

Wireless Update

The Network People

Maurijn van Tol – mtol@cisco.com
Solutions Engineer Cisco Networking

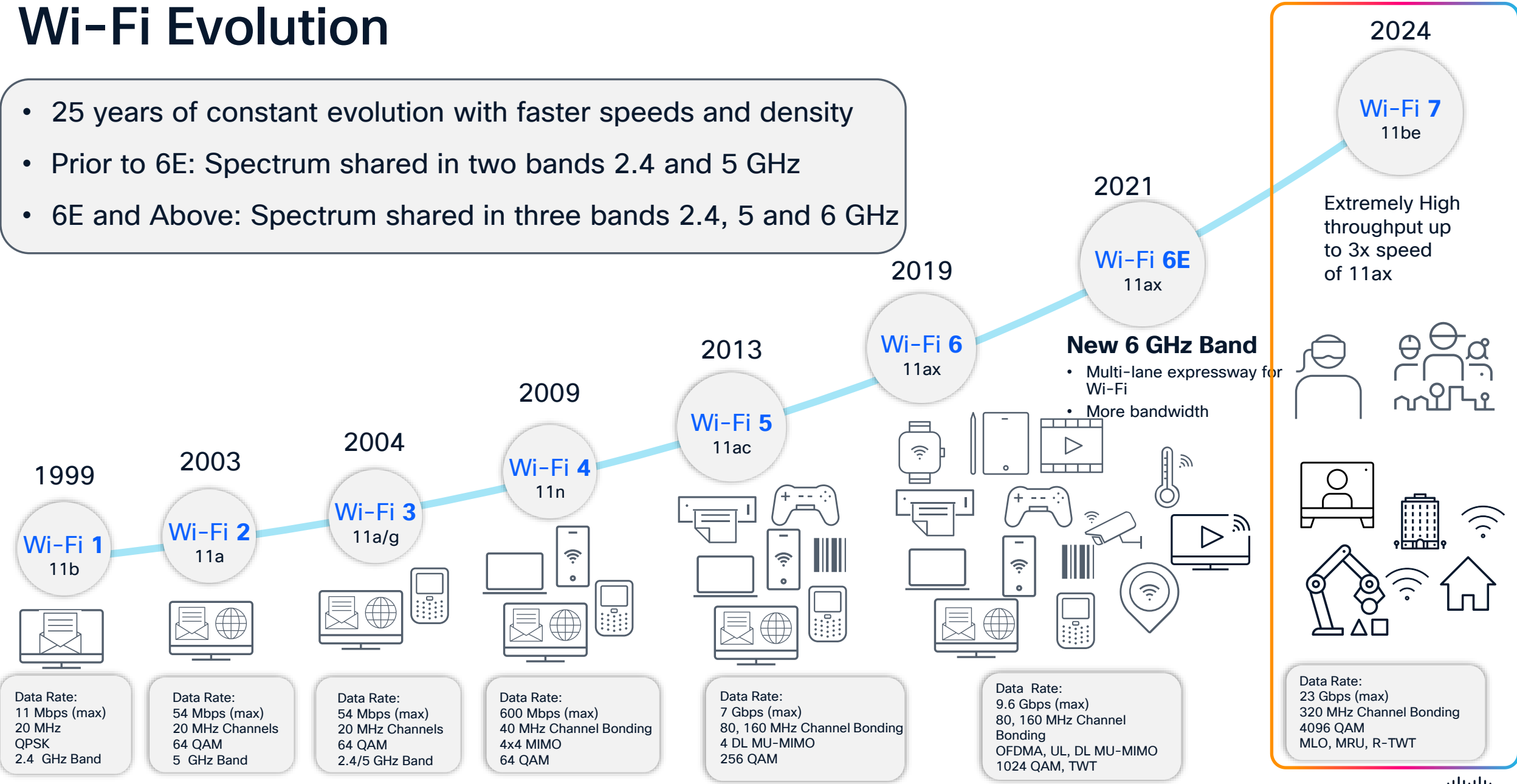
Mei 2026

CISCO Live !

Why 6 GHz & Wi-Fi 7 ?

Wi-Fi Evolution

- 25 years of constant evolution with faster speeds and density
- Prior to 6E: Spectrum shared in two bands 2.4 and 5 GHz
- 6E and Above: Spectrum shared in three bands 2.4, 5 and 6 GHz



Wi-Fi 7 Use Cases



What is Wi-Fi 7?

Wi-Fi 7 & IEEE 802.11be

1

Wi-Fi 7 based on IEEE 802.11be amendment
termed as “Extremely High Throughput”

2

IEEE 802.11be final publication complete.

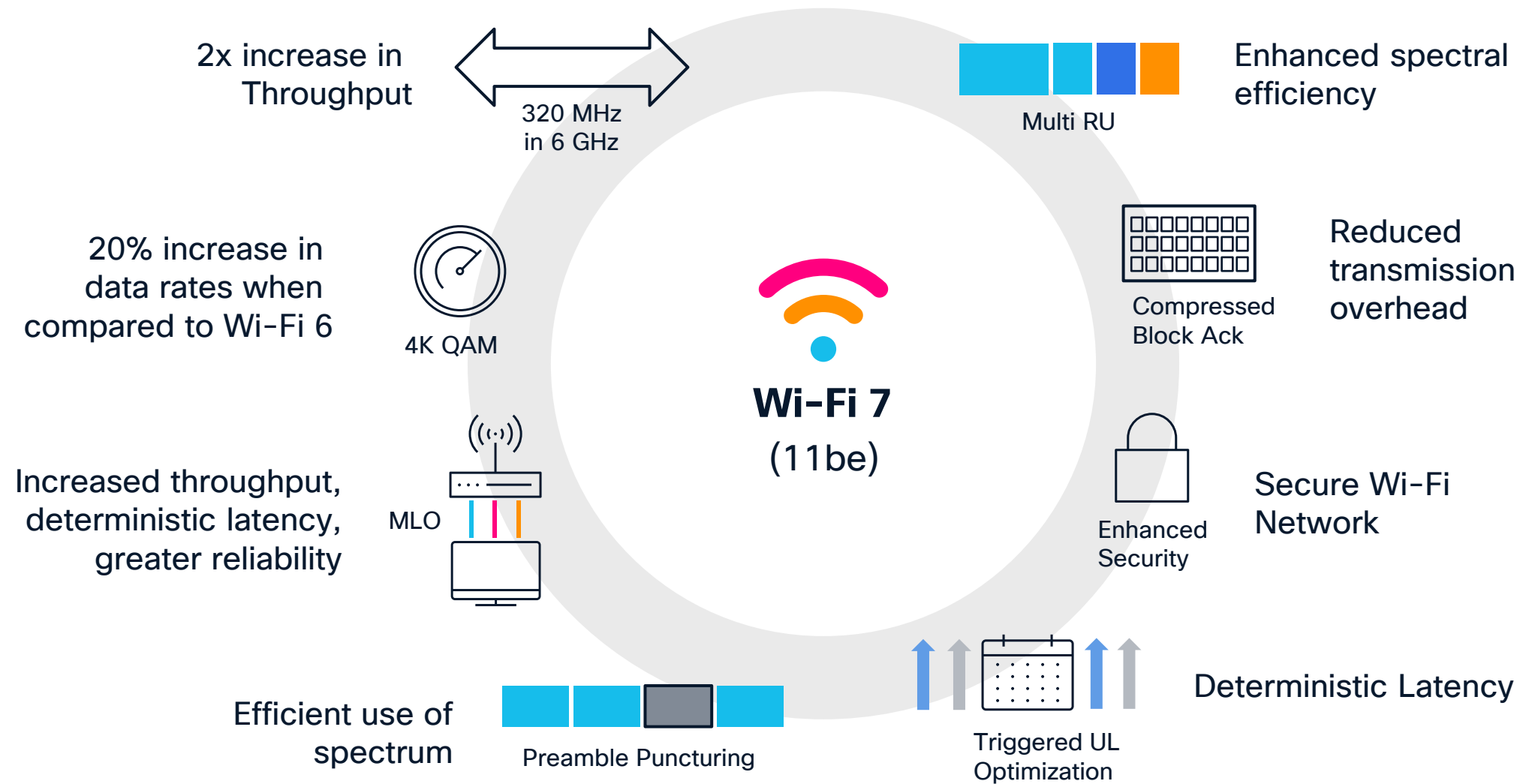
3

Wi-Fi 7 R1 spec finalized in Jan '24. WFA certification for R1 in progress.
R2 certification early 2026.

4

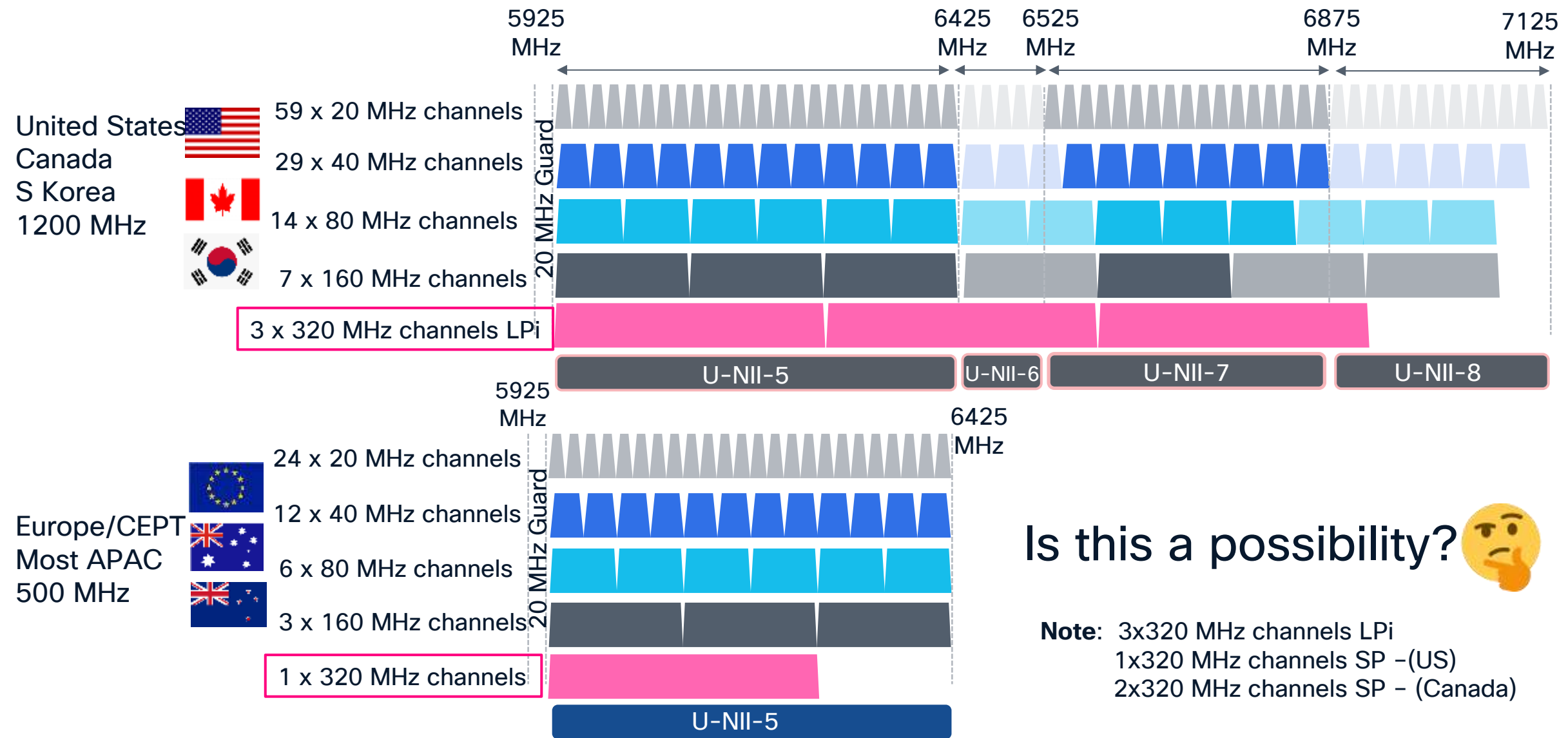
Cisco has been closely involved in development of Wi-Fi 7, and advocates for
thorough client interop testing

Wi-Fi 7 Features



Wi-Fi 7 Feature Overview

Wi-Fi 7 – 320 MHz channel width in 6 GHz



Is this a possibility? 🤔

Note: 3x320 MHz channels LPI
1x320 MHz channels SP –(US)
2x320 MHz channels SP – (Canada)

Wi-Fi 7 4K-QAM

(MCS12/13) increases the peak PHY data rate

- MCS 12 and MCS 13 indicate a 4096-QAM constellation with a code rate of $\frac{3}{4}$ and $\frac{5}{6}$ respectively
- Very short range and most suited to a 1 antenna client with a multi-antenna AP (beamforming, MRC)

Need very high SNR for 4K QAM



Each increment in constellation size reduces range by approx. 50%

Incremental data rate
Relative Range

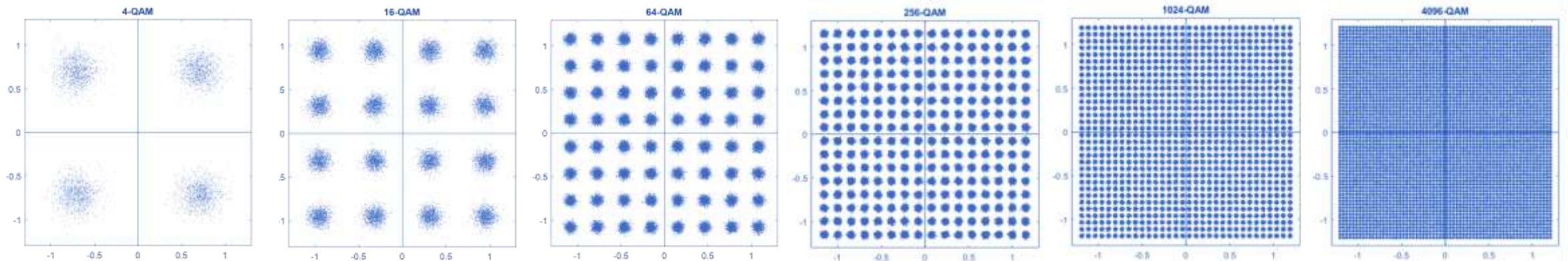
+100%
80

+50%
40

+33%
20

+25%
10

+20%
5



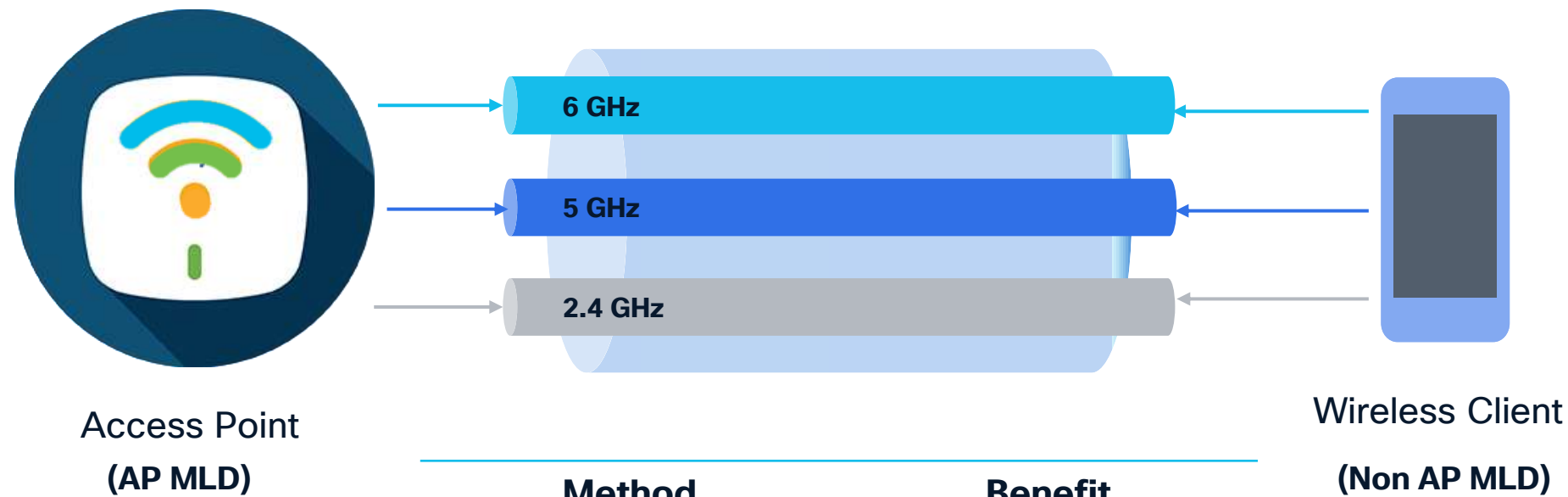
Wi-Fi4

Wi-Fi5

Wi-Fi6

Wi-Fi7

Wi-Fi 7 Multilink (MLO)

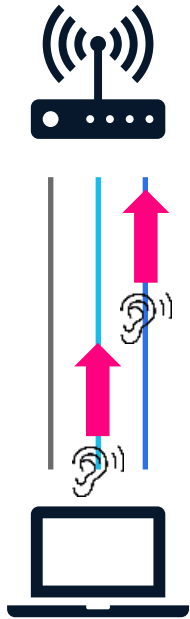


Method	Benefit
Aggregation	Throughput
Steering	Lower Latency
Redundancy	Reliability

MLD: Multi Link Device

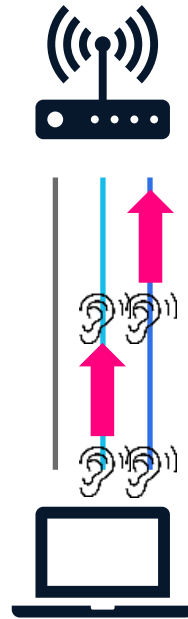
Multi-Link Operation (MLO) for more spectrum usage

Multi Link Single Radio
MLSR



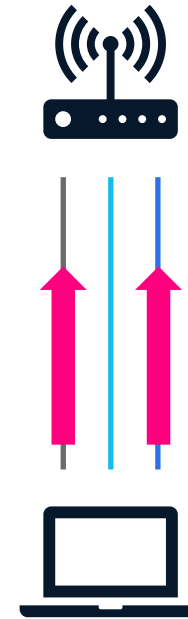
Only one radio
operational at a
given moment

Enhanced
Multi Link Single Radio
EMLSR



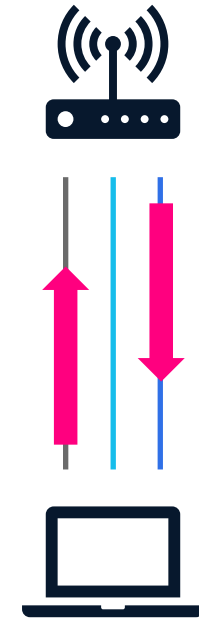
MLSR, but listening on
multiple links in parallel
before selecting one

Multi Link Multi Radio
Non-Simultaneous Tx Rx
MLMR NSTR



Using multiple
radios to transmit
or receive
(not part of the official
Wi-Fi 7 certification)

Multi Link Multi Radio
Simultaneous Tx Rx
MLMR STR



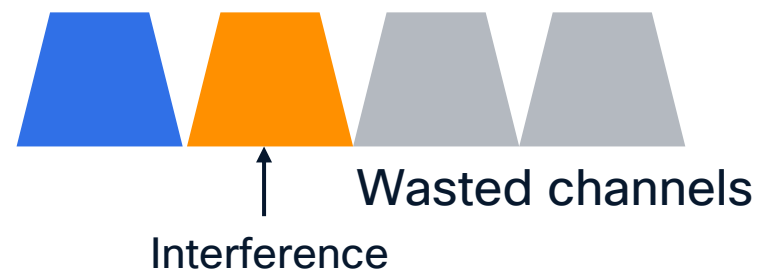
Using multiple
radios to transmit
and/or receive

What to practically expect from MLO today

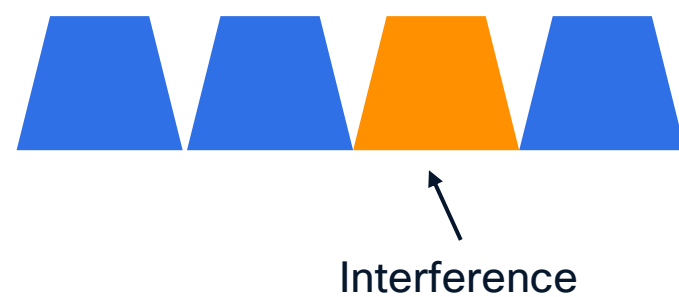


Wi-Fi 7 Preamble Puncturing

Without preamble puncturing :



With preamble puncturing:

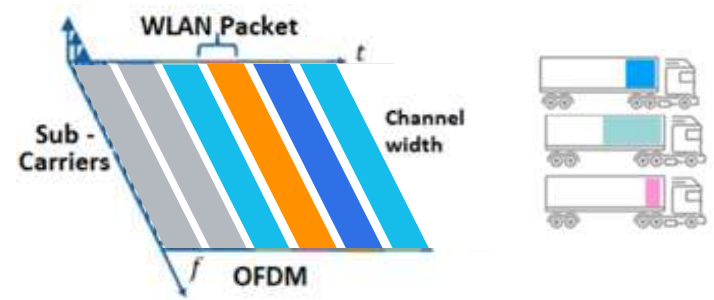


Channel Width	Allowed Puncturing
80 MHz	20 MHz
160 MHz	20 or 40 MHz
320 MHz	40 or 80 MHz (or) 40 + 80 MHz

Puncturing allowed for 80 MHz channel width or wider

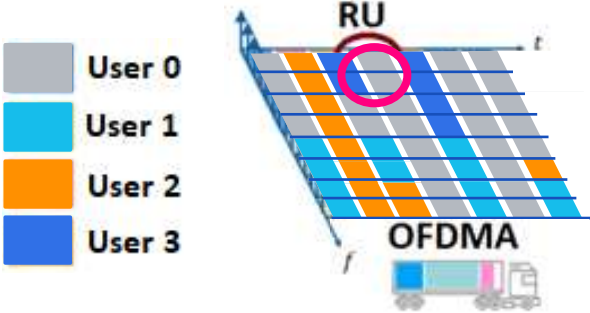
Wi-Fi 7 multiple resource unit (MRU)

OFDM (before Wi-Fi 6)



OFDMA (Wi-Fi 6 and later)

Resource unit (RU) is a unit to denote a group of subcarriers (tones) in OFDMA



Wi-Fi 6

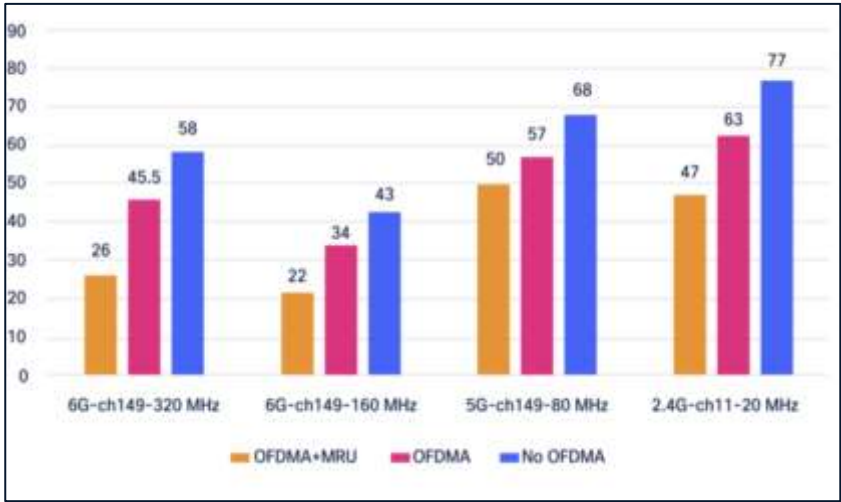


One user can have only one RU

Wi-Fi 7



One user can have multiple RUs



Multiple RUs make efficient use of spectrum

<https://blogs.cisco.com/networking/wi-fi-7-mru-ofdma-turning-rush-hour-into-easy-street-for-wireless-traffic>

Wi-Fi 7 - 512 Compressed Block Ack

Wi-Fi 6/6E



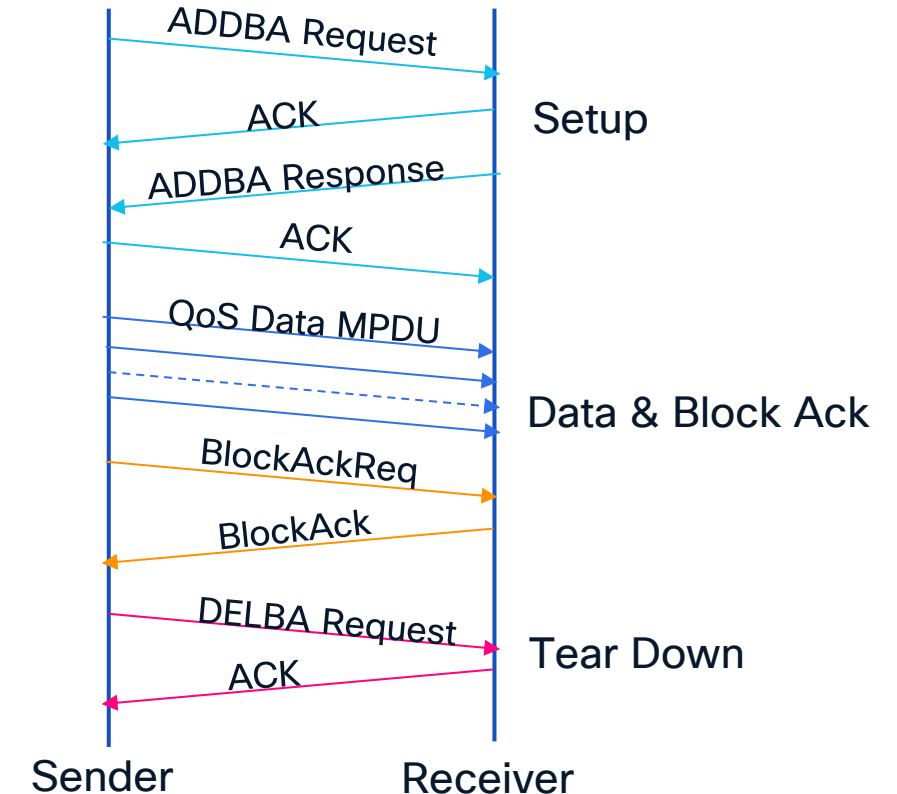
- Aggregation of upto **256** MPDUs in a single frame.
- Acknowledgement upto **256** MPDUs in a single Block Ack Frame

Wi-Fi 7



- Aggregation of upto **512** MPDUs in a single frame.
- Acknowledgement upto **512** MPDUs in a single Block Ack Frame

Block Ack frame exchange sequence



Reduces Protocol Overhead. Improve transmitter's performance at higher rates.

Cisco's Wi-Fi 7 AP Portfolio

One Cisco Wireless Access Point

Global Use AP, Unified Product, Single SKU



Cisco Catalyst Management Mode
C9800 & Catalyst Center Stack

Meraki **Management Mode**
MR Dashboard Stack



Join any stack on Day 0, based on Intent
Management Mode Change from Day 1 to N

Wi-Fi 7 for every operational scale



CW9172H

6 Spatial Streams
2.5 Gig
Hospitality



CW9174E

8/10 Spatial Streams
5 Gig
External antennas
Dec 2025



CW9176D1

12 Spatial Streams
10 Gig
Integrated Directional
UWB



CW9179F

16 Spatial Streams
10 Gig
LPV/Stadium



CW9171I

4 Spatial Streams
2.5 Gig
Omnidirectional
Dec 2025



CW9172I

6 Spatial Streams
2.5 Gig
Omnidirectional



CW9174I

8/10 Spatial Streams
5 Gig
Omnidirectional
Dec 2025



CW9176I

12 Spatial Streams
10 Gig
Omnidirectional
UWB



CW9178I

16 Spatial Streams
10 Gig
Omnidirectional
UWB

Wi-Fi 7 | Global Use AP | Unified License | AI Optimized

The Wi-Fi 7 portfolio



CW9179F

16 Spatial Streams
4x4:4 MU-MIMO
across 4 radios, 3 bands
(2.4 GHz, dual 5GHz, 6GHz)

Indoor or Outdoor Use

Dual 10Gbps multigigabit

Accelerometer

Built-in GPS/GNSS, w/ support for ext. antenna

Integrated Hyper-directional Antenna

Global Use AP

New Articulating Mount Option



CW9178I

16 Spatial Streams
4x4: 4 MU-MIMO
across 4 radios, 3 bands
(2.4 GHz, dual 5GHz, 6GHz)

BLE/IoT radio & accelerometer

Dual 10Gbps multigigabit

Ultra Wide Band (UWB)

USB 2.0 – 9W

Accelerometer

Built-in GPS/GNSS, w/ support for ext. antenna

Integrated Omnidirectional Antenna

Same brackets as always

Already Wi-Fi 7 certified!

The Wi-Fi 7 portfolio



CW9176I

12 Spatial Streams
4x4: 4 MU-MIMO
across 3 radios, 3 bands
(2.4/5GHz (XOR), 5 GHz, 6GHz)

BLE/IoT radio

Single 10Gbps multigigabit

Ultra Wide Band (UWB)
USB 2.0 – 9W

Accelerometer

Built-in GPS/GNSS, w/ support for ext. antenna
Integrated Omnidirectional Antenna



CW9176D1

12 Spatial Streams
4x4: 4 MU-MIMO
across 3 radios, 3 bands
(2.4/5GHz (XOR), 5 GHz, 6GHz)

BLE/IoT radio

Single 10Gbps multigigabit

Ultra Wide Band (UWB)
USB 2.0 – 9W

Accelerometer

Built-in GPS/GNSS, w/ support for ext. antenna
Integrated Directional Antenna (70x70)

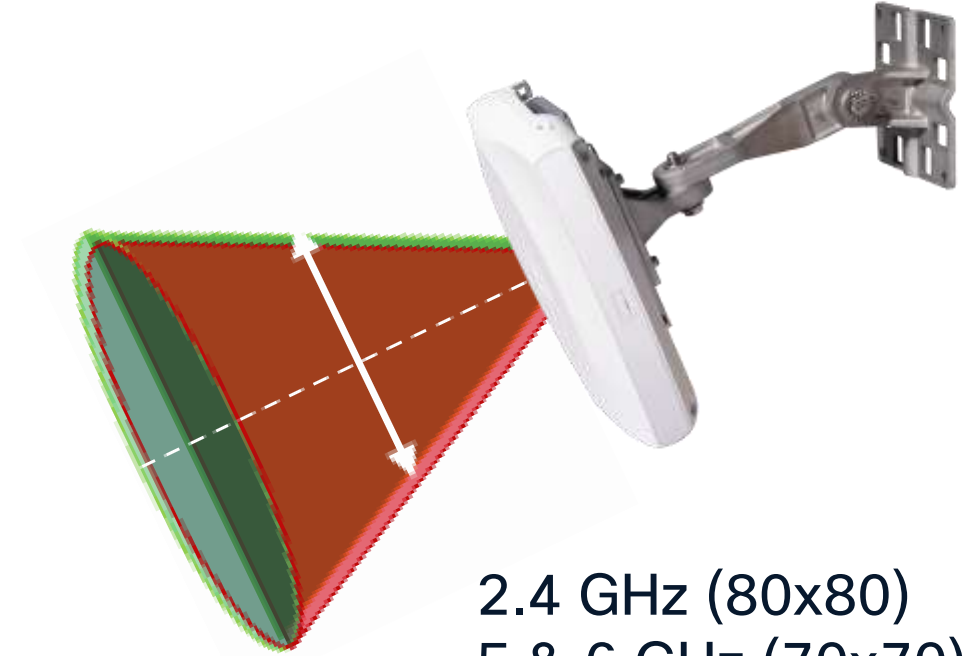
Same brackets as always

Already Wi-Fi 7 certified!

Antenna differences between **CW9176I** and **CW9176D1**



CW9176I designed with an integrated omni-directional antenna ceiling mount for a “360 degree” coverage pattern – ideal for offices, conventional buildings



2.4 GHz (80x80)
5 & 6 GHz (70x70)

CW9176D1 designed with an integrated directional antenna allowing the coverage pattern to favor the area the AP is facing – ideal for warehouse, auditoriums etc.

The Wi-Fi 7 portfolio



CW9174I/E
8 or 10 Spatial Streams

2x2:2 on 2.4GHz and 4x4:4 on 5GHz and 6GHz
-or-
4x4:4 on 2.4GHz and 5GHz

BLE/IoT and dedicated scan radio

Single 5Gbps multigigabit uplink

USB 2.0 – 9W | DC Power Jack

Extended operating temperature range, -20C to 50C (9174E only)

Integrated Omnidirectional or DART-8 External Antenna

Global Use AP

Compared to CW9176I/D1:
2x2 2.4GHz in Tri-radio mode
No GPS
No UWB
No Dual 5GHz
5Gbps Uplink

Same brackets as always

The Wi-Fi 7 portfolio



CW9172I

6 Spatial Streams
2x2:2 across 3 radios, 3 bands
(2.4GHz, 5GHz, 6GHz)

-or-

2x2:2 on 2.4GHz and 4x4:4 on 5GHz
BLE/IoT and dedicated scan radio

Single 2.5Gbps multigigabit uplink
USB 2.0 – 4.5W

DC Power Jack

Integrated Omnidirectional Antenna

Global Use AP



CW9172H

6 Spatial Streams
2x2:2 across 3 radios, 3 bands
(2.4GHz, 5GHz, 6GHz)

BLE/IoT and dedicated scan radio

Single 2.5Gbps multigigabit uplink

3x 1Gbps LAN port with 1x POE out

1x Passthrough port

Integrated Omnidirectional Antenna

Global Use AP

Same brackets as always. 9172H compatible with Meraki or Catalyst brackets

The Wi-Fi 7 portfolio



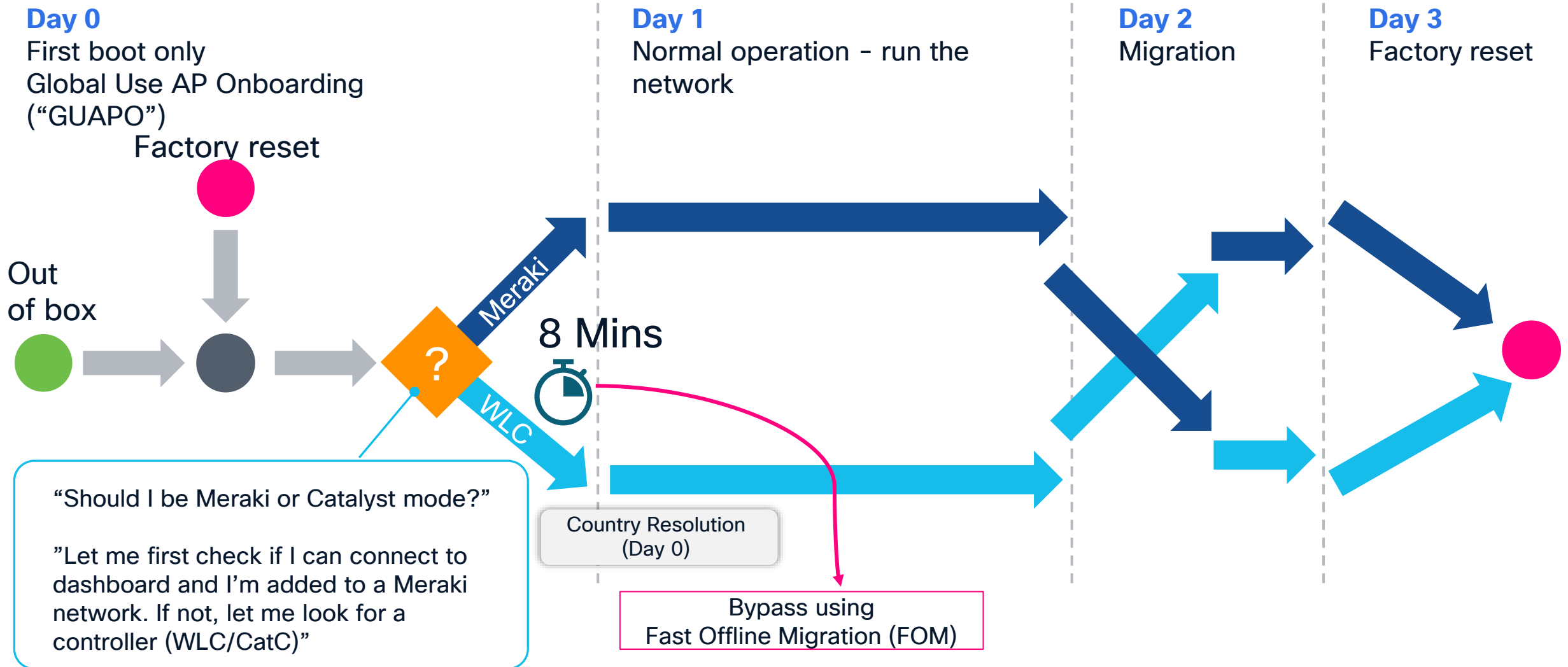
CW9171I

4 Spatial Streams
2x2:2 across 2 radios, 3 bands
(2.4GHz, 5GHz or 6GHz)
BLE/IoT and dedicated scan radio
Single 2.5Gbps multigigabit uplink
USB 2.0 – 4.5W
DC Power Jack
Integrated Omnidirectional Antenna
Global Use AP

Same brackets as always.

Global Use AP

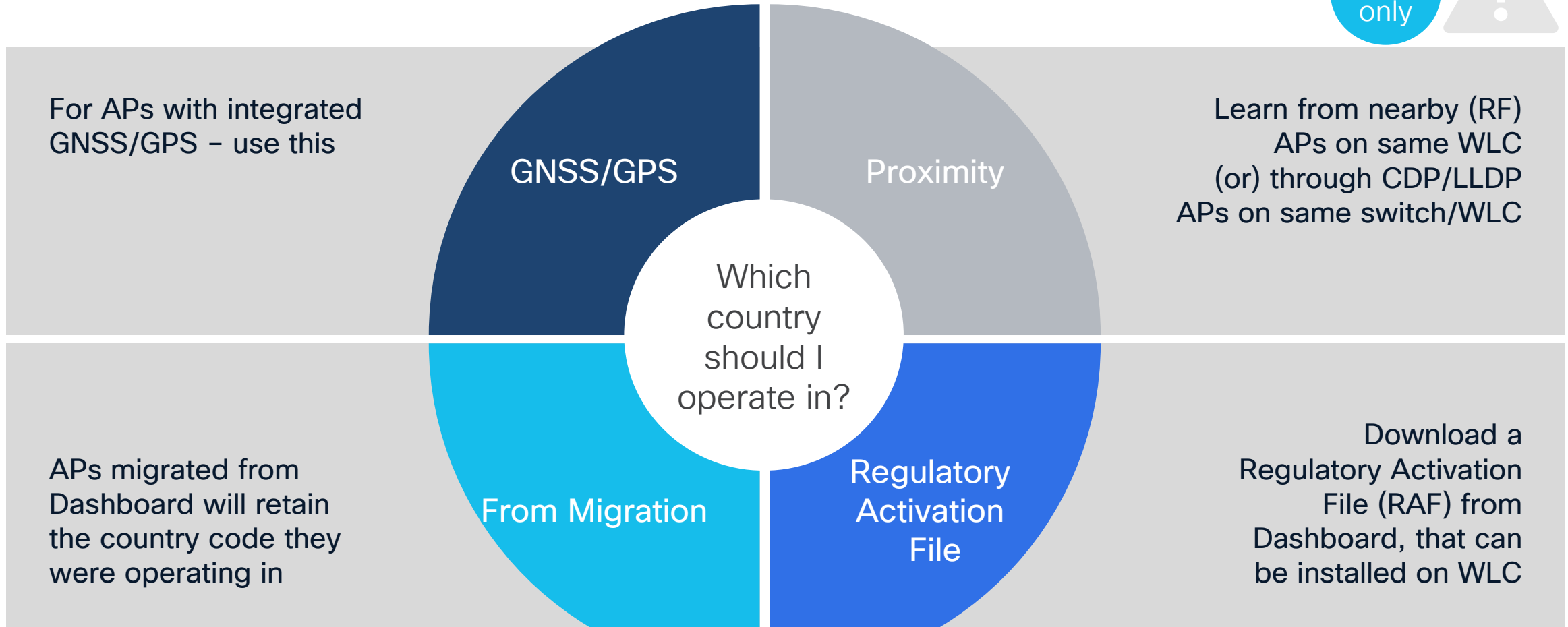
Map of a Global Use AP's journey



GUAP Deployment Guide: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/technical-reference/global-use-ap-dg.html

Let's zoom in on "Country Code"

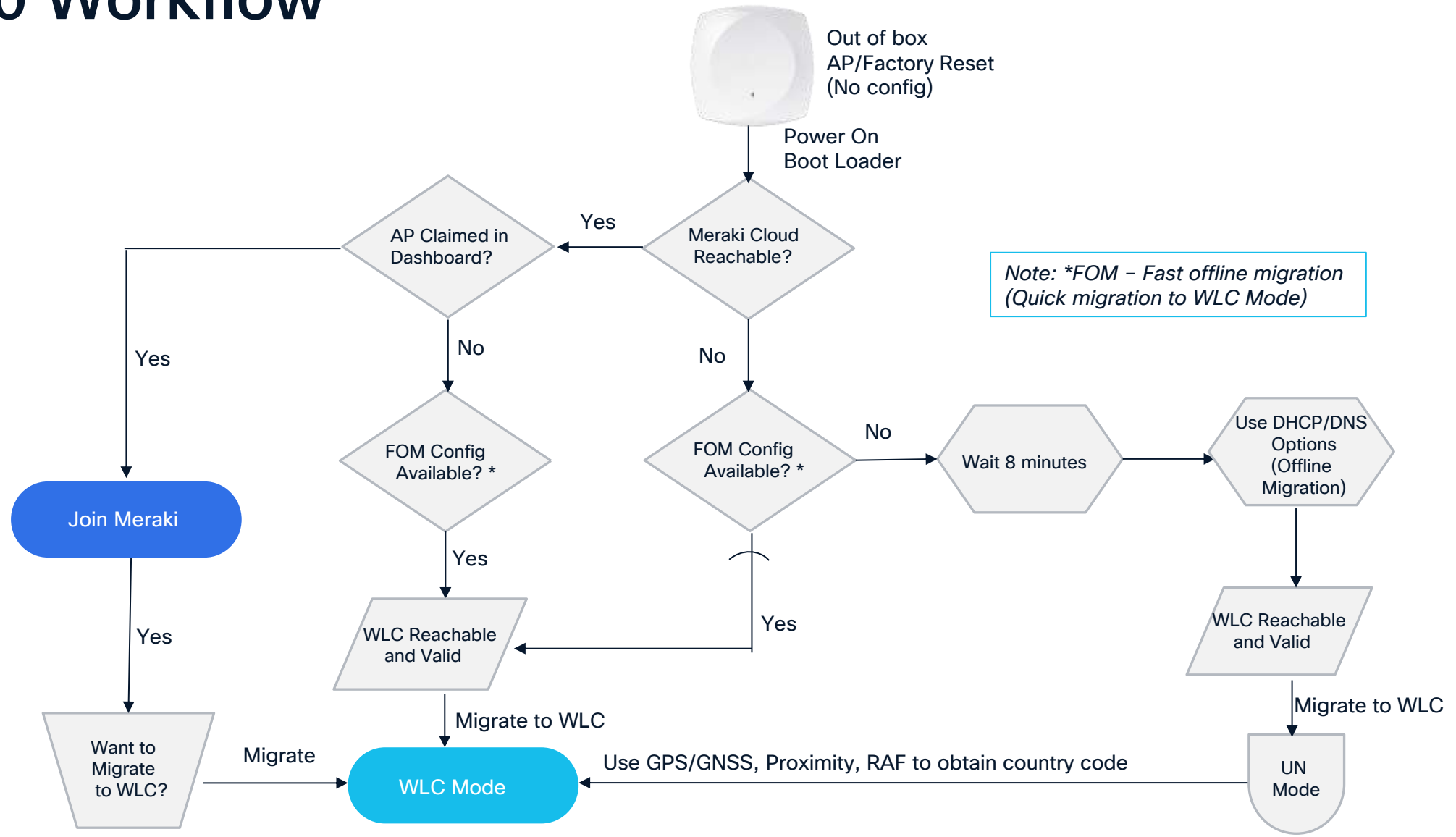
When APs are in WLC mode, APs will determine their Country Code in one of the following ways



Country Code determination is only done once - unless the admin triggers a country reset.
i.e. APs will not auto-change country codes, but network admins can change it!

GUAP Deployment Guide: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/technical-reference/global-use-ap-dg.html

Day 0 Workflow



Network Infrastructure

Cisco Wireless AP to switch connection



AP negotiates power, speed and duplex at boot time via CDP/LLDP

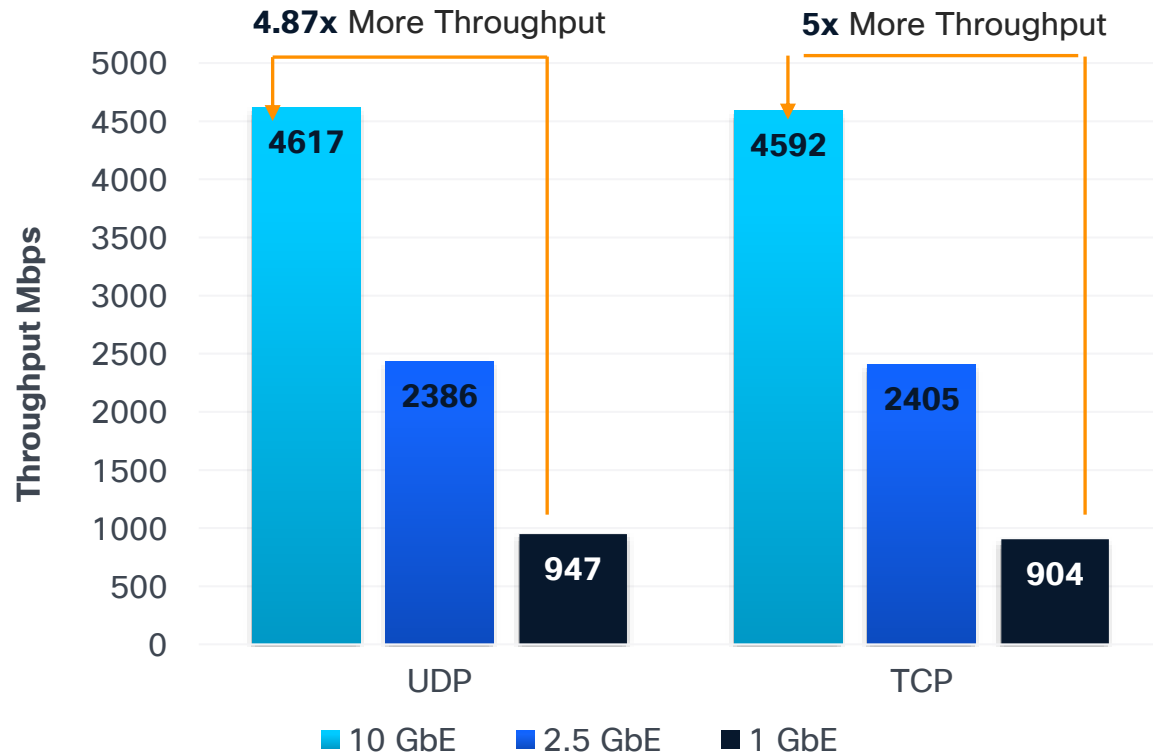
MGig switchport is recommended as Wi-Fi 6E/7 speed may exceed 1 Gbps

Cabling: Cat 6A preferred.

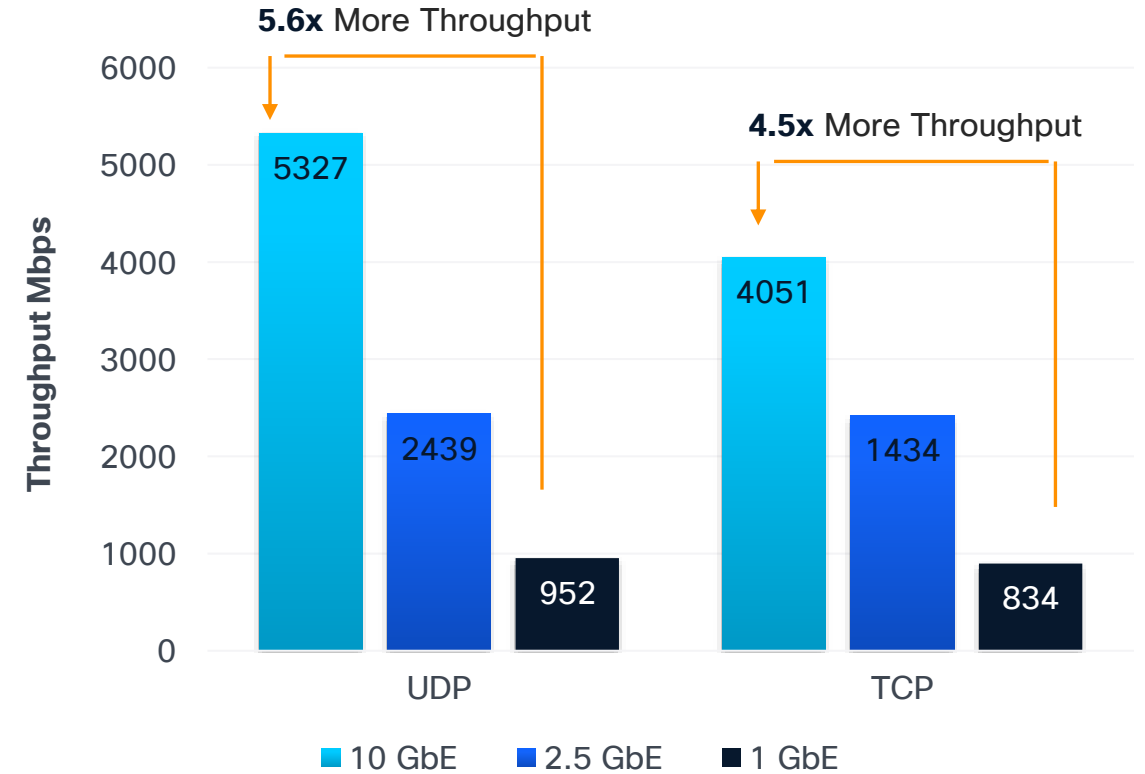
CDP = Cisco Discovery Protocol
LLDP = Link Layer Discovery Protocol
Cat = Category (of ethernet cable)

Cisco 9176 mGig Results

2.4 (20 MHz), 5 (160 MHz), 6 (320 MHz)



3 Clients



10 Clients

Power Considerations

AP Power Consumption



Power Allocated

48.3 W

Power Consumed

16.5 W

PoE Power Negotiation happens at boot time through CDP/LLDP

Power allocation is what you need to consider for power budget

Actual Power consumption is dependent on the AP operation

Recap of Power Over Ethernet Standards



Reference

Spec	Known as	Class	Min PSE Output Power	Min PD Input Power
Type 1 IEEE 802.3af	PoE	Class 1	4 W	3.84 W
		Class 2	7 W	6.49 W
		Class 3	15.4 W	12.95 W
Type 2 IEEE 802.3at	PoE +	Class 4	30 W	25.5 W
Type 3 IEEE 802.3bt	PoE++, Cisco UPOE	Class 5	45 W	40 W
		Class 6	60 W	51 W
Type 4 IEEE 802.3bt	Cisco UPOE+	Class 7	75 W	62 W
		Class 8	90 W	71.3 W

PoE Requirements



CW9179F



CW9178I

IEEE 802.3bt Type 3, Class 6
(For full operation)

IEEE 802.3at Type 2, Class 4
(Reduced Spatial Streams,
Ethernet @2.5 G, No USB)



CW9176I & D1



IEEE 802.3bt Type 3, Class 5
(For full operation)

IEEE 802.3at Type 2, Class 4
(Reduced Spatial Streams,
Ethernet @2.5 G, No USB)



CW9174I & E



IEEE 802.3bt Type 3, Class 5
(For full operation)

IEEE 802.3at Type 2, Class 4
(Ethernet @2.5 Gig, No USB)



CW9172I



CW9172H

IEEE 802.3bt Type 3, Class 5
(For full operation)

IEEE 802.3at Type 2, Class 4
(No USB, No PoE Out)

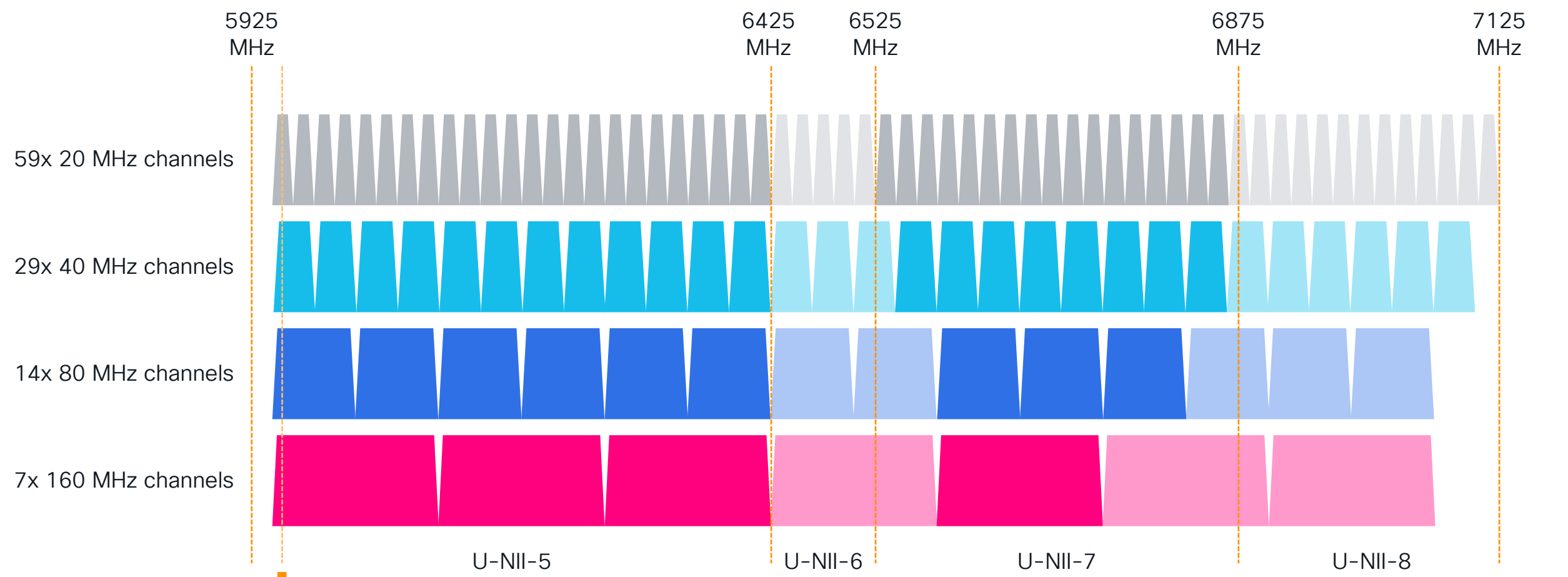


CW9171I

IEEE 802.3at Type 2, Class 4
(For full operation)

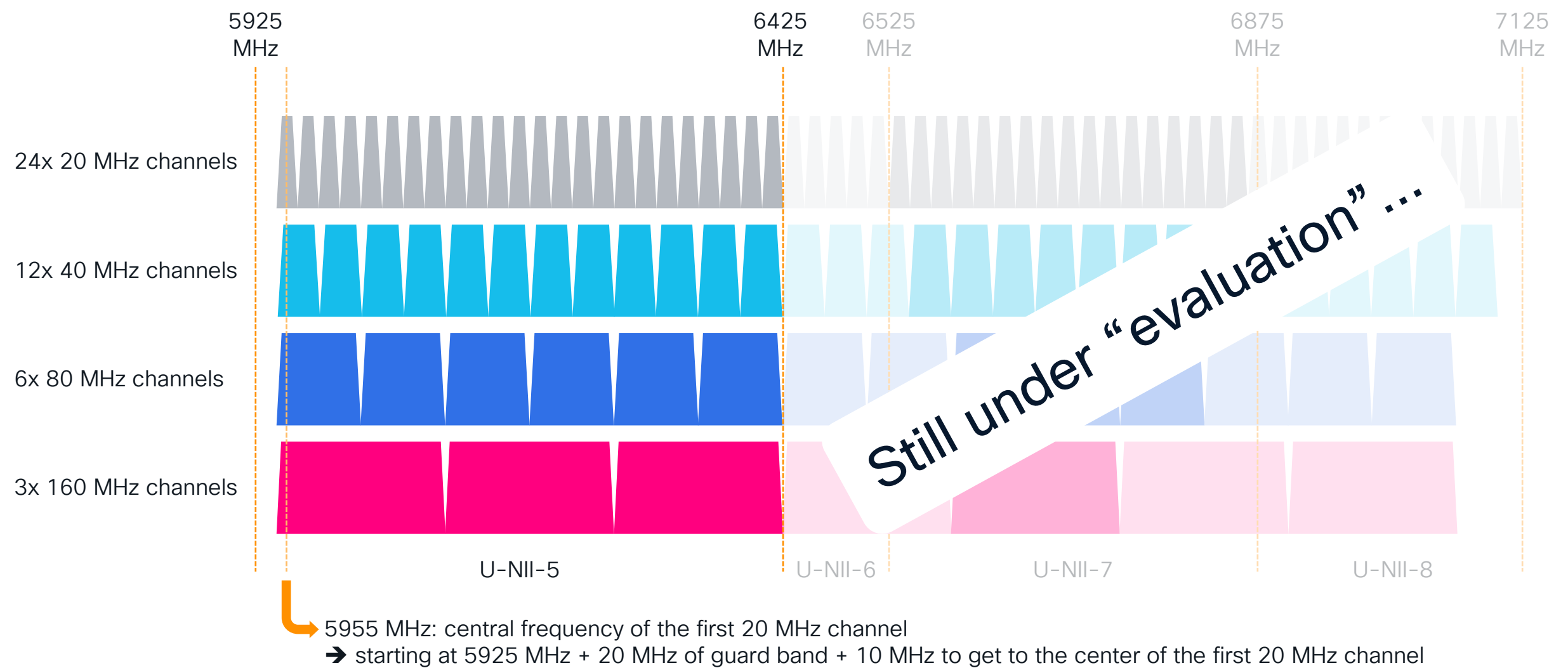
Deploying Wi-Fi 7 APs and endpoints provides pervasive support for 6 GHz (and WPA3)

The new 6 GHz band (starting from Wi-Fi 6E)



5955 MHz: central frequency of the first 20 MHz channel
➔ starting at 5925 MHz + 20 MHz of guard band + 10 MHz to get to the center of the first 20 MHz channel

For ETSI, only U-NII-5 is available “for now”



RF design considerations for 6 GHz



AP antenna patterns for 6 GHz are similar to 5 GHz

Assuming the same Tx power, the 5 GHz cell is slightly larger than 6 GHz

RF design considerations for 6 GHz

AP replacement for **existing deployments**:

- If power levels are 3-4 on 5 GHz radios
 - Similar coverage pattern between 5 GHz and 6 GHz
 - 6 GHz radios likely with one power level higher than 5 GHz
- If power levels are 1-2 on 5 GHz
 - More APs may be necessary for similar 6 GHz coverage
 - ~10-20% additional access points
 - A site survey is probably needed



For **new deployments**, a site survey is always recommended

RF Profiles for limiting the lowest Tx power

(Catalyst) Configuration > Tags & Profiles > RF/Radio

The image displays four screenshots of the Cisco Catalyst configuration interface, specifically the 'Add RF Profile' dialog box, arranged in a 2x2 grid. The top row shows the 'General' tab for two profiles: 'RF_PRFL_5GHz_TPC' (left) and 'RF_PRFL_6GHz_TPC' (right). The bottom row shows the 'RRM' > 'TPC' sub-tab for the same two profiles. Annotations with pink boxes and arrows highlight specific configuration details.

Top Row: General Tab

- Left Screenshot (5 GHz):** The 'Radio Band' dropdown is set to '5 GHz Band'.
- Right Screenshot (6 GHz):** The 'Radio Band' dropdown is set to '6 GHz Band'.

Bottom Row: RRM > TPC Sub-tab

Transmit Power Control

Parameter	5 GHz Profile (Left)	6 GHz Profile (Right)
Maximum Power Level(dBm)*	30	30
Minimum Power Level(dBm)*	5	8
Power Control Threshold(dBm)*	-70	-70

Annotations:

- A pink box and arrow point to the 'Radio Band' dropdown in the top-left screenshot, with the text: "Two RF Profiles, for 5 and 6 GHz, applied through RF Tag(s)".
- A pink box and arrow point to the 'Minimum Power Level(dBm)*' field in the bottom-right screenshot, with the text: "Minimum power level on 6 GHz is 3 dB higher than on 5 GHz".

RF Profiles for limiting the lowest Tx power

(Meraki) Wireless > Radio Settings > RF profiles

The screenshot shows the Meraki management console interface for the 5 GHz band. The left sidebar contains navigation links: Global Overview, Organization (Federico Ziliotto), Network (Lab Network), Network-wide, Assurance, Wireless, Organization, and Automation. The main content area is titled 'General' and includes tabs for 2.4 GHz, 5 GHz (selected), and 6 GHz. Under the 5 GHz tab, there are settings for 'Turn off 5 GHz radio' (disabled), 'Channel width' (set to Auto), and 'Channel assignment method' (set to AutoChannel). A red box highlights the 'Radio transmit power range (dBm)' slider, which is currently set to 'Transmit shorter distance' at approximately 2 dBm. Below this, there is a 'Minimum bitrate' slider set to 'Lower Density' and a note about 802.11b devices not being supported. A red arrow points from the 5 GHz slider to the 6 GHz slider in the adjacent screenshot.

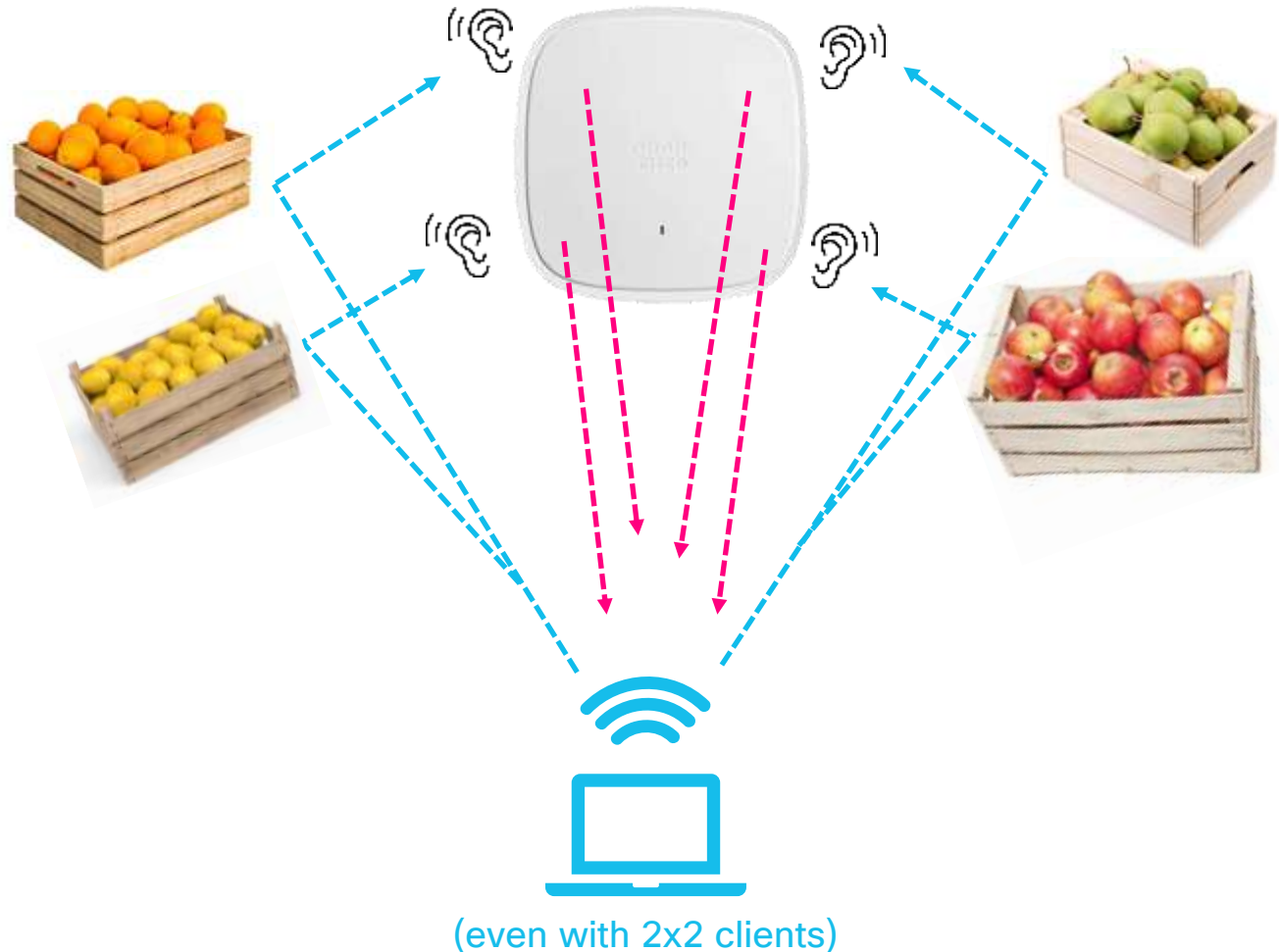
The screenshot shows the Meraki management console interface for the 6 GHz band. The left sidebar is identical to the 5 GHz screenshot. The main content area is titled 'General' and includes tabs for 2.4 GHz, 5 GHz, and 6 GHz (selected). Under the 6 GHz tab, there are settings for 'Turn off 6 GHz radio' (disabled), 'Channel width' (set to Auto), and 'Channel assignment method' (set to AutoChannel). A red box highlights the 'Radio transmit power range (dBm)' slider, which is currently set to 'Transmit shorter distance' at approximately 4 dBm. Below this, there is a 'Minimum bitrate' slider set to 'Lower Density' and a note about 802.11ax devices being supported. A red arrow points from the 5 GHz slider in the previous screenshot to this 6 GHz slider.

Minimum power level on 6 GHz is
2 dB higher than on 5 GHz

More antennas, better MRC and Tx MCS

The more antennas the better the Rx signal resiliency and the Tx signal SNR / MCS

As of 802.11n, MIMO brought us MRC (Maximum Ratio Combining), which leverages multiple receiving antennas to combine multiple received signals and increase the overall (received) signal strength. Also, more transmitters bring better beamforming towards the client (even if 2x2), hence improving the overall SNR and ultimately the MCS (Modulation Coding Scheme).



802.11be / Wi-Fi 7 must be globally enabled

Catalyst

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

Q Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Radio Configurations > High Throughput

6 GHz Band

5 GHz Band

2.4 GHz Band

6 GHz Network is operational. Configuring High Throughput will result in loss of connectivity of clients.

Apply

11ax

11be

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.

Enable 11be

Select All

SS/MCS	SS/MCS	SS/MCS	SS/MCS
☒ 1/9	☒ 1/11	☒ 1/13	☒ 1/14
☒ 1/15	☒ 2/9	☒ 2/11	☒ 2/13
☒ 3/9	☒ 3/11	☒ 3/13	☒ 4/9
☒ 4/11	☒ 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 / Wi-Fi 7 must be globally enabled

Meraki

Wireless > Radio Settings > RF profiles

The screenshot shows the Meraki configuration interface for RF profiles. At the top, there are three tabs: 'All SSIDs', 'Per SSID Group BETA', and 'Off'. The 'Per SSID Group BETA' tab is selected and highlighted with a blue box and a circled '1'. Below the tabs, there is a table with columns for 'SSID Group' and '802.11be'. The '802.11be' column has a toggle switch that is currently turned on, highlighted with a blue box and a circled '2'. The 'SSID Group' column lists several groups: 'SSID #1 - 4', 'SSID #5 - 8', 'SSID #9 - 12', and 'SSID #13 - 15'. The 'SSID #1 - 4' group is expanded, showing a list of SSIDs: '#1 Lab Wi-Fi', '#2 Unconfigured SSID 2 (Disabled)', '#3 Unconfigured SSID 3 (Disabled)', and '#4 Unconfigured SSID 4 (Disabled)'.

SSID Group ⓘ	802.11be
▼ SSID #1 - 4	☒
> SSID #5 - 8	☐
> SSID #9 - 12	☐
> SSID #13 - 15	☐

- 11be support is disabled by default
- With MR 31.1.x all SSIDs must be 11be compliant
- As of MR 32.1.4 we can enable Wi-Fi 7 per SSID groups

Wi-Fi 6E & 7 security for Enterprise (802.1X)

Main examples/combinations

WPA type	AKM[s]	Fast transition	PMF	AES (CCMP128)	GCMP256**	Compatibility	Notes
WPA3 Enterp.	802.1X-SHA256	Disabled	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	GCMP256 added to 17.18.3 Compatibility issues with some Wi-Fi 7 clients
WPA3 Enterp.	FT + 802.1X*	Enabled	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	GCMP256 added to 17.18.3 Compatibility issues with some Wi-Fi 7 clients
WPA3 Enterp.	802.1X-SHA256 FT + 802.1X*	Enabled	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	GCMP256 added to 17.18.3 Compatibility issues with some Wi-Fi 7 clients
WPA3 Enterp.	SUITEB192-1X	Disabled	✓	✗	✓	Wi-Fi 6E Wi-Fi 7	
WPA2 Enterp. WPA3 Enterp.	802.1X 802.1X-SHA256 FT + 802.1X	Enabled	Optional	✓	✓	Legacy Wi-Fi 6E^ Wi-Fi 7^	GCMP256 added to 17.18.x Compatibility issues with some Wi-Fi 7 clients Allows legacy clients on 2.4/5 GHz ^^ In 6GHz PMF is broadcasted as mandatory Max. Compatibility Focus
WPA2 Enterp.	802.1X	Any	Any	✓	✗	Legacy (No 6E & 7)	No 802.11be, no 6GHz

* still uses SHA256, even if not explicit in its naming
** GCMP256 not supported in C9105, C9115 and C9120

AKM = Authentication and Key Management
SHA256 = Secure Hash Algorithm (SHA) 256 bit
PMF = Protected Management Frame

Enterprise (802.1X) for 6 GHz, Wi-Fi 7 & compatibility

Catalyst

Configuration > Tags & Profiles > WLANs

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

☐ WPA + WPA2 ☒ WPA2 + WPA3 ☐ WPA3 ☐ Static WEP ☐ None

MAC Filtering ☐

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

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS ☐

Reassociation Timeout*

Auth Key Mgmt (AKM)

802.1X	☒	FT + 802.1X	☒
802.1X-SHA256	☒	CKKM ⚠	☐
PSK	☐	FT + PSK	☐
PSK-SHA256	☐	SAE	☐
FT + SAE	☐	SAE-EXT-KEY	☐
FT + SAE-EXT-KEY	☐		

WPA2 + WPA3 settings:

- Beacon Protection
- AES(CCMP128)

PMF: Optional (automatically enforced for 6 GHz)

Fast Transition: Enabled

AKMs:

- 802.1X
- FT + 802.1X
- 802.1X-SHA256

- ✓ GCMP supported on Catalyst in 17.18.3
- ✓ Some Wi-Fi 7 endpoints today enforce GCMP256 when associating to a Wi-Fi 7 enabled SSID

802.11be Profiles allow disabling Wi-Fi 7 per-WLAN

Catalyst

Configuration > Tags & Profiles > 802.11be

The screenshot displays the Cisco Catalyst configuration interface. On the left is a dark sidebar with navigation icons for Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area shows the 'Configuration > Tags & Profiles > 802.11be' breadcrumb. A modal window titled 'Add 802.11be Profile' is open, showing fields for Profile Name* (11be_PRFL_Wi-Fi_7_OFF), Description, OFDMA Multi-RU (DISABLED), and an MLO Group section with four radio buttons (Primary 2.4GHz, Primary 5GHz, Secondary 5GHz, Primary 6GHz) all set to DISABLED. A blue box highlights these radio buttons. To the right, another modal window titled 'Edit WLAN' is open, showing settings for Dual Neighbor List, BSS Max Idle Service, BSS Max Idle Protected, and Directed Multicast Service. Below these is a section for '11be' and '11ax' profiles. A dropdown menu for '802.11be Profile' is open, showing a list of values with '11be_PRFL_Wi-Fi_7_OFF' selected. A blue arrow points from the highlighted radio buttons in the 'Add 802.11be Profile' dialog to the selected profile in the 'Edit WLAN' dialog.

802.11be Profile to be applied under the Advanced settings of a WLAN Profile (example to disable Wi-Fi 7 on all radios/bands)

Enterprise (802.1X) for 6 GHz, Wi-Fi 7 & compatibility

Meraki

Security WPA3 Transition Mode Enterprise with 1 RADIUS server and 1 accounting 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) ⓘ Enabled Disabled

WPA encryption ⓘ WPA3 Transition Mode ▼

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

Mandatory DHCP Enabled Disabled

Local Auth Fallback ⓘ Enabled Disabled

Advanced WPA3 settings (Cipher and AKM suite settings) ▼

WPA3 Cipher Suite ☒ GCMP 256

Security settings:

- Enterprise
- WPA3 Transition Mode
- 802.11w Enabled (automatically enforced for 6 GHz)
- WPA3 Cipher Suite GCMP 256

Wi-Fi 6E & 7 security for Personal (passphrase)

Main examples/combinations

WPA type	AKM[s]*	Fast transition	PMF	AES (CCMP128)	GCMP256**	Compatibility	Notes
WPA3 Pers.	SAE FT-SAE SAE-EXT-KEY FT + SAE-EXT-KEY	Enabled	✓	✓	✓	No legacy Wi-Fi 6E Wi-Fi 7	AES (CCMP128) allowed in IOS-XE 17.15 GCMP256 mandatory in IOS-XE 17.18
WPA2 Pers. WPA3 Pers.	PSK SAE FT-SAE SAE-EXT-KEY FT-SAE-EXT-KEY	Enabled	Optional	✓	✓	Legacy Wi-Fi 6E Wi-Fi 7	Transition may need H2E/HPN AES (CCMP128) allowed in IOS-XE 17.15 GCMP256 mandatory in IOS-XE 17.18 Max. Compatibility Focus
WPA2 Pers. WPA3 Pers.	PSK SAE FT-SAE	Enabled	Optional	✓	✗	Legacy Wi-Fi 6E No Wi-Fi 7	No 802.11be, but 6 GHz supported
WPA2 Pers.	PSK	Disabled	✗	✓	✗	Legacy (No 6E & 7)	No 802.11be, no 6 GHz

* SAE hash to element (H2E) is required for Wi-Fi 6E & 7, FT strongly recommended when using any SAE

** GCMP256 not supported in C9105, C9115 and C9120

AKM = Authentication and Key Management
SAE = Simultaneous Authentication of Equals
PMF = Protected Management Frame
H2E = Hash to Element
HPN = Hunting and Pecking

GCMP256 and roaming

- Changing ciphers (GCMP256 to AES or vice versa) when moving between APs requires a brand-new association: not supported for roaming
- A (Wi-Fi 7) client initially associated to an AP with GCMP256 and moving to an AP supporting AES (CCMP128) only will have to associate from scratch



GCMP256 and roaming

- Changing ciphers (GCMP256 to AES or vice versa) when moving between APs requires a brand-new association: not supported for roaming
- A (Wi-Fi 7) client initially associated to an AP with GCMP256 and moving to an AP supporting AES (CCMP128) only will have to associate from scratch



- Today this corner case applies to SAE/Personal/passphrase and OWE/guest SSIDs
- Some former AP series (MR Wi-Fi 5 APs, 1800, 9105, 9115, 9120) do not support GCMP256

Personal (passphrase) for 6 GHz, Wi-Fi 7 & compatibility

Catalyst

The screenshot shows the 'Security' tab in the Catalyst configuration interface. The 'WPA2 + WPA3' radio button is selected. Under 'WPA Parameters', 'WPA2 Policy', 'WPA3 Policy', and 'Beacon Protection' are checked. In the 'WPA2/WPA3 Encryption' section, 'AES(CCMP128)' and 'GCMP256' are both checked. The 'Protected Management Frame' (PMF) is set to 'Optional'. In the 'Auth Key Mgmt (AKM)' section, 'SAE', 'SAE-EXT-KEY', 'FT + SAE', and 'FT + SAE-EXT-KEY' are all checked. Other settings like 'Fast Transition' (Enabled), 'Reassociation Timeout' (20), and 'PSK Format' (ASCII) are also visible.

WPA2 + WPA3 settings:

- Beacon Protection
- AES(CCMP128)
- GCMP256

PMF: Optional (automatically enforced for 6 GHz)

Fast Transition: Enabled

AKMs:

- PSK
- SAE, FT + SAE
- SAE-EXT-KEY, FT + SAE-EXT-KEY

- ✓ This configuration technically supports any 6 GHz and Wi-Fi 7 endpoint, as well as more legacy ones requiring basic WPA2 PSK
- ✓ It is as secure as its weakest security level
- ✓ Are legacy endpoints (e.g. IoT) ready for all the latest 6 GHz / Wi-Fi 7 information elements?

Personal (passphrase) for 6 GHz, Wi-Fi 7 & compatibility

Meraki

The screenshot shows the 'Security' configuration page for a Meraki device, specifically for WPA3 Transition Mode. The page is titled 'Security' and 'WPA3 Transition Mode configured'. The 'Password' option is selected, indicating that users must enter a key to associate. Below this, there are options for 'MAC-based access control (no encryption)', 'Enterprise with Meraki Cloud Authentication', 'Identity PSK with RADIUS', and 'Identity PSK without RADIUS'. The 'WPA encryption' section shows '802.11w' and 'WPA3 Transition Mode' with 'Enabled (allow unsupported clients)' selected. The 'Mandatory DHCP' section shows 'Enabled' and 'Disabled' buttons. The 'Advanced WPA3 settings' section shows 'WPA3 Cipher Suite' set to 'GCMP-256' and 'WPA3 AKM Suite' set to 'SAE' and 'SAE-EXT'.

Security WPA3 Transition Mode configured

☒ Password
Users must enter this key to associate: [password field]

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

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

☐ Identity PSK with RADIUS
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 WPA3 Transition Mode
☒ 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

Security settings:

- Password
 - WPA3 Transition Mode
 - 802.11w Enabled (automatically enforced for 6 GHz)
 - WPA3 Cipher Suite GCMP 256
 - WPA3 AKM Suite SAE, SAE-EXT
- ✓ This configuration technically supports any 6 GHz and Wi-Fi 7 endpoint, as well as more legacy ones requiring basic WPA2 PSK
- ✓ It is as secure as its weakest security level
- ✓ Are legacy endpoints (e.g. IoT) ready for all the latest 6 GHz / Wi-Fi 7 information elements?

Wi-Fi 6E & 7 security for Personal (passphrase)

Main examples/combinations

WPA type	AKM[s]*	Fast transition	PMF	AES (CCMP128)	GCMP256**	Compatibility	Notes
WPA3 Pers.	SAE FT-SAE SAE-EXT-KEY FT + SAE-EXT-KEY	Enabled	✓	✓	✓	No legacy Wi-Fi 6E Wi-Fi 7	AES (CCMP128) allowed in IOS-XE 17.15 GCMP256 mandatory in IOS-XE 17.18
WPA2 Pers. WPA3 Pers.	PSK SAE FT-SAE SAE-EXT-KEY FT-SAE-EXT-KEY	Enabled	Optional	✓	✓	Legacy Wi-Fi 6E Wi-Fi 7	Transition may need H2E/HPN AES (CCMP128) allowed in IOS-XE 17.15 GCMP256 mandatory in IOS-XE 17.18 Max. Compatibility Focus
WPA2 Pers. WPA3 Pers.	PSK SAE FT-SAE	Enabled	Optional	✓	✗	Legacy Wi-Fi 6E No Wi-Fi 7	No 802.11be, but 6 GHz supported
WPA2 Pers.	PSK	Disabled	✗	✓	✗	Legacy (No 6E & 7)	No 802.11be, no 6 GHz

* SAE hash to element (H2E) is required for Wi-Fi 6E & 7, FT strongly recommended when using any SAE

** GCMP256 not supported in C9105, C9115 and C9120

AKM = Authentication and Key Management
SAE = Simultaneous Authentication of Equals
PMF = Protected Management Frame
H2E = Hash to Element
HPN = Hunting and Pecking

Do our IoT endpoints really need Wi-Fi 7 or do they really support 6 GHz?
Would we be better off with a dedicated WPA2 SSID for legacy and a dedicated WPA3 SSID for all the new stuff?

WPA3 Personal for 6 GHz & Wi-Fi 7



For your
reference

Catalyst

The screenshot shows the 'Security' tab in the Catalyst configuration interface. The 'WPA3' radio button is selected and highlighted with a blue box. Below it, the 'WPA Parameters' section has 'WPA2 Policy' and 'Beacon Protection' checked, also highlighted with a blue box. The 'WPA2/WPA3 Encryption' section has 'AES(CCMP128)' and 'GCMP256' checked, highlighted with a blue box. The 'Protected Management Frame' section has 'PMF' set to 'Required', highlighted with a blue box. The 'Fast Transition' section has 'Status' set to 'Enabled', highlighted with a blue box. The 'Auth Key Mgmt (AKM)' section has 'SAE' and 'SAE-EXT-KEY' checked, highlighted with a blue box. Other settings include 'MAC Filtering' (unchecked), 'Lobby Admin Access' (unchecked), 'Transition Disable' (unchecked), 'Over the DS' (unchecked), 'Reassociation Timeout' (20), 'FT + 802.1X' (unchecked), '802.1X-SHA256' (unchecked), 'SUITES192-1X' (unchecked), 'OWE' (unchecked), 'Anti Clogging Threshold' (1500), 'Max Retries' (5), 'Retransmit Timeout' (400), 'PSK Format' (ASCII), 'PSK Type' (Unencrypted), 'Pre-Shared Key' (*****), and 'SAE Password Element' (Both H2E and...).

WPA3 settings:

- Beacon Protection
- AES(CCMP128)
- GCMP256

PMF: Required

Fast Transition: Enabled

AKMs:

- SAE, FT + SAE
- SAE-EXT-KEY, FT + SAE-EXT-KEY

This configuration supports any 6 GHz and Wi-Fi 7 endpoint, as well as more legacy ones supporting WPA3 too

WPA3 Personal for 6 GHz & Wi-Fi 7

Meraki



For your
reference

Security WPA3 SAE configured

☒ Password
User's must enter this key to associate:

.....

☐ MAC-based access control (no encryption)
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 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

Security settings:

- Password
- WPA3 only
- 802.11w Required
- WPA3 Cipher Suite GCMP 256
- WPA3 AKM Suite SAE, SAE-EXT

This configuration supports any 6 GHz and Wi-Fi 7 endpoint, as well as more legacy ones supporting WPA3 too

Wi-Fi 6E & 7 security for Enhanced Open (OWE)

Main examples/combinations

WPA type	AKM[s]	Fast transition	PMF	AES (CCMP128)	GCMP256*	Compatibility	Notes
Enhanced Open	OWE	Disabled	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	AES (CCMP128) allowed in 17.15 GCMP256 mandatory in 17.18
Enhanced Open	OWE	Disabled	✓	✓	✗	Wi-Fi 6E No Wi-Fi 7	No 802.11be, but 6GHz supported
Enhanced Open	OWE-Transition	Disabled	N/A	✓	✗	Legacy No Wi-Fi 6E No Wi-Fi 7	No 802.11be, no 6GHz supported To be coupled with an Open SSID**

* GCMP256 not supported in C9105, C9115 and C9120

** see <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217737-configure-enhanced-open-ssid-with-transi.html>

AKM = Authentication and Key Management
OWE = Opportunistic Wireless Encryption
PMF = Protected Management Frame

If we are introducing an OWE SSID next to a former Open SSID, for the same guest use case, we should better keep them segmented on different networks/VLANs/VRFs

Enhanced Open (OWE) for 6 GHz and Wi-Fi 7

Catalyst

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

MAC Filtering ☐ For CWA 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

Association Comeback Timer*

SA Query Time*

Fast Transition

Status:

Over the DS ☐

Reassociation Timeout *

Auth Key Mgmt (AKM)

FT + 802.1X ☐ 802.1X-SHA256 ☐
SUITEB192-1X ☐ **OWE ☒**
SAE ☐ FT + SAE ☐
SAE-EXT-KEY ☐ FT + SAE-EXT-KEY ☐

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

Enhanced Open (OWE) for 6 GHz and Wi-Fi 7

Meraki

Security Opportunistic Wireless Encryption

☒ 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)
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

Note: OWE still supports web portal redirection configuration, under the “Splash page” options

Security settings:

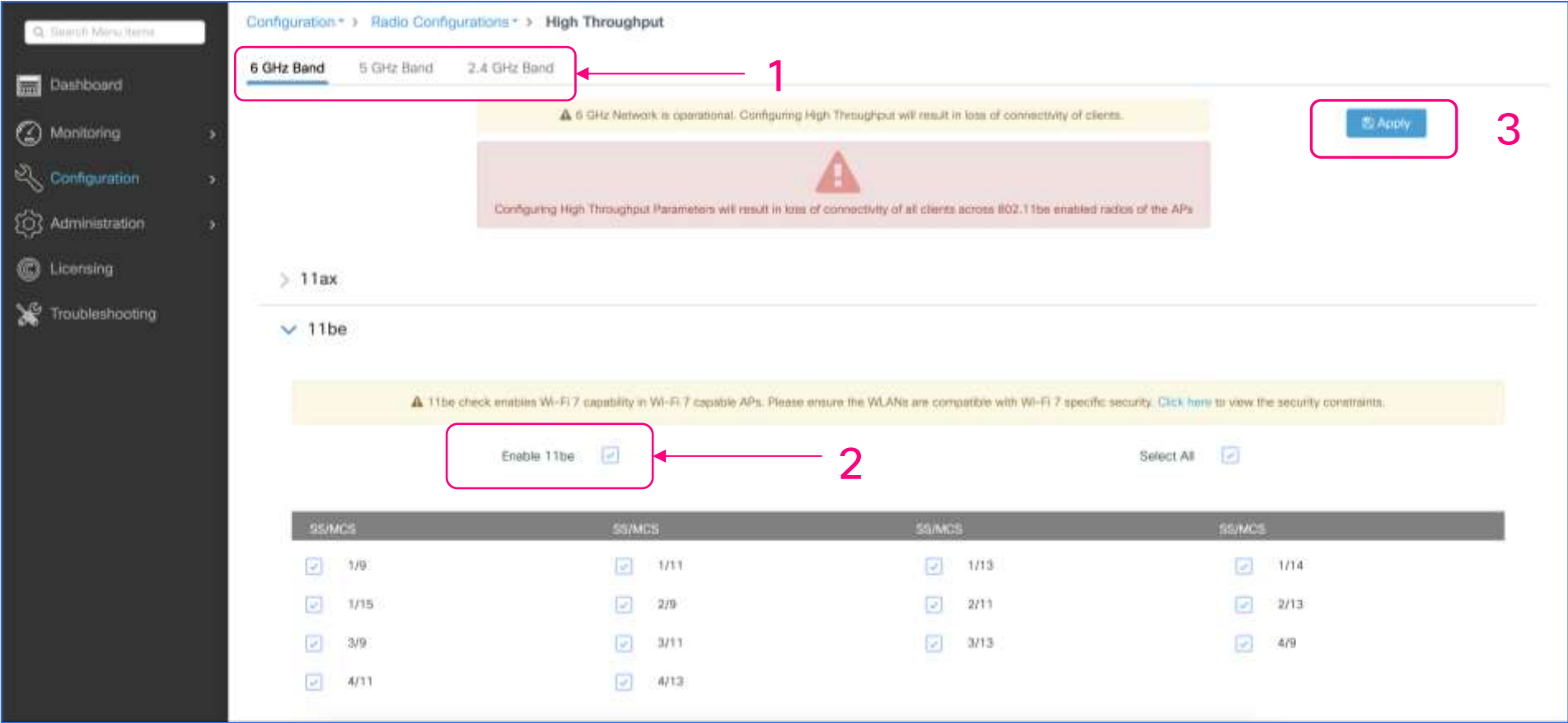
- Opportunistic Wireless Encryption (OWE)
- WPA3 only
- 802.11w Required
- WPA3 Cipher Suite GCMP 256

Configuring Wi-Fi 7

Wi-Fi 7/802.11be – Enable Globally in Catalyst

Catalyst

11be disabled by default



CLI

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

Wi-Fi 7/802.11be profile configuration

Catalyst
Finer control of disabling 11be per WLAN and band.

Configuration > Tags & Profiles > 802.11be

Add 802.11be Profile

Profile Name* 11be Profile

Description Non-default Profile

OFDMA Multi-RU **ENABLED**

MLO Group

Primary 2.4GHz **DISABLED**

Primary 5GHz **ENABLED**

Secondary 5GHz **ENABLED**

Primary 6GHz **ENABLED**

Cancel Apply to Device

Edit WLAN

Per AP Per WLAN 0

Per AP Radio Per WLAN 200

11v BSS Transition Support

BSS Transition ☒

Dual Neighbor List ☐

BSS Max Idle Service ☒

BSS Max Idle Protected ☐

Directed Multicast Service ☒

Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only

11be

802.11be Profile 11be Profile

Apply under Advanced Settings of WLAN →
Above example disables 2.4 GHz band for Wi-Fi 7 MLO

Wi-Fi 7/802.11be – Enable per SSID Group

Meraki

Wireless > Radio Settings > RF profiles

802.11be

All SSIDs Per SSID Group BETA Off

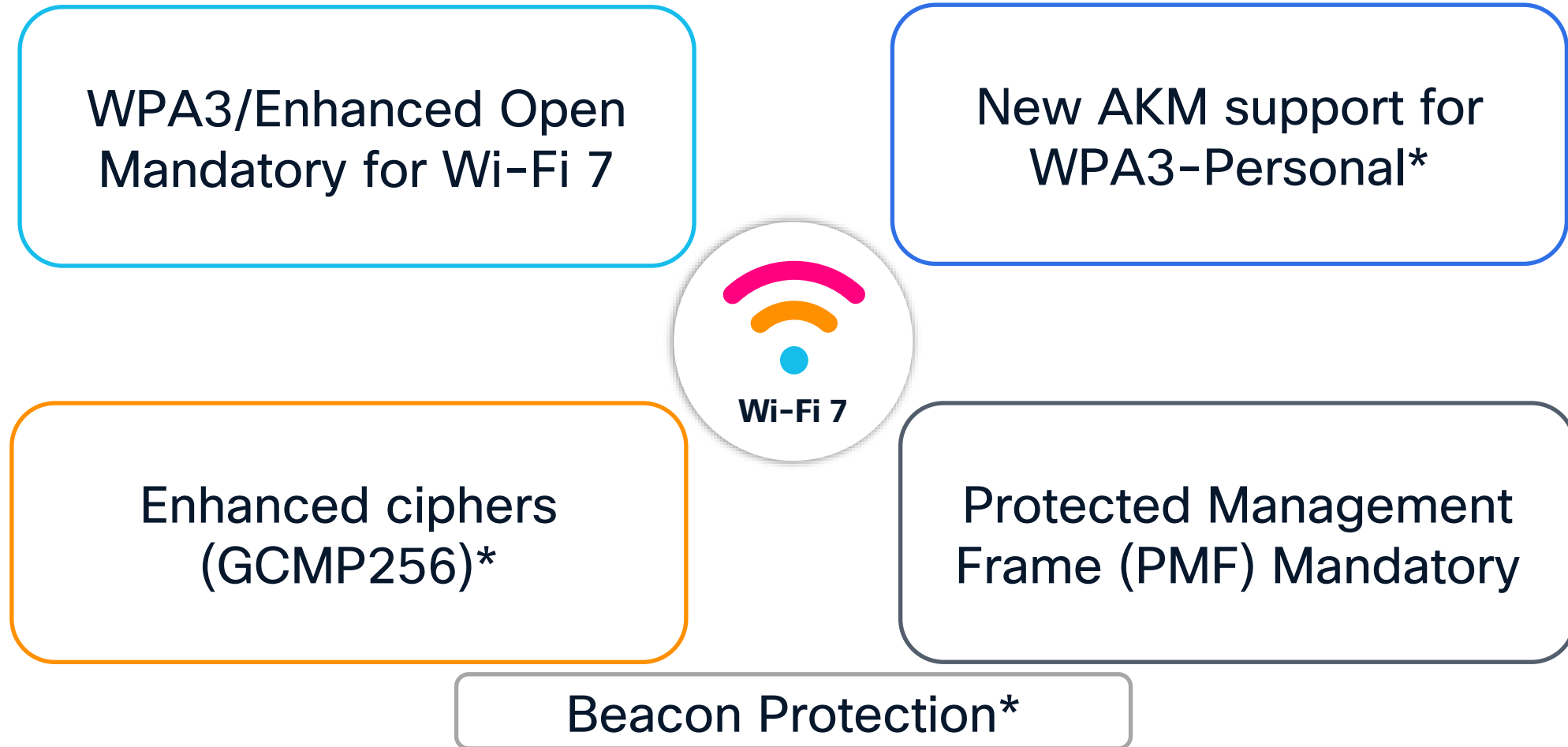
SSID Group ⓘ	802.11be
▼ SSID #1 - 4	☒
#1 wifi7-test #2 wifi6Corp (Disabled) #3 testwpa3 #4 Unconfigured SSID 4 (Disabled)	
> SSID #5 - 8	☒
> SSID #9 - 12	☐
> SSID #13 - 15	☐

Please check [documentation](#) for more details.

- 11be support disabled by default
- Allowed to enable, if security settings of all WLANs in a group comply with Wi-Fi 7 (1-4, 5-8, 9-12, 13-16)

WLAN Security

Wi-Fi 7 Security



** New enhancements in Wi-Fi 7, when compared to Wi-Fi 6E*

Wi-Fi 7 Security

Wi-Fi 7 brings new AKM support for WPA3-SAE and new increased ciphers for ALL WPA3 /OWE mandatory for EHT (11be MCS rates) & MLO



Reference

Cipher: GCMP 256 – Better Encryption & Speed; AKM: Better security

Legacy (Wi-Fi 5)	Wi-Fi 6	Wi-Fi 6E (6 GHz)	Wi-Fi 7
Open	Open (OWE support required)	Enhanced Open (AKM: OWE) (Cipher: CCMP128)	Enhanced Open (AKM: OWE) (Cipher: CCMP128 and GCMP256)
WPA1/WPA2/WPA3 Transition WPA3-Personal, PMF Optional	WPA2/WPA3 Transition/ WPA3-Personal, PMF Optional (WPA 2 – AKM – PSK, FT+PSK, PSK (SHA-256)) (WPA 3 – AKM – SAE, FT+SAE) (Cipher: CCMP 128 or AES)	WPA3-Personal, PMF Mandatory (AKM: SAE, FT+SAE) (Cipher: CCMP128 or AES)	WPA3-Personal, PMF Mandatory (AKM: SAE-EXT-KEY, FT-SAE-EXT-KEY) (Cipher: CCMP128 and GCMP256)
WPA1/WPA2/WPA3 Transition/ WPA3-dot1x (Enterprise), PMF Optional	WPA2/WPA3 Transition/ WPA3-dot1x (Enterprise), PMF Optional (AKM 802.1x, FT+802.1x & 802.1x-SHA256, 802.1x-SuiteB) (Cipher: AES, CCMP 128, GCMP128 GCMP256)	WPA3 Enterprise, PMF Mandatory (AKM: FT+802.1x, 802.1x-SHA256, 802.1x-SuiteB) (Cipher: CCMP128, GCMP 128 & GCMP 256)	WPA3 Enterprise, PMF Mandatory (AKM: FT+802.1x, 802.1x-SHA256, 802.1x-SuiteB) (Cipher: CCMP128, GCMP128 & GCMP 256)

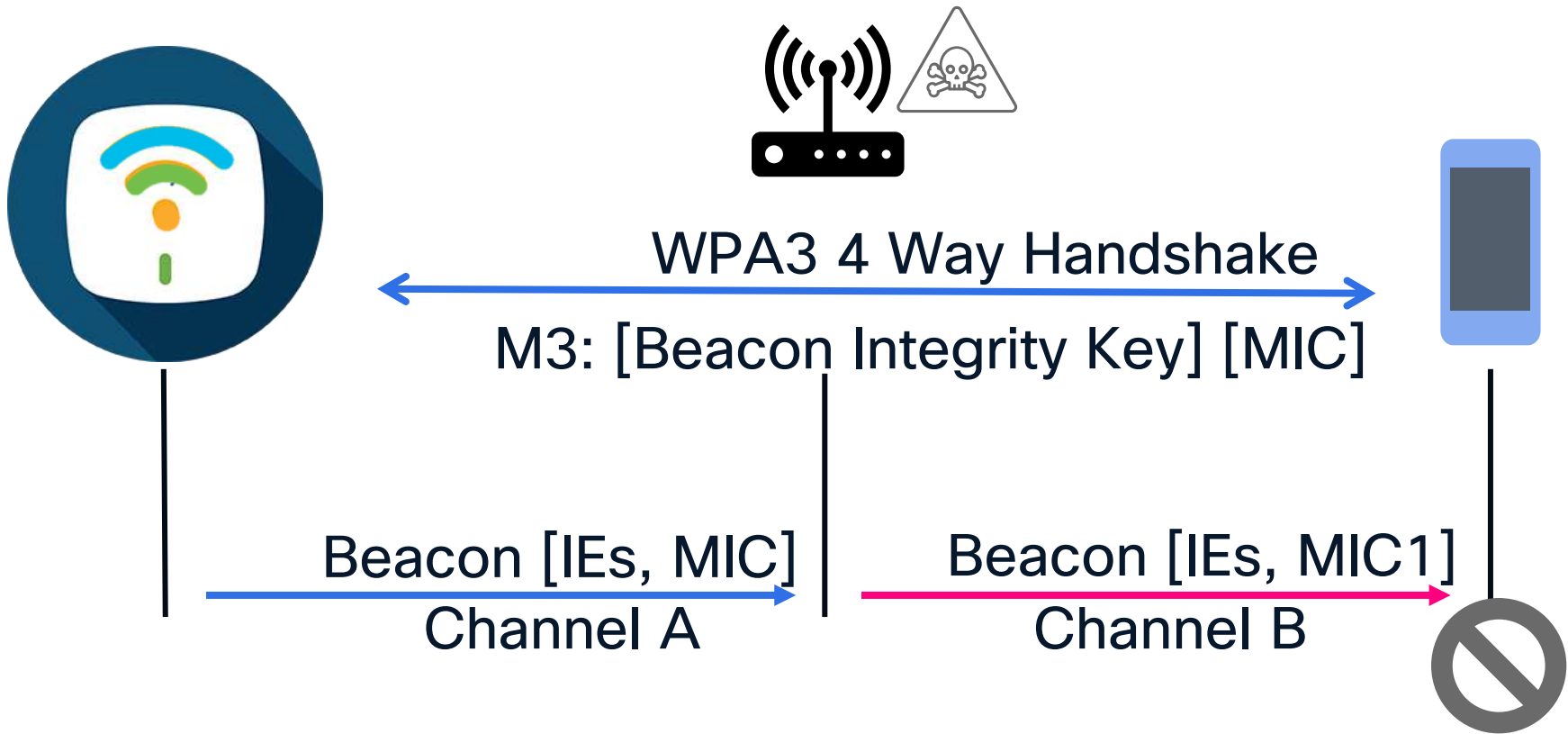
Clients connecting to lower security, can connect to 2.4 & 5 GHz bands of Wi-Fi 7 AP, but restricted to 11ax or earlier. No 11be rates & MLO

Note: All devices since 2018 are required to support WPA3, regardless of generation

BRKEWN-2025

Wi-Fi 7 Beacon Protection

Beacons protected with an Integrity Check



Prevents beacon forging by attacker

Wi-Fi 7 WLAN Design Considerations

What options would you have?

1

"All-In" Option: Reconfigure the existing WLAN to WPA3, one SSID for all radio policies (2.4/5/6 GHz) – **Most unlikely**

2

"Multiple SSIDs" Option: Redesign your SSIDs, adding specific SSID/WLAN with specific security settings – **Most flexible**

3

"One SSID" Option: Use Transition Modes to support multiple security – **Most typical**

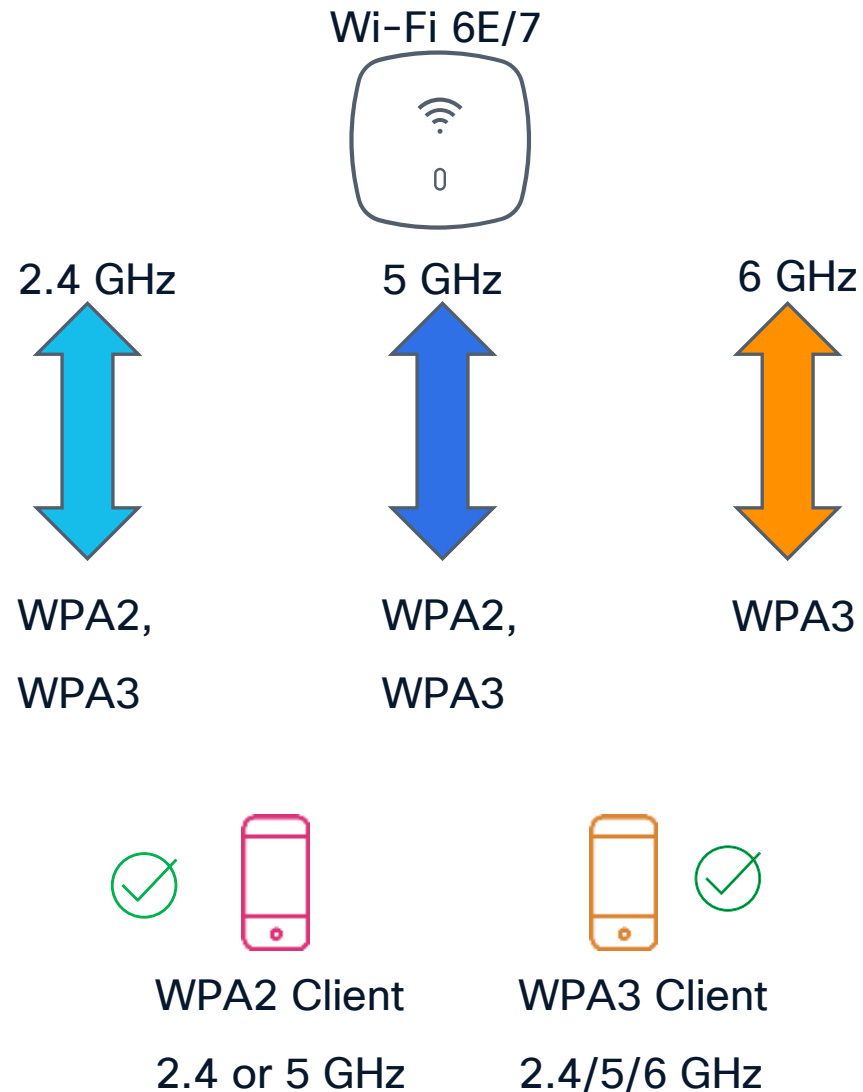
Wi-Fi 7 APs can broadcast SSIDs with lower security; No 11be rates & MLO

Option 3 – One SSID

What is WPA3 Transition Mode ?

Single SSID that supports WPA2+WPA3

- Multiple AKMs
- Multiple Ciphers
- PMF allowed
- Broadcast WPA2+WPA3 in 2.4 and 5 GHz
- Broadcast WPA3 only in 2.4 and 5 GHz



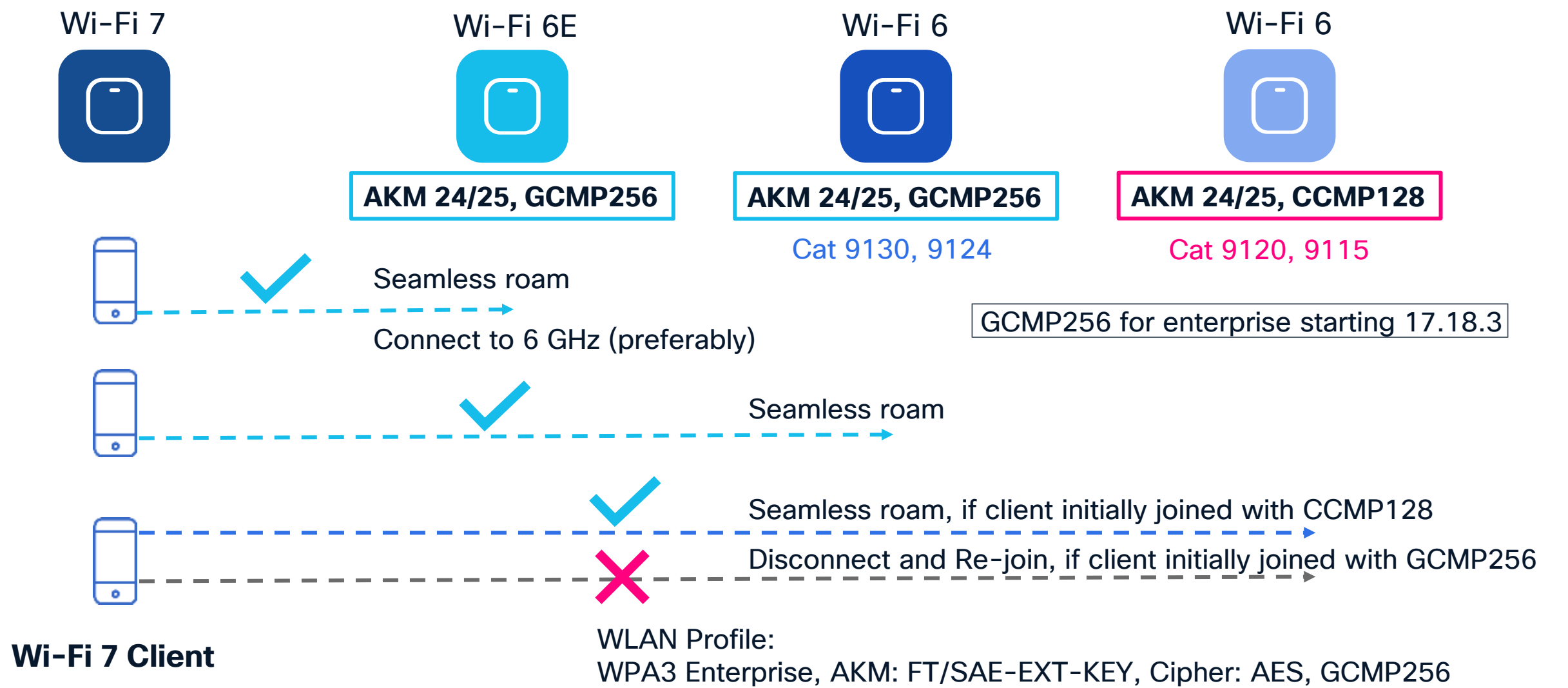
Accommodates Wireless Clients with different security capabilities and standards

What about Roaming ?

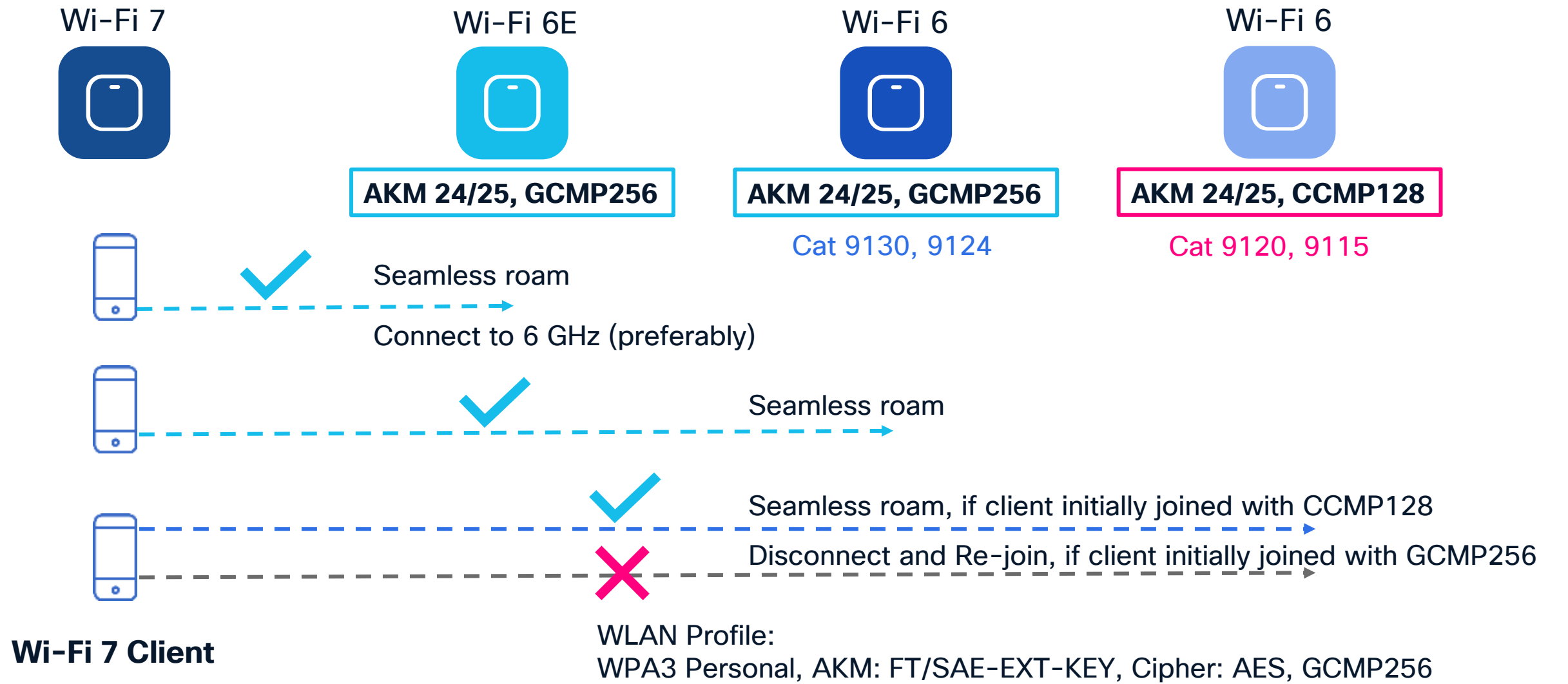


- Seamless roam is possible, as long as there is match in AKM and Ciphers.
- Change in ciphers or AKM when moving between APs, require a brand-new association.
- New AKMs backported to older generation APs (Wi-Fi 6E and Wi-Fi 6)
- Some older Wi-Fi 6 APs like 9120 and 9115 do not support GCMP256

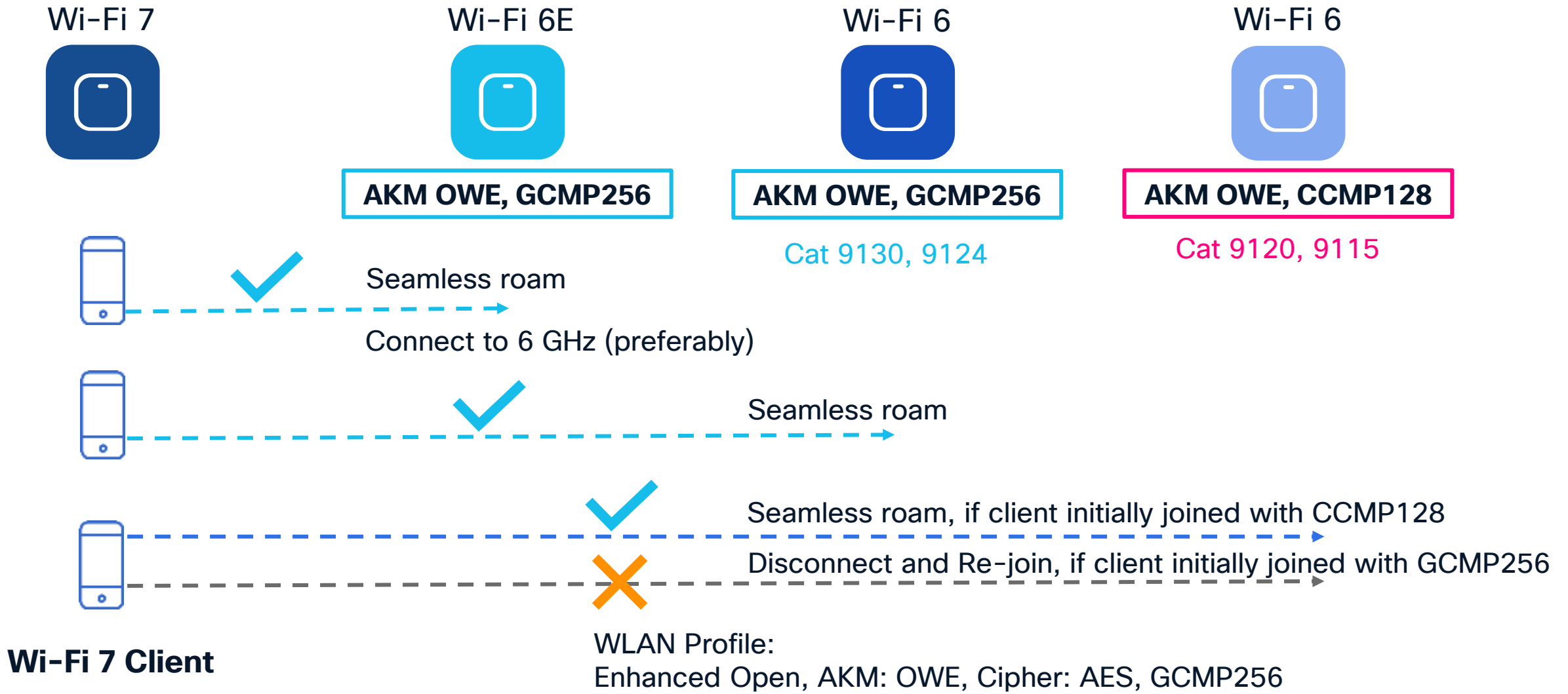
Wi-Fi 7 Client Roam Behavior - Enterprise



Wi-Fi 7 Client Roam Behavior - Personal



Wi-Fi 7 Client Roam Behavior - OWE



Migration

Wi-Fi 7 Software Support Matrix

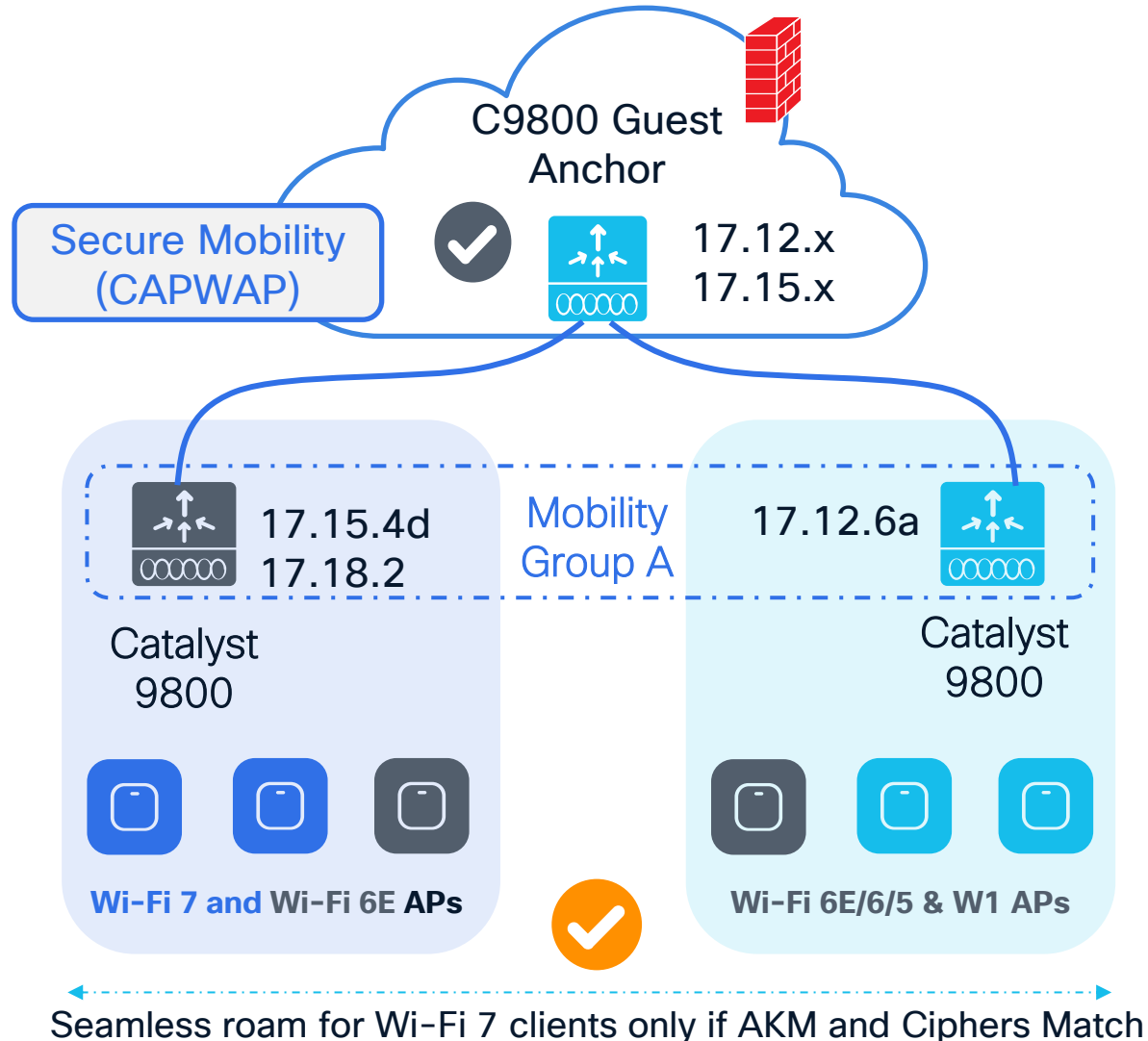


Reference

IOS-XE 17.18.1 or later Catalyst Center 2.3.7.10+ / 3.1.5+	 CW9179F	MR 31.1.7 or later
IOS-XE 17.15.2 or later Catalyst Center 2.3.7.6 (for configuration) Catalyst Center 2.3.7.9 (for maps & assurance)	 CW9178I CW9176I & D1	MR 31.1.5.1 or later
IOS-XE 17.18.2 or later Catalyst Center 2.3.7.11 / 3.2.3	 CW9174I & E	MR 32.1.5 or later
IOS-XE 17.15.2b or later Catalyst Center 2.3.7.10	 CW9172I	MR 31.1.5.1 or later
IOS-XE 17.17.1 or later Catalyst Center 3.1.3	 CW9172H	MR 31.1.6.1 or later
IOS-XE 17.18.2 or later Catalyst Center 2.3.7.11 / 3.2.3	 CW9171I	MR 32.1.5 or later

How do I start adopting Wi-Fi 7?

Answer: Inter Release Controller Mobility (IRCM)



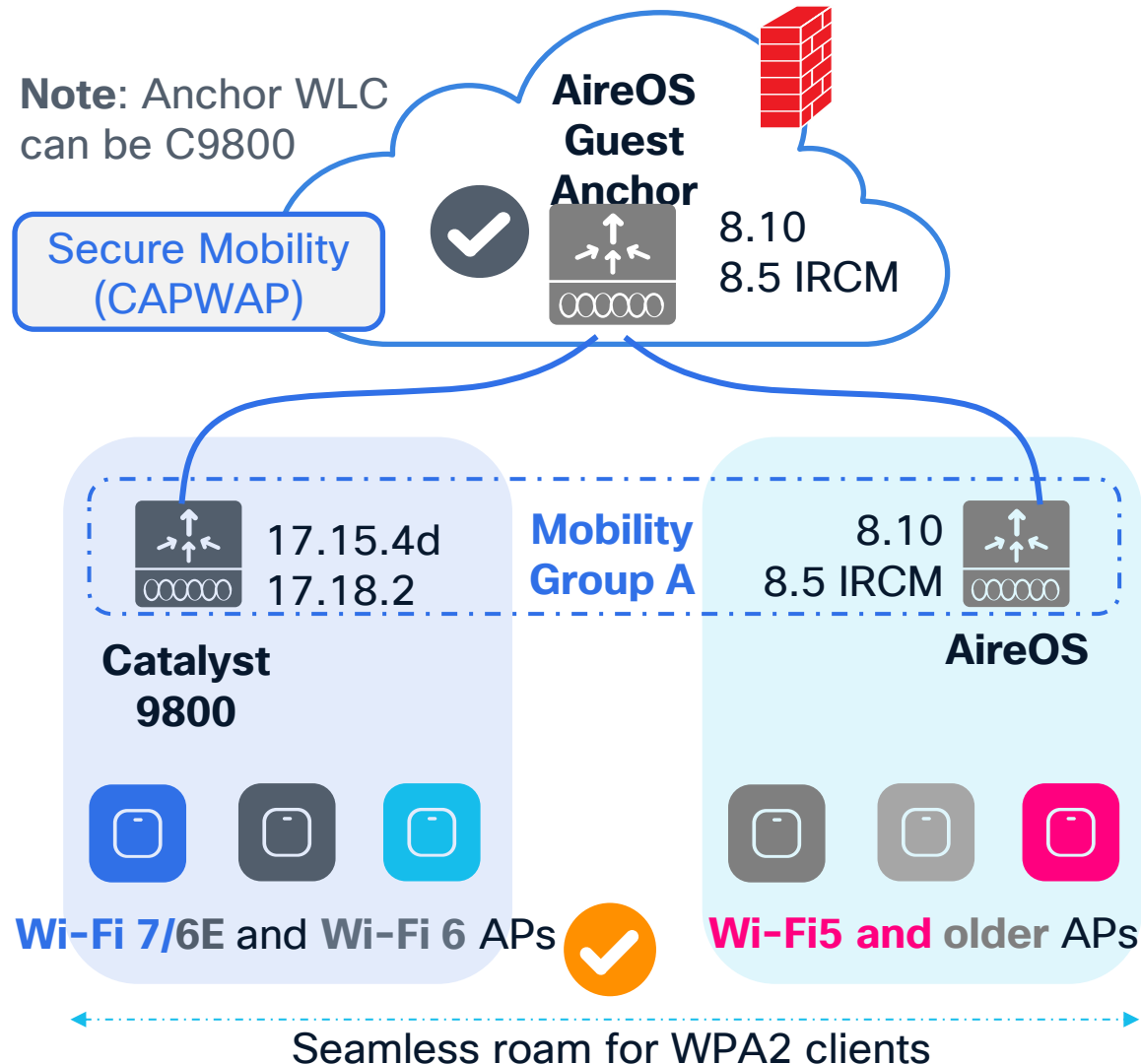
Scenario 1: If you're in IOS-XE 17.12.x code

- If you have already started your C9800 journey... & Wave 1 Aps are still present (1700/2700/3700).
- Introduce new AP hardware on the new supported IOS XE release and support seamless roaming and Guest Anchor with existing C9800 networks
- The release combinations shown have been tested at scale, check IRCM deployment guide*
- Fast & secure roam will only be supported if the WLAN profile is the same on the two WLCs
- **Note:** Anchor can be on AireOS as well (8.10 or 8.5 IRCM latest)

*https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-aires_ircm_dg.html

How do I start adopting Wi-Fi 7?

Answer: Inter Release Controller Mobility (IRCM)



Legacy Controller Supports IRCM

- Introduce new Wi-Fi 7 AP hardware on the new C9800 and support seamless roaming and Guest Anchor with existing networks
- This method allows the smooth coexistence of both controllers, with RF areas migrated as needed, without any overnight switchover.
- Things to consider:
 - If the controller is limited to 8.5 (5508, 8510), we will need a special IRCM version (8.5.182.104), to connect them to IOS-XE
 - Best to split the RF network into different areas, configuring different RF group names between the legacy and IOS-XE controllers.
 - Always configure the primary/secondary controller name in access points. The new controllers will reject unsupported APs, but if any AP could work in both controller types, this will avoid APs joining the wrong one, or flip-flopping between them, until the migration is ready to proceed
- Fast & secure roam will only be supported if the WLAN profile is the same on the two WLCs

*https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-airesos_ircm_dg.html

Summary

Deploying and migrating to Wi-Fi 7

Key considerations & requirements

Power considerations

Recommendation:
802.3bt (Cisco UPOE)
is the suggested
power input for full operation of AP

802.3at (PoE+) and 802.3af (PoE)
are also supported by the
CW9179/CW9178I/CW9176I&D/
CW9174I&E/CW9172I &H/CW9171I

Security requirements

Mandatory:
WPA3 is mandatory for 11be rates
and MLO.

WPA3 was not required for prior
Wi-Fi generations (6 and below);
hence, it must be top of mind.

Multigigabit switching

Recommendation:
Use a Multigigabit switch with 10G
Capability.

Better user experiences with
speeds beyond 1 Gbps. Cat 6A
cabling recommended,

Wireless coverage

Recommendation:
Ensure uniform cell size for 5 and 6
GHz cells. 2.4 & 5 GHz does not
need a new site survey

Review the current RF coverage of
5 GHz network to achieve similar
coverage for 6 GHz network.

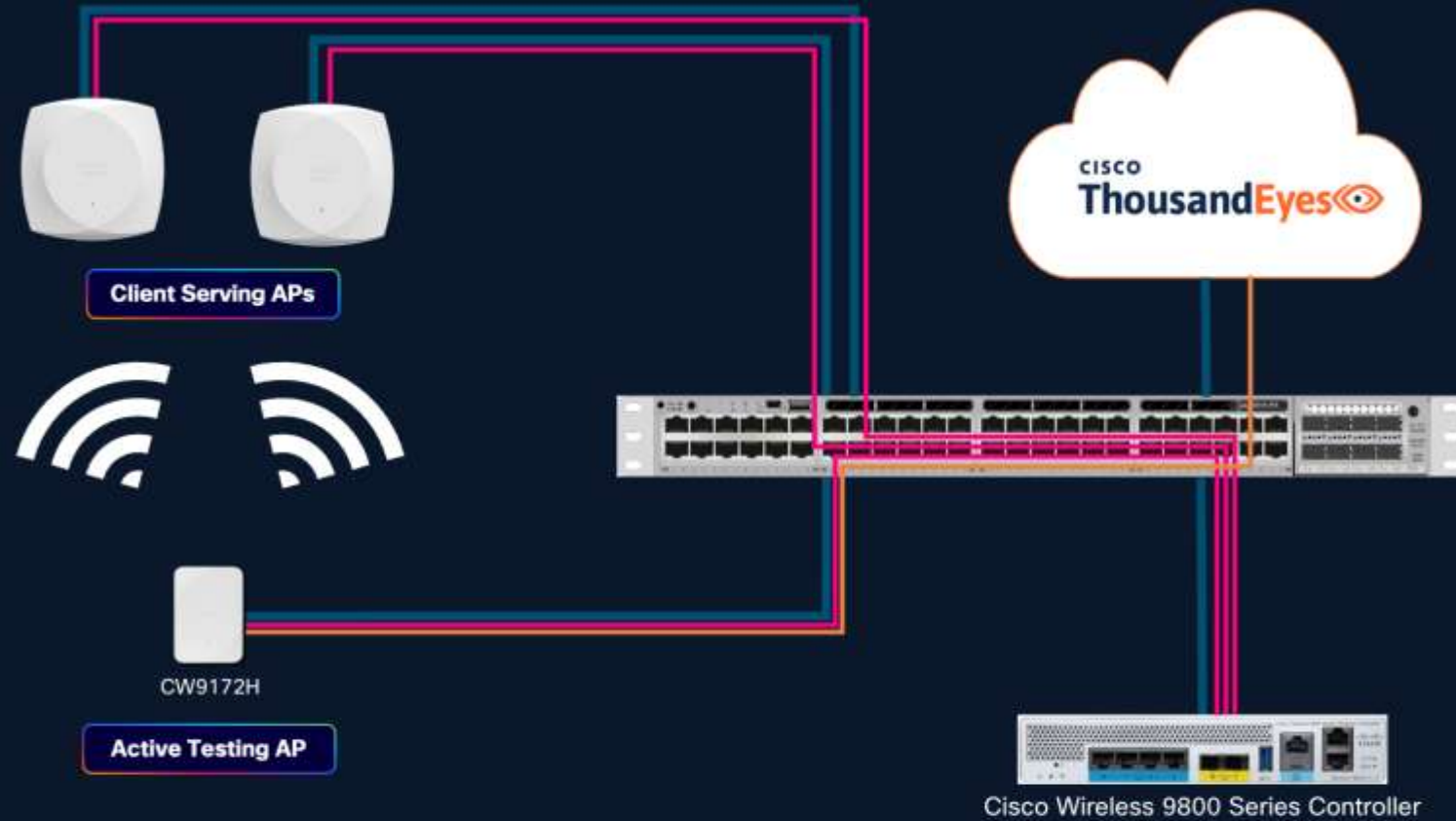
Recommended IOS-XE version for Wi-Fi7 today: 17.18.3

Wireless Active Testing powered by ThousandEyes on-prem

cisco
ThousandEyes 



High-level architecture

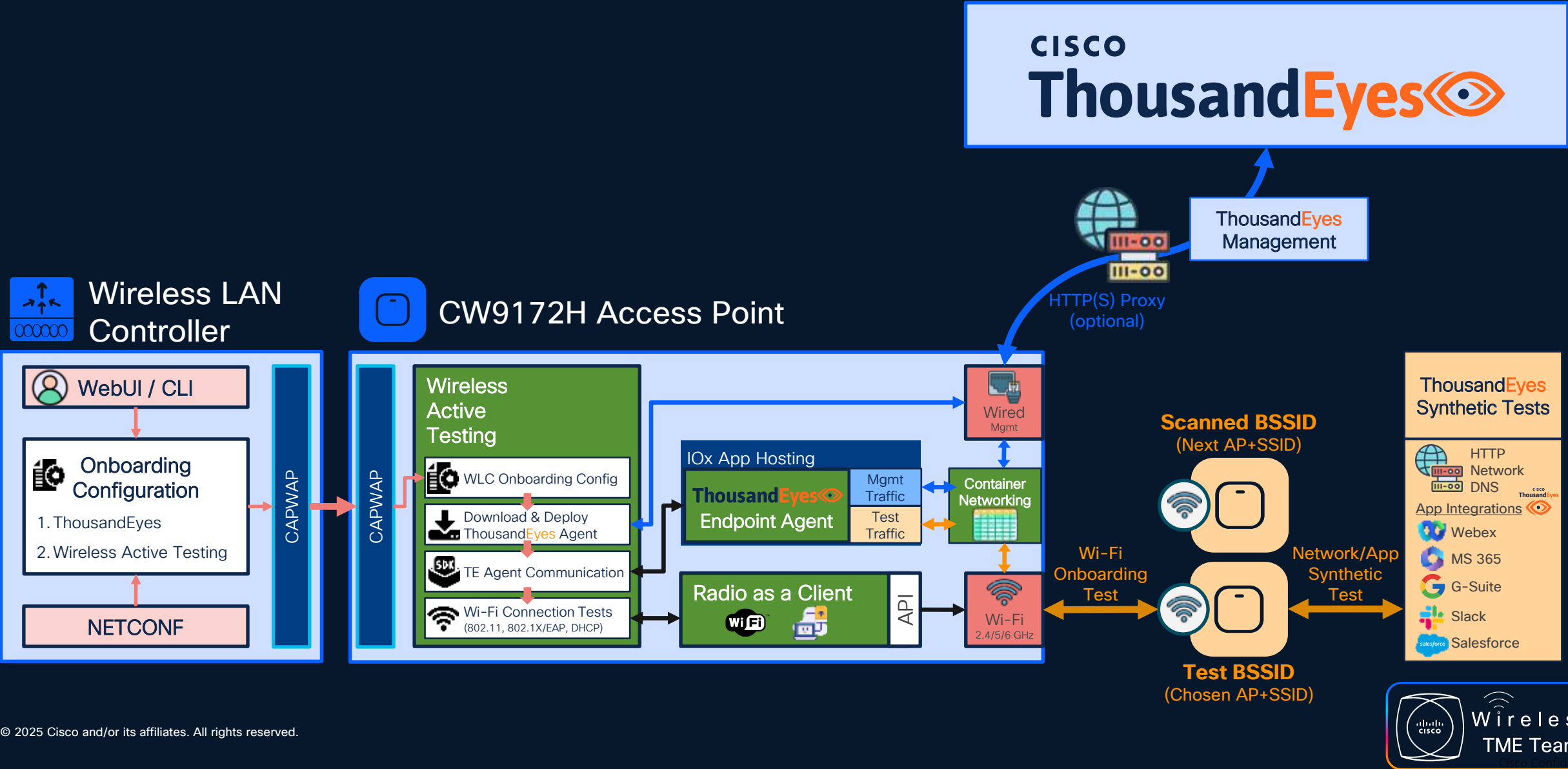


Only APs need connectivity to the ThousandEyes backend

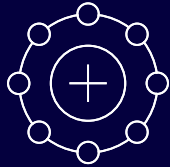


Detailed architecture

ThousandEyes Endpoint Agent
Cloud Platform / Dashboard



Minimum requirements



Hardware & software

CW9172H access point

Any WLC type running 17.18.2+



Licensing

Cisco Wireless Essentials per access point

ThousandEyes End User Monitoring Advantage license per access point

Supported tests

IOS-XE Software

17.18.2 or later

Onboarding Tests

- 2.4 GHz, 5GHz and 6GHz
- WPA2 and WPA3 Open, Personal and Enterprise
- Up to 3 SSIDs and up to 5 BSSIDs on a single band per AP

Network Services Tests

- DHCP failures
- DNS
- EAP failures
- Ping tests
- First Hop Router/Default Gateway
- Intranet Host
- External Host

Application Connectivity

- HTTP & HTTPS
- Collaboration (e.g. Webex, Teams, Zoom)

Network Performance

- Packet Loss
- Jitter
- Latency

Roadmap Items for 26.2.1

- SCEP

Max. number of SSIDs per AP

3

Deployment steps

Deployment overview

1

Upgrade WLC to supported image

2

CW9172H connected to the WLC

3

Configure Active Testing in WLC

4

Configure tests in ThousandEyes Dash

5

Consume results in ThousandEyes Dash

ThousandEyes connection string:

- A connection string can be obtained from the ThousandEyes dashboard

Create specific tags for testing APs and assign them:

- As with normal APs, tags are used to configure testing APs
- Specific tags should be created and assigned to testing APs

Create SSID configs

- Specific SSID, authentication and scheduling

Create Wireless Sensor configuration:

- Map agents (APs) to SSIDs to be tested
- Agent labels can be created to further automate

Create synthetic tests for endpoint agents

- As always in ThousandEyes create endpoint agent tests
- Manually assign tests to agents or leverage agent labels to automate





Cisco Ultra-Reliable Wireless Backhaul FKA Fluid Mesh

Mei 2026

AGVs in manufacturing



Situational awareness in rail



Cranes and straddle carriers in ports



Teleremote applications in mining



Autonomous robots and vehicles are transforming industries and enterprises



Asset management in data centers



Delivery services in hospitality



Shelf scanning to keep stores stocked in retail



Picking, packing, loading, unloading in logistics

Good Wi-Fi Is No Longer Good Enough

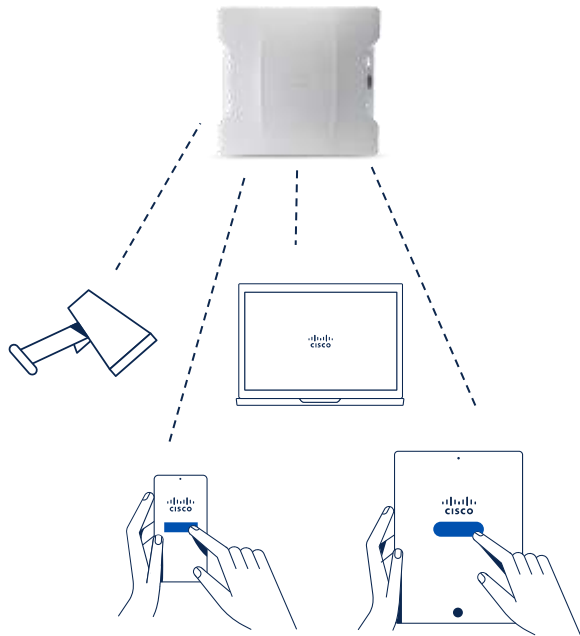
High-stakes applications need more than just fast connections.
They need wireless that stays up *every time*, even in motion.

Traditional Wi-Fi wasn't built for this.
Speed alone won't cut it. You need ultra-reliability beyond what
Wi-Fi delivers

Access and backhaul networks

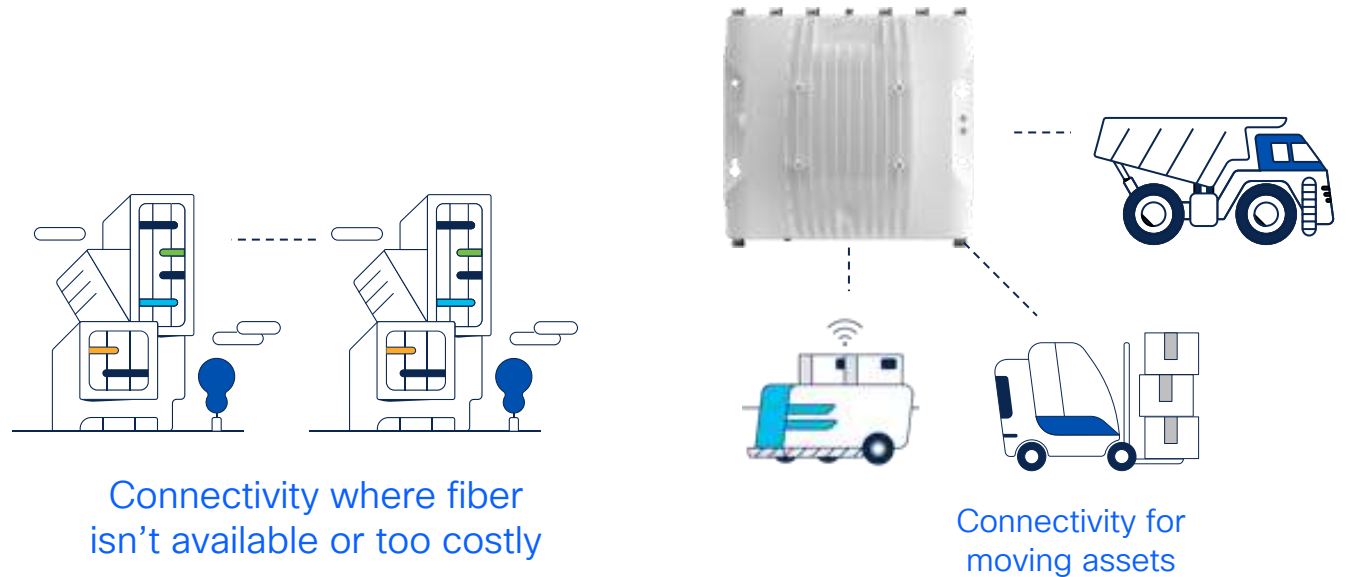
Access networks

Provide connectivity to end-user devices (such as computers, smartphones, and IoT devices)



Backhaul networks

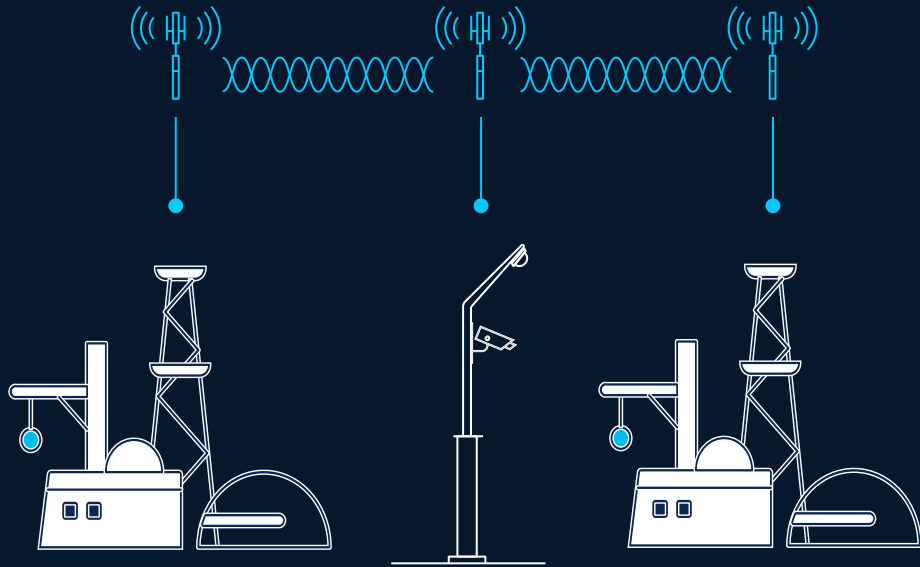
extends the core connectivity to remote assets for which wired connectivity is not possible



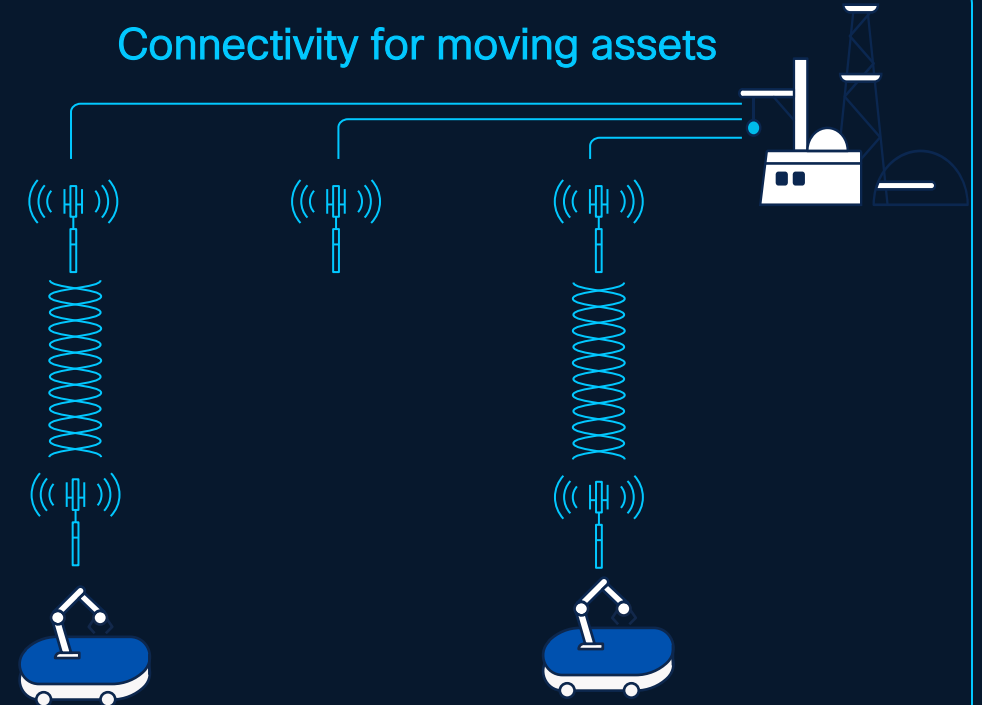
What is Cisco Ultra-Reliable Wireless Backhaul?

Reliable fiber-like wireless connectivity, anywhere

Connectivity where fiber isn't available or is too costly



Connectivity for moving assets



End-to-End Overlay



Make-before-break handoff



Multipath operation



Ultra-fast failover
Carrier-grade availability

The R isn't Silent

URWB $\neq$ UWB

UWB is location awesomeness

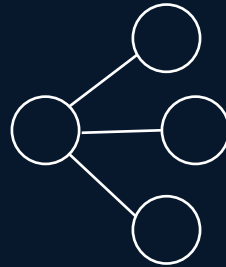
URWB is roaming awesomeness

Supports highly flexible wireless architectures

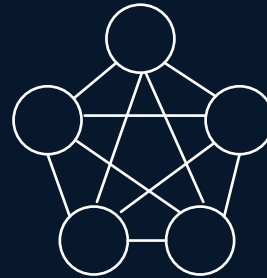
Point to Point



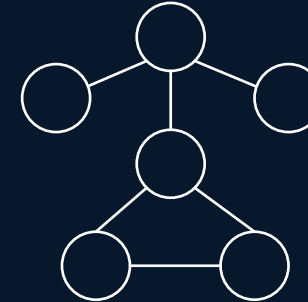
Point to Multipoint



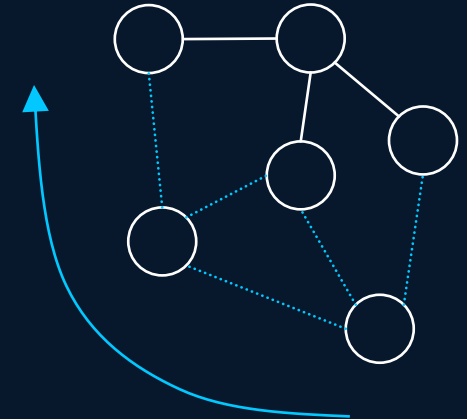
Mesh



Mixed



Mobility



Ultra-Reliable Wireless Backhaul to connect fixed and mobile assets for Ports OTS, T2G, Entertainment, Mining, Smart Cities

What makes URWB Ultra-Reliable?



End-to-End Overlay



Make-before-break handoff



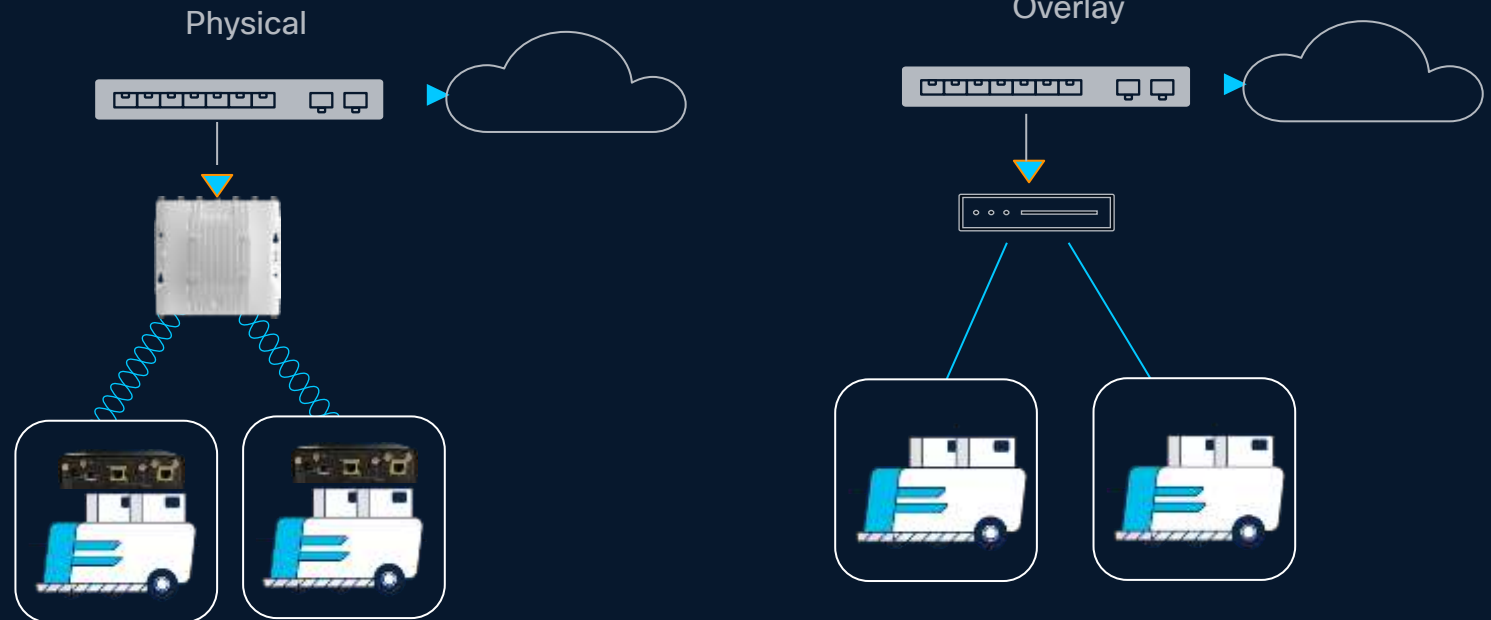
Multipath operations (MPO)



Ultra-fast failover
Carrier-grade availability



End-to-End Overlay



Overlay technology emulates a virtual switch over 802.11 wireless links, to extend ultra-low latency (<10ms) connectivity to fixed or mobile assets

What makes URWB Ultra-Reliable?

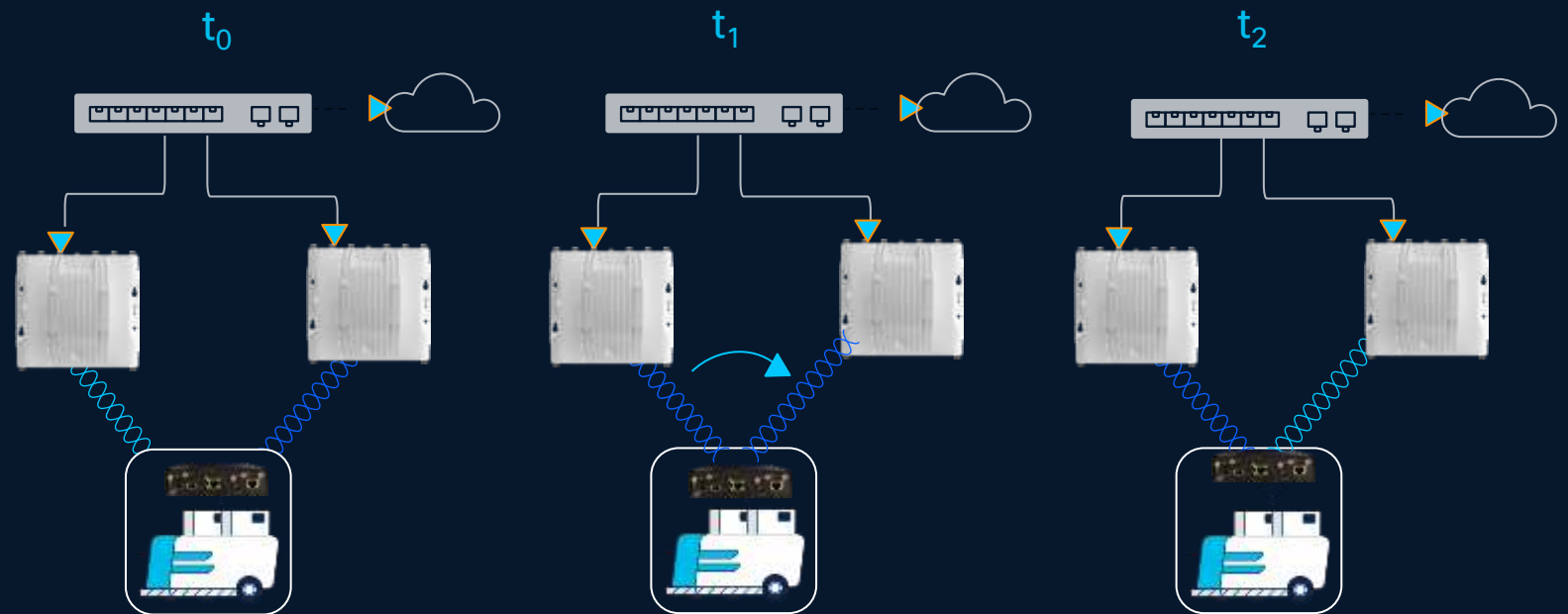
 End-to-End Overlay

 Make-before-break handoff

 Multipath operations (MPO)

 Ultra-fast failover
Carrier-grade availability

 Make-before-break handoff



Make-before-break handoff ensures connectivity is established with a new AP before dropping connectivity from the previous AP

Multipath Operations



End-to-End Overlay



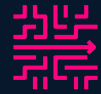
Make-before-break handoff



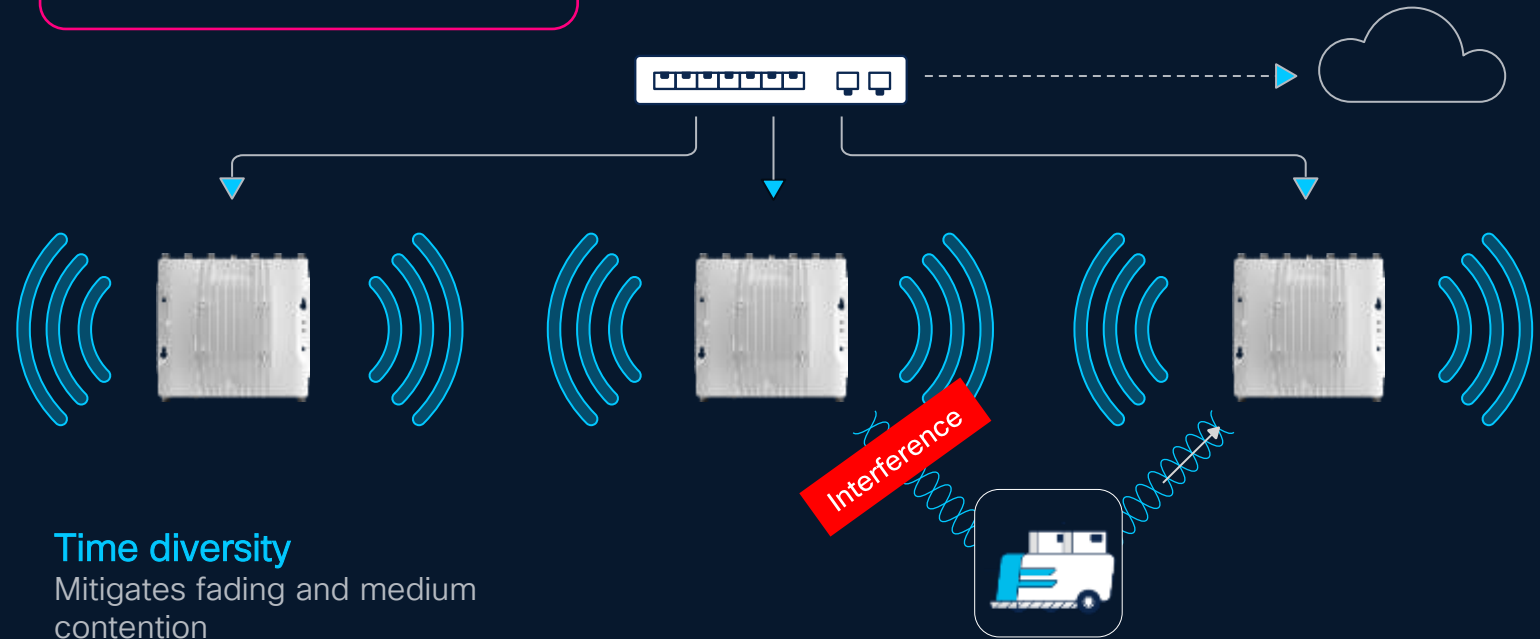
Multipath operations (MPO)



Ultra-fast failover
Carrier-grade availability



Multipath operations (MPO)



Time diversity

Mitigates fading and medium contention

Spatial diversity

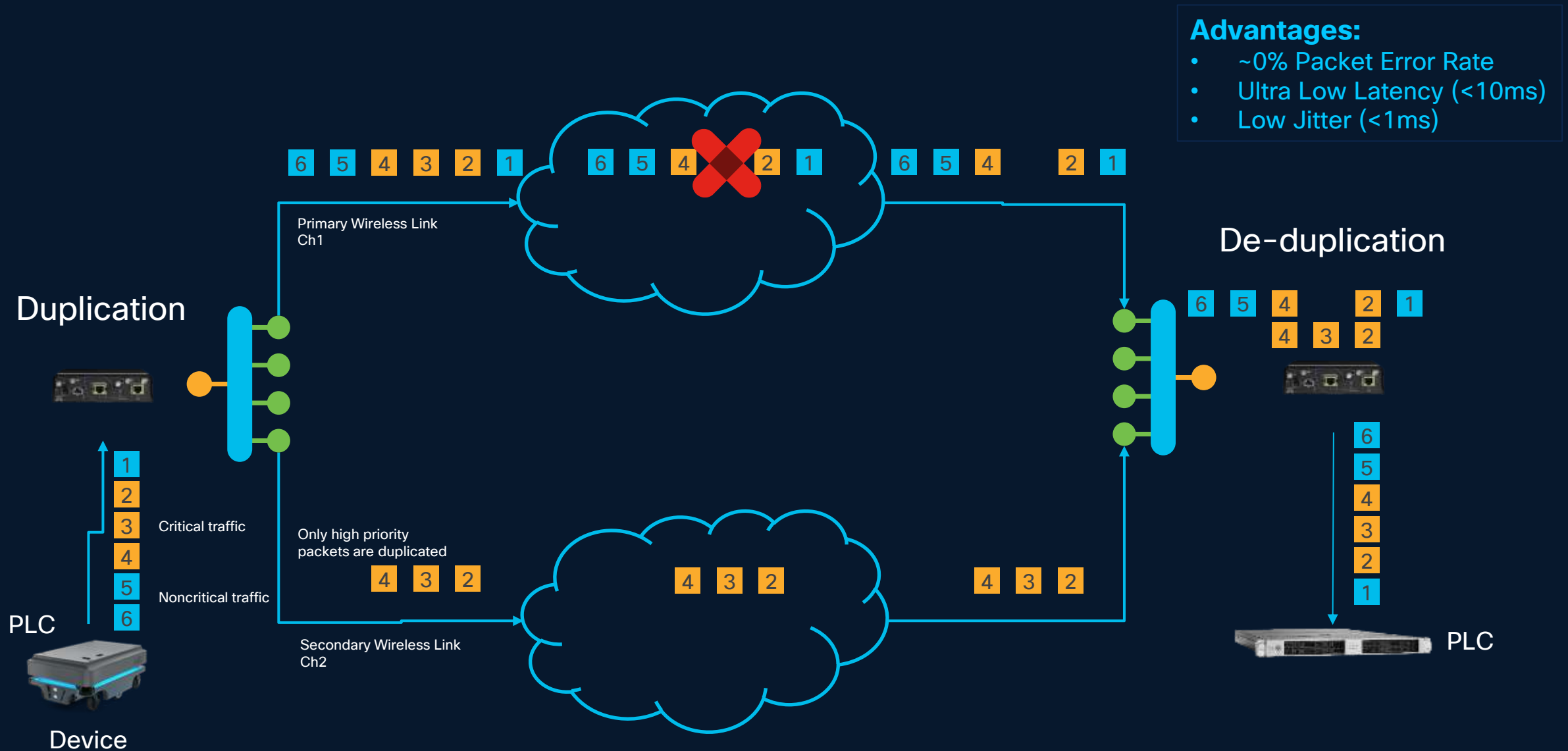
Mitigates blockages and obstacles

Frequency diversity

Mitigates Interference

MPO duplicates high priority packets over up to 8 different paths on uncorrelated frequencies at the same time to multiple access points

MPO Duplication and Deduplication



One platform for Wi-Fi and URWB infrastructure



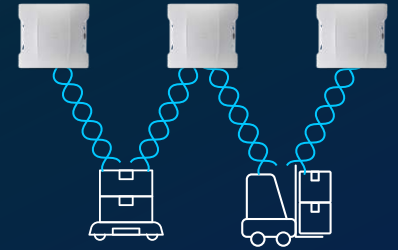
Ultra-Reliable Wireless
Backhaul built-in Enterprise
Wi-Fi Access Points

Others

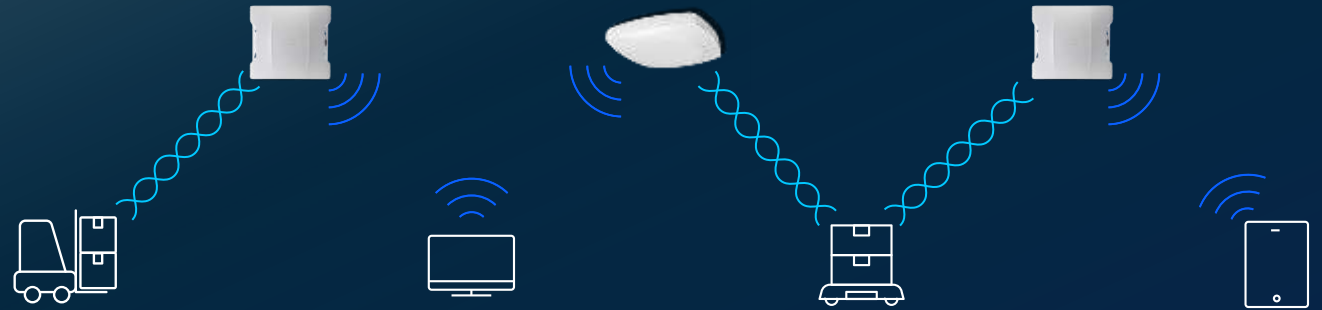
Wi-Fi
access
network



Backhaul
wireless
network



Cisco



Unified Wireless Infrastructure

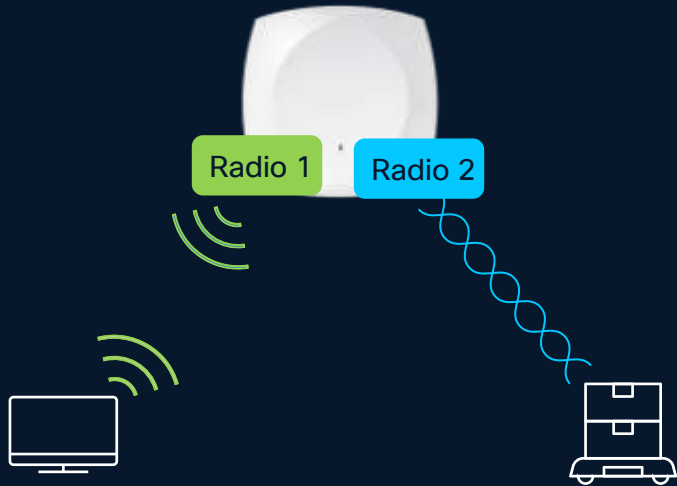
One management platform, One wireless infrastructure to install

Best of Wi-Fi combined with ultra-reliability by URWB to unlock unlimited use cases

Unified infrastructure in a nutshell

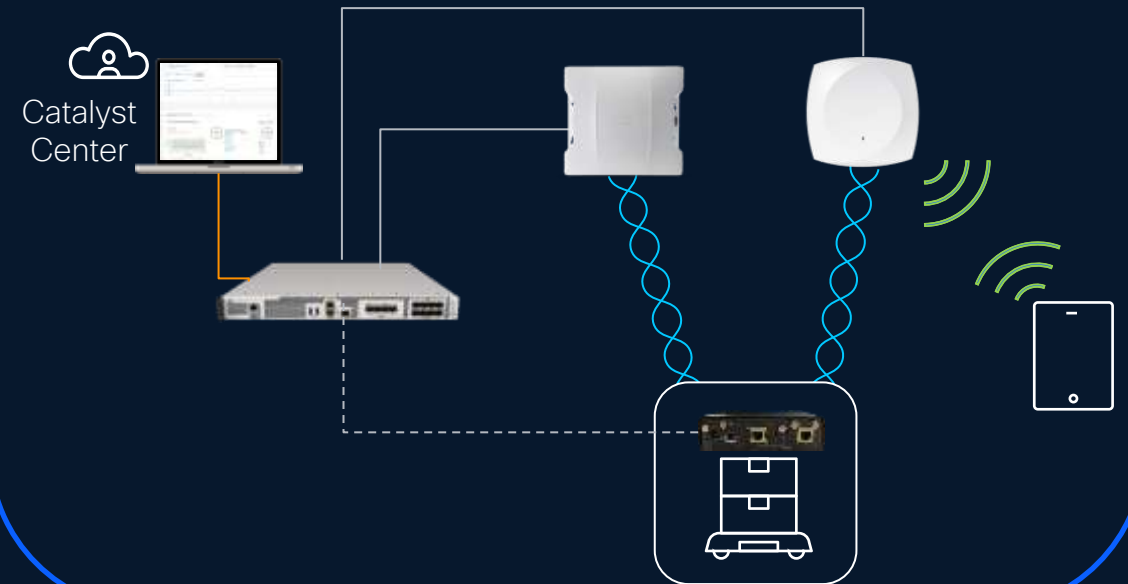
Unified platform

- ✓ Simultaneous URWB and Wi-Fi operations on the same AP
- ✓ Enable URWB on many WiFi6/6E and Wi-Fi7 APs (IWs and CWs)



Unified management

- ✓ Centralize management via WLC and Catalyst Center, for both APs and wireless clients
- ✓ Unified License experience



Cisco Wireless with URWB

Supported platforms and priority

- IOS XE 17.18.1
- IOS XE 17.18.2

Wi-Fi 7



CW9176I,
CW9176D1



CW9178I

Wi-Fi 6E



CW9136I



CW9166I,
CW9166D1



IW9165E



IW9165D



IW9167E
IW9167E-HZ



IW9167I

Wi-Fi 6



C9130
(AXE, AXI)



C9124
(AXE, AXI, AXD)

Full list of supported APs: cisco.com/go/urwbmatrix

URWB on Cisco Wireless Use Case and Country Support:

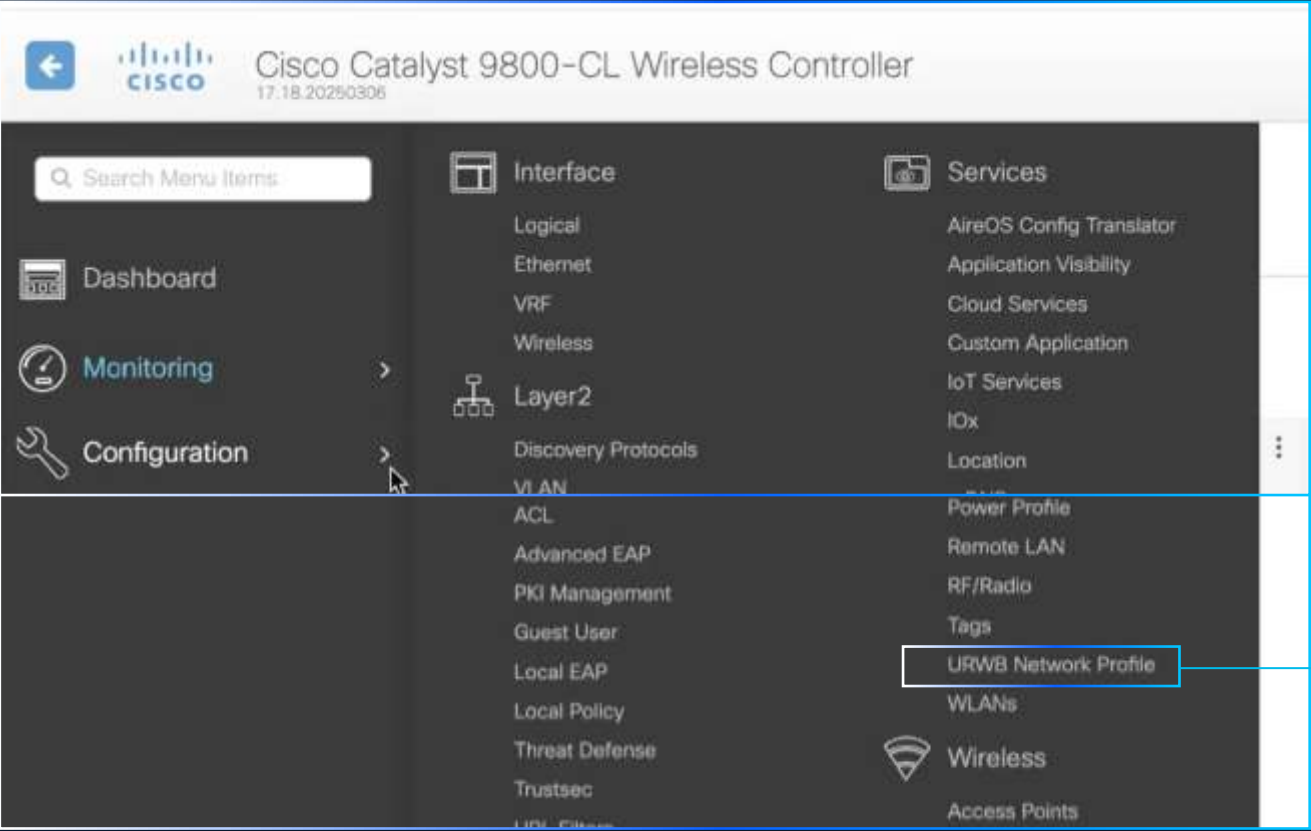
Licensing

URWB functionalities included as part of the current DNA or Unified Licensing model

	Wi-Fi 6 and Wi-Fi 6E platforms	Wi-Fi 7 platforms
Functionality	DNA License	Unified License
URWB Fixed Infrastructure (Point-to-point links)	DNA Essentials	Cisco Wireless Essentials
URWB Mobility (Mobile assets)	DNA Advantage	Cisco Wireless Advantage

Simultaneous URWB and Wi-Fi operations

URWB Configuration on WLC



URWB configurable as a network capability in the WLC

Add URWB Network Profile

General

Mobility

MPO

Advanced

URWB Enabled

☒

URWB Network Profile Name*

Description

Enter Description

Network-Key ⓘ

Enter Passphrase

Cancel

Apply to Device

Feature available via an IOS-XE software upgrade

Thank you

