Guide Cisco confidential IIIIII CISCO The bridge to possible

# Cisco Catalyst 9162I, 9164I, and 9166I Access Points Deployment Guide

## Contents

Introduction	4
Cisco Catalyst 9162I, 9164I, and 9166I overview	5
Supported software matrix	6
Supported wireless controller platforms	6
Access point capability matrix	6
Interoperability	7
Power options	7
Mechanical design	8
Physical dimensions	10
Physical ports	11
Cabling	12
Brackets and mounting	13
Getting started with Wi-Fi 6E	16
Wi-Fi 6E overview	16
Wi-Fi 6E migration and deployment tips	16
Creating a Wi-Fi 6E WLAN	25
6-GHz AP discovery mechanisms	31
6-GHz radio resource management	36
Enabling 6-GHz networks	40
Configuring 6 GHz Client Steering	41
Dual 5 GHz in the Catalyst 9166	42
6-GHz roaming behavior	46
Wi-Fi 6E client devices	46
Viewing 6-GHz clients	46
Migration between management modes	47
Regulatory domain	48
Cisco DNA management mode to Meraki management mode	49
Meraki management mode to Cisco management mode	52
Special considerations	52
Analytics and RF visibility	53
Cisco CleanAir Pro and the AI/ML-driven scanning radio	53
Cisco DNA Center and Wi-Fi 6E	54

Internet of Things integration	56
Environmental sensors and IoT Services with Cisco Spaces	56
Environmental sensors and IoT radio without Cisco Spaces	64
Enterprise wireless IoT with application hosting	68
Site Survey mode	69
Antenna patterns	70
Software solution compatibility	78
Useful links	91



## Introduction

The Cisco Catalyst 9162I, 9164I, and 9166I access points (APs) are the first in Cisco's history to have a common hardware that has the capability to join either an on-premises Cisco DNA and Catalyst-based wireless LAN controller or a cloud-based Cisco Meraki wireless network.

Cisco understands that selecting your next platform is not an easy choice. With the Cisco Catalyst Wi-Fi 6E access points, you don't need to make the decision now. Keep the operational mode you use today, whether on premises or cloud management. If your needs change–either way–it's an easy switch. No new hardware required. That's investment protection for your network that you can count on.



#### Figure 1. Cisco Catalyst 9162l, 9164l, and 9166l common hardware

## Cisco Catalyst 9162I, 9164I, and 9166I overview

The Cisco Catalyst 9162I, 9164I, and 9166I APs are Cisco's first common wireless Wi-Fi 6E access point platforms, with a penta-radio architecture providing the full capability of 802.11ax, such as orthogonal frequency-division multiple access (OFDMA), multiuser multiple-input multiple-output (MU-MIMO), Target Wake Time (TWT), BSS Coloring, overlapping BSS packet detection (OBSS-PD), and Wi-Fi Protected Access 3 (WPA3), all while being able to leverage advanced RF visibility with Cisco CleanAir<sup>®</sup> Pro together with an artificial intelligence and machine learning (AI/ML)-driven scanning radio.

The Catalyst 9162I, 9164I, and 9166I, when operated in an on-premises deployment, support the entire Cisco Catalyst wireless stack functionality with Cisco DNA Center (Automation and Assurance), Cisco Spaces (formerly Cisco DNA Spaces) (location and IoT), Cisco Identity Services Engine (ISE) (security), and more.

The Catalyst 9162I, 9164I, and 9166I are indoor Wi-Fi 6E APs that operate in Low Power mode\* with the capabilities listed in the table below.

Feature	91661	91641	91621	Comments
2.4 GHz (slot 0)	4x4:4SS	2x2:2SS	2x2:2SS	
5 GHz (slot 1)	4x4:4SS	4x4:4SS	2x2:2SS	
5 GHz (slot 2)	4x4:4SS	-	-	The 9166I has an XOR radio that can operate in 5+5 or 5+6 GHz
6 GHz (slot 2)	4x4:4SS	4x4:4SS	2x2:2SS	
AI/ML-driven scanning radio	Yes	Yes	Yes	
2.4-GHz IoT radio	Yes	Yes	Yes	For Bluetooth Low Energy (BLE) purposes
Ethernet	5 Gbps (Multigigabit)	2.5 Gbps (Multigigabit)	2.5 Gbps (Multigigabit)	
USB	Up to 4.5W	Up to 4.5W	Up to 4.5W	
Power options	802.3af/at/bt, DC input power: 54V	802.3af/at/bt, DC input power: 54V	802.3af/at/bt, DC input power: 12V	
Environmental sensors	Yes	No	No	Air quality, humidity, and temperature

#### Table 1. Cisco Catalyst 9162l, 9164l, and 9166l capabilities

<sup>\*</sup>Definition of a Low Power mode AP:

Wi-Fi 6E introduced different device classes, namely:

Standard Power AP

Low Power AP

Very Low Power AP

By definition, Low Power APs can operate in the entire spectrum of 6 GHz, can be indoor only with an integrated antenna, and cannot have any external attached antenna or have weather-resistant enclosures.

## **Supported software matrix**

Table 2. Supported Cisco IOS XE Software

#### Catalyst 9800 controller software release

Cisco IOS XE 17.9.1 and later for Catalyst 9164l and 9166l Cisco IOS XE 17.9.2/17.10.1 and later for Catalyst 9162l

## Supported wireless controller platforms

The Catalyst 9162l, 9164l, and 9166l are supported in the following wireless controller platforms:

- Catalyst 9800-L
- Catalyst 9800-40
- Catalyst 9800-80
- Catalyst 9800-CL (virtual controller for both private and public cloud)

#### Access point capability matrix

Table 3.	Cisco	Catalyst	9162I,	9164I,	and 9166	capability	matrix
----------	-------	----------	--------	--------	----------	------------	--------

Feature	91661	91641	91621
Scale	1200 clients total (400 clients per radio)	1200 clients total (400 clients per radio)	1200 clients total (400 clients per radio)
Client-serving radios	4x4 2 GHz 11ax, 4x4 5 GHz 11ax, 4x4 6 GHz 11ax (or) 4x4 2 GHz 11ax, (dual 5 GHz) 4x4 5 GHz 11ax, 4x4 5 GHz 11ax	4x4 2 GHz 11ax, 4x4 5 GHz 11ax, 4x4 6 GHz 11ax	2x2 2 GHz 11ax, 2x2 5 GHz 11ax, 2x2 6 GHz 11ax
Features	Download and upload OFDMA and MU-MIMO, BSS Coloring, TWT	Download and upload OFDMA and MU-MIMO, BSS Coloring, TWT	Download and upload OFDMA and MU-MIMO, BSS Coloring, TWT
LAN port	PoE-IN Multigigabit 5 Gbps	PoE-IN Multigigabit 2.5 Gbps	PoE-IN Multigigabit 2.5 Gbps
Ports	mGig0, console	mGig0, console	mGig0, console
Antenna	Integrated	Integrated	Integrated
Dimensions (W x L x H)	9.5 x 9.5 x 2.2 in. (241.3 x 241.3 x 56.9 mm)	9.5 x 9.5 x 2.2in. (241.3 x 241.3 x 56.9 mm)	7.8 x 7.8 x 1.7 in. (200 x 200 x 44.45 mm)
Weight	3.5 lb (1.60 kg)	3.5 lb (1.60 kg)	2.05 lb. (0.93 kg)
SSIDs	2.4 GHz: 16, 5 GHz: 16, 6 GHz: 8	2.4 GHz: 16, 5 GHz: 16, 6 GHz: 8	2.4 GHz: 16, 5 GHz: 16, 6 GHz: 8

Please refer to the product data sheets for the complete product specifications.

Catalyst 9166 Series data sheet: <u>https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9166-series-access-points-ds.html</u>

Catalyst 9164 Series data sheet: <u>https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9164-series-access-points/catalyst-9164-series-access-points-ds.html</u>

Catalyst 9162 Series data sheet: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/cat-9162-series-access-points-ds.html

## Interoperability

The Catalyst 9162I, 9164I, and 9166I are interoperable with the network management and security solution in the table below.

 Table 4.
 Software interoperability matrix

Access point	Catalyst 9800	Cisco DNA Center	Cisco Prime Infrastructure	Cisco CMX	Cisco Spaces	Cisco ISE
Catalyst 9164l and 9166l	17.9.1	2.3.4.X	3.10	10.6.3-113 MR2	2.3.1	2.6 and above
Catalyst 91621	17.9.2/17.10.1	2.3.5.x	3.10	10.6.3-113 MR2	2.3.1	2.6 and above

## Power options

The following tables provide the different power options for the Catalyst 9162I, 9164I, and 9166I.

Power source	Number of spatial streams	2.4-GHz radio	5-GHz radio	5-GHz / 6-GHz radio	mGig link speed	USB	Max power draw
802.3af	-	-	-	-	1 Gbps	Disabled	14.0W
802.3at	12	4x4	4x4	4x4	5 Gbps	Disabled	25.5W
802.3bt	12	4x4	4x4	4x4	5 Gbps	Y/4.5W	30.5W
DC power	12	4x4	4x4	4x4	5 Gbps	Y/4.5W	

 Table 5.
 PoE specifications for the Catalyst 9166I

Power source	Number of spatial streams	2.4-GHz radio	5-GHz radio	6-GHz radio	mGig link speed	USB	Max power draw
802.3af	-	-	_	Disabled	1 Gbps	Disabled	14.0W
802.3at	10	2x2	4x4	4x4	2.5 Gbps	Disabled	25.0W
802.3bt	10	2x2	4x4	4x4	2.5 Gbps	Y/4.5W	30.0W
DC power	10	2x2	4x4	4x4	2.5 Gbps	Y/4.5W	

#### **Table 6.**PoE specifications for the Catalyst 91641

 Table 7.
 PoE specifications for the Catalyst 9164I

Power source	Number of spatial streams	2.4-GHz radio	5-GHz radio	6-GHz radio	mGig link speed	USB	Max power draw
802.3af	2	-	1x1	1x1	1 Gbps	Disabled	13.3W
802.3at	6	2x2	2x2	2x2	2.5 Gbps	Y/4.5W	25.5W
802.3bt	6	2x2	2x2	2x2	2.5 Gbps	Y/4.5W	25.5W
DC power	6	2x2	2x2	2x2	2.5 Gbps	Y/4.5W	

#### Notes:

- 1. External power injector model: AIR-PWRINJ7
- 2. 802.3af is only for day-0 Control and Provisioning of Wireless Access Points (CAPWAP) connectivity between the AP and the Catalyst 9800 controller.

## Mechanical design

The Catalyst 9162I, 9164I, and 9166I have a brand new design compared to the previous Catalyst 9100 Wi-Fi 6 APs. They are designed with two ridges on the top, allowing you to identify them among the other APs instantly. Not only is the design aesthetically pleasing, but it is functional as well. A larger recessed cable access area is provided for better access to cabling and faster, easier deployment.



#### Figure 2.

Front and back view of Catalyst 9162I, 9164I, and 9166I

This enlarged recessed area allows cables to be inserted into the ports without bending, for an improved cabling experience. This is depicted in the figure below, when compared with a Catalyst 9130 Series AP.



#### Figure 3.

Comparison of cabling experience of Catalyst 9162I, 9164I, and 9166I vs. Catalyst 9130AXI

## **Physical dimensions**

The Catalyst 9162I, 9164I, and 9166I have an incredible ratio of dimensions/weight to performance. They are similar in size and weight to the midrange and high-end Catalyst Wi-Fi 6 APs and smaller and lighter than many of the Cisco Aironet APs. However, they boast a much more robust penta-radio architecture and support the entirety of Wi-Fi 6E.

Refer to the figures below for the dimensions and weight.



#### Figure 4.

Dimensions and weight of the Catalyst 9164I and 9166I



## **Figure 5.** Dimensions and weight of the Catalyst 9162



#### Figure 6.

Comparing the Catalyst 9162I, 9164I, and 9166I with previous-generation access points

## **Physical ports**

The following figure depicts the ports and reset button on the Catalyst 9162I, 9164I, and 9166I.



#### Figure 7.

Physical ports and buttons of the Catalyst 9162I, 9164I, and 9166I

#### Ethernet port

The Catalyst 9166l comes with a 5-Gbps uplink port, the Catalyst 9164l comes with a 2.5-Gbps uplink port, and the Catalyst 9162l comes with a 2.5-Gbps uplink Multigigabit Ethernet port.

#### Console port

The console port (RJ-45) is used to access the AP's command-line interface (CLI).

#### DC input power

The Catalyst 9164I and 9166I have an optional DC input power of 54V to operate the AP at full capability. The Catalyst 9162I has an optional DC input power of 12V to operate the AP at full capability.

#### **Reset button**

The Reset button is used to reset the AP to the factory settings.

Follow these steps to reset the AP.

- 1. Connect the console cable.
- 2. Unplug the PoE network cable from the switch.
- 3. Press and hold the Reset button.
- 4. Plug the power back into the AP.
- 5. Wait until the output on the console says "Button pressed. Configuration Reset is Activated." Hold the button for 20 seconds for a full configuration reset and 30 seconds for a factory reset. Once the button is released, the AP will reboot to the state listed above.

#### **Environmental sensors**

The Catalyst 9166l has three built-in environmental sensors: air quality, humidity, and temperature. As shown in Figure 7, the openings on the right are where these sensors are located on the AP.

More details on these sensors are provided in the "Internet of Things Integration" section of this deployment guide.

#### Cabling

The use of proper cable types will directly affect the performance of the Catalyst 9136l. Since this AP has 5-Gbps ports, the recommendation is to use either CAT6 or CAT6a cable, which support speeds of up to 10 Gbps. CAT5e cables can still be used; however, there may be an effect on the AP's performance.

Refer to the table below to compare cable types that can be used with the Catalyst 9162I, 9164I, and 9166I.

Cable type	Speeds	Maximum length
CAT5e	5 Gbps	328 feet (100 meters)
CAT6	1, 2.5, or 5 Gbps	330 feet (100 meters)
	10 Gbps	164 feet (50 meters)
САТ6а	10 Gbps	330 feet (100 meters)

Table 8.Cable types supported

### **Brackets and mounting**

Regarding mounting, the Catalyst 9162l, 9164l, and 9166l are compatible with the AIR-AP-Bracket-1 (default option) and AIR-AP-Bracket-2 brackets, and with the AIR-AP-T-RAIL-R and AIR-AP-T-RAIL-F for T-rail drop ceilings. These brackets are the same AP brackets provided for all Tier 2 and 3 enterprise-class APs for the last 15 years. This backward compatibility streamlines the day-0 process for brownfield deployments, allowing the Catalyst 9162l, 9164l, and 9166l to be mounted on the existing bracket.

For more details on mounting the APs, refer to the following:

- <u>Catalyst 9166I Hardware Installation Guide</u>
- <u>Catalyst 9164I Hardware Installation Guide</u>
- <u>Access Point Mounting Instructions</u>

The following figures provide details about the AIR-AP-Bracket-1 and AIR-AP-Bracket-2 for reference.



Figure 8. AIR-AP-BRACKET-1



#### Figure 9. AIR-AP-BRACKET-1 schematics



#### Figure 10.

AIR-AP-BRACKET-1 schematics continued



Figure 11. AIR-AP-BRACKET-2



Figure 12. AIR-AP-BRACKET-2 schematics



## Figure 13.

AIR-AP-BRACKET-2 schematics continued

## Getting started with Wi-Fi 6E

## Wi-Fi 6E overview

Wi-Fi 6E takes the 802.11ax protocol to the next level by introducing a brand new spectrum, 6 GHz. This new spectrum is much wider than the legacy bands (2.4 GHz and 5 GHz) and allows wireless devices to take advantage of the performance enhancements introduced with Wi-Fi 6. The new spectrum is reserved for greenfield Wi-Fi 6 client operation only. This means that no previous generations of Wi-Fi will be permitted to operate there. This eliminates the performance-robbing requirements of backward compatibility often experienced in previous spectrums. In addition, the amount of spectrum provided encourages and enables the use of wider 80- and 160-MHz channels, which dramatically increases the speed while simultaneously providing enough room to operate without the co-channel interference issues experienced in the 2.4- and 5-GHz spectrums.

## Wi-Fi 6E migration and deployment tips

Wi-Fi 6E (6 GHz) is a new spectrum standard, and with it comes several new requirements that were not present in the past. This section goes over key points about Wi-Fi 6E that play a part in the deployment of the Catalyst 9162I, 9164I, and 9166I APs.

The figure below depicts a high-level representation of Cisco's recommendations, tips, and tricks for deploying the Catalyst 9162I, 9164I, and 9166I APs, while the sections that follow expand upon the details of each.

Deploying and migrating to Wi-Fi 6E Recommendations, tips, and tricks						
Migrating to 6 GHz	Power considerations	Security requirements	Wireless coverage			
<b>Top of mind:</b> For brownfield, 1:1 AP replacement. For greenfield, coverage area per AP is now 1500 to 2000 sq. ft.	Recommendation: 802.3bt (Cisco UPOE) is the suggested power input.	Mandatory: WPA3 is required for Wi-Fi 6E networks to be enabled.	<b>Recommendation:</b> Use Ekahau and iBwave to analyze 6-GHz AP coverage.			
Legacy clients must still be considered. Shorter distance = Better data rate.	802.3at (PoE+) and 802.3af (PoE) are also supported by the Catalyst CW9166I and CW9164I.	WPA3 was not required for prior Wi-Fi generations; hence, it must be top of mind.	The 916x is not available on Ekahau or iBwave yet; however, a generic 6-GHz AP is available on both for reference.			
Spectrum considerations	Multigigabit switching	Cisco DNA Center migration	WLAN considerations			
Note: Wi-Fi 6E's wider spectrum enables 80/160-MHz channel widths to be viable.	<b>Recommendation</b> : Use a Multigigabit switch with 2.5/5G capability.	Note: Use AP refresh workflow to replace existing APs managed by Cisco DNA Center.	Note: 8 Wi-Fi 6E SSIDs per AP can be created in Cisco IOS XE Release 17.7.1 will be raised to 16 SSIDs in a future release.			
Increased spectrum provides better data rates with less co-channel interference.	Better user experiences with speeds beyond 1 Gbps on existing cabling.	Access point refresh workflow can be found on Cisco DNA Center's guide.	This differs from the 16 SSIDs allowed for the 2.4- and 5-GHz bands.			

#### Figure 14.

Wi-Fi deployment and migration recommendations

#### Migration to 6 GHz

When deploying a new Wi-Fi 6E AP, there are two categories of considerations: whether you have a greenfield (no existing APs) or a brownfield (have existing APs) deployment.

Brownfield deployment: While we always recommend that you conduct site surveying and wireless coverage planning with tools such as Ekahau or iBwave, the general rule of thumb for a brownfield deployment is to have a one-to-one AP replacement. The reason is that you will likely still have to serve legacy band clients such as 2.4 or 5 GHz. If the legacy APs were strategically placed at the current location for the best legacy band coverage, the Catalyst 9162I, 9164I, and 9166I will likely provide the best coverage there.

Greenfield deployment: If there are no existing APs, the suggestion is to use Ekahau or iBwave to conduct proper wireless planning before deploying any APs physically to ensure the best wireless coverage. Another rule of thumb is that each AP can cover an area of around 1500 to 2000 square feet (139.35 to 185.8 square meters). The figure below provides a visualization of the predicted coverage provided by the Catalyst 9136l and can be used as a general reference when deploying a Catalyst 9162l, 9164l, or 9166l AP.



#### Figure 15.

Catalyst 9100 RF propagation on 5 GHz and 6 GHz as represented on Ekahau

#### **Power considerations**

The Catalyst 9162I, 9164I, and 9166I support three power types: 802.3bt (Cisco UPOE<sup>®</sup>, equivalent to 60W), 802.3at (PoE+, equivalent to 30W), and 802.3af (PoE, equivalent to 15W) or through DC input power. The AP can be powered by any of these power types; however, to get all the capabilities of the AP, an input power of 802.3bt must be used. Refer to the "Power Options" section above for a detailed overview of what input power type supports what radio, port, and USB settings.

When it comes to selecting a proper switching infrastructure to connect and power your wireless infrastructure, there are several factors to consider. To ensure that you have the most optimal switching infrastructure deployed, refer to the following Cisco UPOE+ white paper:

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/nb-06-upoe-plus-it-ot-wp-cteen.html.

#### Multigigabit switching

The Catalyst 9166l has one 5-Gbps Multigigabit port, the Catalyst 9164l has one 2.5-Gbps Multigigabit port, and the Catalyst 9162l has one 2.5-Gbps Multigigabit port, so to take advantage of their performance, your switches need to support Multigigabit speeds.

To learn more about Cisco Multigigabit switching technology, refer to the following webpage: <a href="https://www.cisco.com/c/en/us/solutions/enterprise-networks/catalyst-multigigabit-switching/index.html#~benefits">https://www.cisco.com/c/en/us/solutions/enterprise-networks/catalyst-multigigabit-switching/index.html#~benefits</a>

#### 6-GHz spectrum considerations

With the introduction of Wi-Fi 6E, the spectrum has been significantly expanded compared with 5 GHz and especially 2.4 GHz. Spanning from 5925 MHz to 7125 MHz, we now have 59x 20-MHz channels, 29x 40-MHz channels, 14x 80-MHz channels, and 7x 160-MHz channels.



## Figure 16.

The 6-GHz spectrum

Certain countries have yet to allow parts of or the entire 6-GHz spectrum. At the time this document was written, Europe/CEPT has approved only 5925 MHz to 6425 MHz, compared to the U.S., which has approved the whole spectrum.

The increase in spectrum width provides several advantages, with one of the most prominent being a lowered risk of co-channel interference. Since there are more channels to select from, it's much less likely that APs in a similar physical location will be broadcasting RF on the same channels. In the past, this concern for co-channel interference is what prevented users from taking advantage of 80-MHz or 160-MHz bonded channel widths. Although throughput tests showed that they could provide great performance numbers, the problem was that deploying them in such a fashion was simply not practical in most production enterprise settings, because fewer channels meant a greater chance of interference and reduced overall capacity. With the introduction of Wi-Fi 6E, 80 and 160 MHz can now be used, allowing us to take advantage of the increased speeds in a production scenario.

To configure your access point's 6-GHz radio as 80 or 160 MHz, navigate to the following in your Catalyst 9800 controller: Configuration > Wireless > Access Points > [Select a 6 GHz radio] > Configure > Channel Width > [select 80 MHz or 160 MHz] > [Click Update & Apply to Device].

Configuration * > Wireless * > Access Points	Edit Radios 6 GHz Band	×
All Accors Points	Configure Detail	
	General Role A	ssignment
Total APs : 1	AP Name POD1-C9136 Assignm	nent Method   Auto (Client Serving)
AP Name : AP Model : Stots : Status Up Time :	Admin Status	Client Serving
POD1-C9136 👫 🕍 C9136I-B 4 💇 30 mins 4	Antenna Parameters	annel Assignment
secs	Antenna Type Internal v	inner Assignment
	Antenna Mode Omni	Channel 1
<ul> <li>6 GHz Radios</li> </ul>	Antenna A 🔽 Assignm	20 MHz
Total 6 GHz radios : 1	Antenna B	40 MHz 80 MHz
AP Name V Slot No V Base Radio MAC V Status Status	Antenna C	160 MHz
POD1-C9136 🔤 3 687d.b45f.8690 💿 📀	Antenna D Current	Tx Power Level 3
H K 1 > H 10 V Items per page	units) units and the state of t	
> 5 GHz Radios	855 0	JIOT
2.4 CHr Dedice	BSS Cc Configu	lor Global 👻
	BSS Co	lor Status
> Dual-Band Radios	Current	BSS Color 28
> Country	Download Core Dump to bootflash	
SC Provision	Cancel	🖂 Hadata 8 Azabuta Davies
		Update & Apply to Device

#### Figure 17.

Configuring a 6-GHz radio channel width

The instruction above demonstrates how to change the channel width manually as a reference. However, we recommend using the Catalyst 9800's radio resource management (RRM) feature with dynamic channel and bandwidth selection to automatically determine the channel and bandwidth the radios should be serving on for best performance. Refer to the "6-GHz Radio Resource Management" section below for more details.

Another benefit of the 6-GHz spectrum is that it is still clean and without much interference compared with legacy bands such as 2.4 GHz, which shared the spectrum with the likes of BLE, Zigbee, microwave, and various other RF devices. With 6 GHz, we can expect that a majority of the spectrum use will be by other Wi-Fi 6E wireless clients of similar speeds, resulting in not only a more efficient spectrum but also a more secure one, thanks to the WPA3 mandate described in the "Security Requirements" section below.

#### **Security requirements**

Wi-Fi 6E requires that all WLANs be configured with WPA3 and Opportunistic Wireless Encryption (OWE), together with Protected Management Frames (PMF) enabled in both the AP and the client. Because previous bands didn't require WPA3, this requirement allows Wi-Fi 6E to be the most secure spectrum. From a deployment perspective, this will likely affect how you create WLANs, since many legacy clients might not support WPA3 security. This is covered in the "WLAN Design Considerations" section.

The requirement to configure a Wi-Fi 6E WLAN with WPA3 security is not specific to Cisco but general to Wi-Fi 6E and applies to all vendors.

To learn more about WPA3, refer to the WPA3 Deployment Guide: <u>https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.html</u>

#### Wireless coverage planning

6 GHz is a new spectrum and therefore requires special planning and site surveying to determine the best areas for AP placement, especially in greenfield deployments. While 6 GHz provides faster speeds, its wavelengths are shorter, meaning that its range is shorter as well compared to 5 and 2.4 GHz. This factor may result in the Catalyst 9162I, 9164I, and 9166I being placed in slightly different locations than previous APs that broadcast only 2.4 and 5 GHz to ensure optimal RF coverage in a greenfield deployment.

Cisco recommends always conducting a site survey and using Ekahau or iBwave for wireless planning. These tools will allow you to upload floor plans of your building and simulate the RF of a Catalyst 9162I, 9164I, and 9166I to determine where the APs should be placed for the best coverage. Once you've determined the optimal locations for your Catalyst 9162I, 9164I, and 9166I, you can deploy them physically.

#### **Cisco DNA Center AP refresh workflow**

When migrating to new APs in a brownfield deployment, the new APs often take the place of incumbent APs with a one-to-one replacement. Assuming that your wireless infrastructure is being managed by Cisco DNA Center, you would also need to replace both the APs managed by the inventory and those assigned to a floor map. To do this efficiently, Cisco DNA Center has an AP refresh workflow that allows you to easily replace old APs with new ones. This eliminates the tedious manual process of deleting old APs and streamlines the entire workflow.

Refer to the Build and Deploy Workflows chapter of the Cisco DNA Center User Guide for reference on the AP refresh workflow: <u>https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-2-3/user guide/b cisco dna center ug 2 2 3/m dnac workflows.html.</u>

#### WLAN design considerations

As stated in the "Security Requirements" section, for an SSID to be broadcast on 6 GHz you need:

- WPA3 or OWE as Layer 2 security
- Protected Management Frames (PMF)
- No other Layer 2 security method is allowed a mixed mode is not possible

On one hand this is good, because it makes 6 GHz extremely secure, but it also means that you need to reconsider your SSID/WLAN design, as multiple legacy clients you have in your network might not support these requirements, and most likely your current WLAN configuration would prevent them from being supported on 6 GHz.

So how would you design your SSID and define your security settings in order to adopt 6 GHz but at the same time guarantee backward compatibility for existing clients?

There are three options available:

- "ALL-IN" Option: Reconfigure the existing WLAN to WPA3, one SSID for all Radio Policies (2.4/5 and 6 GHz)
- 2. "One SSID" Option: Configure multiple WLANs (profiles) with the same SSID name, but different security settings
- 3. "Multiple SSIDs" Option: Re-design your SSIDs adding specific SSID/WLAN with specific security settings

The recommended option for enterprise is to add a separate WPA3 SSID (Option 3), with a different SSID name, and broadcast it in all bands. The WPA3-capable clients in the 2.4-GHz, 5-GHz, and 6-GHz bands would be able to connect and enjoy the most secure wireless network possible. Since you are not touching your existing SSIDs, legacy clients not supporting WPA3 will continue to connect to legacy SSIDs. The drawback of this option is that you need to broadcast an additional SSID, and you need to manage an additional wireless profile on the new WPA3-capable clients.

#### Example:

A new SSID with WPA3 with dot1x only Security for employees and an SSID with WPA3 with SAE for guest.

Existing SSIDs (2.4/5 GHz):

Corporate SSID: employee Security: WPA2 with dot1x

Guest SSID: guest Security: WPA2 with PSK

New SSIDs (2.4/5/6 GHz):

Corporate SSID: employee\_wpa3 Security: WPA3 with dot1x

Guest SSID: guest\_wpa3 Security: WPA3 with SAE

However, in the education sector (Example: eduroam), there will be a need to have the same SSID name across all the bands with support for older security mechanism like WPA/WPA2 and at the same time support for only WPA3 in 6 GHz band.

If there is a requirement to keep the SSID name the same, another option (Option 2) would be to create an additional WLAN profile with the same SSID name and a different profile name, configure the security settings with WPA3 and PMF required, and broadcast it only on the 6-GHz band. The existing SSID in 2.4 and 5 GHz will not be touched, so clients not supporting 6 GHz will continue to connect. This is illustrated in the figure below.

neral Security Advar	nced Add To Policy Tags		General Security	Advanced Add To I	Policy Tags
Profile Name* emplo	yee Radio	Policy ()	Profile Name*	employee-6GHz	Radio Policy (i)
SSID* emplo	yee	Show slot configuration	SISID*	employee	Show slot configura
WLAN ID* 9	-6 GHz Status	DISABLED	WLAN ID*	10	Status ENABLED  WPA2 Disabled
Status	ED 5 GHz- Status		Broadcast SSID		© WWX3 Enabled © Dot11ax Enabled
Broadcast SSID ENABLI					Status DISABLED
	-2.4 GH				- 2.4 GHz
	Status	ENABLED			Status

#### **Figure 18.** Same SSID, but different profile

There are again two sub-options here:

a) WPA3 Transition Mode

WLAN Security Configuration for 2.4/5 GHz - > Enable WPA3 Transition Mode (mixed mode)

- L2 Security would be WPA2 + WPA3.
- AKM should be set to 802.1x-SHA256 and 802.1x (SHA1).
- PMF set to optional

General	Security	Advanced							
Layer2	Layer3	AAA							
O WF	○ WPA + WPA2 ● WPA2 + WPA3 ○ WPA		PA3	3 O Static WEP		() None			
MAC	Filtering	D							
Lobby	Admin Acce	ss 🗖							
WPA P	arameters				Fast 1	ransition			
WPA Policy		WPA2 Policy			Statu	S		Adaptive	Enabled
GTK Rando	omize	WPA3 Policy			Over	the DS			
Transi Disabl	tion 🛛				Reas	sociation Ti	meout *	20	
WPA2/	WPA3 Encr	yption			Auth	Koy Maret			
AES(C	CMP128)	CCMP25	56 🗖		Auti			DSK	
GCMP	2128 C	GCMP25	56		CC	z. ix KM	0	SAE	
Protect	ted Manage	ement Frame			FT FT	+ SAE + 802.1x		OWE FT + PSK	
PMF		O	ptional	•	80 SH	2.1x- IA256			

**Figure 19.** WPA3 Transition Mode

#### **Client-side settings**

For clients that do not support 6 GHz, configure a WPA2 profile.

For clients that support 6 GHz, configure a WPA3 Enterprise. They will use this setting to connect to both 2.4/5 GHz and 6 GHz.

#### **Pros:**

- This provides an adoption path to more secure Wi-Fi via WPA3 Transition mode.
- No new SSID profile to be managed on the client side.

#### Cons:

- Older clients may have problem connecting to an SSID with WPA3 Transition mode.
- Roaming across different WLANs (same SSID) is not supported.
- Not supported by Cisco DNA Center Automation

#### b) WPA/WPA2

- Layer 2 Security would be WPA + WPA2.
- AKM should be set to 802.1x-SHA1.
- PMF set to disabled.

General	Security	Advanced							
Layer2	Layer3	AAA							
• WF	PA + WPA2	O WPA2 + WPA3			43	O Sta	atic WEP	O Nor	ie
MAC F	Filtering								
Lobby	Admin Access								
WPA P	arameters —				Fast	Transition			
WPA Policy		WPA2 Policy			Status		Adaptive Enabled		
GTK Rando	omize	OSEN Policy			Over the DS				
WPA2	Encryption —				Reas	sociation Ti	meout *	20	
AES(C	CMP128)	CCMP256							
GCMP	128	GCMP256			C Auth	Key Mgmt			
- Protect	ed Managem	ent Frame			80 Ea	)2.1x isy-PSK		PSK CCKM	
					FT	+ 802.1x		FT + PSK	
PMF		Disable	ed	•	80 SH	)2.1x- 1A256		PSK-SHA256	
					MDC	Configur	otion		

## Figure 20.

WPA/WPA2 Security setting

#### **Client-side settings**

For legacy clients, keep the existing WPA2 profile.

For clients that are configured for 6 GHz with a WPA3 profile, connecting to the 2.4/5 GHz WLAN could be seen as a security downgrade attack.

#### Pros:

- Maintain support for older clients using WPA/WPA2.
- No new SSID profile to be managed on the client side.

#### Cons:

- WPA2 only security for 2.4/5 GHz I not as secure as using WPA3.
- Clients may complain going from a WPA3 SSID to a lower security.
- Roaming across different WLANs (same SSID) is not supported.
- Not supported by Cisco DNA Center Automation

#### Note:

The following blog walks through the different scenarios and options available that administrators can chose to deploy depending on their network conditions and requirements. <u>https://blogs.cisco.com/networking/wlan-ssid-security-migration-into-6ghz-networks</u>

More details on WLAN creation can be found in the "Creating a Wi-Fi 6E WLAN" section below.

In Release 17.7.1, 17.8.1, and 17.9.1, you are limited to eight Wi-Fi 6E SSIDs. However, this limit will be increased to the standard 16 SSIDs in a future release This limitation affects only 6 GHz; for legacy bands you can configure up to 16 SSIDs.

#### **Creating a Wi-Fi 6E WLAN**

The workflow for creating a 6-GHz WLAN is similar to that for all legacy bands with only a couple of differences, one being the security requirement of WPA3.

To create a 6-GHz WLAN, navigate to Configuration > Tags & Profiles > WLANs > [Click +Add]. Input a Profile Name (WLAN profile identifier) and SSID (Wi-Fi name being broadcasted), and then change the Status to Enabled.

Add WLAN		ж
General Security	Advanced	
Profile Name*	Wi-Fi 6E WLAN	Radio Policy (i)
SSID*	Wi-Fi 6E WLAN	Show slot configuration
WLAN ID*	6	6 GHZ Status ENABLED
Status	ENABLED	WPA2 Disabled WPA3 Enabled
Broadcast SSID	ENABLED	Dot11ax Enabled
		5 GHz Status ENABLED
		2.4 GHz
		Status ENABLED 802 11b/a 802.11b/a
Cancel		Apply to Device

#### Figure 21.

WLAN creation

Notice that although 6 GHz is enabled, it's highlighted in red. This is because by default, the security of WLANs is set to WPA + WPA2, which doesn't meet the requirement of 6 GHz. Notice that the text within the 6 GHz Status box highlights the requirements.

To change the security to WPA3, click the Security tab and then, from the radio button menu located at Layer2 > select WPA3.

General	Security A	dvanced						
Layer2	Layer3 AA	A						
O WP	A + WPA2	O WPA2 + WPA3		WPA3	05	Static WEP	O No	ne
MAC F	iltering	0						
- WPA Pa	arameters	0		Fast	Transition	1		
WPA		WPA2 Policy		Status		Adaptive E	nabled	
GTK Rando	mize	WPA3 Policy		Over the DS				
Transit Disable	ion 🖸			Rea	ssociation <sup>•</sup>	Timeout *	20	
WPA2/	WPA3 Encryption	1		Auth	Key Mgr	nt		
AES(C	CMP128)	CCMP256		S	AE		FT + SAE	
Drotoot		GCIMP200	0	0	WE		FT + 802.1x	0
- Protecti	eu wanagement	Frame			TA200			
PMF		Requir	ed	•				
							_	

#### Figure 22.

Configuring security parameters

Select at least one Authentication Key Management (AKM) option: Secure Agile Exchange (SAE), OWE, Fast Transition (FT) + 802.1X, or 802.1X-SHA256.

Navigate back to the General tab, and you'll notice that the 6 GHz Status is now enabled and green, meaning that all configurations are satisfactory. Click Apply to Device to complete the WLAN creation workflow.

Add WLAN			×
General Security	Advanced		
Profile Name*	Wi-Fi 6E WLAN	Radio Policy	
SSID*	Wi-Fi 6E WLAN	Show slot configuration	
WLAN ID*	6	Status ENABLED	
Status	ENABLED	<ul> <li>WPA2 Disabled</li> <li>WPA3 Enabled</li> <li>Dot11ax Enabled</li> </ul>	
Broadcast SSID		5 GHz Status ENABLED	
		2.4 GHz Status ENABLED	
Cancel		802 11b/a 802.11b/a -	

#### Figure 23.

6-GHz radio status in WLAN

**Option:** If you want to verify that 802.11ax features such as downlink and uplink OFDMA, downlink and uplink MU-MIMO, and BSS Target Wake Time are enabled, click Advanced, and scroll to the bottom.

Note: On the Catalyst 9162l, we currently recommend disabling MU-MIMO.

Add WLAN				×
Coninguration of TTT TO DISASSO supported from Command Line In	Configuration of TTV BSS Disassociation infiniment is supported from Command Line Interface (CLI) only		ort 🗹	
11ax		Advertise PC A Support	nalytics 🖸	
Enable 11ax 0		Share Data with	n Client	
Downlink OFDMA		11k Beacon R Client Scan Rep	adio Measurement	
Uplink OFDMA				
Downlink MU-MIMO		On Association		
Uplink MU-MIMO		On Roam	D	
BSS Target Wake Up Time				
Cancel				Apply to Device

#### Figure 24. Enabling 11ax features



#### Figure 25. IRCM: AireOS <--> Catalyst 9800

Note: Anchor WLC can be a Catalyst 9800 as well.

The exact software release combinations that have been tested for full functionality and at scale can be obtained from the following link: <u>https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b c9800 wireless controller-aireos ircm dg.html</u>

**Scenario 2:** Customers who have already migrated to Catalyst 9800 controllers can have their Wi-Fi 6/Wi-Fi-5 Wave 1 APs in a Catalyst 9800 controller running Cisco IOS XE Release 17.3.x and Wi-Fi 6/Wi-Fi 6E access points in Cisco IOS XE Release 17.9.x.



#### Figure 26.

IRCM: Catalyst 9800 <--> Catalyst 9800

#### Note:

- 1. Catalyst 9136 Wi-Fi 6E access points are supported from Cisco IOS XE Release 17.7.1, Catalyst 9166I and 9164I access points are supported from Cisco IOS XE Release 17.9.1, and Catalyst 9162I access points are supported from Cisco IOS XE Release 17.9.2/17.10.1.
- 2. Anchor controller can be an AireOS-based controller (running latest 8.10 or 8.5 software versions)

The following blog explains in detail the strategy that can be employed to migrate an older-generation network to a 6-GHz network. The strategies explain a methodical way to migrate the controller and access points without compromising on the downtime or reduced functionality.

Link to the blog on Migrating to 6 GHz: https://blogs.cisco.com/networking/migrating-to-6ghz

## 6-GHz AP discovery mechanisms

AP discovery is how wireless clients discover APs with WLANs that they would like to join. The legacy method includes two options, passive scanning and active scanning.

Passive scanning: The AP will periodically broadcast beacon frames that the wireless client can detect, providing metadata for each WLAN the AP is broadcasting, such as the SSID name, data rates, etc.

Active scanning: The wireless client will send probe requests to nearby APs when it wants to join a WLAN. If an AP detects this probe request, it will send back a probe response with WLAN information such as the SSID name, data rates, etc.

In both cases, using the information received from the AP in either the beacon frame or probe response, the wireless client can request to join the AP's WLAN.



#### Figure 27.

Legacy AP discovery mechanisms

These methods worked well with the previous 2.4- and 5-GHz bandwidth networks, since 2.4 GHz had only 3x 20-MHz channels and 5 GHz had 25x 20-MHz channels, as depicted in the figure below.



**Figure 28.** Depiction of 2.4- and 5-GHz spectrum

However, with the introduction of 6 GHz, we now have 59x 20-MHz channels (depicted in the figure below), more than two times what we had in 5 GHz. Because wireless clients can send probe requests only on 20-MHz channels, this increases the passive scan time significantly to 6 seconds, which is far too much delay in the world of wireless.



#### Figure 29.

Depiction of 6-GHz spectrum

Since legacy AP discovery mechanisms are not efficient when addressing the expanded spectrum of 6 GHz, new AP discovery mechanisms have been created. Of these new discovery mechanisms, there are two categories, out-of-band and in-band discovery, as shown in the figure below.

Out-of-band discovery mechanism: Used when 2.4-, 5-, and 6-GHz bands all exist in the RF environment.

In-band discovery mechanisms: Used when only the 6-GHz band exists in the RF environment.



**Figure 30.** 6-GHz WLAN discovery mechanisms

#### Out-of-band AP discovery mechanism

For the out-of-band discovery mechanism, we have the Reduced Neighbor Report (RNR), as depicted in the figure below, which includes WLAN information for all 6-GHz-capable WLANs within the beacon and probe responses of the AP's 2.4- and 5-GHz radios. Concatenating all 6-GHz WLAN data into these existing frames eliminates the need for additional packets to be sent, which conserves airtime and allows the network to steer the clients toward 6 GHz if they are capable.

RNR is enabled by default as part of 6 GHz.



#### Figure 31.

Visual representation of RNR



Figure 32. RNR IE shown in Wireshark

#### In-band AP discovery mechanisms

#### Fast Initial Link Setup

For the first in-band discovery mechanism, we have the Fast Initial Link Setup (FILS) frame, which is part of the 802.11ai standard. A problem that exists in wireless today is APs being overwhelmed by probe requests, and this is especially true in high-density environments. FILS directly addresses this and helps to make AP discovery in a 6-GHz band more efficient by reducing probe request overhead and prolonging a wireless client's dwell time between beacon frames.

The following step-by-step explanation is based on the figure below.

- 1. APs broadcast beacon frames that contain detailed WLAN metadata every 100 ms.
- 2. If a wireless client starts WLAN discovery right after a beacon is sent, it will continuously send probe requests until the next beacon is detected, taking up airtime.
- FILS frames, which are smaller than beacon frames, are sent every 20 ms between beacon frames and contain high-level WLAN information such as the short SSID name, channel, and Target Beacon Transmission Time (TBTT), but are sufficient to tell a wireless client whether the WLAN is something it wants to join.
- 4. If a client starts discovery right after a beacon frame is sent, within 20 ms it will detect a FILS frame. If it decides that this is a WLAN it would like to join, it will go into sleep mode (stop sending probe requests) until the next beacon frame is detected.
- 5. When the next beacon frame is detected, the wireless client will use the WLAN's detailed metadata from that frame to join the WLAN.

Ultimately, FILS frames help to reduce the number of probe requests being sent from clients and make the airtime more efficient.

	wlan.fixed.publicact =	= 0x22							Expression	
No	Time	Source	Destination	Protocol Lengt Signal s	tre Info					_
	1 16:57:45.318	68:7d:b4:5e	e:5f:41 ff:ff:ff:ff:ff:ff: o:5f:41 ff:ff:ff:ff:ff:	ff 802.11 154 -43dBm	Action, SN=3947, Reacon frame SI	, Flags=C	C RT-100	Seno-Sach-0122	SSTD-wood-SuiteR-GCMD2	
	3 16:57:45.359	68:7	d:b4:5e:5f:41 1	ff:ff:ff:ff:ff:ff:ff:f	f 802.11	154 -43dBm	Action.	SN=3949	Flags=	
2	16:57:45.379	68:7	d:b4:5e:5f:41 f	ff:ff:ff:ff:ff:ff:f	f 802.11	154 -43dBm	Action.	SN=3950.	Flags=C	
1	16:57:45.399	68:7	d:b4:5e:5f:41 1	ff:ff:ff:ff:ff:ff	f 802.11	154 -43dBm	Action.	SN=3951.	Flags=C	:
1 e	16:57:45.420	68:7	d:h4:5e:5f:41 f	ff.ff.ff.ff.ff.ff.	f 802.11	154 -43dBm	Action.	SN=3952	Flags=C	
1	9 10:5/:45.482	08:/0:04:56	e:5T:41 TT:TT:TT:TT:TT:	TT 802.11 154 -4305M	ACT100, 5N=3955,	, Fiags=	Acciony	011-0002,	1 Lugo=	1
	10 16:57:45.502	68:7d:b4:56	e:5f:41 ff:ff:ff:ff:ff:ff: e:5f:41 ff:ff:ff:ff:ff:ff:	ff 802.11 154 -43dBm ff 802.11 154 -43dBm	Action, SN=3956, Action, SN=3957	, Flags=C				
	12 16:57:45.543	68:7d:b4:56	e:5f:41 ff:ff:ff:ff:ff:ff:	ff 802.11 609 -43dBm	Beacon frame, SI	N=3958, Flags=	C, BI=100, 5	SSID=wap3-owe,	SSID=wpa3-sae	
	13 16:57:45.564	68:7d:b4:5e	e:5f:41 ff:ff:ff:ff:ff:ff: e:5f:41 ff:ff:ff:ff:ff:ff:	ff 802.11 154 -43dBm ff 802.11 154 -43dBm	Action, SN=3959, Action, SN=3969	, Flags=C				
-	46 46.67.46 604	co.74.64.5		## 000 44 454 4000m	Action CN-2061	Flags- C				-
1	Radiotap Header v0.	Length 56	2 Dits), 154 bytes capt	ured (1232 bits) on inte	rtace 0					
>	802.11 radio informa	ation								
1	IEEE 802.11 Action, IEEE 802.11 wireless	Flags: s LAN								
	- Fixed parameters									
	Category	code:	Public Actio	n (4)						
	Public A	ction:	ETLS Discove	ry Request (A)	221					
	FUDILC F	= Shor	rt SSID Indicator: 1	iy nequest (o)	22)					
	<del>0</del>	= AP-C	CSN Presence Indicator:	0						
	0	= ANO = Chan	Presence Indicator: 0	eament 1 Presence: 0						
	0	= Prim	nary Channel Presence In	ndicator: 0						
	0	= RSN	Info Presence Indicator	r: 0						
		= MD P	Presence Indicator: 0							
	00	= Rese	erved: 0							
	Beacon Interva	1: 100	116							
	Short SSI	[D: 0x4	fa04e3e							
	FD Capability:	4704								
		0 = ESS:	: 0							
			Acy: 0							

#### Figure 33.

FILS discovery request frames shown in Wireshark

#### **Unsolicited Broadcast Probe Response**

The second in-band method is the Unsolicited Broadcast Probe Response (UBPR). When this feature is enabled and a client sends a probe request, the AP will send a probe response; however, rather than being sent to the client's MAC address, the probe response is broadcasted, as the name suggests. Broadcasting the probe response enables other wireless clients to use this same probe response to join the WLAN, reducing probe request overhead. The UBPR frames are transmitted every 20 seconds, carry multiple BSSIDs, and contain all information needed for the association, as any normal beacon frame does.

	and the second se							
No. Time Source Destination Pro Broadcast str/info								
1 16:36:27.556 68:7d:b4:5e:d2:f8 ff:ff:ff:ff:ff:ff:ff:	SSID=wpa							
2 16:36:27.577 68:7d:b4:5e:d2:f8 ff:ff:ff:ff:ff:ff:f8.11 802.11 550 -36dBm Probe Response, SN=2636, Flags=C, BI=100, SSID=wpa3-sae, SSID=GCMP25	6, SSID=W_							
3 16:36:27.597 68:7d:b4:5e:d2:f8 ff:ff:ff:ff:ff:ff 802.11 550 -36dBm Probe Response, SN=2637, Flags=C, BI=100, SSID=wpa3-sae, SSID=GCMP25	6, SSID=W							
4 16:36:27.518 68:70:b4:5e:02:T8 ff:ff:ff:ff:802.11 550 -36dBm Probe Response, SN=2638, FLags=C, BI=100, SSID=wpa3-sae, SSID=GCMP25	6, SSID=W_							
5 16:3647.638 68:70:04:59:02:78 TT:TT:TT:TT:TT:TT: 802.11 500.3608m Probe Response, SN=2639, Flags=	5, SSID=W_							
Sent every 20 ms 7 679 68:70:10-12 (2):78 ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	6. SSID=W							
8 10:30:77,700 68:7d;b4:5e;d2:f8 ff:ff:ff:ff:ff:ff:ff:802.11 550 -36d8m Probe Response, SN=2642, Flags=C. BI=100, SSID=wpa3-sae, SSID=GCMP25	6. SSID=W_							
9 16:36:27.720 68:7d:b4:5e:d2:f8 ff:ff:ff:ff:ff:ff 802.11 550 -36dBm Probe Response, SN=2643, Flags=C, BI=100, SSID=wpa3-sae, SSID=GCMP25	6, SSID=W							
10 16:36:27.741 68:7d:b4:5e:d2:f8 ff:ff:ff:ff:ff:ff:f802.11 550 -36dBm Probe Response, SN=2644, Flags=C, BI=100, SSID=wpa3-sae, SSID=GCMP25	6, SSID=W_							
11 16:36:27.761 68:7d:b4:5e:d2:f8 ff:ff:ff:ff:ff:ff 802.11 599 -36dBm Beacon frame, SN=2645, Flags=C, BI=100, SSID=wpa3-sae, SSID=GCMP256,	SSID=wpa							
12 16:36:27.782 68:70:b4:5e:d2:F8 ff:ff:ff:ff:ff 802.11 550 -36dBm Probe Response, SN=2646, Flags=C, BI=100, SSID=wpa3-sae, SSID=GCMP25	6, SSID=W							
13 16:36:27.802 68:70:04:59:02:78 TT:TT:TT:TT:TT:TT: 802:11 550 -3608m Probe Response, SM=2647, Flags=	6, SSID=W_							
14 10:30:27:022 00:70.04 9:02:70 11:11:11:11:11:10 00:211 050 -3000m Probe Response, on=2000, PingS=0, Di=100, SSID=mna3-sae, SSID=00-00=20 15 16:36:27 A3	6. SSID=W							
16 16:36:27.863 68:7d:b4:5e:d2:f8 ff:ff:ff:ff:ff:ff 802.11 599 -36dBm Beacon frame. SN=2659, Flags=C, BI=100, SSID=wpa3-sae, SSID=GCMP256,	SSID=wpa_							
<pre>&gt; Frame 2: 558 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface 0 &gt; Radiotap Header v0, Length 56 &gt; 802.11 radio information &gt; IEEE 802.11 wireless LAN &gt; Fixed parameters (12 bytes) &gt; Tanoen darameters (454 bytes)</pre>								
▶ Tag: SSID parameter set: wpa3-sae ▶ Tag: Supported Pates and RSS Membership Salectors 6 0/R) 0 12 0/R) 18 24/R) 26 48 54 [Mbit/sec]								
<ul> <li>Fig. Country Information: Country Code US, Environment Unknown (804)</li> </ul>								
▶ Tag: Power Constraint: 6								
▶ Tag: TPC Report Transmit Power: 23, Link Margin: 0								
Finds: Extended Supported Rates and BSS Membership Selectors BSS requires support for direct mashing to elements in SAE, [Molt/Sec] 5 Tag: ORSE load Element 202 11a CCA Version								
Fing, Good Lament out life for version								
Tag: RM Enabled Capabilities (5 octets)								
▶ Tag: Extended Capabilities (11 octets)								
Ext Tag: HE Capabilities (IEEE Std 802.11ax/D2.0)								
EXT lag: HE Operation (LEEE Sto 802.11aX/D2.0)								
Fix Lag. Sonz Santal Regiss Darameter Set								
▶ Ext Tag: MU EDCA Parameter Set								
▶ Tag: Vendor Specific: (null): WMM/WME: Parameter Element								
▶ Tag: Vendor Specific: (null): Unknown ▶ Tag: Vendor Specific: (null)								

**Figure 34.** UBPR frames in Wireshark

#### **Enabling FILS or UBPR**

FILS and UBPR are equivalent greenfield, in-band, 6-GHz discovery mechanisms.

To enable FILS discovery or UBPR, on your Catalyst 9800 controller, navigate to Configuration > Tags & Profiles > RF/Radio > [Select RF profile] > 802.11ax.

Next to 6 GHz Discovery Frames, you have the option to enable either None, Broadcast Probe Response, or FILS Discovery. The default is None. If you select Broadcast Probe Response, you can also configure the response interval if desired.

Edit RF Profile								
General	802.11	RRM	Advanced	802.11ax				
6 GHz Dis	scovery Frame	es (i)		<ul> <li>None</li> <li>Broadcast Probe Response</li> <li>FILS Discovery</li> </ul>				
Broadcas	t Probe Respo	onse Interva	20					
Multi BSS	SID Profile		default-multi-bssi 🔻 💈					

#### Figure 35.

Configuring 6-GHz discovery on the Catalyst 9800 controller

Only one of these 6-GHz discovery frames methods can be enabled at a time.

#### 6-GHz radio resource management

Radio resource management (RRM) is a collection of algorithms that allow the Catalyst 9800 controller to automatically manage your network through a few key features, including Dynamic Channel Assignment (DCA), Preferred Scanning Channels (PSC), Dynamic Bandwidth Selection (DBS), Transmit Power Control (TPC), and Flexible Radio Assignment (FRA). This section will walk you through a few notable changes to RRM with the introduction of 6 GHz.

#### **Dynamic Channel Assignment**

Dynamic Channel Assignment (DCA) is a feature that dynamically manages channel assignments, channel width, and many other factors for an RF profile. It evaluates the channels for each AP radio and will automatically adjust the assigned channels based on environmental factors such as co-channel interference, rogues, noise, channel load, and DCA sensitivity. By default, this feature is enabled on the Catalyst 9800 controller for your 6-GHz network, and the recommendation is to keep it enabled.

To verify that DCA is enabled for the RF group that the Catalyst 9162I, 9164I, or 9166I is assigned to, navigate to Configuration > Tags & Profiles > RF/Radio > [Select an RF Profile] > RRM > DCA.

You can see a list of DCA channels in the figure below, many of which are specific to the 6-GHz band.
General	802.11	RRM	Advanced	802.11a	x			
General	Coverage	TPC	DCA					
Dynami	c Channel As	signment						
Avoid AF	P Foreign AP In	terference						
Channel	Width		<ul><li>20</li><li>Bes</li></ul>	MHz () st	40 MHz (	) 80 MHz	0 160	MHz
DCA Cha	annels		<ul> <li>1</li> <li>25</li> <li>49</li> <li>73</li> <li>97</li> <li>121</li> <li>145</li> <li>169</li> <li>193</li> <li>217</li> </ul>	<ul> <li>5</li> <li>29</li> <li>53</li> <li>77</li> <li>101</li> <li>125</li> <li>149</li> <li>173</li> <li>197</li> <li>221</li> </ul>	<ul> <li>9</li> <li>33</li> <li>57</li> <li>81</li> <li>105</li> <li>129</li> <li>153</li> <li>177</li> <li>201</li> <li>225</li> </ul>	<ul> <li>13</li> <li>37</li> <li>61</li> <li>85</li> <li>109</li> <li>133</li> <li>157</li> <li>181</li> <li>205</li> <li>229</li> </ul>	<ul> <li>17</li> <li>41</li> <li>65</li> <li>89</li> <li>113</li> <li>137</li> <li>161</li> <li>185</li> <li>209</li> <li>233</li> </ul>	<ul> <li>21</li> <li>45</li> <li>69</li> <li>93</li> <li>117</li> <li>141</li> <li>165</li> <li>189</li> <li>213</li> </ul>
PSC Enfo	orcement		ENABL	E				
PSC Cha	annel List		5,21,37	,53,69,85,1	01,117,13	3,149,165,	181,197,21	3,229
Client Ne	etwork Preferer	nce	Defau	lt	•			

#### Figure 36.

6-GHz DCA configuration in the RF profile

For more details on DCA, refer to the Radio Resource Management white paper: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b RRM White Paper/dca.html

#### **Preferred Scanning Channels**

Preferred Scanning Channels (PSC) is a feature categorized under DCA that designates every fourth 20-MHz channel for active probing by Wi-Fi 6E clients. It is used when channels are bonded in 80 MHz and restricts scanning down to 15 channels rather than 59, increasing the overall efficiency of RF scanning.

PSC enforcement is disabled by default, and the recommendation is to enable it. The PSC list is provided in the Catalyst 9800 controller interface at Configuration > Tags & Profiles > RF/Radio > [Select an RF Profile] > RRM > DCA, as shown in the figure above. When enabled, only PSC channels will be offered as the primary channel with 80-MHz channel bandwidth. The recommendation is to enable PSC when using 80-MHz bonded channels for more efficient network scanning from both the wireless client and other APs in the network.

The figure below depicts how PSC works.



#### Figure 37.

Visual presentation of PSC

#### **Dynamic Bandwidth Selection**

Dynamic Bandwidth Selection (DBS) is a feature that is categorized under DCA. It automatically dictates the channel width of the network. For 6 GHz, it has a bias toward selecting 80-MHz channel bandwidth in countries with full 6-GHz spectrum (such as the U.S. and South Korea) and 40 MHz in countries with partial 6-GHz spectrum. The DBS starts at 80 MHz as the default bandwidth and will lower the bandwidth based on DCA metrics such as neighbor density, high interference, and noise floor, and if it detects that most clients are only 20 MHz.

DBS is enabled by default when the Channel Width is set to Best, as shown in the figure below, and will help ensure that the most optimal channel width is selected; no static assignment is possible. You can navigate to the window shown below on the Catalyst 9800 controller via Configuration > Tags & Profiles > RF/Radio > [Select an RF Profile] > RRM > DCA.

Edit RF Pr	ofile							
General	802.11	RRM	Advanced	802.11a	×			
General	Coverage	TPC	DCA					
Dynamie	c Channel As	signment						
Avoid AP	P Foreign AP In	terference						
Channel	Width		<ul> <li>20 M</li> <li>Best</li> </ul>	MHz ⊖ 4 t	40 MHz (	) 80 MHz	0 160	MHz
DCA Cha	annels		<ul> <li>✓ 1</li> <li>✓ 25</li> <li>✓ 49</li> <li>✓ 73</li> <li>✓ 97</li> <li>✓ 121</li> <li>✓ 145</li> <li>✓ 169</li> <li>✓ 193</li> <li>✓ 217</li> </ul>	<ul> <li>5</li> <li>29</li> <li>53</li> <li>77</li> <li>101</li> <li>125</li> <li>149</li> <li>173</li> <li>197</li> <li>221</li> </ul>	<ul> <li>9</li> <li>33</li> <li>57</li> <li>81</li> <li>105</li> <li>129</li> <li>153</li> <li>177</li> <li>201</li> <li>225</li> </ul>	<ul> <li>13</li> <li>37</li> <li>61</li> <li>85</li> <li>109</li> <li>133</li> <li>157</li> <li>181</li> <li>205</li> <li>229</li> </ul>	<ul> <li>17</li> <li>41</li> <li>65</li> <li>89</li> <li>113</li> <li>137</li> <li>161</li> <li>185</li> <li>209</li> <li>233</li> </ul>	<ul> <li>21</li> <li>45</li> <li>69</li> <li>93</li> <li>117</li> <li>141</li> <li>165</li> <li>189</li> <li>213</li> </ul>
PSC Enfo	prcement		ENABLE					
PSC Cha	innel List		5,21,37,	53,69,85,1	01,117,133	3,149,165,	181,197,21	3,229
Client Ne	etwork Preferer	nce	Defaul	t	•			

#### Figure 38.

Channel Width configuration with default set to Best

#### **Transmit Power Control**

Transmit Power Control (TPC) automatically optimizes a radio's transmit (Tx) power based on neighboring RF to maximize coverage while minimizing co-channel interference. The TPC algorithm is run after the convergence of DCA and DBS. When it comes to 6 GHz, it considers the Tx power increase due to the width and revised effective isotropic radiated power (EIRP) adjustments on the Neighbor Discovery Packet (NDP). The TPC algorithm also allows it to maintain a higher Tx power compared to the 2.4- and 5-GHz bands due to the lower chance of co-channel interference.

To view the configured TPC threshold, navigate to Configuration > Tags & Profiles > RF/Radio > [Select an RF Profile] > RRM > TPC.

The figure below depicts the default but configurable thresholds of TPC. The recommendation is to leave the values at their defaults.

Edit RF Pro	ofile				×
	A Change	es may resu	It in loss of conne	activity for clients that are associated to APs with this profile.	
General	802.11	RRM	Advanced	802.11ax	
General	Coverage	TPC	DCA		
Transmit	Power Cont	rol			
Maximum	Power Level(	dBm)*	30		
Minimum	Power Level(c	dBm)*	-10		
Power Th	reshold V1(dE	3m)*	-70		

#### Figure 39.

TPC thresholds

## **Enabling 6-GHz networks**

OFDMA is an 802.11ax feature that allows the AP to share the bandwidth resources and send out multiple packets in parallel, which both maximizes the efficiency of the channel width and mitigates any network contention. With Wi-Fi 6E, OFDMA works in the same way, except that it has an increased spectrum to work with. By default, 6-GHz radio configurations are enabled; to verify this, navigate to Configuration > Radio Configuration > High Throughput.

The figure below depicts the different spatial stream and modulation and coding scheme (MCS) combinations, all enabled by default.

Dano	5 GHz Band	2.4 GHz Band						
		۵	6 GHz Network is operational.	Configuring High Throughput	will result in loss of connectivit	ty of clients.		El Apply
						Select All	Ø	
				5504	~c	22	MCS	
SS/N	ACS	SS/I	MCS	-35/M			11100	
ss <i>i</i> r	1/7	ss <i>n</i>	1/9	33/m	1/11		2/7	
ss/i	MCS 1/7 2/9	ss <i>n</i> e e	1/9 2/11	23.7mm 27 27	1/11 3/7		2/7 3/9	

#### Figure 40.

Verifying the spatial streams and MCS of the 6-GHz configuration on a Catalyst 9800 controller

## **Configuring 6 GHz Client Steering**

Since the 6-GHz bandwidth is new, most clients will automatically associate to the AP's 2.4- and 5-GHz radios by default. 6 GHz Client Steering is a feature that suggests that clients on the 2.4- and 5-GHz bands join the 6-GHz band when certain criteria are met.

6 GHz Client Steering is configurable at the WLAN level.

1. Navigate to Configuration > Tags & Profiles > WLANs > [Edit existing WLAN or add new WLAN] > Advanced, then check the box next to 6 GHz Client Steering.

Cont	figuratio	n * > Tags & Profile	Edit WLAN						×
+		X Delete En	A Changing	WLAN parameters while it is e	nabled will result in loss	of connectivity	for clients c	onnected to	o it.
Sele	cted WLA	Ns : 0	General Security	Advanced Add To P	olicy Tags				
	Status	Name	Coverage Hole Detection		Universal	Admin (			
O	O	TME_DNAC_LAN	Aironet IE	0	OKC	(	2		
0	o	@TME_DNAC LAN		-			_		
0	o	@TME_DNAC 802.1x L	Advertise AP Name	U	Load Bala	ance (			
0	o	Apple_Fastlane+	P2P Blocking Action	Disabled	Band Sele	ect (			
	0 0	Security_Richard	Multicast Buffer	DISABLED	IP Source	e Guard			
м	∢ 1	▶ N 10 <b>v</b>	Media Stream Multicast-	O	WMM Po	licy	Allowed	•	
			11ac MU-MIMO		mDNS M	ode	Bridging	•	
			WiFi to Cellular Steering	O	Off Char	nnel Scanning	g Defer		
			Fastlane+ (ASR)		Defer Price	ority 🔲 0	01	2	
			Deny LAA (RCM) clients	Ο			Ο.		
			6 GHz Client Steering			<b>□</b> 3		⊻5	

#### Figure 41.

Enabling 6 GHz Client Steering

 Navigate to Configuration > Wireless > Advanced > 6 GHz Client Steering, then configure the thresholds for 6 GHz Client Steering as you see fit.

The recommendation is to leave these thresholds at their defaults.

The configurable thresholds in the figure below include:

- 6 GHz Transition Minimum Client Count
  - The minimum number of clients that must be associated with the AP for 6 GHz Client Steering to be triggered.
- 6 GHz Transition Minimum Window Size
  - The minimum difference in wireless client count between the 6-GHz band and 2.4- or 5-GHz band.
     The purpose of this threshold is to load-balance clients between different radios.
- 6 GHz Transition Maximum Utilization Difference (%)
  - Indicates the maximum channel utilization difference at which 6 GHz Client Steering will be triggered.

- 6 GHz Transition Minimum 2.4 GHz RSSI Threshold (dBm)
  - Indicates the minimum 2.4-GHz received signal strength indicator (RSSI) value at which 6 GHz Client Steering will be triggered.
- 6 GHz Transition Minimum 5 GHz RSSI Threshold (dBm)
  - Indicates the minimum 5-GHz RSSI value at which 6 GHz Client Steering will be triggered.

onfiguration * >	Wireless > A	dvanced					
oad Balancing	Band Select	Optimized Roaming	High Density	Preferred Calls	RFID	Cellular Steering	6 GHz Client Steering
6 GHz Client	t Steering (i)						🖺 Apply
6 GHz Transit	ion Minimum Clien	at Count* 3					
6 GHz Transit	ion Minimum Wind	low Size* 3					
6 GHz Transit Difference (%	ion Maximum Utiliz )*	zation 20					
6 GHz Transit Threshold (dB	ion Minimum 2.4 G 3m)*	GHz RSSI -60					
6 GHz Transit Threshold (dB	ion Minimum 5 GH 3m)*	Iz RSSI -65					

#### Figure 42.

Configuring thresholds for 6 GHz Client Steering

## Dual 5 GHz in the Catalyst 9166

The Catalyst 9166I has the flexibility to operate in a tri-band mode for client serving, that is, 2.4, 5, and 6 GHz, or to operate in 2.4, 5, and 5 GHz (dual 5 GHz) using the XOR radio capability under the following circumstances:

- For countries where 6-GHz spectrum is not yet available for use of Wi-Fi.
- In wireless networks, where 6-GHz client density is very minimal and most clients are still 5 GHz.

The Flexible Radio Assignment (FRA) algorithm in RRM has the capability to dynamically convert the 6-GHz radio to a 5-GHz radio when either of the above criteria are met, or to revert back to 6-GHz operation when it sees more 6-GHz-capable clients joining the AP.

**Note:** This is not the legacy FRA available in AireOS and Catalyst 9800 Wireless LAN Controller for 2.4 and 5 GHz.

The Catalyst 9166l, when operated as dual 5 GHz, offers two independent macro-macro omnidirectional cells, even though it's an internal-antenna AP, which creates the simplicity of this feature. The two cells are band-locked. The 5 GHz in slot 1 operates only in the UNII1 and 2 bands – that is, channels 36 to 64, and the XOR radio in slot 2, when operated in 5 GHz, is locked to the UNII2E and 3 bands – that is, channels 100 to 165.

Note: This restriction of band lock applies only when the access point is operating as dual 5 GHz.



#### Figure 43.

Visual representation of dual 5-GHz macro cells

The RRM algorithm runs independently on both radios and assigns the best channel and transmit power that it comes up with.

The decision to change the band is based on two parameters, Client Density and Channel Utilization. By default, the FRA runs every 1 hour. Unlike legacy FRA, the decision to change the band is based not on a single decision, but on a collective decision over several intervals. This is done to avoid frequent changes of radios and the resulting disruptions to client connectivity.

The WLC has the capability to maintain the snapshot of every run for a period of 1 week. – for a total of 168 intervals. As an example, if 10% of FRA decisions favor 5 GHz, the radio will be changed to 5 GHz, and if 90% favor 6 GHz, the radio will be changed to 6 GHz.

To enable FRA, navigate to Configuration > Radio Configurations > RRM > FRA and toggle FRA Status to "Enabled" in 5/6 GHz Flexible Radio Assignment.

Configuration * > Radio Config	urations * > RRM
6 GHz Band 5 GHz Band	2.4 GHz Band FRA
FRA Freeze	DISABLED
5/6 GHz Flexible Radio As	signment
FRA Status	
FRA Operation State	Up
Last Run	2150 second(s) ago
FRA Interval	1 Hour 🔻

#### Figure 44. Enabling 5/6 GHz FRA

It is recommended to leave the FRA Interval and thresholds at the defaults. However, these thresholds are configurable.

To configure the FRA Interval, select the FRA Interval from the pull-down menu. The minimum is 1 hour and is the default value, and the maximum is 24 hours. We recommend leaving the FRA Interval at 1 hour.

To change the threshold parameters, navigate to Configuration >Tags & Profiles > RF/Radio > RF > RF Profile and change the Client Reset Count and Client Utilization Threshold. Client Reset Count indicates the number of 6-GHz-capable clients appearing on the AP, and Client Utilization Threshold indicates the load. If the threshold is above the configured parameter in an interval, the interval is marked as 6 GHz favorable. A similar configuration is available for 5-GHz threshold parameters.

Edi	t RF Pi	rofile						3	6
Ger	neral	802.11	RRM	Advanced	802.11ax				
	High (	Density Para	ameters			FRA			
	Max Cl	ients*		200		Client Reset Count	1		
	Multica	st Data Rate	(Mbps)	Auto	•	Client utilization	5		
	Rx Sop	Threshold (d	lbm)	Auto	•	threshold (%)			
	Client	Distribution	ı						
	Load B	alancing Wind	*wob	5					
	Load B	alancing Deni	al Count*	3					

#### Figure 45.

FRA threshold configuration

#### Note:

The 5-GHz threshold configuration can be made from the Configuration > RRM > FRA page; change the Client Select and Client Reset in 2.4/5 GHz Flexible Radio Assignment.

#### Important points

Whenever the Catalyst 9166l changes the XOR radio in slot 2 from 6 to 5 GHz and vice versa, the radios in slot 0 (2.4 GHz) and slot 1 (5 GHz) get reset as well, resulting in client disconnect in all three radios. Due to this issue, and to avoid disruptions in service, band change based on an FRA decision will be skipped when:

- The AP is serving 10 or more clients overall in any band.
- the Load on the AP is greater than 10%.

The 6-GHz radio in the Catalyst 9166l can also be manually converted to a 5-GHz radio. To do so, navigate to Configuration > Wireless > Access Points > Dual-Band Radios.

С	onfiguration *	*> Wir	eless *	> Access F	Points																					
		oss Poi	inte																							
		655 PU	ints																lisconfigure	d ADe						
																	Tag : 0	Country	Code : 0		LSC Fall	back : (		Select	an Action	•
	Total APs : 2	0																								
	AP Name		:	AP Model	:	Slots	: \$	Admin : Status	Up Time	:	IP Addre	ss :	Base Radi	o MAC	Ethernet MAC	:	AP Mode	Powe	er Derate ble	:	Operation Status	:	Configura Status	ation	Country Miscon	y Code
	CM66i-2		<u>њ</u> (Ш	CW9166I-B		3		٢	0 days 6 hr: mins 59 sec	s 23 :s	20.20.20	.52	10f9.20fd	a480	cc9c.3ef4.c5d0		Local	Yes			Registere	đ	Healthy		No	
	C9136-1		њы.	C9136I-B		4		•	0 days 6 hr mins 56 sec	s 23 :s	20.20.20	.51	687d.b45	.6680	687d.b45c.1df8		Local	Yes			Registere	đ	Healthy		No	
	∺ ∢ 1	F F		10 🔻																			1 - 2	of 2 acc	ess points	Ċ
	> 6 GHz F	Radios																								
	5 GHz F	Radios																								
	> 2.4 GH	z Radio	s																							
•	<ul> <li>Dual-B</li> </ul>	and Ra	dios																							
	Total Dual-Bar	nd radios :	:1 0																							
	AP Name		:	Slot No	Subban	d :	Radio	Туре	Radi	o Subty	pe :	Base Ra	dio MAC	Admin Status	: Operation Status	•	Operation Mode	:	Channel W	Vidth	: 0	hannel		: F	ower Level	0:
	CM66i-2		Lat	2	All		5/6 G	Hz Dual Ba	nd Tx-R	bx .		1019.201	d.a480	۲	0	А	utomatic (6 GH	iz)	40 MHz		(2	5,29)*		•	1/8 (16 dBm	n)
	∺ < 1	1 H		10 🗸																				1 - 1	of 1 items	Ċ

#### Figure 46.

Viewing the 9166I 5/6-GHz dual-band radio

Click on the AP that you want to convert to dual 5-GHz mode. Under Role Assignment, choose Client Serving. From the Band Selection drop-down menu, select 5 GHz and click Update & Apply to Device to apply the configuration to the access point.

Edit Dual-band Radios			
Configure Detail			
General		Role Assignment	
AP Name	CM66i-2	Assignment Method	Auto
AP Base Radio MAC	10f9.20fd.a480		Client Serving
Slot ID	2		Monitor
			Sniffer
Admin Status	ENABLED	Band Selection	6ghz 🔻
Antenna Parameters		Dart Connector Status	6ghz
		Dart Connector Status	5ghz

#### Figure 47.

Manual configuration of 5/6-GHz dual band in the Catalyst 9166l

## 6-GHz roaming behavior

When deploying APs, one wireless design consideration is roaming, or how wireless clients can seamlessly move from one AP to another when they physically change locations. The main thing to keep in mind is the need to support clients that do not support WPA3 or Wi-Fi 6E. In such a scenario, clients that are currently on a 2.4- or 5-GHz band will not be able to roam to areas that contain only 6 GHz. Therefore, when designing your network, you may want to ensure that every access point is still broadcasting legacy bands with legacy security methods to ensure that there are no coverage holes for those wireless clients.

## Wi-Fi 6E client devices

A wide variety of Wi-Fi 6E client devices are available now in the market. We recommend updating the client devices to the latest firmware driver. We also recommend updating the BIOS, in case the Wi-Fi 6E-capable laptop does not see the 6-GHz SSID.

## Viewing 6-GHz clients

When a Wi-Fi 6E client associates with the Catalyst 9162I, 9164I, or 9166I access point, you will be able to verify that it's associated as a Wi-Fi 6E client by navigating to Monitoring > Wireless > Clients > [Select Wi-Fi 6E client] > 360 View.

In the figure below, the data next to Capabilities reads 802.11ax – 6 GHz, indicating that the wireless client is associated with the Wi-Fi 6E network.



#### Figure 48. Wi-Fi 6E wireless client metadata

## Migration between management modes

The Catalyst 9162l, 9164l, and 9166l can convert from the Cisco DNA management mode to the Meraki management mode and vice versa. This converged hardware gives you the flexibility of on-premises or cloud management. It also provides investment protection for the future in case you want to switch between the two management options or between the Cisco DNA management mode and Meraki management mode later on.

Within the hardware itself, there are two boot partitions. The Cisco DNA partition will have the Cisco DNA image, and the Meraki partition will contain the Meraki image. Within the device there are three saved configurations, one for each management mode and one shared configuration that is used during the conversion process.



#### Figure 49.

Catalyst 9162I, 9164I, and 9166I boot procedure

Two serial numbers are provided on the access point. The Meraki serial number is vertically aligned and is used for any processes related to the Meraki management mode, such as claiming the device to a Meraki Dashboard account. The Cisco DNA serial number is horizontally aligned and is used for any processes related to the Cisco DNA management mode, such as Plug and Play using a Cisco Smart Account.

The following figure depicts the product information provided on the back of the access point.

cisco Ci	odel/Modèle: CW9 sco Catalyst 9166I Ser	1661-MR ies Wi-Fi 6E Access Points
Clean Bystems, Inc. (SUBH /WURH) 170 West Taxman Drive, San Jose, CA 95124 USA This device complies with pa harmful interference, and (S)	Model (Modèlle, 585/591): CW9168 Poese (Alimentation, 80./181); E.42 Product Name (Billion, Nillen); Al Made in Talean - Tabriquè à Talvan Horoqueneo a Talaase (Krraik) - II FCC D. LDK-CW9168 K: 246 115 di te FCC Rues. Qenation is subjet to miciden mut accost any interference noise	14-MB     5-57 V == 847 - 652 ± 94.     86-347 - 652 ± 94.     96-50 = 10446 +     10450 = 10446 +     10450 = 10450 =     10470 = 104506 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     104.     74-004166 =     74.     74-004166 =     74.     74-004166 =     74.
		Complex with MDA Standards DB101992
WRCODE		BARCODE PID VID: 3000-30000-30000 BARCODE SN (NVS): 3000-30000-30000
Merakit	BARCODE MFG Date: MM/YYYY	BARCODE MAC : X02X02X02X02X02X0

#### Figure 50.

Table 9.

Dual serial numbers on the Catalyst 91661

Regulatory domain SKUs

## **Regulatory domain**

There are different regulatory domains based on the specific country in which you want to use the Catalyst 9162I, 9164I, or 9166I. When purchasing in the Cisco DNA management mode, use the correct SKU when ordering.

Cisco DNA management mode SKUs	Country/region
-A domain	Canada
-B domain	United States and Puerto Rico
-E domain	Europe
-F domain	Indonesia
-Q domain	Japan
-R domain	Russia
-Z domain	Australia and New Zealand
-ROW domain	Rest of the world

To see a specific country's compliance regulatory domains for the Catalyst 9162, 9164I, or 9166I, please visit the wireless compliance tool: https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliancetool/index.html

In Meraki, there are no specific country SKUs; there is only an -MR SKU. The access point in Meraki will automatically detect the country where the access point is currently functioning when connected to Meraki Dashboard.

## **Cisco DNA management mode to Meraki management mode**

The conversion process from the Cisco DNA management mode to the Meraki management mode can be done from the Catalyst 9800 wireless controller.



#### Figure 51.

Conversion overview from Cisco DNA management mode to Meraki management mode

The following are the steps to perform the conversion process:

1. First, go to the Change to Meraki Persona section in Configuration.



#### Figure 52.

Cisco DNA to Meraki Conversion - Workflow, step 1

## 2. Then select the APs you want to convert to the Meraki management mode.

Confi	Configuration * > Wireless * > Change to Meraki Persona														
	<ul> <li>This workflow allows persona change from DNA persona to Meraki persona.</li> <li>Personas changed in the past can be visualized in the 'Previously changed APs' tab.</li> </ul>														
Char	Change to Meraki Persona Previously changed APs														
			Selec	t APs O			\ \	/alidate 0			Exp	ort O			
			_												ona
	0	AP Name	:	Meraki Serial : Number	AP Model	Up Time	IP Address	Base Radio MAC	Ethernet MAC	Country Code : Misconfigured	Site Tag	Count	try : A	Persona Change Attempted	:
ſ	0	APCC9C.3EF4.C600		Q5AF-LXYQ- WFJW	CW9166I-B	14 days 17 hrs 30 mins 56 secs	173.37.54.187	10f9.20fd.a4e0	cc9c.3ef4.c600	No	default-site-tag	US	N	No	
	ο	APCC9C.3EF4.C610		Q5AF-62CH- 6BZV	CW9166I-B	14 days 17 hrs 30 mins 49 secs	173.37.54.188	10f9.20fd.a500	cc9c.3ef4.c610	No	default-site-tag	US	٨	No	
	ο	APCC9C.3EF4.C650		Q5AF-3Z9H- XFQM	CW9166I-Q	14 days 17 hrs 30 mins 58 secs	128.107.85.10	10f9.20fd.a580	cc9c.3ef4.c650	No	default-site-tag	J4	N	No	
	ο	APCC9C.3EF4.D0B0		Q5AF-GMPN- EGNX	CW9166I-B	14 days 17 hrs 30 mins 53 secs	173.37.54.162	10f9.20fd.ba40	cc9c.3ef4.d0b0	No	default-site-tag	US	Ν	No	
	ο	APCC9C.3EF4.D1C0		Q5AF-KQEB-S5D6	CW9166I-B	14 days 17 hrs 30 mins 56 secs	173.37.54.176	10f9.20fd.bc60	cc9c.3ef4.d1c0	No	default-site-tag	US	Ν	No	
	0	APCC9C.3EF4.DDF0		Q5AF-UNK5- M9K2	CW9166I-B	14 days 17 hrs 30 mins 48 secs	173.37.54.181	10f9.20fd.e220	cc9c.3ef4.ddf0	No	default-site-tag	US	N	No	
	0	APCC9C.3EF1.1C00		Q5AD-TTQX-AG8Y	CW9164I-B	14 days 17 hrs 30 mins 57 secs	173.37.54.163	10f9.20fe.4260	cc9c.3ef1.1c00	No	default-site-tag	US	Ν	No	
	н	$\leftarrow$ 1 $\rightarrow$ $\rightarrow$	10 🗸	)									1 - 7 of 7 a	access points	¢

#### Figure 53.

Select APs to convert to the Meraki management mode

#### The controller will then validate the APs.



#### Figure 54.

Conversion to Meraki management mode - Validation

3. Confirm the change on the selected APs

Q. Search Mena Items	Configuration * > Wireless * > Change to Meraki Persona
Dashboard	This workflow allows persona change from DNA persona to Meraki persona.     Personas changed in the past can be visualized in the 'Previously changed APs' tab.
Monitoring >	Change to Meraki Persona Previously changed APs
Configuration >	0®
O Administration	Select APs 0 Confirm Persona Change x Expert 0 Book Validation Status: Completed Next
C Licensing	Base Radio Y Etherne ry Domain Y Slot 1 Regulatory Domain Y Slot 2 Regulatory Domain Y
X Troubleshooting	AP Name         Y         MAC         MAC         Are you sure you want to change the selected AP(s) to Meraki         Check         Check           APCC9C.3EE7.4530         cel4.0cde.3zad         cel6.3m         Persona?         ©         ©
	This will cause the APs to reboot and they will no longer be manageable from this Wileless LAN Controller. Persona changed libe attempted only on those AP(s) that have passed country code check and regulatory domain check on at least one siot. No

#### Figure 55.

Conversion to Meraki management mode - Validation

4. Lastly, export the APs.

Configur	ation * > Wireless * > Change t	o Meraki Persona					
0 0	This workflow allows persona change Personas changed in the past can be	from DNA persona to Meraki visualized in the 'Previously c	persona. hanged APs' tab.				
Change	to Meraki Persona Previously c	hanged APs					
~	Select APs	0		Validate Ø			Export 0
	AP Name	Y Meraki Serial Number	▼ Base Radio MAC	T Ethernet MAC	Y AP Model	Y Cisco Serial Number	▼ Persona Change Timestamp
	APCC9C.3EF1.01E0	Q5AD-C89Y-CSQX	10f9.20fd.8f40	cc9c.3ef1.01e0	CW9164I-B	KWC26020JCN	04/14/2022 18:06:50
	APCC9C.3EF1.0480	Q5AD-EJKL-K7J6	10f9.20fd.c4a0	cc9c.3ef1.0480	CW9164I-B	KWC2604062F	04/14/2022 18:06:50
	(i i 1 )⊨ (i) <b>10 v</b>						1 - 2 of 2 access points

#### Figure 56.

Conversion to Meraki management mode - Status

There are flexible options for exporting the AP information that is used to claim the device on Meraki Dashboard.

Export		×
◯ Serial Number	đ Copy 📥 Downic	bad
<pre>[[" name":" APCC9C.3EF1.01E0"," mac":" 10:f9:20:fd:8f:40"," merakiSerialNumber":" Q5AD-C89Y-CSQX\n" ),[" name":" APCC9C.3EF1.0480"," mac":" 10:f9:20:fd K7J6\n" }]</pre>	d:c4:a0" ," merakiSerialNumber" :" Q5AD-E	JKL-

#### Figure 57.

Export conversion data to Meraki Dashboard

'listo' Meraki	Access	Access points										
ORGANIZATION	ON List Health Map Connection log Timeline											
Cisco-EN-Aurora-DMZ *		ecommendations from Ne	twork Like Yours									
NETWORK	reduce latency by up to 40% Run diagnostics											
Cisco-EN-Aurora-DMZ 🛛 🔻												
	APs for the	e last day 👻										
Network-wide		OFFLINE		ALEF	TING	ONLINE	REPEATERS					
Wireless		•7		•0		•2	°0					
Organization	Edit * Sea	rch 👻	19 access points				Add APs Download As -					
	🗆 # Status	0 Name	MAC address	Model	Connectivity	Conversion Status	1					
	01 🔍	CM661-2	cc:9c:3e:f4:c5:d0	MR57		Conversion signal received by node at 3/30/202	2, 3:27:19 PM					
	□2 <b>●</b>	CM66-P28-NB2	cc:9c:3e:f4:d1:90	MR57		Conversion signal received by node at 4/6/2022	, 10:01:38 AM					
	□3 ●	CM66-P2B-MR-NB3	cc:9c:3e:14:bf:c0	MR57		Conversion signal received by node at 4/6/2022	, 10:01:30 AM					
	10 0	CM64-1-PREM	cc:9c:3e:14:f2:a0	MR57	-	Conversion signal received by node at 4/13/202	2, 7:29:31 AM					
	011 •	AP-MR64-Scale13	cc:9c:3e:f1:12:70	MR57		Conversion signal received by node at 4/13/202	2, 2:27:31 PM					

The figure below depicts converted APs on Meraki Dashboard.

#### Figure 58.

AP status in Meraki Dashboard after conversion

### Meraki management mode to Cisco management mode

Contact Meraki Support to migrate from Meraki management mode to Cisco management mode.

## **Special considerations**

When converting from Cisco management mode to Meraki management mode, keep these two regulatory considerations in mind:

- 1. Make sure to set -ROW Access Point countries in the AP join profile and as a global configuration to properly migrate to the correct country.
  - a. Example: -ROW with AP join profile and global set to US. During migration, the country is set as AE.
- 2. The controller will match the regulatory domain of the access point and global AP countries when using multiple different regulatory domains in the global settings.
  - a Example 1: -E with AP join profile US and Global config set as US and France. During migration, the country is set as FR.
  - b. Example 2: -B AP with AP profile as France and Global config set as US and France. During migration, the country is set as US.

## Analytics and RF visibility

## Cisco CleanAir Pro and the AI/ML-driven scanning radio

Wi-Fi 6E (6 GHz) was introduced with the Catalyst 9136l, and with it came new challenges for RF visibility and much more spectrum to monitor. In the past, the Catalyst 9100 APs relied on Cisco CleanAir<sup>®</sup> (software) and the RF-ASIC (hardware) for features such as packet capture, spectrum analysis, interference detection, and rogue and wireless intrusion prevention system (WIPS) detection. CleanAir and the RF-ASIC were great for RF visibility for the 2.4- and 5-GHz bands; however, with 6 GHz, Cisco CleanAir Pro and the AI/ML-driven scanning radio are being introduced to increase the performance and granularity required to manage this new spectrum (all 1200 MHz of it).

CleanAir Pro is software designed specifically for 6 GHz and the all-new challenges that have come with the introduction of 1200 MHz of spectrum. While many of its features work in conjunction with the Al/ML-driven scanning radio, CleanAir Pro also works with the Catalyst 9162I, 9164I, and 9166I APs' serving radios. Unlike previous generations of APs, CleanAir Pro can even decode high-efficiency (HE, 802.11ax) frames, which is crucial since Wi-Fi 6E uses only HE frames. In the future, there will even be an ML-based interferer classification built directly into the AP software for more efficient interferer analysis, rather than loading the WLC or Cisco DNA Center.



#### Figure 59.

High-level comparison of CleanAir Pro and CleanAir

## **Cisco DNA Center and Wi-Fi 6E**

Cisco DNA Center is Cisco's network monitoring software, for everything related to analytics. With the introduction of Wi-Fi 6E, Cisco DNA Center Release 2.3.2 will support 6 GHz from all perspectives. This includes the Wi-Fi 6E dashboard, Intelligent Capture for packet capture and spectrum analysis on 6 GHz, rogue and aWIPS detection on 6 GHz, and many others.



The following are a few examples of the features on Cisco DNA Center related to Wi-Fi 6E.

#### Figure 60.

Wi-Fi 6/6E dashboard: View network readiness and benefits for Wi-Fi 6/6E



#### Figure 61.

Spectrum analysis: Visualize RF spectrum energy, not only for 2.4-, 5-, and 6-GHz bands

Spectrum analysis is part of the Intelligent Capture feature set.



#### Figure 62.

Data packet capture: Capture unencrypted data packets

Data packet capture is part of the Intelligent Capture feature set.



#### Figure 63.

Rogue management and aWIPS: Detects wireless threats in the environment, not only for 2.4 and 5 GHz, but now also for 6 GHz

#### Rogue management and aWIPS dashboard

#### Note:

- Refer to the "Software Solution Compatibility" section in this guide for the exact features released with Cisco IOS XE 17.9.1 and Cisco DNA Center 2.3.4.
- Please refer to the Cisco DNA Center user guide for a detailed overview.

## Internet of Things integration

## **Environmental sensors and IoT Services with Cisco Spaces**

The Catalyst 9166l has three built-in environmental sensors, air quality, humidity, and temperature, that will be integrated with Cisco Spaces' rich map. This integration will provide an immersive experience for facility managers to help ensure a safe working environment, especially geared toward back-to-office safety use cases.



The figure below depicts the details of the three environmental sensors built into the Catalyst 9166l.

#### Figure 64.

Overview of environmental sensors on the Catalyst 9166

#### Note:

- The support for environmental sensors is available starting with Cisco IOS XE Release 17.9.1.
- The area where the sensors are located is separated from the rest of the AP's internal circuitry.

The figure below depicts the environmental sensor data in Cisco Spaces on a particular access point.



#### Figure 65.

Environmental sensor data in Cisco Spaces

The figure below depicts how environmental sensor data is sent from the Catalyst 9166l to Cisco Spaces.



#### Figure 66.

Environmental sensor on Catalyst 9166l topology

The Catalyst 9162I, 9164I, and 9166I have a built-in IoT radio that can be used in conjunction with the IoT Services platform service in Cisco Spaces. IoT Services is designed to enable management of Internet of Things (IoT) devices across vendors, form factors, and technology protocols.

Within IoT Services, you can enable a Catalyst 9162I, 9164I, or 9166I to be in Scan mode or Transmit mode. In Transmit mode, the AP can broadcast iBeacon, Eddystone URL, and Eddystone UID profiles. While in Scan mode, the AP can scan the vicinity for other BLE devices and receive telemetry data from floor beacons, which can be decoded in Cisco Spaces.

The Catalyst 9162I, 9164I, and 9166I can manage and configure wireless IoT devices if you enable the Advanced AP Gateway feature, which installs a Cisco IOx application on the access point. This saves the user the trouble of having several gateways across different vendors.



#### Figure 67.

Capabilities of the built-in IoT radio on the Catalyst 9162I, 9164I, and 9166I

#### Note:

- Support for the IoT radio is available starting with Cisco IOS XE Release 17.9.1, or for the Catalyst 9162I with Cisco IOS XE Releases 17.9.2/17.10.1.
- Support for enabling Scan and Transmit mode at the same time for the IoT radio is available starting with Cisco IOS XE Release 17.9.1.

The figure below depicts the telemetry data received from a BLE device that is decoded in Cisco Spaces.



#### Figure 68.

BLE telemetry data on Cisco Spaces

The figure below depicts how BLE data is sent from the Catalyst 9162I, 9164I, and 9166I to Cisco Spaces.



#### Figure 69.

IoT radio on the Catalyst 9162I, 9164I, and 9166I topology

Both the environmental sensors and IoT radio require Cisco Spaces and IoT Services to be configured. Please use the following guides for configuring Cisco Spaces and IoT Services.

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/DNA-Spaces/cisco-dna-spacesconfig/dnaspaces-configuration-guide.html

https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/iot-services/b\_iot\_services.html

To enable the IoT radio or environmental sensors in Cisco Spaces, go to the specific access point in IoT Services in Cisco Spaces and select the feature to turn on or bulk-enable each feature in the AP Beacons page.

The figures below depict how to enable or disable the IoT radio or environmental sensors on Cisco Spaces through a specific access point.

<b>Cisco</b> DNA Spaces									
Cisco DNA Spaces	IoT Services								
🔂 Home	Device Management								
Cocation Hierarchy	Device Monitoring								
Integrations >									
🗠 Monitor									
Admin Management									
loT Services >									
ې Setup ک									

#### Figure 70.

Cisco Spaces IoT Services



#### Figure 71.

Cisco Spaces AP Beacons within IoT Services

Floor Beacons	AP Beacons Wired	d Devices 🚺	
All Campuses	~		
All Profiles 4	Sensor AP Sensors 9	Tr IBeacon O	ansmit
Disabled O AP Name contains 9166 ×	Save as New	Bulk Request H	istory
Mac Address	AP Name 🔺	BLE	AP Model
10:f9:20:fe:83:a0	AP-SJC14-F1-9166-01	✓ Enabled	CW9166I-B

### Figure 72.

IoT Services AP profiles

✓ Settings			
Sensor			
BLE			
BLE mode			
s	Scan Scans for nearby bluetooth devices	$\oslash$	
T	Transmit Only does beacon transmitting	Enable	
D	Dual Does both Scan & Transmit	Enable	

## Figure 73.

Enabling sensor or BLE functionality on the Catalyst 9166l or 9164l in Cisco Spaces

The figures below depict how to bulk-enable or disable the IoT radio or environmental sensors in Cisco Spaces on the AP Beacons page.



#### Figure 74.

Cisco Spaces IoT Services

Home	Devices	Groups	Policies	Settings
Floor Be	acons A	P Beacons	Wired Dev	vices ()

#### Figure 75.

Cisco Spaces AP Beacons within IoT Services

F100	r Beacons A	P Beacons	Wired Devices ()		
All Cam	puses	×			
		Sen	sor	Transmit	Trans
All Profil	es	AP Sensors	IBeacon		Eddystone U
7		9	0		0
O AP Name co List View	ntains <b>916</b> × Sa Map View	ve as New ∑ Filters Ar	tions 🛩 Bulk Request I	listory	
	Mac Address				
		AP Name	Manage BLE >	AP Model	Profile Type
	10:f9:20:fe:9b:40	AP-SJC14	Manage BLE > Manage Sensors >	AP Model CW9164I-B	Profile Type Scan
	10:f9:20:fe:9b:40 10:f9:20:fe:a3:80	AP-SJC14	Manage BLE     >       Manage Sensors     >       Manage Profile     >       Add Attributes     >	AP Model CW9164I-B CW9164I-B	Profile Type Scan Scan
	10.f9:20:fe:9b:40 10.f9:20:fe:a3:80 10.f9:20:fe:9a:a0	AP-SJC14 AP-SJC14 AP-SJC14	Manage BLE     >       Manage Sensors     >       Manage Profile     >       Add Attributes     >	AP Model CW9164I-B CW9164I-B CW9164I-B	Profile Type Scan Scan Scan

#### Figure 76.

Cisco Spaces bulk-enable or disable of BLE or sensor capabilities

The figure below depicts the Cisco Spaces Smart Workspaces application and how the environmental sensor data and BLE IoT integration would be used within the application.



#### Figure 77. Cisco Spaces Smart Workspaces

To learn more about Smart Workspaces or to request a demo, visit <u>https://dnaspaces.cisco.com/smart-workspaces/</u>

## **Environmental sensors and IoT radio without Cisco Spaces**

Users can utilize model-driven telemetry to subscribe to environmental sensor data on the Catalyst 9166I and subscribe to BLE device data that is captured from the Catalyst 9162I, 9164I, and 9166I access points via YANG with gRPC, gNMI, or NETCONF.

The environmental sensors and IoT radio can be turned on manually on the access point through the wireless controller via the AP join profile. A user can create IETF telemetry subscriptions in the WLC to send telemetry data to a receiver such as Telegraf. The receiver will then be able to get the environmental sensor data or BLE device data from the WLC and send that data to the appropriate forums for use.

The figure below depicts how BLE data is sent from the Catalyst 9162l, 9164l, and 9166l to a wireless controller and then to an administrator.



#### Figure 78. Model-driven telemetry

The figure below depicts an example of how to create an IETF telemetry subscription on the wireless controller.



#### Figure 79.

Wireless controller IETF telemetry subscription example

Here is a breakdown of what these commands are doing in the figure above:

**telemetry ietf subscription 20:** This is the subscription ID that groups together all the config to stream one set of data.

**encoding encode-kvgpb:** This matches the encoding specified inside "cisco\_telemetry\_mdt" that is used by the receiver. KVGPB stands for Key Value Google Protocol Buffer.

**filter xpath /wireless-access-point-oper:access-point-oper-data/ap-temp:** This is the data we want to send; it is the xpath for the AP temperature data.

**source-address 172.16.99.3:** This is where we want to send the data from, that is, the wireless controller's management interface.

stream yang-push: Stream the data using YANG.

update-policy periodic 5000: Send new data every 5 seconds.

**receiver ip address 172.16.99.3 57500 protocol grpc-tcp:** Send the data to the receiver (172.16.99.3) on the port that receiver is listening on (TCP 57500) using grpc-tcp.

We can similarly create this subscription for other data coming from the wireless controller, including the air quality data and BLE data.

The figure below depicts how to enable the environmental sensors on an AP join profile.

# Enabling the Air Quality and Temperature Sensor on AP Join Profile 9800# conf t 9800(config)# ap profile default-ap-profile 9800(config-ap-profile)# sensor environment air-quality 9800(config-ap-profile)# sensor environment temperature

#### Figure 80.

Telemetry data AP profile configuration

Once the air quality and temperature sensor are enabled, the user can create IETF telemetry subscriptions pointing to their specific receiver and be able to get the raw data coming from the environmental sensors.

The xpath for the air quality data is: /wireless-access-point-oper:access-point-oper-data/ap-air-quality

The xpath for the temperature data is: wireless-access-point-oper:access-point-oper-data/ap-temp

The figure below depicts sample temperature data coming from the Catalyst 9800 wireless controller and collected from the Catalyst 9166l environmental sensor.



#### Figure 81.

Temperature telemetry data output

The figure below depicts sample air quality data coming from the Catalyst 9800 wireless controller and collected from the Catalyst 9166l environmental sensor.



#### Figure 82.

Air quality telemetry data output

The figure below depicts how to enable the BLE radio on a wireless controller.

## Enabling the BLE Radio on the Wireless Controller

## 9800# conf t 9800(config)# no ap dot15 shutdown

#### Figure 83.

Enabling the BLE radio on the wireless controller

Once the BLE radio is enabled on the wireless controller and the access point, the user can create IETF telemetry subscriptions pointing to their specific receiver and be able to get the raw data coming from the surrounding BLE sensors that are scanned by the access point's BLE radio.

The xpath for the BLE data is: wireless-ble-ltx-oper:ble-ltx-oper-data/ble-ltx-ap-streaming.

The figure below depicts sample BLE data coming from the Catalyst 9800 wireless controller and collected from the Catalyst 9162I, 9164I, or 9166I IoT radio.



Figure 84. BLE telemetry data output For more information on programmability and model-driven telemetry, refer to the configuration guide: <u>https://www.cisco.com/c/en/us/td/docs/ios-</u>

xml/ios/prog/configuration/178/b 178 programmability cg/m 178 prog ietf telemetry.html

## **Enterprise wireless IoT with application hosting**

The Catalyst 9162I, 9164I, and 9166I allow users to load Cisco IOx applications onto the platform to solve IoT use cases by acting as an IoT gateway. These IOx applications can communicate with an RF-USB dongle connected to the USB port of the AP and talk to the surrounding IoT devices. IoT device data is then sent through the AP and to a back-end server. With the Catalyst 9162I, 9164I, and 9166I, the USB port outputs a total of 4.5 watts of power.

Use cases for application hosting include retail management with electronic shelf labels, asset management with environmental sensors and real-time location, and medical management with tracking of patient vitals.

The figure below depicts the basic topology of application hosting with the Catalyst 9162I, 9164I, and 9166I.



#### Figure 85.

Application hosting

Support for the IOx framework on the Catalyst 9164I and 9166I is available starting with Cisco IOS XE Release 17.9.1 and Cisco DNA Center Release 2.3.4. Support for the IOx framework on the Catalyst 9162I is available starting with Cisco IOS XE Release 17.9.2/17.10.1 and Cisco DNA Center Release 2.3.5.

For more information on application hosting, refer to the deployment guide: <u>https://www.cisco.com/c/en/us/products/collateral/wireless/access-points/guide-c07-744305.html</u>

## Site Survey mode

The Cisco Catalyst 9162I, 9164I, and 9166I support a new mode called Site Survey. The purpose of this mode is to allow users to conduct wireless site survey testing using a single access point, including understanding RF propagation, client join metrics, and so on, without the need for a controller. This mode converts the AP into a limited standalone mode, enabling it to broadcast 2.4-, 5-, and 6-GHz SSIDs. Site Survey mode provides all the control needed to configure and conduct a site survey while reducing the additional equipment required to a power source (battery or PoE switch port). It lets users bring the AP into any environment with either a power source or battery backup and conduct a site survey test.

When the Catalyst 9162I, 9164I, or 9166I is in Site Survey mode, you will be able to access the AP's WebUI for each configuration and view various RF metrics for RF coverage and planning.

These configurations include channel number, channel width, Tx power, SSID, and data rates.

altala cisco	Cisco Access	Point WebUI			Home	Configuration	Event log	02 0
System 2.4GHz 5GHz 6GHz	Cor Log User Pass	nfiguration in name add word	Imin	]				Apply
SSID	Radi Radio Statu	io o Interface 5G us En	Shz					
DHCP	Powe 802.	er Type PoE 11 n-mode En	E/25.5 W power mode nabled V					
васкир/н	802.1 802.1 Band	11 ac-mode En 11 ax-mode En width 80	nabled V nabled V					
	Chan Tx-Po	inel Selection Au ower Level 1	uto V					
	Data 6 Mb	a Rates ps Ma	andatory ~					
	9 Mb 12 M 18 M	ps Su bps Ma bos Su	andatory ~					
	24 M 36 M	bps Ma bps Su	andatory ~ upported ~					
	48 M 54 M	bps Su bps Su	upported V					
	62010 - 202	2 Cisco Systems Inc. All rights reserved.						

#### Figure 86.

Configuration page of the Catalyst 9162I, 9164I, and 9166I in Site Survey mode

The steps below describe how to convert a Catalyst 9162I, 9164I, or 9162I AP into Site Survey mode:

1. Change the AP to Site Survey mode (Run command on the AP's CLI):

ap-type site-survey

- 2. After booting up, the AP is automatically assigned a static IP of 10.0.23.1.
- The AP will start broadcasting the C9166\_site\_survey SSID if it's a Catalyst 9166I, C9164\_site\_survey SSID if it's a Catalyst 9164I, or C9162\_site\_survey SSID if it's a Catalyst 9162I with open authentication security.
- 4. Connect your wireless client with the C9166\_site\_survey, C9164\_site\_survey SSID, or C9162\_site\_survey SSID and it will receive an IP from 10.0.23.0/24.
- 5. Access the AP's Site Survey WebUI via 10.0.23.1.
- 6. The first time, the default username and password are admin/admin. You will be directed to reset that insecure password on the first login.

7. When done, convert your AP back to CAPWAP mode to join the controller again (AP CLI):

## ap-type capwap

If an AP is converted to Site Survey mode while connected to a WLC, it will disjoin and go into standalone mode.

## Antenna patterns



#### Figure 87.

2.4-GHz client-serving radio (slot 0) for Catalyst 9164I and 9166I



#### Figure 88.





#### Figure 89.

5-GHz client-serving radio (slot 2) for Catalyst 91661



#### Figure 90.





#### Figure 91.

2.4-GHz AI/ML-driven scanning radio for Catalyst 9164I and 9166I


### Figure 92.





#### Figure 93.

6-GHz AI/ML-driven scanning radio for Catalyst 9164I and 9166I



### Figure 94.





### Figure 95.

2.4-GHz client-serving radio (slot 0) for Catalyst 91621



### Figure 96.

5-GHz client-serving radio (slot 1) for Catalyst 9162I



### **Figure 97.** 6-GHz client-serving radio (slot 2) for Catalyst 91621



### Figure 98.





## Figure 99.

5-GHz AI/ML-driven scanning radio for Catalyst 9162I



### Figure 100.

6-GHz AI/ML-driven scanning radio for Catalyst 9162I



### Figure 101. 2.4-GHz IoT radio for Catalyst 9162I

# Software solution compatibility

This section lists the software features and their versions compatible with the Cisco Catalyst 9162I, 9164I, and 9166I access points.

Access points	Cisco IOS XE	AireOS	Cisco DNA Center	Cisco Prime	СМХ	Cisco Spaces Connector	ISE
Catalyst 91621	17.9.2/17.10.1	-	2.3.5	3.10	10.6.3	2.3.2	2.6
Catalyst 9166l/9164l	17.9.1	-	2.3.4	3.10	10.6.3	2.3.2	2.6
91361	17.7.1	-	2.3.2	3.10	10.6.3-75	2.3.2	2.6
9130AXE	17.1.1	8.10MR1	1.3.2	3.7	10.6.2	2.3.2	2.3 2.4 2.6
9130AXI	16.12.1s with AP DP	8.10	1.3.1.2	3.7	10.6.2	2.3.2	2.3 2.4 2.6
9120AXE, 9120AXP	16.12.2	8.10	1.3.2	3.7	10.6.2	2.3.2	2.3 2.4 2.6
9115AX, 9120AXI	16.12.1s	8.9.111	1.3.1.2	3.7	10.6.2	2.3.2	2.3 2.4 2.5
9105AX Series	17.3	8.10 (MR3)	2.1.2.0	3.9	10.6.2 (MR2)	2.3.2	2.4 2.6 2.7
Wave 2 APs	16.12.1s	8.5MR5	1.3.1.2	3.7	10.6.2	2.3.2	2.3 2.4 2.6

 Table 10.
 Software support matrix

Feature	Cisco IOS XE version	Cisco DNA Center version	Cisco Spaces Connector version	Meraki	Notes
FRA: Dual 4x4:4SS 5- GHz radios (slots 1 and 2)	17.9.x	-	-	Flex Radio	Applicable only to Catalyst 9166I (and MR57 for Meraki)
Temperature, humidity, air quality sensors	17.9.1	-	2.3.2	MT Series*	*Discrete sensors in Meraki
CleanAir Pro/Spectrum Analysis (Intelligent Capture)	17.9.1	2.3.4	-	Spectrum Analyzer/ Packet Capture (PCAP)	No anomaly PCAP support available in Meraki management mode
Rogue management with AI/ML-driven scan radio	17.9.1	2.3.4	-	Air Marshal	
aWIPS with AI/ML- driven scan radio	17.9.1	2.3.4	-	Air Marshal	
Application hosting	17.9.1	2.3.4	-	-*	*USB support available for select partners
FastLocate	17.9.1	-	2.3.2	Location Analytics	
BLE	17.9.1*	-	2.3.2	Scanning API/MQTT	*Some BLE data can also be subscribed from the WLC through YANG
Zero-Wait Dynamic Frequency Selection	Roadmap	-	-	-	
Al-Enhanced RRM (6 GHz)	17.9.1	2.3.4	-	Auto RF	
Mesh	Roadmap	Roadmap	-	Yes (indoor mesh*)	Meraki Mesh is the default mesh for the Meraki management mode
Work Group Bridge	Roadmap	-	-	-	

### Table 11. Cisco Catalyst 9164I and 9166I feature release timelines

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Network Assurance	2.3.4	AireOS	-	-
		Cisco IOS XE	17.9.1	Local, Cisco FlexConnect®, fabric
Application Experience	2.3.4	AireOS	-	-
Experience		Cisco IOS XE	17.9.1	Local (FlexConnect and fabric support are on roadmap)
Application Visibility	2.3.4	AireOS	-	-
		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric
Rogue	2.3.4	AireOS	-	-
(with CleanAir)		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric
aWIPS	2.3.4	AireOS	-	-
(with CleanAir)		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric
Wi-Fi 6 dashboard	2.3.4	AireOS	-	-
		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric
Wireless Network Service Analytics	2.3.4	AireOS	-	-
·····, ····		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric
Wireless 3D maps	Roadmap	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric
True Trace	2.3.4	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric
Webex <sup>®</sup> 360	2.3.4	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.1	Local, FlexConnect, fabric

### Table 12. Wireless Assurance compatibility matrix for the Catalyst 9164I and 9166I

Feature	WLC hardware	WLC software	Cisco DNA Center	AP modes
AI-driven issues	AireOS	_	-	
	Cisco IOS XE	17.9.1	2.3.4.0	
Network Insights	AireOS	-	-	
	Cisco IOS XE	17.9.1	2.3.4.0	
Heatmaps	AireOS	-	-	
	Cisco IOS XE	17.9.1	2.3.4.0	
Peer Comparison	AireOS	-	-	Local, FlexConnect, fabric
	Cisco IOS XE	17.9.1	2.3.4.0	
Network Comparison	AireOS	-	-	
(previously called Site Comparison)	Cisco IOS XE	17.9.1	2.3.4.0	
Al-driven baselines	AireOS	-	-	
	Cisco IOS XE	17.9.1	2.3.4.0	

### Table 13. AI Network Analytics compatibility matrix for the Catalyst 9164I and 9166I

 Table 14.
 Client Analytics compatibility matrix for the Catalyst 9164I and 9166I

Feature	Cisco DNA Center	WLC	Software version
Apple Analytics	2.3.4	AireOS	-
			17.9.1
Samsung Analytics	2.3.4	AireOS	-
		Cisco IOS XE	17.9.1
Intel <sup>®</sup> Connectivity Analytics	Roadmap	AireOS	-
		Cisco IOS XE	17.9.1

### Table 15. Intelligent Capture compatibility matrix for the Catalyst 9164I and 9166I

Feature	Cisco DNA Center	WLC	Software version
Anomaly PCAP	2.3.4	AireOS	-
Scheduled PCAP AP and client statistics		Cisco IOS XE	17.9.1
Data PCAP	2.3.4	AireOS	-
		Cisco IOS XE	17.9.1
Spectrum Analysis	2.3.4	AireOS	-
		IOS XE	17.8.1

Table 16.	Wireless automation	compatibility matrix for the	Catalyst 9164I and 9166I

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Wireless provisioning	2.3.4	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.1	
Cisco Umbrella <sup>®</sup>	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
Cloud Device Provisioning	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
SD-Access	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
Wide Area Bonjour	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
User Defined Network	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
Command Runner	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
AP Plug and Play	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Software Image Management	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
Cisco Secure Network	Roadmap	AireOS	-	
, indigited		Cisco IOS XE	17.9.1	
Application hosting	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
Application policy	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
Ekahau integration	Roadmap	AireOS	-	
		Cisco IOS XE	17.9.1	
Security advisories	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	

**Table 17.** Policy application compatibility matrix for the Catalyst 9164I and 9166I

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Group-Based Access Control	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	
AI Endpoint Analytics	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	Least FlavConnect fabric
Group-Based Policy Analytics	2.3.4	AireOS	-	Local, FlexConnect, Tablic
		Cisco IOS XE	17.9.1	
Policy Analytics Dashboard	2.3.4	AireOS	-	
		Cisco IOS XE	17.9.1	

Feature	Cisco Spaces Connector	Cisco Prime	Cisco DNA Center	WLC hardware	WLC software	Meraki	AP modes
Wi-Fi location	2.3.2	3.10.1	2.3.4	AireOS	-	Yes	
				Cisco IOS XE	17.9.1		
FastLocate	2.3.2	3.10.1	2.3.4	AireOS	-	Yes	
				Cisco IOS XE	17.9.1		
<b>BLE location</b>	2.3.2	3.10.1	2.3.4	AireOS	-	Yes	
				Cisco IOS XE	17.9.1		
BLE	2.3.2	-	-	AireOS	-	Yes	
(Advanced Gateway)				Cisco IOS XE	17.9.1		
Concurrent BLE	2.3.2	-	-	AireOS	-	_	
transmit				Cisco IOS XE	17.9.1		Local, FlexConnect, fabric
IoT sensors	2.3.2	-	-	AireOS	-	MT Series	
				Cisco IOS XE	17.9.1		
Analytic	2.3.2	-	-	AireOS	-	Analytic	
(Behavior Metrics, Location Analytics, Right Now, Impact Analysis				Cisco IOS XE	17.9.1	approvidence	
Proximity	2.3.2	-	-	AireOS	-	Location	
Reporting				Cisco IOS XE	17.9.1	Analytics	
OpenRoaming	2.3.2	3.10.1	2.3.4	AireOS	Roadmap	OpenRoaming	
				Cisco IOS XE	17.9.1		
Detect and	2.3.2	3.10.1	2.3.4	AireOS	-	Location	
				Cisco IOS XE	17.9.1	nouthap	
Captive portals	2.3.2	3.10.1	2.3.4	AireOS	-	Captive	
				Cisco IOS XE	17.9.1	P 91 610	

### Table 18. Cisco Spaces compatibility matrix for the Catalyst 9164l and 9166l

Feature	Cisco IOS XE version	Cisco DNA Center version	Cisco Spaces Connector version	Meraki	Notes
CleanAir Pro/Spectrum Analysis (Intelligent Capture)	17.9.2/17.10.1	2.3.5	-	Spectrum Analyzer/Packet Capture (PCAP)	No anomaly PCAP support available in Meraki management mode
Rogue management with AI/ML-driven scan radio	17.9.2/17.10.1	2.3.5	-	Air Marshal	
aWIPS with AI/ML- driven scan radio	17.9.2/17.10.1	2.3.5	-	Air Marshal	
Application hosting	17.9.2/17.10.1	2.3.5	-	-*	*USB support available for select partners
FastLocate	17.9.2/17.10.1	-	2.3.2	Location Analytics	
BLE	17.9.2/17.10.1	-	2.3.2	Scanning API/MQTT	*Some BLE data can also be subscribed from the WLC through YANG
Zero-Wait Dynamic Frequency Selection	Roadmap	-	-	-	
Al-Enhanced RRM (6 GHz)	17.9.2/17.10.1	2.3.5	-	Auto RF	
Mesh	Roadmap	Roadmap	-	Yes (indoor mesh*)	Meraki Mesh is the default mesh for the Meraki management mode
Work Group Bridge	Roadmap	-	-	-	

### Table 19. Cisco Catalyst 9162I feature release timelines

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Network Assurance	2.3.5	AireOS	-	-
		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
Application Experience	2.3.5	AireOS	-	-
Experience		Cisco IOS XE	17.9.2/17.10.1	Local (FlexConnect and fabric support are on roadmap)
Application Visibility	2.3.5	AireOS	-	-
		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
Rogue	2.3.5	AireOS	-	-
(with CleanAir)		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
aWIPS	2.3.5	AireOS	-	-
(with CleanAir)		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
Wi-Fi 6 dashboard	2.3.5	AireOS	-	-
		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
Wireless Network Service Analytics	2.3.5	AireOS	-	-
		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
Wireless 3D maps	Roadmap	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
True Trace	2.3.5	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric
Webex 360	2.3.5	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.2/17.10.1	Local, FlexConnect, fabric

### Table 20. Wireless Assurance compatibility matrix for the Catalyst 9162I

Table 21.	Al Network	Analytics	compatibility	matrix for the	Catalyst 9162
			00111001101		00.00.9000.01

Feature	WLC hardware	WLC software	Cisco DNA Center	AP modes
AI-driven issues	AireOS	-	-	
	Cisco IOS XE	17.9.2/17.10.1	2.3.5.0	
Network Insights	AireOS	-	-	
	Cisco IOS XE	17.9.2/17.10.1	2.3.5.0	
Heatmaps	AireOS	-	-	
	Cisco IOS XE	17.9.2/17.10.1	2.3.5.0	
Peer Comparison	AireOS	-	-	Local, FlexConnect, fabric
	Cisco IOS XE	17.9.2/17.10.1	2.3.5.0	
Network Comparison	AireOS	-	-	
(previously called Site Comparison)	Cisco IOS XE	17.9.2/17.10.1	2.3.5.0	
AI-driven baselines	AireOS	-	-	
	Cisco IOS XE	17.9.2/17.10.1	2.3.5.0	

 Table 22.
 Client Analytics compatibility matrix for the Catalyst 9162I

Feature	Cisco DNA Center	WLC	Software version
Apple Analytics	2.3.5	AireOS	-
		Cisco IOS XE	17.9.2/17.10.1
Samsung Analytics	2.3.5	AireOS	-
		Cisco IOS XE	17.9.2/17.10.1
Intel Connectivity Analytics	Roadmap	AireOS	-
		Cisco IOS XE	17.9.2/17.10.1

### Table 23. Intelligent Capture compatibility matrix for the Catalyst 9162I

Feature	Cisco DNA Center	WLC	Software version
Anomaly PCAP	2.3.5	AireOS	-
Scheduled PCAP AP and client statistics		Cisco IOS XE	17.9.2/17.10.1
Data PCAP	2.3.5	AireOS	-
		Cisco IOS XE	17.9.2/17.10.1
Spectrum Analysis	2.3.5	AireOS	-
		IOS XE	17.9.2/17.10.1

Table 24.	Wireless	automation	compatibility	/ matrix	for the	Catalys	t 9162
	VVII CIC33	automation	compationity	/ maun	ior the	Oatarys	1 31021

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Wireless provisioning	2.3.5	AireOS	-	Local, FlexConnect, fabric
		Cisco IOS XE	17.9.2/17.10.1	
Cisco Umbrella	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Cloud Device Provisioning	2.3.5	AireOS	-	
approation		Cisco IOS XE	17.9.2/17.10.1	
SD-Access	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Wide Area Bonjour	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
User Defined Network	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Command Runner	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
AP Plug and Play	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Software Image Management	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Cisco Secure Network	Roadmap	AireOS	-	
, and y loo		Cisco IOS XE	17.9.2/17.10.1	
Application hosting	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Application policy	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Ekahau integration	Roadmap	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Security advisories	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	

**Table 25.** Policy application compatibility matrix for the Catalyst 91621

Feature	Cisco DNA Center	WLC hardware	WLC software	AP modes
Group-Based Access Control	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
AI Endpoint Analytics	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	Local ElexConnect fabric
Group-Based Policy Analytics	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	
Policy Analytics Dashboard	2.3.5	AireOS	-	
		Cisco IOS XE	17.9.2/17.10.1	

Feature	Cisco Spaces Connector	Cisco Prime	Cisco DNA Center	WLC hardware	WLC software	Meraki	AP modes	
Wi-Fi location	2.3.2	3.10.1	2.3.5	AireOS	-	Yes		
				Cisco IOS XE	17.9.2/17.10.1			
FastLocate	2.3.2	3.10.1	2.3.5	AireOS	-	Yes		
				Cisco IOS XE	17.9.2/17.10.1			
<b>BLE location</b>	2.3.2	3.10.1	2.3.5	AireOS	-	Yes		
				Cisco IOS XE	17.9.2/17.10.1			
BLE management	2.3.2	-	-	AireOS	-	Yes		
(Advanced Gateway)				Cisco IOS XE	17.9.2/17.10.1			
Concurrent BLE scan and	2.3.2	-	-	AireOS	-	_		
transmit				Cisco IOS XE	17.9.2/17.10.1			
IoT sensors	2.3.2	-	-	AireOS	-	MT Series		
				Cisco IOS XE	17.9.2/17.10.1		Local, FlexConnect, fabric	
Analytic applications	2.3.2	-	-	AireOS	-	Analytic		
(Behavior Metrics, Location Analytics, Right Now, Impact Analysis				Cisco IOS XE	17.9.2/17.10.1	applications		
Proximity	2.3.2	-	-	AireOS	-	Location		
Reporting				Cisco IOS XE	17.9.2/17.10.1	Analytics		
OpenRoaming	2.3.2	3.10.1	2.3.5	AireOS	Roadmap	OpenRoaming		
				Cisco IOS XE	17.9.2/17.10.1			
Detect and	2.3.2	3.10.1	2.3.5	AireOS	-	Location		
				Cisco IOS XE	17.9.2/17.10.1			
Captive portals	2.3.2	3.10.1	2.3.5	AireOS	-	Captive		
				Cisco IOS XE	17.9.2/17.10.1	1		

Table 26.	Cisco	Spaces	compatibility	v matrix	for the	Catalyst 9	91621

### **Useful links**

- <u>Catalyst 9166 Series data sheet</u>
- <u>Catalyst 9164 Series data sheet</u>
- <u>Catalyst 9162 Series data sheet</u>
- What Is Wi-Fi 6E?
- Getting Started
- <u>Catalyst 9800 Deployment Guide</u>
- WPA3 Guide

Americas Headquarters Cisco Systems, Inc.

San Jose, CA

Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA