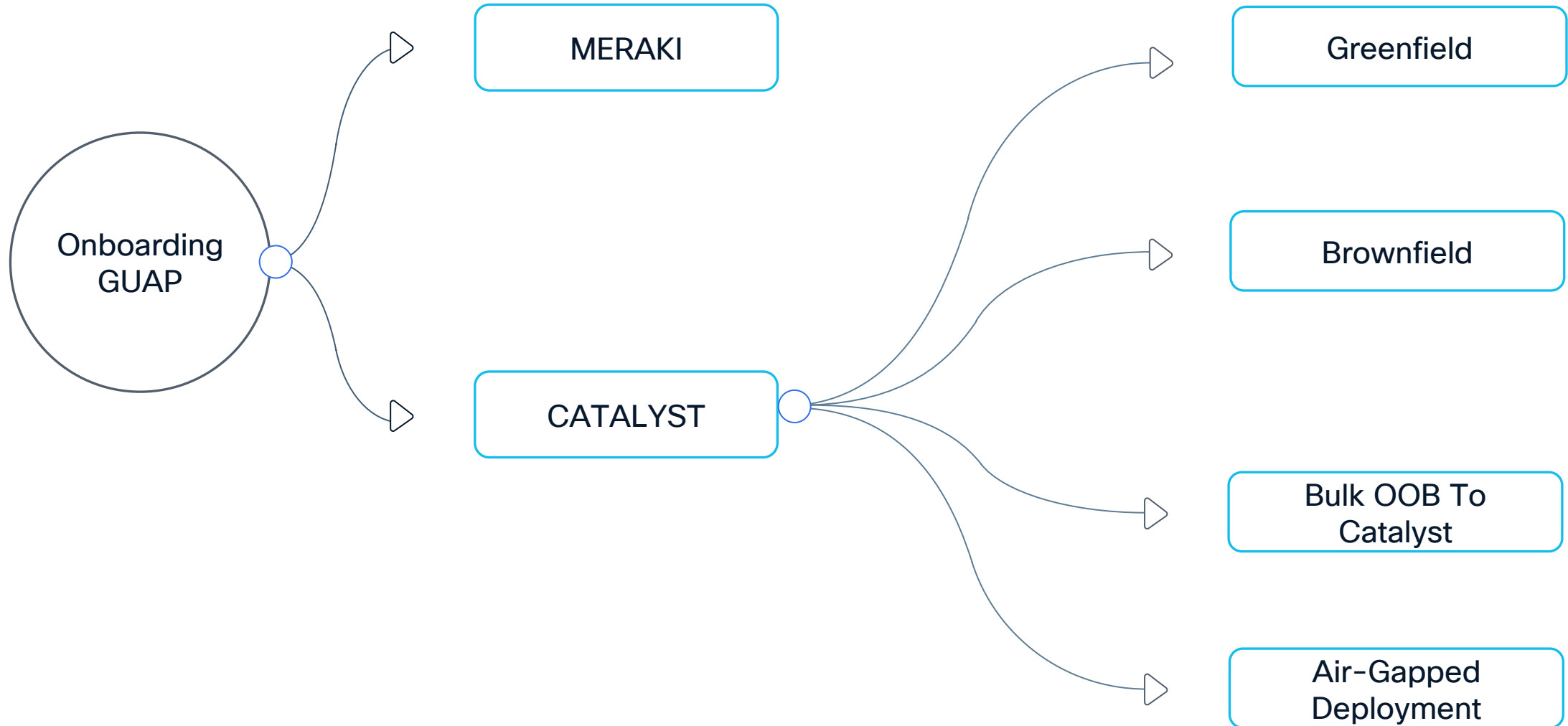
```
[*04/25/2024 13:44:26.9084] GPS/GNSS signal acquired
[*04/25/2024 13:44:26.9345] Country Code US resolved through GPS/GNSS
[*04/25/2024 13:44:26.9779] AP Rebooting: Reset Reason - Country Code Changed
```



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

```
[ 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 \geq 17.15.3; reachable
RAF uploaded
site-tag country matches target site





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.

OOB AP



Normal Trigger COS



Proximity CC



Join WLC &
Radios Up



Scenario 3 - Bulk OOB to Catalyst



Onboarding

Primary: Meraki Dashboard

Secondary: Fast Offline migration

Regulatory Domain

Primary: RAF

Backup: Proximity

Operations and Planning

Batches per building/floor
Validate WLC IP

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



Scenario 4: Air-Gapped Deployment

Onboarding

Primary: Fast Offline Migration

Secondary: Normal Offline migration

Regulatory Domain

Primary: RAF/GPS

Backup: Proximity

Operations and Planning

Based on above scenarios we can decide on the Operations and Planning.



OOB AP

Fast Trigger

COS

RAF CC in Bulk

Join WLC & Radios Up

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.<do main>	Normal	CAPWAP to resolved IP.	ip host cisco-capwap- controller.cisco.com 200.1.0.100	Publish cisco-do-not-automigrate.<dom ain>.
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;J8 0	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



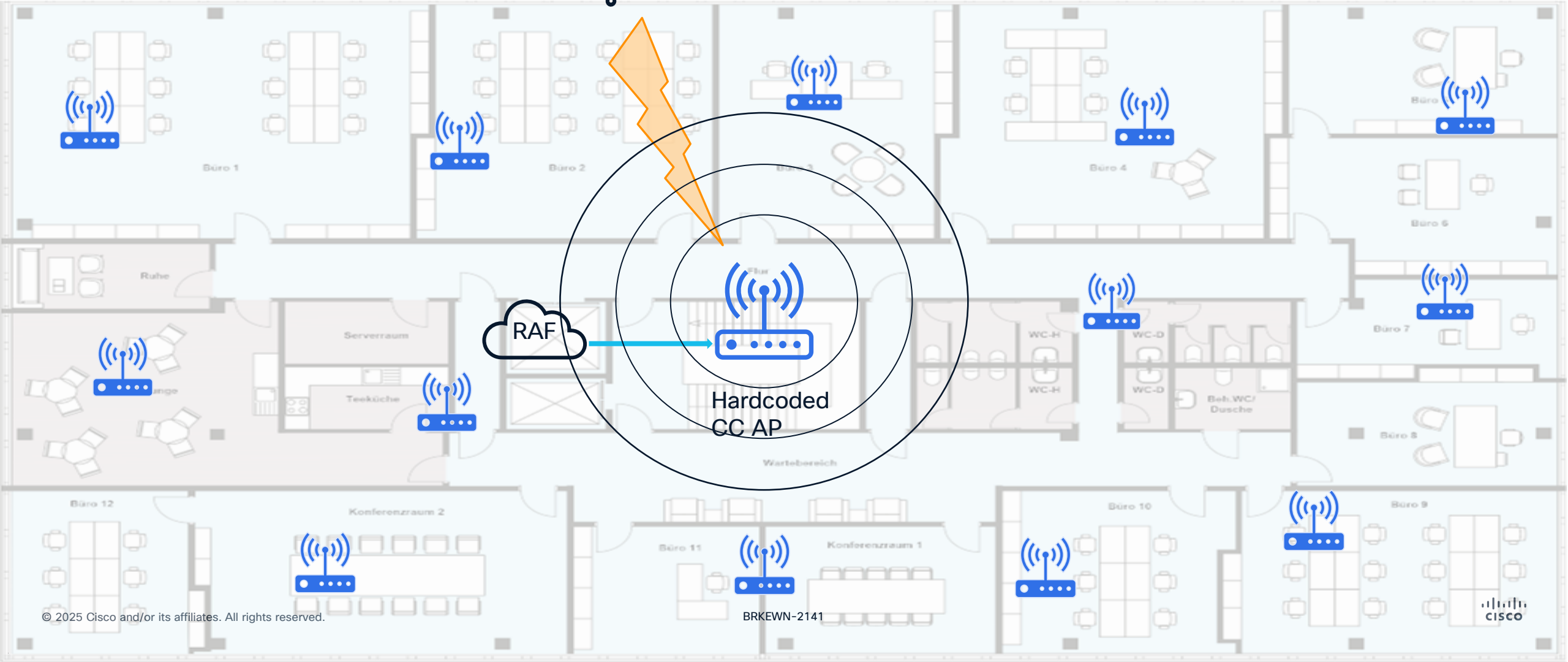
Method	How Country Is Determined	Best Fit Scenarios	Limitations / Edge Cases	Validation (WLC/AP)
Meraki Cloud (Geo IP)	AP reaches Dashboard; country inferred from Geo IP and stored with device.	Cloud-ready sites; hybrid deployments.	Depends on public IP geolocation accuracy; not applicable in air-gapped 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

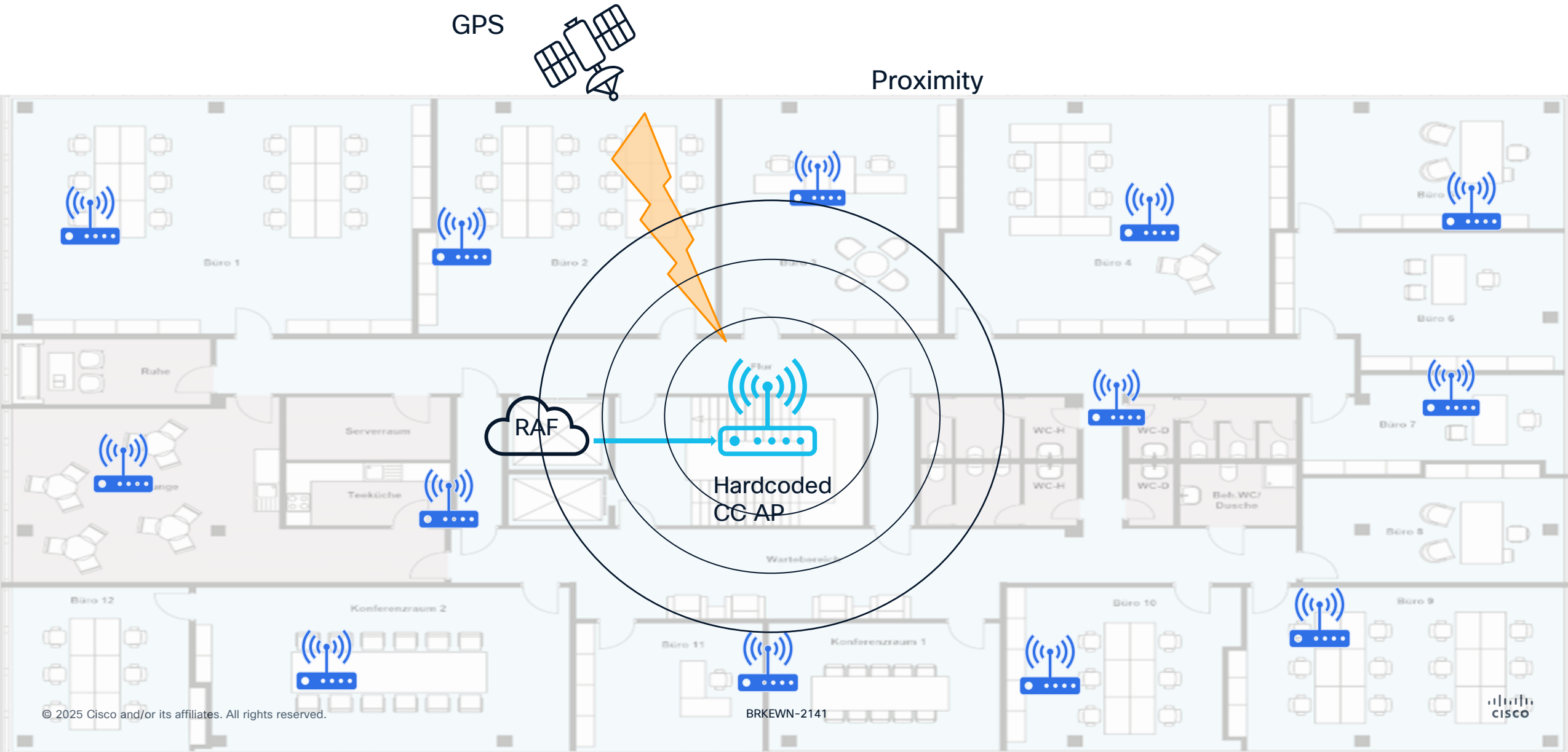
GPS



Proximity



Country Code for Bulk Migration – Best Method

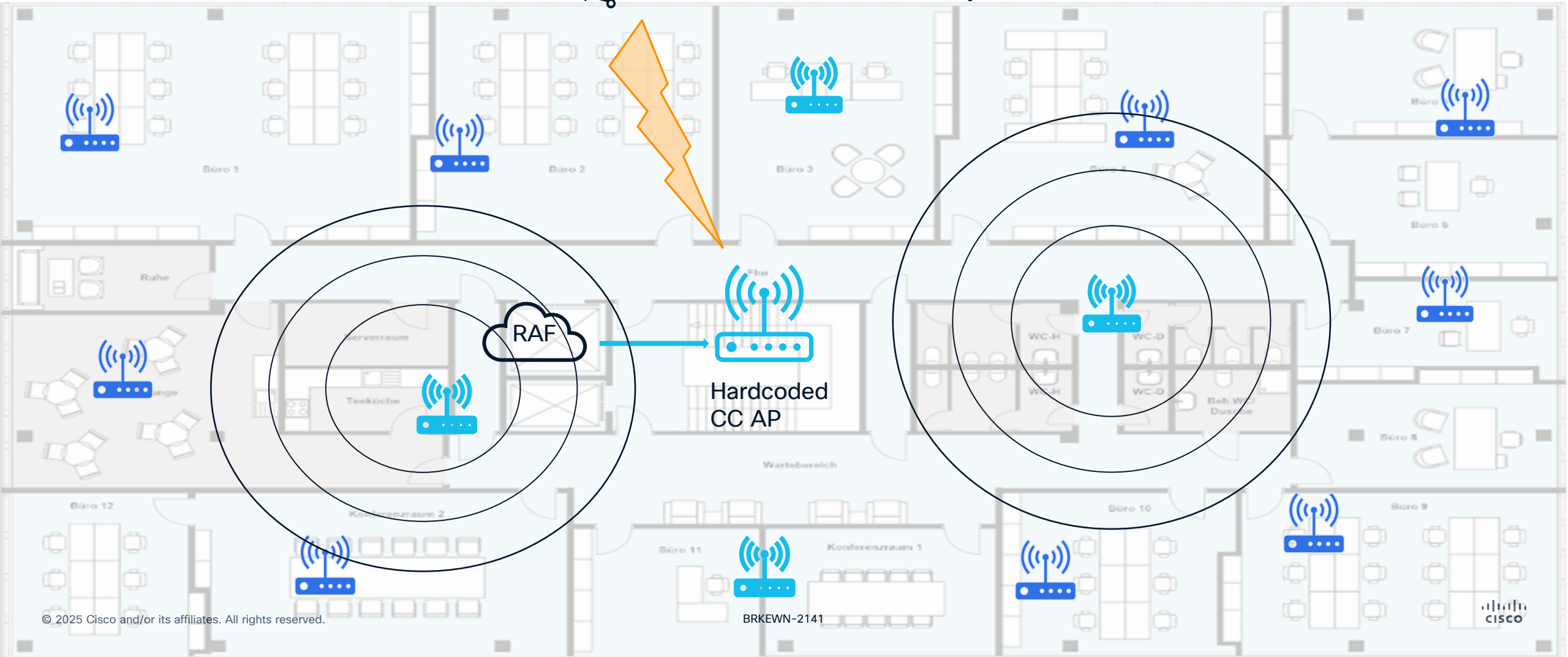


Country Code for Bulk Migration – Best Method

GPS



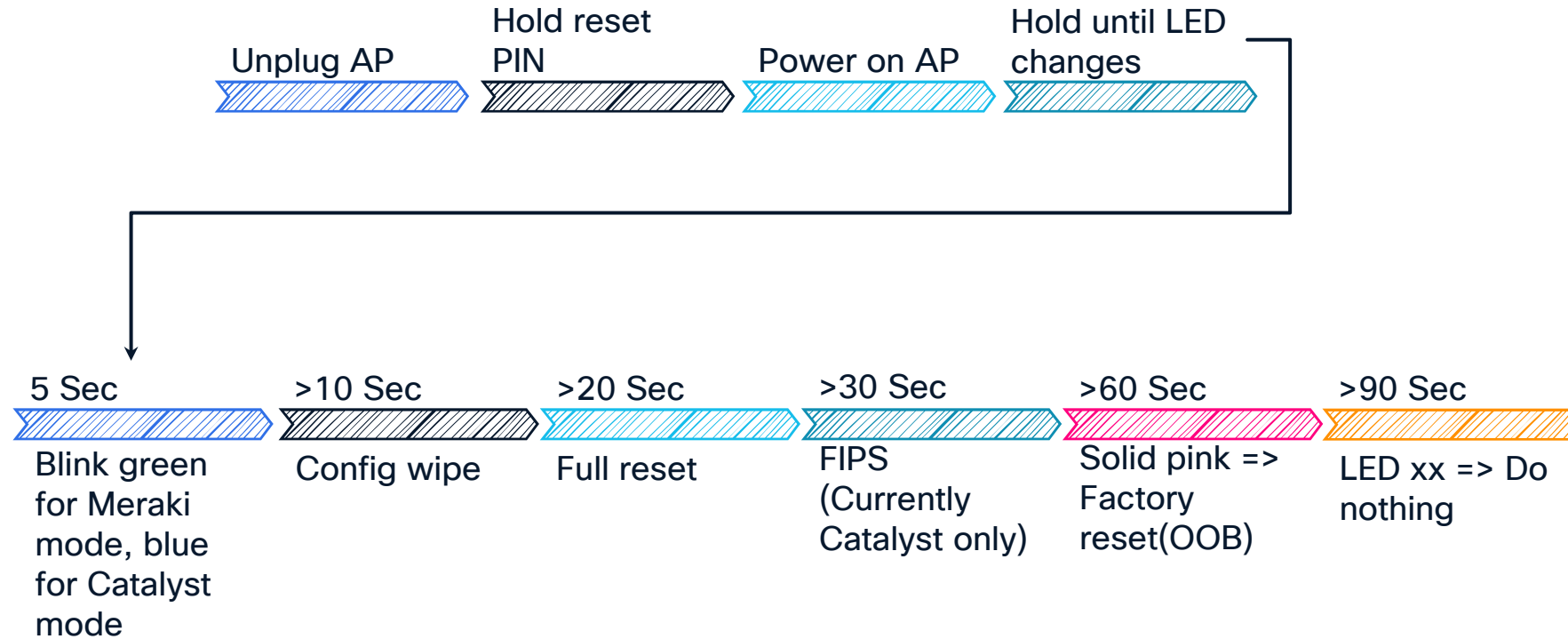
Proximity



Country Code for Bulk Migration – Best Method



Mode Recovery with Factory Reset



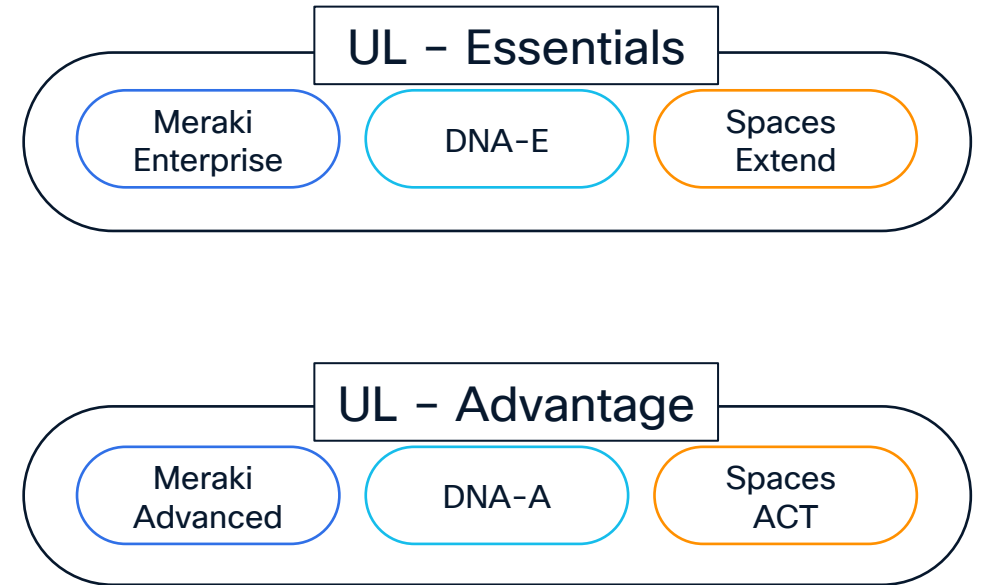
```
Reset button is pressed. Mode = Catalyst
Keep the button pressed for > 10 seconds for config reset
Keep the button pressed for > 20 seconds for full reset
Keep the button pressed for > 30 seconds for FIPS reset
Keep the button pressed for > 60 seconds for deep (factory) reset

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:

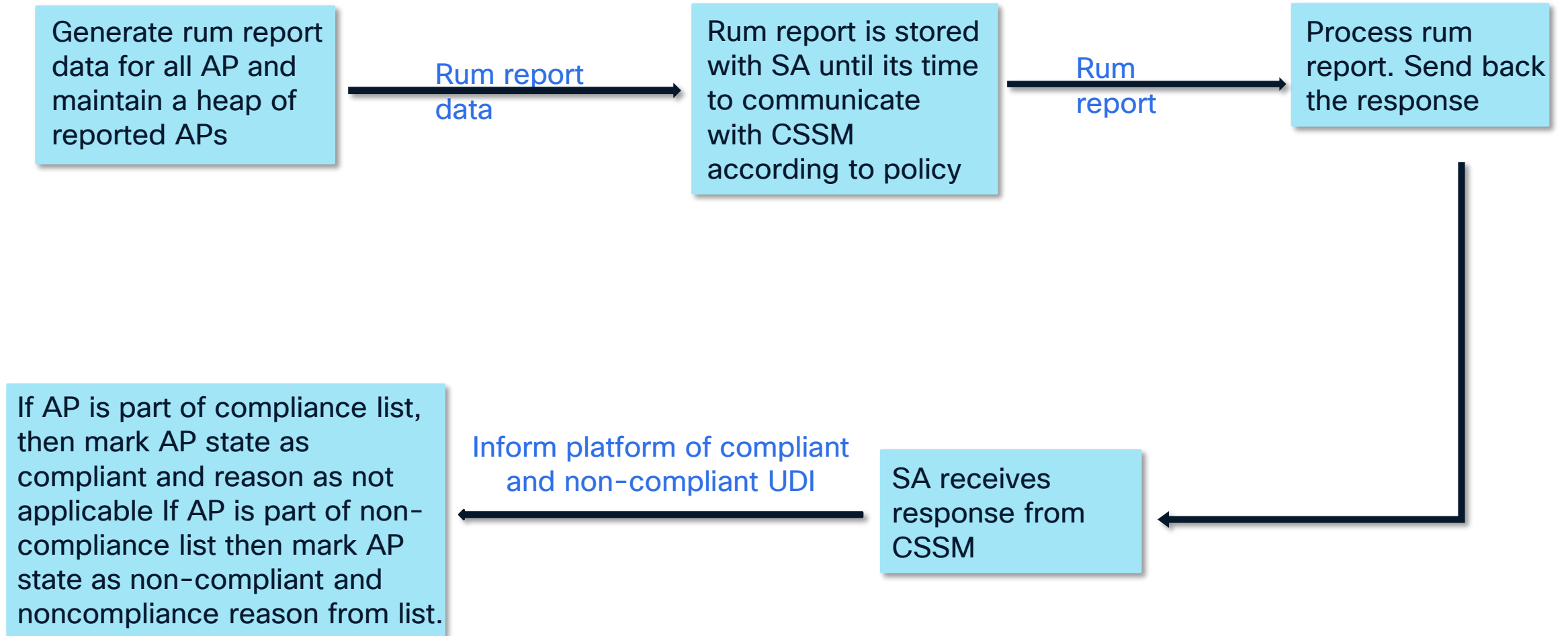
- Full device functionality restricted until licensed
- For Cisco Wireless: 2.4GHz only until licensed

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

The screenshot shows the Cisco AP Statistics interface. The breadcrumb navigation is 'Monitoring > Wireless > AP Statistics'. The 'General' tab is selected. A summary box indicates 'Total APs : 5'. Below this is a table of APs with columns for AP Name, AP Model, and AP Ra. A detailed table is highlighted with a red border, showing the following data:

License Type	License State	Non Compliant Reason
CNS	Non Compliant	Never Licensed
CNS	Non Compliant	Never Licensed
CNS	Non Compliant	Never Licensed
CNS	Non Compliant	Never Licensed
CNS	Non Compliant	Never Licensed

One time set up for non-compliant APs

2

The screenshot displays the Cisco Licensing console interface. On the left is a navigation sidebar with options: Dashboard, Monitoring, Configuration, Administration, Licensing (highlighted), and Troubleshooting. The main content area is titled 'Licensing' and has a sub-tab 'CSSM Connect'. A large modal window is centered on the screen, outlined in pink, showing a progress bar with two steps: 'GENERATE TOKEN' and 'ESTABLISH TRUST', both marked with blue checkmarks. Above the progress bar, the text reads 'Trust has been established between Device and CSSM'. Below the progress bar, the text 'Trust Established' is visible. To the right of the modal, there is a 'Sync Report' button. At the bottom of the modal, there are 'Back' and 'Save' buttons.

One time set up for non-compliant APs

3

The screenshot shows the Cisco AP Statistics interface. The breadcrumb navigation is Monitoring > Wireless > AP Statistics. The 'General' tab is selected, showing 'Total APs : 6'. A table lists APs with columns for License Type, License State, and Non Compliant Reason. A red box highlights the table content.

License Type	License State	Non Compliant Reason
CNS	Compliant	Not Applicable
CNS	Compliant	Not Applicable
CNS	Compliant	Not Applicable
CNS	Compliant	Not Applicable
CNS	Compliant	Not Applicable
AIR	Non Compliant	Never Licensed

Which is the
SSID?

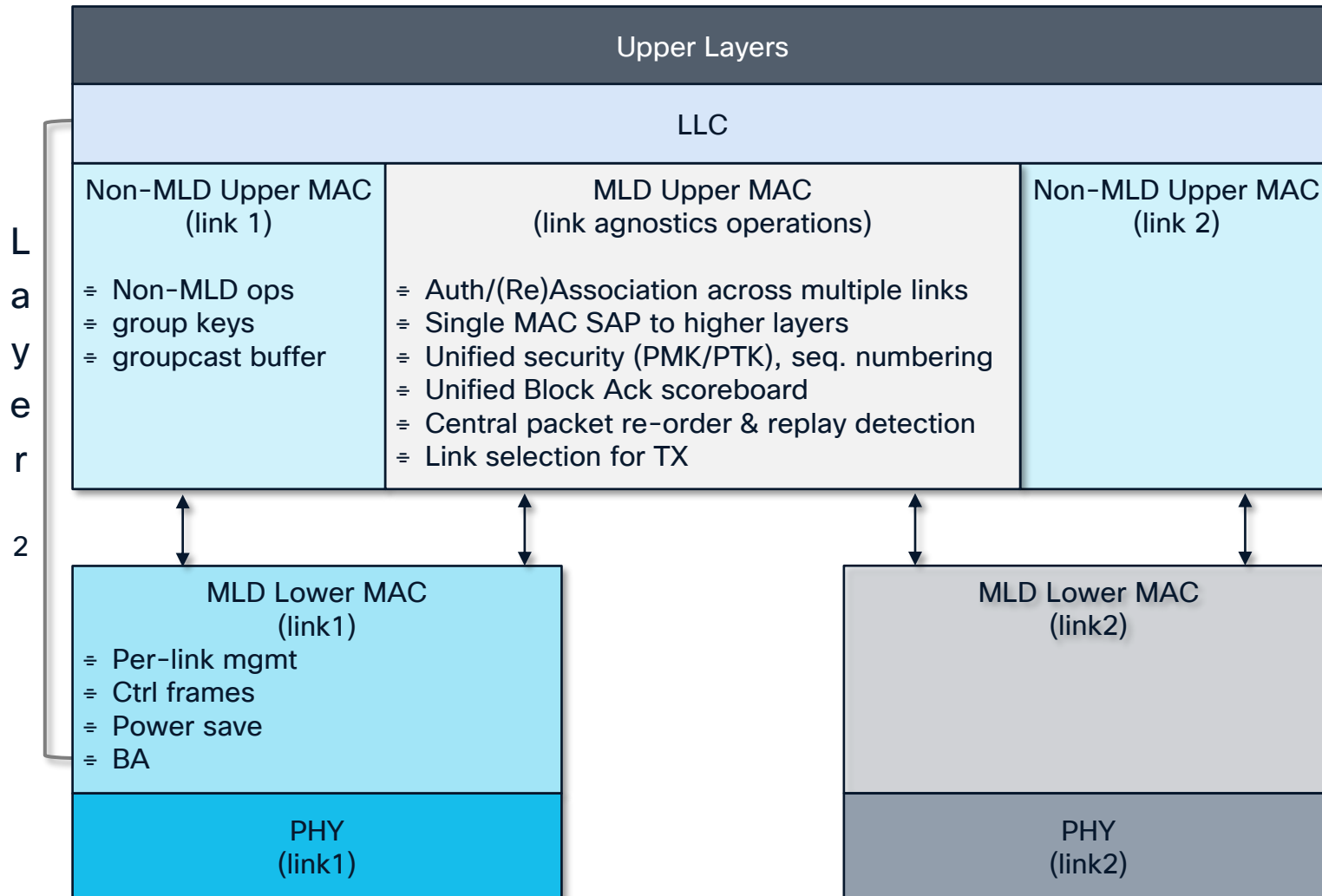
What should I
configure?



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 at least 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	<ul style="list-style-type: none"> 802.1X (SHA1) for earlier standards 802.1X-SHA256 mandatory FT + 802.1X (SHA256) highly recommended* 	<ul style="list-style-type: none"> 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

General **Security** Advanced

Layer2 Layer3 AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input type="checkbox"/>	Beacon Protection	<input checked="" type="checkbox"/>

WPA2/WPA3 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input checked="" type="checkbox"/>

Protected Management Frame

PMF: Required

Association Comeback Timer*: 1

SA Query Time*: 200

Fast Transition

Status: Enabled

Over the DS:

Reassociation Timeout*: 20

Auth Key Mgmt (AKM)

FT + 802.1X	<input type="checkbox"/>	802.1X-SHA256	<input type="checkbox"/>
SUITEB192-1X	<input type="checkbox"/>	OWE	<input type="checkbox"/>
SAE	<input checked="" type="checkbox"/>	FT + SAE	<input checked="" type="checkbox"/>
SAE-EXT-KEY	<input checked="" type="checkbox"/>	FT + SAE-EXT-KEY	<input checked="" type="checkbox"/>

Anti Clogging Threshold*: 1500

Max Retries*: 5

Retransmit Timeout*: 400

PSK Format: ASCII

PSK Type: Unencrypted

Pre-Shared Key*:

SAE Password Element: Both H2E and

- 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

The screenshot shows the Cisco configuration interface for WPA3 settings. The 'Security' tab is selected, and the 'WPA3' section is highlighted with a red box. Below this, the 'WPA Parameters' section is highlighted with a red box, showing 'WPA3 Policy' and 'Beacon Protection' checked. The 'WPA2/WPA3 Encryption' section is also highlighted with a red box, showing 'AES(CCMP128)' and 'GCMP256' checked. The 'Auth Key Mgmt (AKM)' section is highlighted with a red box, showing 'SAE' and 'SAE-EXT-KEY' checked. The 'PSK Type' is set to 'Unencrypted' and the 'Pre-Shared Key' is masked with dots. The 'SAE Password Element' is set to 'Both H2E and...'. Other settings like 'Association Comeback Timer' (1), 'Anti Clogging Threshold' (1500), and 'SA Query Time' (200) are visible.

- WPA3 settings:

- Beacon Protection
- AES(CCMP128)
- GCMP256

- DMF: Required (for Device Analytics too) Fast Transition 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

Basic info

Security WPA3 SAE configured

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter this key to associate: ⓘ
.....

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

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

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

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

WPA encryption ⓘ WPA3 only ▾

802.11w ⓘ

Enabled (allow unsupported clients)

Required (reject unsupported clients)

Disabled (never use)

Mandatory DHCP

Enabled Disabled

Advanced WPA3 settings (Cipher and AKM suite settings) ▾

WPA3 Cipher Suite GCMP 256

WPA3 AKM Suite SAE

SAE-EXT

Meraki Personal (passphrase) for Wi-Fi 7

Basic info

Security WPA3 SAE configured

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)

Password
Users must enter this key to associate: ⓘ
.....

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

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

WPA encryption ⓘ

WPA3 only ▾

802.11w ⓘ

Enabled (allow unsupported clients)

Required (reject unsupported clients)

Disabled (never use)

802.11w ⓘ

Enabled (allow unsupported clients)

Required (reject unsupported clients)

Disabled (never use)

Advanced WPA3 settings (Cipher and AKM suite settings)

WPA3 Cipher Suite GCMP 256

WPA3 AKM Suite SAE

SAE-EXT

SAE-EXT

9800 Enterprise (802.1X) for Wi-Fi 7

General **Security** Advanced

Layer2 **Layer3** AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input type="checkbox"/>	Beacon Protection	<input checked="" type="checkbox"/>

WPA2/WPA3 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS

Reassociation Timeout *

Auth Key Mgmt (AKM)

802.1X	<input checked="" type="checkbox"/>	FT + 802.1X	<input checked="" type="checkbox"/>
802.1X-SHA256	<input checked="" type="checkbox"/>	CCKM ⚠	<input type="checkbox"/>
PSK	<input type="checkbox"/>	FT + PSK	<input type="checkbox"/>
PSK-SHA256	<input type="checkbox"/>	SAE	<input type="checkbox"/>
FT + SAE	<input type="checkbox"/>	SAE-EXT-KEY	<input type="checkbox"/>
FT + SAE-EXT-KEY	<input type="checkbox"/>		

- 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

General **Security** Advanced

Layer2 **Layer3** AAA

ensuring WLAN compatibility with Wi-Fi 7 security [click here.](#)

WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Policy WPA2 Policy

WPA3 Policy

GTK Randomize Beacon Protection

Transition Disable

Reassociation Timeout * 20

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256

GCMP128 GCMP256

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256

GCMP128 GCMP256

Auth Key Mgmt (AKM)

802.1X FT + 802.1X

802.1X-SHA256 CCKM

SAE

SAE-EXT-K

SA Query Time* 200

- 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 points only
 - checked
 - Over the PSK (SAE) is the technique all endpoints are supporting

Meraki Enterprise (802.1X) for Wi-Fi 7

Security WPA3 Enterprise with 0 RADIUS servers

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

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

Enterprise with
my RADIUS server ▾
User credentials are validated with 802.1X at association time

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

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

Wi-Fi Personal Network (WPN) ⓘ Enabled Disabled

WPA encryption ⓘ WPA3 only ▾

802.11w ⓘ Enabled (allow unsupported clients)
 Required (reject unsupported clients)
 Disabled (never use)

Mandatory DHCP Enabled Disabled

Advanced WPA3 settings (Cipher and AKM suite settings)

WPA3 Cipher Suite GCMP 256

Meraki Enterprise (802.1X) for Wi-Fi 7

Security *WPA3 Enterprise with 0 RADIUS servers*

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

MAC-based access
my RADIUS server
RADIUS server is

Enterprise with
my RADIUS server
User credentials are validated with 802.1X at association time

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

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

Wi-Fi Personal Network (WPN) ⓘ

WPA encryption ⓘ

802.11w ⓘ Enabled (allow unsupported clients)
 Required (reject unsupported clients)
 Disabled (never use)

Mandatory DHCP

Advanced WPA3 settings *(Cipher and AKM suite settings)*

WPA3 Cipher Suite GCMP 256

9800 OWE for Wi-Fi 7

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering For CWA or other web portal scenarios

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input type="checkbox"/>	Beacon Protection	<input checked="" type="checkbox"/>

WPA2/WPA3 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input checked="" type="checkbox"/>

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS

Reassociation Timeout *

Auth Key Mgmt (AKM)

FT + 802.1X	<input type="checkbox"/>	802.1X-SHA256	<input type="checkbox"/>
SUITEB192-1X	<input type="checkbox"/>	OWE	<input checked="" type="checkbox"/>
SAE	<input type="checkbox"/>	FT + SAE	<input type="checkbox"/>
SAE-EXT-KEY	<input type="checkbox"/>	FT + SAE-EXT-KEY	<input type="checkbox"/>

Transition Mode WLAN ID

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

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

9800 OWE for Wi-Fi 7

WPA + WPA2 WPA2 + WPA3 **WPA3** Static WEP None

MAC Filtering A or other web portal scenarios

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy
GTK Randomize WPA3 Policy
Transition Disable

Beacon Protection

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256
GCMP128 GCMP256

Protected Management Frame

PMF Required

Association Comeback Timer* 1
SA Query Time* 200

OWE

Transition Mode WLAN ID 0-4096

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**

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

Meraki OWE for Wi-Fi 7

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

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

Enterprise with
my RADIUS server ▾
User credentials are validated with 802.1X at association time

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

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

WPA encryption ⓘ

802.11w ⓘ

Mandatory DHCP

Advanced WPA3 settings (Cipher and AKM suite settings) ▾

WPA3 Cipher Suite

WPA3 only ▾

Enabled (allow unsupported clients)

Required (reject unsupported clients)

Disabled (never use)

Enabled Disabled

GCMP 256

Meraki OWE for Wi-Fi 7

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

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

Enterprise with
my RADIUS server ▾
User credentials are validated with 802.1X at association time

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

Identity PSK without RADIUS
Devices are assigned a group policy

WPA encryption ⓘ

802.11w ⓘ

WPA3 only ▾

Enabled (allow unsupported clients)

Required (reject unsupported clients)

Disabled (never use)

Disabled (never use)

Mandatory DHCP

Enabled Disabled

Advanced WPA3 settings ▾

WPA3 Cipher Suite

GCMP 256

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

Security *WPA3 Enterprise with 0 RADIUS servers*

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

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

Enterprise with
my RADIUS server ▾
User credentials are validated with 802.1X at association time

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

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

Wi-Fi Personal Network (WPN) ⓘ

Enabled Disabled

WPA encryption ⓘ

802.11w ⓘ

WPA3 192-bit Security ▾

Enabled (allow unsupported clients)

Required (reject unsupported clients)

Disabled (never use)

Mandatory DHCP

Enabled Disabled

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

Security *WPA3 Enterprise with 0 RADIUS servers*

Open (no encryption)
Any user can associate

Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

Password
Users must enter a passphrase to associate ⓘ

MAC-based access control (no encryption)
my RADIUS server ▾

Enterprise with
my RADIUS server ▾
User credentials are validated with 802.1X at association time

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

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

Wi-Fi Personal Network (WPN) ⓘ

WPA encryption ⓘ

802.11w ⓘ

Mandatory DHCP

WPA3 192-bit Security ▾

Enabled (allow unsupported clients)

Required (reject unsupported clients)

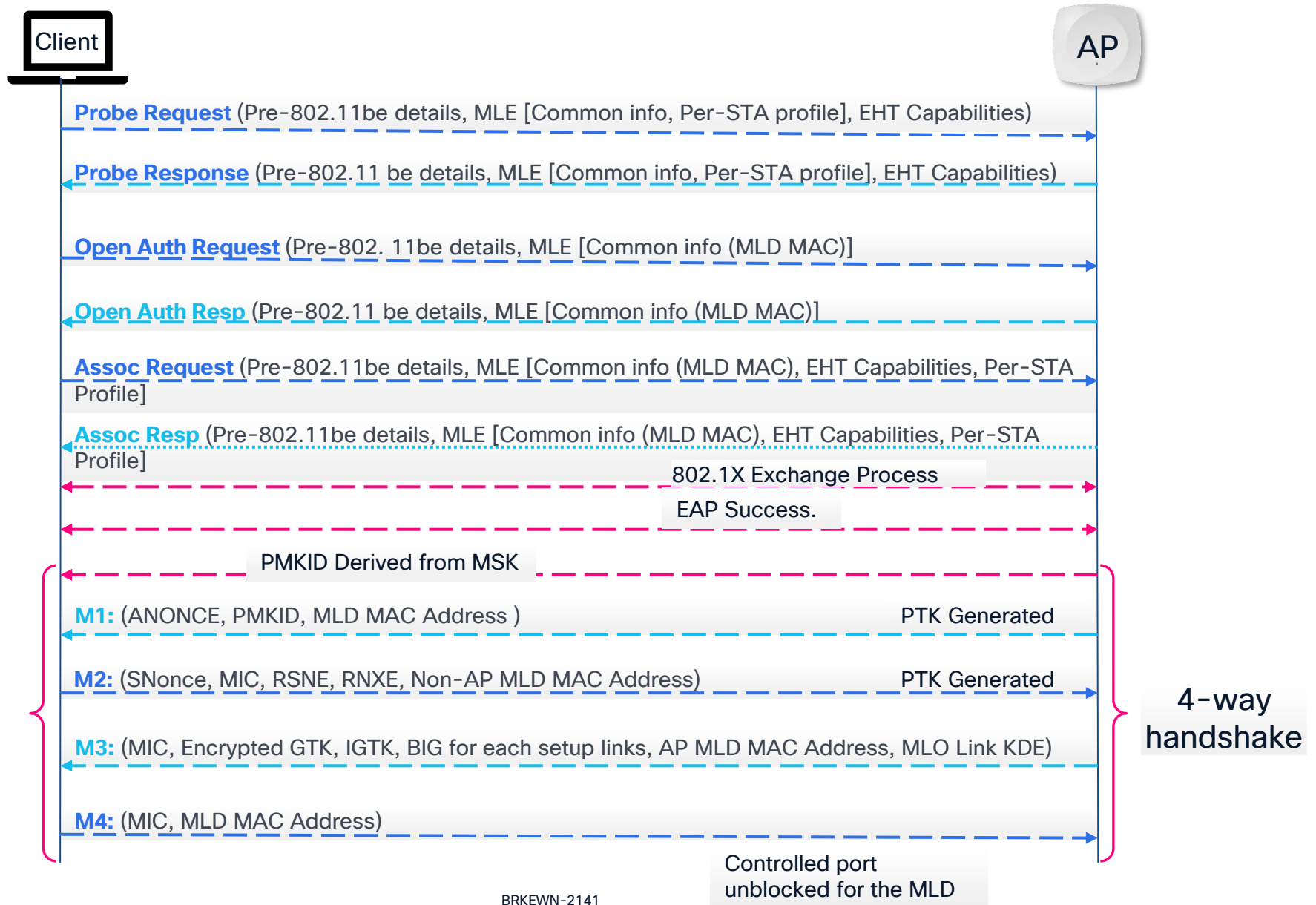
Disabled (never use)

Enabled Disabled

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



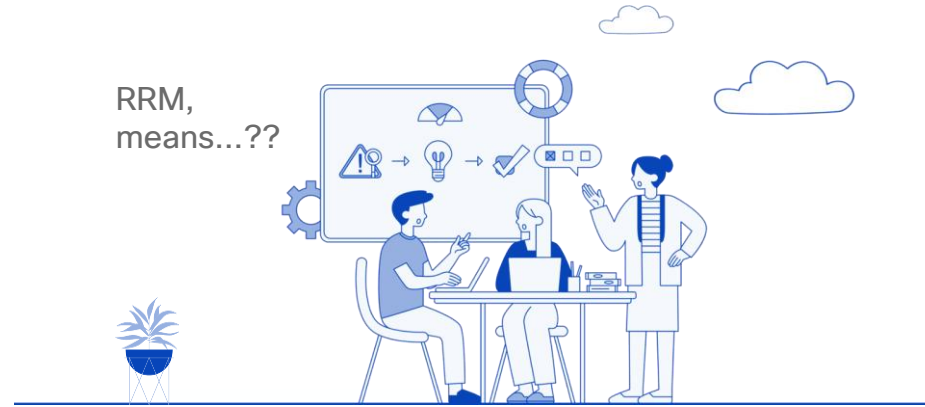
No.	Time	Source	Destination	Protocol	Length	Channel	Info
1187163	09:05:35.988097	Microsoft_b4:05:25	Cisco_6a:00:02	802.11	264	1	Probe Request, SN=256, FN=0, Flags=.....C, SSID="Ghost"
1187170	09:05:35.991821	Cisco_6a:00:02	Microsoft_b4:05:...	802.11	439	1	Probe Response, SN=3829, FN=0, Flags=.....C, BI=100, SSID="Ghst"
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="Ghst"
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	Microsoft_b4:05:25	Cisco_6a:00:02	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



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 $\geq 80\text{MHz}$

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

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 $\geq 80\text{MHz}$

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 $\geq 80\text{MHz}$

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 $\geq 80\text{MHz}$

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.

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.

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

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.

Access points that do not support Wi-Fi 7 will use their maximum supported channel width.

802.11be Datarates

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

The screenshot shows the Cisco configuration interface for High Throughput settings. The breadcrumb path is Configuration > Radio Configurations > High Throughput. The '6 GHz Band' tab is selected. A warning message states: '6 GHz Network is operational. Configuring High Throughput will result in loss of connectivity of clients.' Below this, a red warning box indicates: 'Configuring High Throughput Parameters will result in loss of connectivity of all clients across 802.11be enabled radios of the APs'. The '11ax' section is collapsed, and the '11be' section is expanded. A yellow warning box states: '11be check enables Wi-Fi 7 capability in Wi-Fi 7 capable APs. Please ensure the WLANs are compatible with Wi-Fi 7 specific security. Click here to view the security constraints.' The 'Enable 11be' checkbox is checked. The 'Select All' checkbox is also checked. Below these are four columns of SS/MCS settings, each with a checked checkbox and a value:

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/9	<input checked="" type="checkbox"/> 1/11	<input checked="" type="checkbox"/> 1/13	<input checked="" type="checkbox"/> 1/14
<input checked="" type="checkbox"/> 1/15	<input checked="" type="checkbox"/> 2/9	<input checked="" type="checkbox"/> 2/11	<input checked="" type="checkbox"/> 2/13
<input checked="" type="checkbox"/> 3/9	<input checked="" type="checkbox"/> 3/11	<input checked="" type="checkbox"/> 3/13	<input checked="" type="checkbox"/> 4/9
<input checked="" type="checkbox"/> 4/11	<input checked="" type="checkbox"/> 4/13		

```
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

The screenshot shows the Cisco configuration interface for High Throughput parameters. The '6 GHz Band' tab is selected. A warning message states: 'Configuring High Throughput Parameters will result in loss of connectivity of all clients across 802.11be enabled radios of the APs'. The '11be' section is expanded, showing a table of datarates. The 'Enable 11be' checkbox is checked. A 'Select All' checkbox is also checked. A yellow warning banner at the top of the table states: '11be check enables Wi-Fi 7 capability in Wi-Fi 7 capable APs. Please ensure the WLANs are compatible with Wi-Fi 7 specific security. Click here to view the security constraints.'

SS/MCS	SS/MCS	SS/MCS	SS/MCS
<input checked="" type="checkbox"/> 1/9	<input checked="" type="checkbox"/> 1/11	<input checked="" type="checkbox"/> 1/13	<input checked="" type="checkbox"/> 1/14
<input checked="" type="checkbox"/> 1/15	<input checked="" type="checkbox"/> 2/9	<input checked="" type="checkbox"/> 2/11	<input checked="" type="checkbox"/> 2/13
<input checked="" type="checkbox"/> 3/9	<input checked="" type="checkbox"/> 3/11	<input checked="" type="checkbox"/> 3/13	<input checked="" type="checkbox"/> 4/9
<input checked="" type="checkbox"/> 4/11	<input checked="" type="checkbox"/> 4/13		

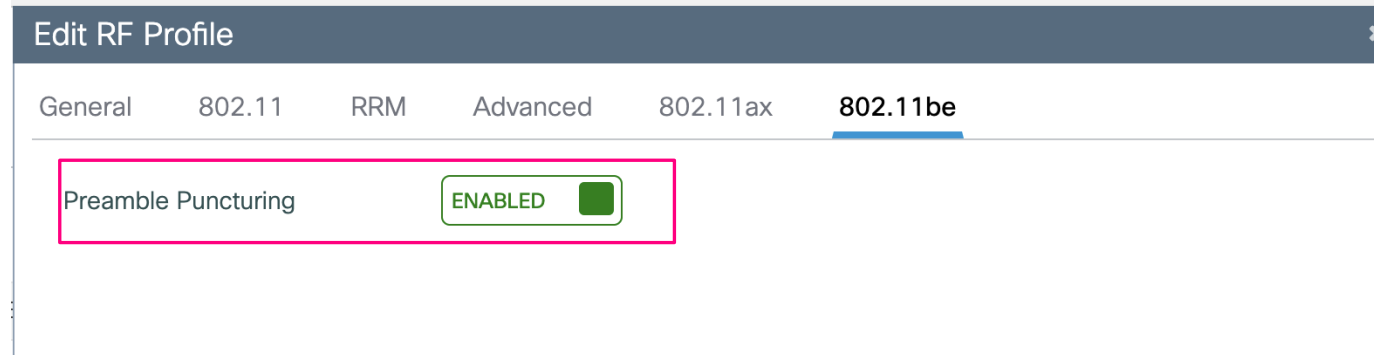
```
ap dot11 24ghz dot11be
ap dot11 5ghz dot11be
ap dot11 6ghz dot11be
```

- 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 $\leq 80\text{MHz}$

Configuration>Tags &



The screenshot shows the 'Edit RF Profile' configuration page for the 802.11be standard. The page has a dark blue header with the title 'Edit RF Profile' and a close button. Below the header, there are tabs for 'General', '802.11', 'RRM', 'Advanced', '802.11ax', and '802.11be'. The '802.11be' tab is selected and highlighted in blue. In the main content area, the 'Preamble Puncturing' option is shown with a green 'ENABLED' label and a green toggle switch. A pink rectangular box highlights the 'Preamble Puncturing' label and the 'ENABLED' toggle.

Configure OFDMA Multi RU

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

Edit 802.11be Profile

Profile Name* default-dot11be-profile

Description Default 802.11be profile

OFDMA Downlink **ENABLED**

OFDMA Uplink **ENABLED**

MU-MIMO Downlink **ENABLED**

MU-MIMO Uplink **ENABLED**

OFDMA Multi-RU **ENABLED**

MLO Group

Primary 2.4GHz **DISABLED**

Primary 5GHz **ENABLED**

Secondary 5GHz **ENABLED**

Primary 6GHz **ENABLED**

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

Edit Multi BSSID Profile

Name* default-multi-bssid-profile

Description Default multi bssid profile

Target Waketime **DISABLE**

TWT Broadcast Support **DISABLE**

802.11ax

OFDMA Downlink **ENABLE**

OFDMA Uplink **ENABLE**

MU-MIMO Downlink **ENABLE**

MU-MIMO Uplink **ENABLE**

802.11be

OFDMA Downlink **ENABLE**

OFDMA Uplink **ENABLE**

MU-MIMO Downlink **DISABLE**

MU-MIMO Uplink **DISABLE**

OFDMA Multi-RU **ENABLE**

Configure OFDMA Multi RU

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

Edit 802.11be Profile

Profile Name* default-dot11be-profile

Description Default 802.11be profile

OFDMA Downlink **ENABLED**

OFDMA Uplink **ENABLED**

MU-MIMO Downlink **ENABLED**

MU-MIMO Uplink **ENABLED**

OFDMA Multi-RU **ENABLED**

MLO Group

Primary 2.4GHz DISABLED

Primary 5GHz **ENABLED**

Secondary 5GHz **ENABLED**

Primary 6GHz **ENABLED**

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

Edit Multi BSSID Profile

Name* default-multi-bssid-profile

Description Default multi bssid profile

Target Waketime DISABLE

TWT Broadcast Support DISABLE

802.11ax

OFDMA Downlink **ENABLE**

OFDMA Uplink **ENABLE**

MU-MIMO Downlink **ENABLE**

MU-MIMO Uplink **ENABLE**

802.11be

OFDMA Downlink **ENABLE**

OFDMA Uplink **ENABLE**

MU-MIMO Downlink DISABLE

OFDMA Multi-RU **ENABLE**

Meraki: Enable 802.11be

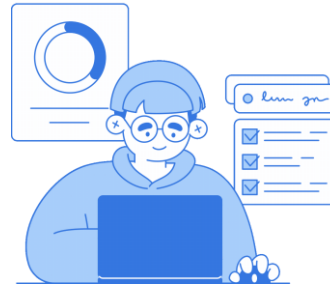
Wireless>Radio Setting>RF Profile>General

The screenshot shows the Meraki configuration interface for an RF Profile. The breadcrumb path is 'Wireless>Radio Setting>RF Profile>General'. There are three tabs: 'General', '2.4 GHz', and '6 GHz'. The 'General' tab is selected and highlighted with a pink box. Below the tabs, the '802.11be' setting is visible, with a pink box around the 'On' and 'Off' toggle buttons. The 'On' button is currently selected. Below the toggle, the text 'Enable 802.11be on supported APs.' is displayed.

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			MERAKI		
Pattern	Color	Meaning / Status	LED Color / Pattern	Visual	Meaning / Status
Solid Orange / Amber		AP booting up (Day 0 Mode)	Solid Orange		AP booting up
Rainbow (cycling colors)		AP discovering mode (deciding Meraki or Catalyst)	Rainbow (cycling colors)		AP initializing / scanning channels
Blinking Blue		Software upgrade or image migration in progress	Blinking Blue		Firmware upgrade in progress
Solid Green		AP joined WLC successfully, no clients	Solid Green		AP online, healthy, no clients connected
Solid Blue		AP connected to Meraki Cloud, clients active	Solid Blue		AP online with clients connected
Blinking Orange		Unable to determine mode (no Cloud or WLC found)	Blinking Orange		AP cannot reach Meraki Cloud
Red (steady)		Hardware or image fault	Blinking Green		Site Survey Mode
Blinking Green		Site Survey / Local mode (for testing)	Solid Orange (post boot)		Hardware or image fault
Off (configured)		LED disabled via configuration	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 location	3	CW9176I	cc6e.2a67.d840	9056.715f.eee0	US	-B	10.107.70.73	Registered	default
9178_2	4	CW9178I	8c88.814f.0050	ecf4.0cb3.cae0	US	-B	10.107.70.36	Registered	AP2
9176D_1 location	3	CW9176D1	cc6e.2a3c.ca70	ecf4.0cbd.bce0	US	-UN	10.107.70.49	Registered	default
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
```

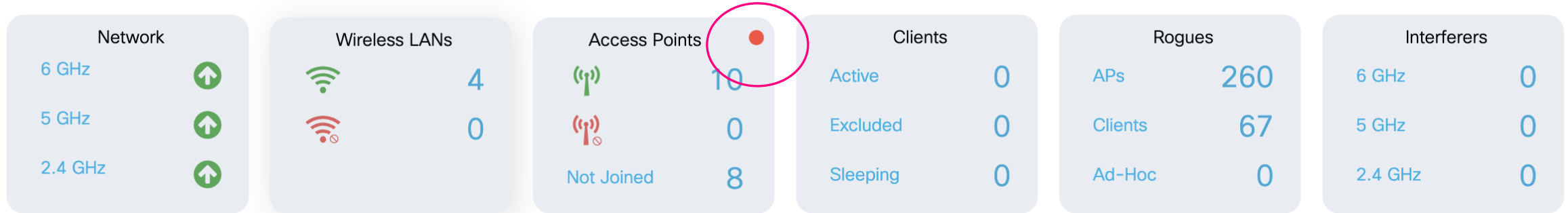
RA Traces:

```
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.

Dashboard



Misconfigured APs	Count
Tag	0
Country Code	2
LSC Fallback	0

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

SSIDS
Aurora
[BSSID Details](#)


RADIO SETTINGS
RF profile: [Basic Indoor Profile](#)


LAN IP 
PUBLIC IP

PREFERRED MESH GATEWAY 
(Default)

LAN IPV6 
Not configured

SERIAL NUMBER

TAGS 

NOTES 

FIRMWARE
Up to date
Current version: MR 31.1.7
[Open source licenses](#)

CONFIG
Out of date
(changed 3 hours ago)

REGULATORY INFO
Enforced Country: US
Detected Country: IN

DEVICE UPTIME
—

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.

```
content:
  devices:
    0: {}
    1:
      mac: "c4:14:a2:d2:b0:90"
      serial: "WNT281300XY"
      regulatoryDomain:
        country: "US"
        method: "automatic"
    2: {}
    3:
      mac: "cc:9c:3e:ec:1c:f0"
      serial: "WNH26160034"
      regulatoryDomain:
        country: "US"
        method: "automatic"
    4: {}
    5:
      mac: "68:49:92:01:a4:e0"
      serial: "WNH264001RQ"
      regulatoryDomain:
        country: "US"
        method: "automatic"
    6: {}
    7: {}
    8: {}
    9: {}
    10: {}
  details:
    schemaVersion: "1.0.0"
    organizationId: "821110"
    createdAt: "2024-10-22T00:46:49Z"
    counts:
      devices: 11
    createdBy:
      id: "1030235"
      email:
  signature: "rn3zB6h10882140j0N8uC3zTybdfLsVZ+Zwwx9ZnkyVgoh8dUEZFdSrZkg19aRHxi+Mwoc/DC8H2Ttwu5w37uBjZdkI8t+Wiyxbwam4kQMBc++pLJX4iFwisUJhEjo3uf2ZbiWdLIX55+4xo25sLhbKcjg9WmERhxoRKN0L4HuvIHRx97vIpGyg8c76z46ahj+kBzPSI1j1Ys3M7FsJy9su1rcGvTWscPMD+/U1IqS80cdZSntNt6D7zsrnQAR9gSFC"
  certificates:
    0:
      purpose: "signature"
      content: "LS0tLS1CRUdJTiB0RVJUSUZ0Q0FURS0tLS0tDQpNSUlhWgp0Q0JYVWd0d0LCQWdJUUUNIT2p1SmVEVEJmdXR0b3JPMjNKSzVSRVBTk0na3Foa2lHOXcwQkFRc0ZBREJUDQpNUXN3Q1FZRFZRUUd0pWVXpFVU1CSUdBMVVFQ2hNTFRXVn1ZV3RwTENCTVRFTXhMakFzQmd0VkJBTVRKVTFsDQpjbUZYVWNCUMNtdDZlZWZJcSUV0dmJtWnBaeUJKYm55Sgk"
```

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

Probe Request - Response

The image displays two Wireshark packet capture windows. The left window shows a Probe Request frame (No. 1814) and its detailed structure. The right window shows the corresponding Probe Response frame (No. 181725) and its detailed structure. Both frames are IEEE 802.11 Wireless Management frames. The Probe Request frame includes tags for SSID, Supported Rates, DS Parameter, Country Information, Power Constraint, ERP, RSN, QoS, RM, Mobility Domain, HT, and HE Capabilities. The Probe Response frame includes tags for SSID, Supported Rates, DS Parameter, Country Information, Power Constraint, ERP, RSN, QoS, RM, Mobility Domain, HT, HE Capabilities, and MLD Capabilities. The HE Capabilities tag in both frames is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Channel	Info
1814...	06:26:29.197668	c6:cb:76:b4:05:25	Cisco_6a:00:...	802.11	280	1	Probe Request, SN=...

Frame 181471: Packet, 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface \Device...
> Ethernet II, Src: CiscoMeraki_6f:53:27 (c4:14:a2:6f:53:27), Dst: Intel_e0:b1:b3 (64:32:a8:e0:b1:b3)
> Internet Protocol Version 4, Src: 10.106.107.251, Dst: 10.106.107.248
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPeek/OmniPeek encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags:C
> IEEE 802.11 Wireless Management
 > Tagged parameters (190 bytes)
 > Tag: SSID parameter set: "Workoholic"
 > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
 > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
 > Tag: HT Capabilities
 > Tag: Extended Capabilities (12 octets)
 > Tag: VHT Capabilities
 > Ext Tag: HE Capabilities
 > Ext Tag: Multi-Link (802.11be D3.0)
 Ext Tag length: 8 (Tag len: 9)
 Ext Tag Number: Multi-Link (802.11be D3.0) (107)
 > Multi-Link Control: 0x0011 Probe Request
001 = Type: Probe Request (1)
0... = Reserved: 0x0
1... = AP MLD ID Present: True
0... = MLD MAC Address Present: False
 0000 0000 00... = Reserved: 0x000
 > Common Info
 Subelement ID: Per-STA Profile (0x00)
 Subelement Length: 2
 > Per-STA Profile 1
 Probe Request STA Profile Count: 1
 STA Profiles LinkIds: 1
 > Ext Tag: EHT Capabilities (802.11be D3.0)
 Ext Tag length: 15 (Tag len: 16)
 Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
 > EHT MAC Capabilities Information: 0x0097, EPCS Priority Access Support, EHT OM Control Support,
 > EHT PHY Capabilities Information
 > Supported EHT-MCS and NSS Set
 > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience
 > Tag: RM Enabled Capabilities (5 octets)
 > Tag: Vendor Specific: Qualcomm Inc.

No.	Time	Source	Destination	Protocol	Length	Channel	Info
181725	06:26:29.214820	c6:cb:76:b4:05:25	Cisco_6a:00:00	802.11	795	1	Probe Response, SN=3671, FN=0, Flags=.....C, BI=100, Authentication: SN=257, FN=0, Flags=.....C

> AiroPeek/OmniPeek encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags:C
> IEEE 802.11 Wireless Management
 > Fixed parameters (12 bytes)
 > Tagged parameters (693 bytes)
 > Tag: SSID parameter set: "Workoholic"
 > Tag: Supported Rates 24(B), 36, 48, 54, SAE Hash to Element Only, [Mbit/sec]
 > Tag: DS Parameter set: Current Channel: 1
 > Tag: Country Information: Country Code US, Environment Global operating classes
 > Tag: Power Constraint: 0
 > Tag: TPC Report Transmit Power: 5 dBm
 > Tag: ERP Information
 > Tag: RSN Information
 > Tag: QoS Load Element 802.11e CCA Version
 > Tag: RM Enabled Capabilities (5 octets)
 > Tag: Mobility Domain
 > Tag: HT Capabilities
 > Tag: HT Operation
 > Tag: Extended Capabilities (11 octets)
 > Tag: Reduced Neighbor Report
 > Tag: RSN eXtension (1 octet)
 > Ext Tag: HE Capabilities
 > Ext Tag: HE Operation
 > Ext Tag: Spatial Reuse Parameter Set
 > Ext Tag: MLD EDCA Parameter Set
 > Ext Tag: Multi-Link (802.11be D3.0)
 Ext Tag length: 359 (Tag len: 360)
 Ext Tag Number: Multi-Link (802.11be D3.0) (107)
 > Multi-Link Control: 0x01f0 Basic
 > Common Info
 Common Info Length: 15
 MLD MAC Address: f2:d8:05:6a:00:10 (f2:d8:05:6a:00:10)
 > Link ID subfield: 0x00
 > BSS Parameters Change Count: 14
 > Medium Sync Field: 0x00ab
 > EML Capabilities: 0x4001, EMLSR Support
1... = EMLSR Support: True
000... = EMLSR Padding Delay: 0
000... = EMLSR Transition Delay: 0
0... = EMLMR Support: False
000... = EMLMR Delay: 0
 .100 0... = Transition Timeout: 8
 0... = Reserved: 0x0
 > MLD Capabilities: 0x0021
 Subelement ID: Per-STA Profile (0x00)
 Subelement Length: 338
 > Per-STA Profile 1
 Basic STA Profile Count: 1
 STA Profiles LinkIds: 1
 > Ext Tag: EHT Capabilities (802.11be D3.0)
 > Ext Tag: EHT Operation (802.11be D3.0)
 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)

OTA Packet Flow

Open Auth Request - Response

<pre>182208 06:26:29.260664 c6:cb:76:b4:05:25 Cisco_6a:00:00 802.11 142 1 Authentication, SN=259, FN=0, Flags=... 182210 06:26:29.260664 Cisco_6a:00:00 Broadcast 802.11 4 > Frame 182208: Packet, 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{06000E34-376B-416A-B8F9-000000000000} > Ethernet II, Src: CiscoMeraki_6f:53:27 (c4:14:a2:6f:53:27), Dst: Intel_e0:b1:b3 (64:32:a8:e0:b1:b3) > Internet Protocol Version 4, Src: 10.106.107.251, Dst: 10.106.107.248 > User Datagram Protocol, Src Port: 5555, Dst Port: 5000 > AiroPeek/OmniPeek encapsulated IEEE 802.11 > 802.11 radio information IEEE 802.11 Authentication, Flags:C Type/Subtype: Authentication (0x000b) Frame Control Field: 0xb000 .000 0000 0010 1100 = Duration: 44 microseconds > Receiver address: Cisco_6a:00:00 (f0:d8:05:6a:00:00) > Destination address: Cisco_6a:00:00 (f0:d8:05:6a:00:00) > Transmitter address: c6:cb:76:b4:05:25 (c6:cb:76:b4:05:25) > Source address: c6:cb:76:b4:05:25 (c6:cb:76:b4:05:25) > BSS Id: Cisco_6a:00:00 (f0:d8:05:6a:00:00) 0000 = Fragment number: 0 0001 0000 0011 = Sequence number: 259 Frame check sequence: 0x00000000 [unverified] [FCS Status: Unverified] [WLAN Flags:C] IEEE 802.11 Wireless Management Fixed parameters (40 bytes) Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3) Authentication SEQ: 0x0002 Status code: Successful (0x0000) SAE Message Type: Confirm (2) Send-Confirm: 0 Confirm: 870aacb3271f6717cd506c6b515cc8b625bdb1b5edc28cc41bd756834f645f35 Tagged parameters (12 bytes) Ext Tag: Multi-Link (802.11be D3.0) Ext Tag length: 9 (Tag len: 10) Ext Tag Number: Multi-Link (802.11be D3.0) (107) Multi-Link Control: 0x0000 Basic 000 = Type: Basic (0) 0... = Reserved: 0x0 0... = Link ID Info Present: False 0. = BSS Parameters Change Count Present: False 0. = Medium Synchronization Delay Info Present: False 0... = EML Capabilities Present: False 0... = MLD Capabilities Present: False 0. = AP MLD ID Present: False 0. = Extended MLD Capabilities and Operations Present: False 0000 0... = Reserved: 0x00 Common Info Common Info Length: 7 MLD MAC Address: Microsoft_b4:05:25 (c4:cb:76:b4:05:25) Basic STA Profile Count: 0</pre>	<pre>182262 06:26:29.274199 Cisco_6a:00:00 c6:cb:76:b4:05:25 802.11 142 1 Authentication, SN=3674, FN=0, Flags=... > Frame 182262: Packet, 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{06000E34-376B-416A-B8F9-000000000000} > Ethernet II, Src: CiscoMeraki_6f:53:27 (c4:14:a2:6f:53:27), Dst: Intel_e0:b1:b3 (64:32:a8:e0:b1:b3) > Internet Protocol Version 4, Src: 10.106.107.251, Dst: 10.106.107.248 > User Datagram Protocol, Src Port: 5555, Dst Port: 5000 > AiroPeek/OmniPeek encapsulated IEEE 802.11 > 802.11 radio information IEEE 802.11 Authentication, Flags:C Type/Subtype: Authentication (0x000b) Frame Control Field: 0xb000 .000 0000 0010 1100 = Duration: 44 microseconds > Receiver address: c6:cb:76:b4:05:25 (c6:cb:76:b4:05:25) > Destination address: c6:cb:76:b4:05:25 (c6:cb:76:b4:05:25) > Transmitter address: Cisco_6a:00:00 (f0:d8:05:6a:00:00) > Source address: Cisco_6a:00:00 (f0:d8:05:6a:00:00) > BSS Id: Cisco_6a:00:00 (f0:d8:05:6a:00:00) 0000 = Fragment number: 0 1110 0101 1010 = Sequence number: 3674 Frame check sequence: 0x00000000 [unverified] [FCS Status: Unverified] [WLAN Flags:C] IEEE 802.11 Wireless Management Fixed parameters (40 bytes) Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3) Authentication SEQ: 0x0002 Status code: Successful (0x0000) SAE Message Type: Confirm (2) Send-Confirm: 0 Confirm: 4abe918107baa64799b63c9073dce16a372ab074820cea2e2d13513fd866acef Tagged parameters (12 bytes) Ext Tag: Multi-Link (802.11be D3.0) Ext Tag length: 9 (Tag len: 10) Ext Tag Number: Multi-Link (802.11be D3.0) (107) Multi-Link Control: 0x0000 Basic 000 = Type: Basic (0) 0... = Reserved: 0x0 0... = Link ID Info Present: False 0. = BSS Parameters Change Count Present: False 0. = Medium Synchronization Delay Info Present: False 0... = EML Capabilities Present: False 0... = MLD Capabilities Present: False 0. = AP MLD ID Present: False 0. = Extended MLD Capabilities and Operations Present: False 0000 0... = Reserved: 0x00 Common Info Common Info Length: 7 MLD MAC Address: f2:d8:05:6a:00:10 (f2:d8:05:6a:00:10) Basic STA Profile Count: 0</pre>
--	--

Link 1 Mac address

SAE Auth Successful

MLD Mac address

OTA Packet Flow

Association Request - Response

```
182482 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"
> Frame 182482: Packet, 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface Device\NPF_{06000E34-376B-416A-BBF0-F2FCF5A1CF53}_id_0
> Ethernet II, Src: CiscoMeraki_6f:53:27 (c4:14:a2:6f:53:27), Dst: Intel_e0:b1:b3 (64:32:a8:e0:b1:b3)
> Internet Protocol Version 4, Src: 10.106.107.251, Dst: 10.106.107.248
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AiroPeek/OmniPeek encapsulated IEEE 802.11
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
< IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  > Tagged parameters (321 bytes)
    > Tag: SSID parameter set: "Workoholic"
    > Tag: Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: RSN Information
    > Tag: HT Capabilities
    > Tag: Extended Capabilities (12 octets)
    > Ext Tag: HE Capabilities
    > Ext Tag: Multi-Link (802.11be D3.0)
      Ext Tag length: 143 (Tag len: 144)
      Ext Tag Number: Multi-Link (802.11be D3.0) (107)
    > Multi-Link Control: 0x0100 Basic
  < Common Info
    Common Info Length: 9
    MLD MAC Address: Microsoft_b4:05:25 (c4:cb:76:b4:05:25)
  < MLD Capabilities: 0x0021
    .... 0001 = Maximum Number of Simultaneous Links: 1
    .... 0000 = SRS Support: False
    .... 0001 = TID-To-Link Mapping Negotiation Support: 1
    .... 0000 0... = Frequency Separation For STR/AP MLD Type Indication: 0
    .... 0000 = AAR Support: False
    ..0. .... = Link Reconfiguration Operation Support: False
    .0.. .... = Aligned TWT Support: False
    0... .... = Reserved: 0x0
  Subelement ID: Per-STA Profile (0x00)
  Subelement Length: 130
  > Per-STA Profile 1
  Basic STA Profile Count: 1
  STA Profiles LinkIds: 1
  < Ext Tag: EHT Capabilities (802.11be D3.0)
  Ext Tag length: 15 (Tag len: 16)
  Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
  > EHT MAC Capabilities Information: 0x0097, EPCS Priority Access Support, EHT OM Control Support
  > EHT PHY Capabilities Information
  > Supported EHT-MCS and NSS Set
  > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
  > Tag: RSN eXtension (1 octet)
  > Tag: Vendor Specific: Qualcomm Inc.

182723 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, SSID="Workoholic"
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: .....C
< IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
  < Tagged parameters (391 bytes)
    > Tag: Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    > Tag: HT Capabilities
    > Tag: HT Operation
    > Tag: Extended Capabilities (10 octets)
    > Tag: BSS Max Idle Period
    > Tag: RSN eXtension (1 octet)
    > Ext Tag: HE Capabilities
    > Ext Tag: HE Operation
    > Ext Tag: MU EDCA Parameter Set
    < Ext Tag: EHT Operation (802.11be D3.0)
    Ext Tag length: 5 (Tag len: 6)
    Ext Tag Number: EHT Operation (802.11be D3.0) (106)
    > EHT Operation Parameters: 0x04, EHT Default PE Duration
    Basic EHT-MCS And Nss Set: 0x00000011
    < Ext Tag: Multi-Link (802.11be D3.0)
    Ext Tag length: 206 (Tag len: 207)
    Ext Tag Number: Multi-Link (802.11be D3.0) (107)
    > Multi-Link Control: 0x01b0 Basic
  < Common Info
    Common Info Length: 13
    MLD MAC Address: f2:d8:05:6a:00:10 (f2:d8:05:6a:00:10)
  > Link ID subfield: 0x00
  BSS Parameters Change Count: 0
  < EML Capabilities: 0x4001, EMLSR Support
    .... 0001 = EMLSR Support: True
    .... 0000 = EMLSR Padding Delay: 0
    .... 0000 = EMLSR Transition Delay: 0
    .... 0000 = EMLMR Support: False
    .... 0000 = EMLMR Delay: 0
    .100 0... = Transition Timeout: 8
    0... .... = Reserved: 0x0
  < MLD Capabilities: 0x0001
    .... 0001 = Maximum Number of Simultaneous Links: 1
    .... 0000 = SRS Support: False
    .... 0000 = TID-To-Link Mapping Negotiation Support: 0
    .... 0000 0... = Frequency Separation For STR/AP MLD Type Indication: 0
    .... 0000 = AAR Support: False
    ..0. .... = Link Reconfiguration Operation Support: False
    .0.. .... = Aligned TWT Support: False
    0... .... = Reserved: 0x0
  Subelement ID: Per-STA Profile (0x00)
  Subelement Length: 189
  > Per-STA Profile 1
  Basic STA Profile Count: 1
  STA Profiles LinkIds: 1
  < Ext Tag: EHT Capabilities (802.11be D3.0)
  Ext Tag length: 14 (Tag len: 15)
  Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
  > EHT MAC Capabilities Information: 0x0086, EHT OM Control Support, Triggered TXOP Sharing Mode 1 Support, Maximum MPDU Length: 11 454,
  > EHT PHY Capabilities Information
  > Supported EHT-MCS and NSS Set
```

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 Failed 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 Failed 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 S

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 

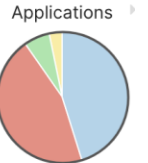
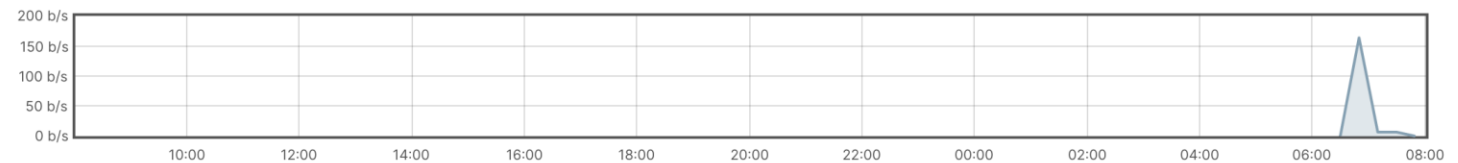
Current client connection




Health for the last 2 hours



Usage for the last day



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

80 ms 
40 ms 
0 ms 
Loss rate: -
Average latency: -

Wi-Fi 7 Client details on Meraki Cloud

Signal quality ⓘ

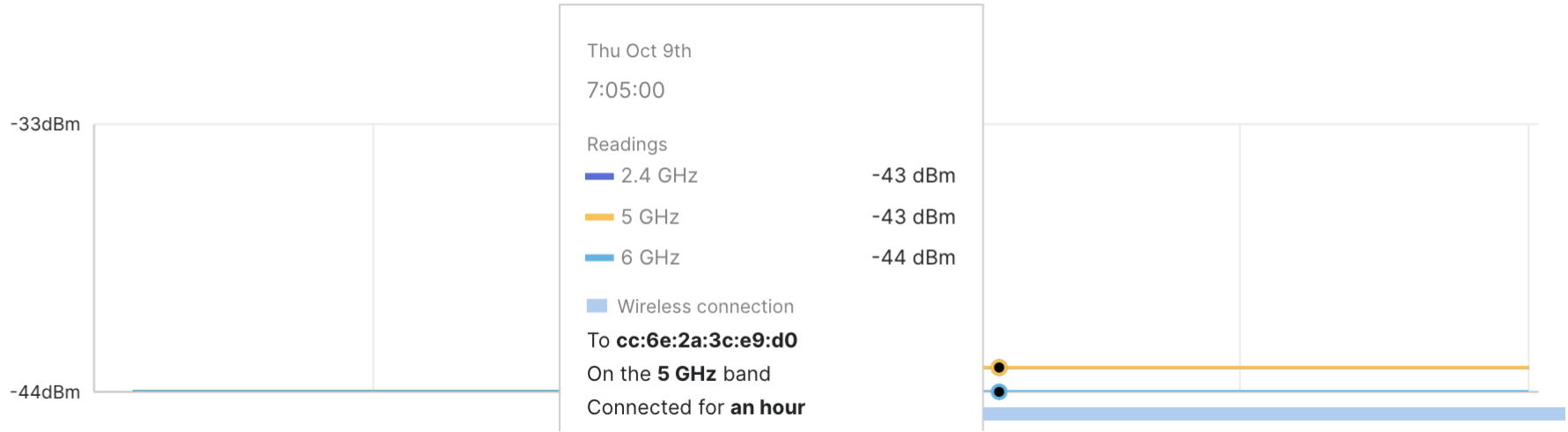
in RSSI ▾



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



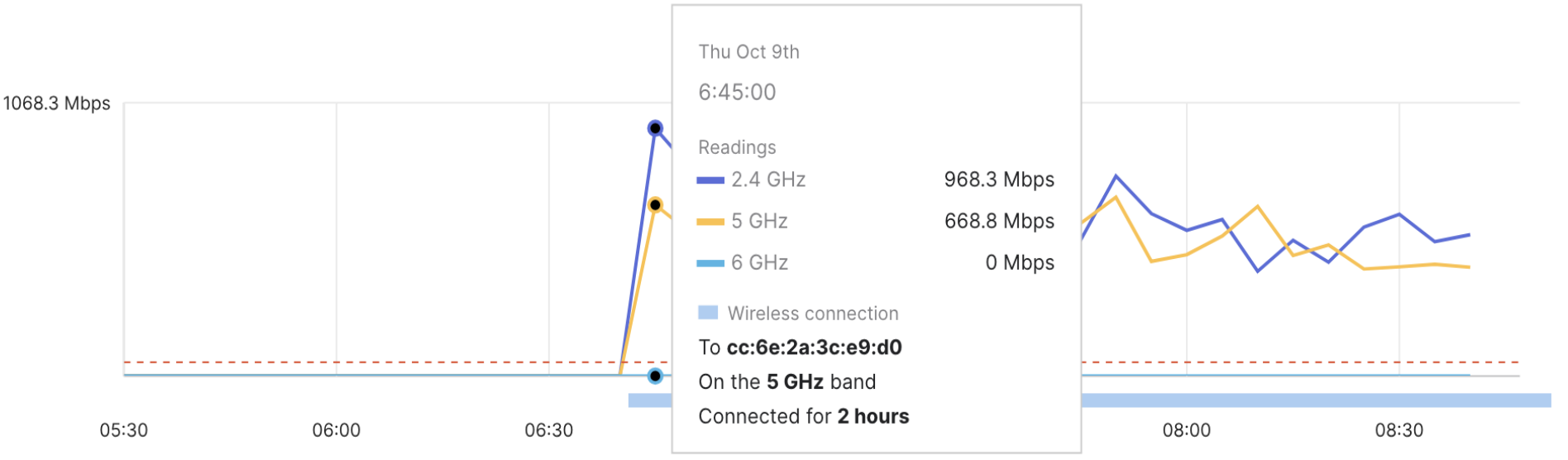
Wi-Fi 7 Client details on Meraki Cloud

Data rates ⓘ All traffic ▾

Absolute Normalized

2.4 GHz
100% Data rates > 54Mbps

5 GHz
100% Data rates > 54Mbps



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"

<ul style="list-style-type: none"> ▼ IEEE 802.11 Wireless Management <ul style="list-style-type: none"> ▼ Tagged parameters (454 bytes) <ul style="list-style-type: none"> ➤ Tag: VHT Operation ➤ Tag: Tx Power Envelope ➤ Tag: Reduced Neighbor Report ➤ Ext Tag: HE Capabilities ➤ Ext Tag: HE Operation 		<input type="text" value=""/>	<pre> 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 d0n*<.. 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. </pre>
---	--	-------------------------------	--

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

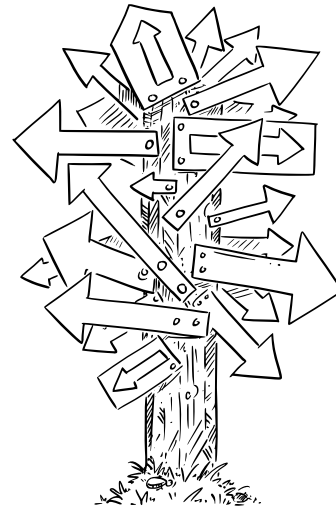
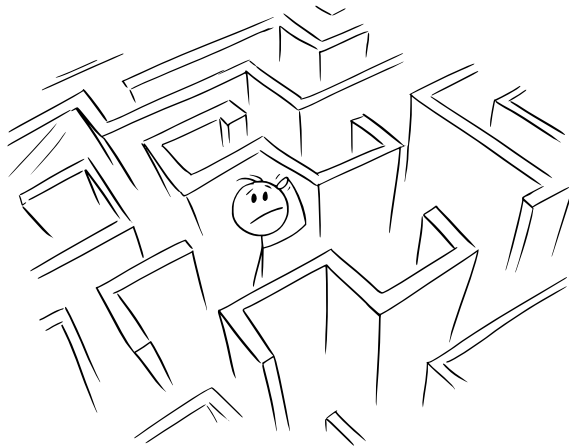
- IoT & automation
- Real-time analytics
- Smart offices & cities
- Massive device handling

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?



The background features a vibrant blue and purple abstract design with flowing, wavy lines. In the center, a white rectangular area contains an illustration of several hands of various skin tones raised in a gesture of appreciation or applause. The hands are wearing colorful sleeves and accessories like bracelets and bangles.

Thank you

CISCO Live !

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



Management Changes in .be – PPDU Layer

