The bridge to possible

Cisco Wireless CW9176 Deployment Guide

Cisco Wireless CW9176x Overview

The Cisco Wireless CW9176x is Cisco's high end Wi-Fi 7 Access Point Platform with an hexa radio architecture providing the full capability of Wi-Fi 7 Features based on 802.11be amendment such as 4K Modulation, Multi Link Operation (MLO), 320 MHz channel width, Pre-amble puncturing, Multi Resource Units, compressed block ack enhacements of upto 512 MPDUs and Wi-Fi Protected Access 3 (WPA3) security, all while being able to leverage advanced RF visibility with Cisco CleanAir® Pro together with an artificial intelligence and machine learning (AI/ML)-driven scanning radio.

The Cisco Wireless CW9176x is a Unified Product with one SKU, that can be deployed with a Cisco Catalyst Wireless LAN Controller or Meraki Cloud based deployments. The CW9176x access can be deployed anywhere in the world just with the single SKU and avoids the need to buy a region or country specific SKU based on regulatory domain.

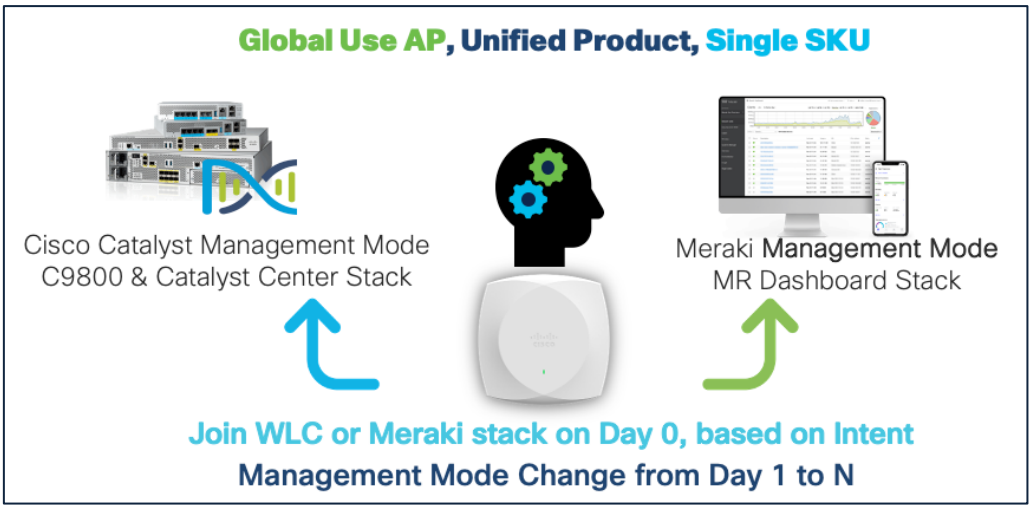


Figure 1. Global Use AP - Management Mode

The Cisco Wireless CW9176x supports the entire Cisco Catalyst wireless stack functionality with Cisco Catalyst Center (Automation and Assurance), Cisco Spaces (Location and IoT), Identity Services Engine (security), and more. Throughout this guide, you will learn how the CW9176x is a wireless powerhouse that can take your network to the next level.

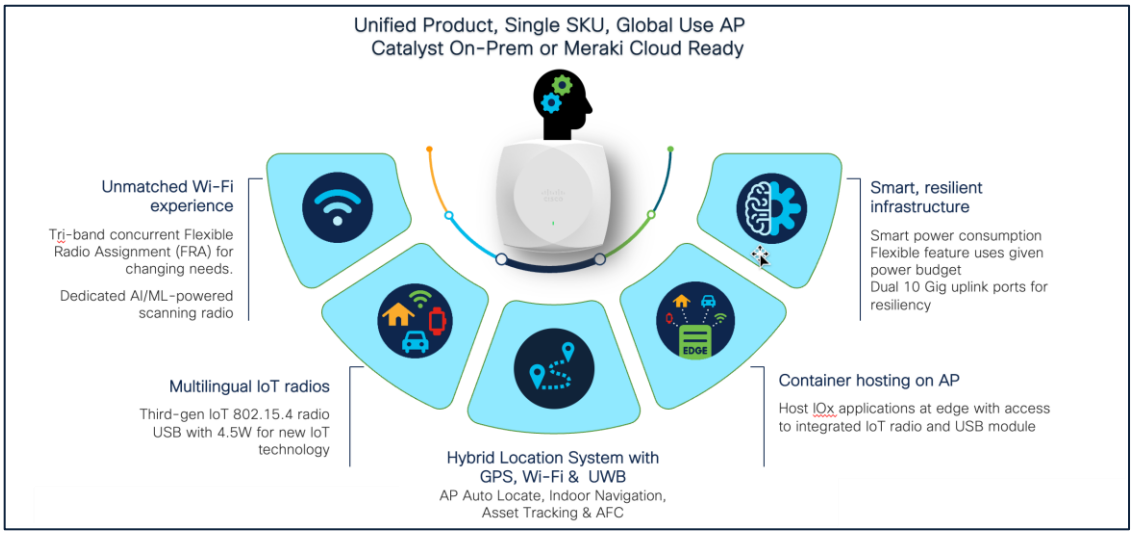


Figure 2. Global Use AP – Controller Stack Agnostic

Table 1. Cisco® Catalyst® Wireless 9800 Series controller software support matrix

Supported IOS XE releases
Cisco IOS XE 17.15.2 and later

Supported Controller platforms

CW9176x APs are supported with the following Catalyst 9800 Series Controllers:

- 9800-H1
- 9800-H2
- 9800-M
- 9800-80
- 9800-40
- 9800-L
- 9800-CL

Note: Embedded wireless controller on AP (EWC) functionality is not supported on the CW9176x, both as an active EWC or a subordinate AP.

Technical Specifications

Table 2. CW9176x At a Glance

Capability	Details
Product ID	CW9176x
Scale	1200 Clients (400 clients per radio)
Serving Radio	• 2.4 GHz (Slot 0), 4x4:4 spatial streams • 5 GHz (Slot 1), 4x4:4 spatial streams • 6 GHz (Slot 3), 4x4:4 spatial stream
IoT Capabilities	• Dedicated 2.4 GHz IoT Radio • Application Hosting Capabilities
Scanning Radio	Yes
Wi-Fi 7 Features	• 4K QAM • 320 MHz Channel Width • Multi-Link Operation • Preamble Puncturing • Multi Resource Units • Compressed Block Ack with 512 MPDUs • UL Triggered OFDMA

Capability	Details
Wi-Fi 6 Features	• MU-MIMO • OFDMA • BSS Coloring • TWT
LAN Port	POE-IN 10Gig mGig Port
Ports	mGig, Console
Antenna	Directional, Omnidirectional
Dimensions	9.5x9.5x2.0 inches 24x24x5.1 cm
Weight	3.4 lb (1.56 kg)
USB	9W Output
SSIDs	• 2.4 GHz: 16 • 5 GHz: 16 • 6 GHz: 16
MTBF	• 25° C: 942,282 hrs • 50° C: 332,257 hrs
Environment	• Non-operating (storage) temperature: -22° to 158° F (-30° to 70° C) • Non-operating (storage) altitude test: 25° C (77° F) at 15,000 ft (4570 m) • Operating temperature: 32° to 122° F (0° to 50° C) • Operating humidity: 10% to 90% (noncondensing) • Operating altitude test: 40° C (104° F) at 9843 ft (3000 m)
Antenna Gain	9176I • 2.4 GHz: 5 dBi • 5 GHz: 5 dBi • 6 GHz: 6 dBi 9176D1 • 2.4 GHz: 7 dBi • 5 GHz: 8 dBi • 6 GHz: 8 dBi
Geo Location	Inbuilt GPS/GNSS Module; provision to connect an external GPS/GNSS Antenna.

Table 3. Serving Radio Specifications

Mode	2.4 GHz Slot 0/ 5 GHz Slot 0	Primary 5 GHz (Slot 1)	6 GHz (Slot 2)
Tri-radio, Tri-Band 12SS	• 4x4:4SS • (20 MHz)	• 4x4:4SS • (20/40/80/160 MHz)	• 4x4:4SS • (20/40/80/160/320 MHz)

Mode	2.4 GHz Slot 0/ 5 GHz Slot 0	Primary 5 GHz (Slot 1)	6 GHz (Slot 2)
Tri-radio, Dual Band (Dual 5 GHz), 12SS	• 4x4:4SS • (20/40/80/160 MHz)	• 4x4:4SS • (20/40/80/160 MHz)	• 4x4:4SS • (20/40/80/160/320 MHz)

The Cisco Wireless 9176x is interoperable with the following network management and security solutions.

Table 4. Software Interoperability

Catalyst 9800	Cisco Catalyst Center	Cisco Spaces	ISE
17.15.2	TBD	TBD	TBD

Mechanical Design

The CW9176x has an altogether new design which is aesthetically appealing allowing you to identify it among other APs instantly.

Figure 3. CW9176x - Front and back views

Physical Dimensions

The CW9176x Wi-Fi 7 AP is similar in size and weight to the mid-range and high-end Catalyst Wi-Fi 6 and Wi-Fi 6E APs and smaller and lighter **than** many of the Cisco Catalyst APs prior to Wi-Fi 6. However, it boasts a much more robust hexa-radio architecture, a dedicated scanning radio, a dedicated IoT radio, an inbuilt GPS and GNSS module, Ultra Wide Band Radio, two 10 Gig Multigigabit ports, and supports Wi-Fi 7.

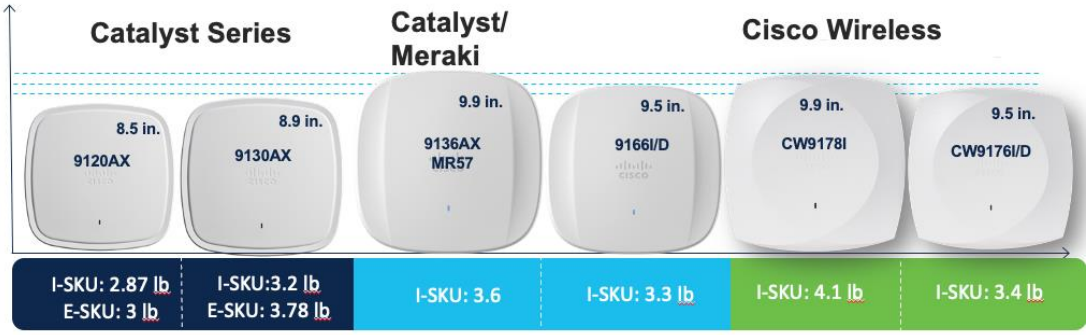


Figure 4. CW9176x showing physical comparison with existing Catalyst APs

Physical Ports

The following figures depict the ports and reset button on the CW9176x:

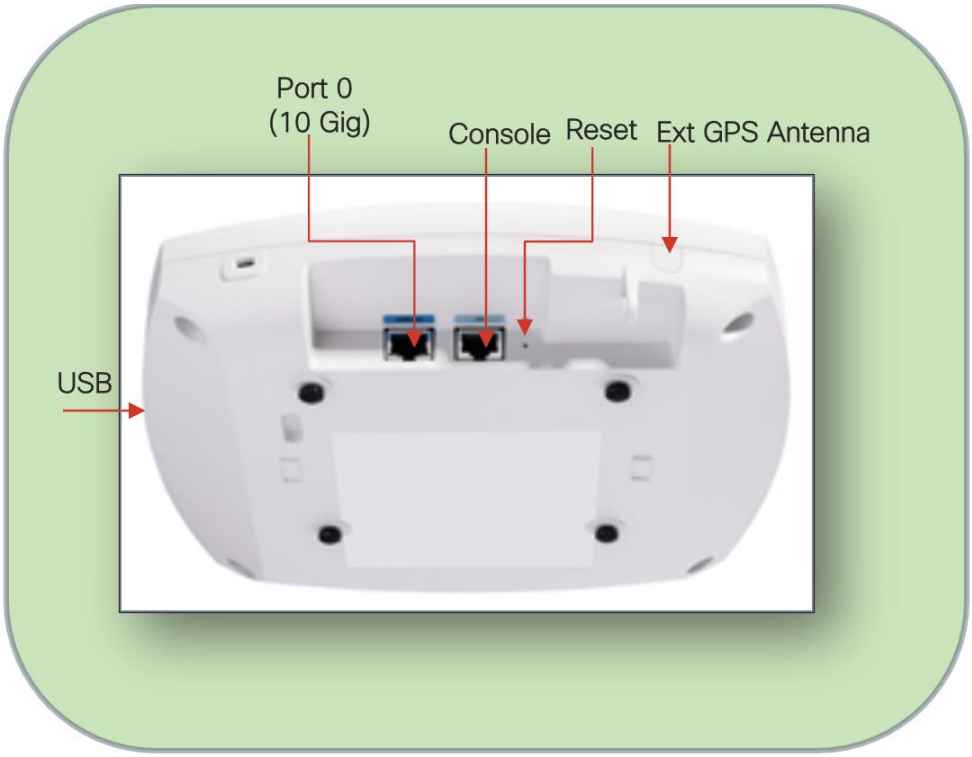


Figure 5. CW9176x Top View with Connectors and Ports

Brackets & Mounting

The CW9176I is compatible with the Cisco Low Profile Mounting Bracket AIR-AP-BRACKET-1 (default option) and Cisco Universal Mounting Bracket AIR-AP-BRACKET-2 mounting brackets. This AP is also compatible with the AIR-AP-T-RAIL-R and AIR-AP-T-RAIL-F for T-rail drop ceiling. 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 CW9176I to be mounted on existing brackets. The CW9176I can be mounted using the AIR-CHNL-ADAPTER clip for channel-rail ceiling grid profiles.

The CW9176D1 uses AIR-AP-BRACKET-2 as the default bracket. While AIR-AP-BRACKET-1 would fit the CW9176D1, that bracket is designed for ceiling mounting and therefore is better suited for the CW9176I, as it's designated for ceiling installations, whereas the CW9176D1 with its directional antenna array is primarily designed for wall mounting.

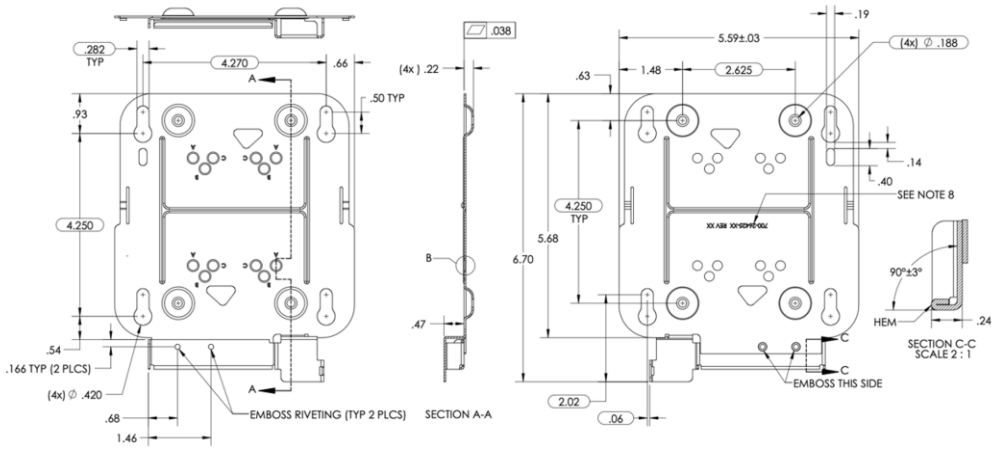
For more details on mounting the access point, refer the following documents:

- Cisco Wireless 9176x Hardware Installation Guide
- Access Point Mounting Instructions

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

AIR-AP-BRACKET-1 photos

Figure 6. Mounting brackets (AIR-AP-BRACKET-1) - front & back views



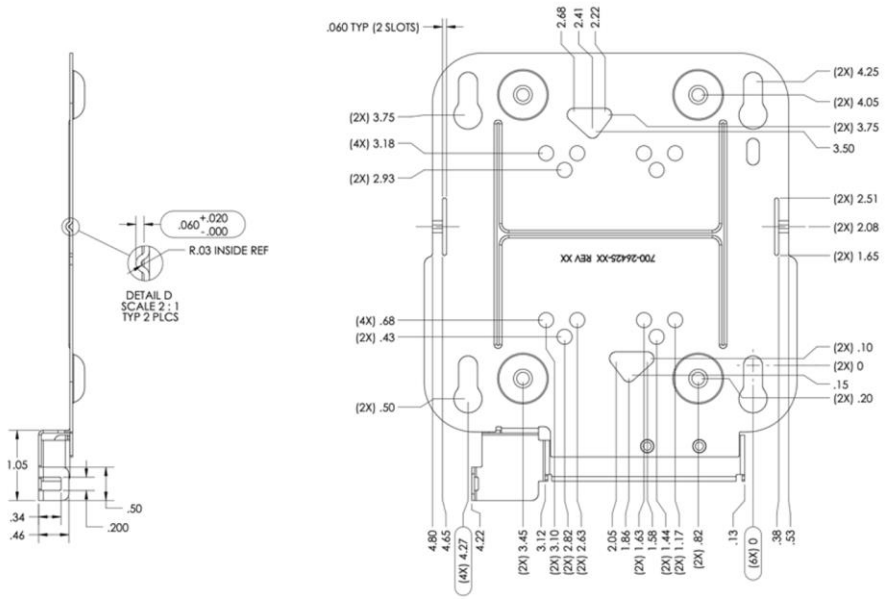


Figure 7. AIR-AP-BRACKET-1 Schematics

AIR-AP-BRACKET-2 photos

Figure 8. Mounting brackets (AIR-AP-BRACKET-2) - front & back views

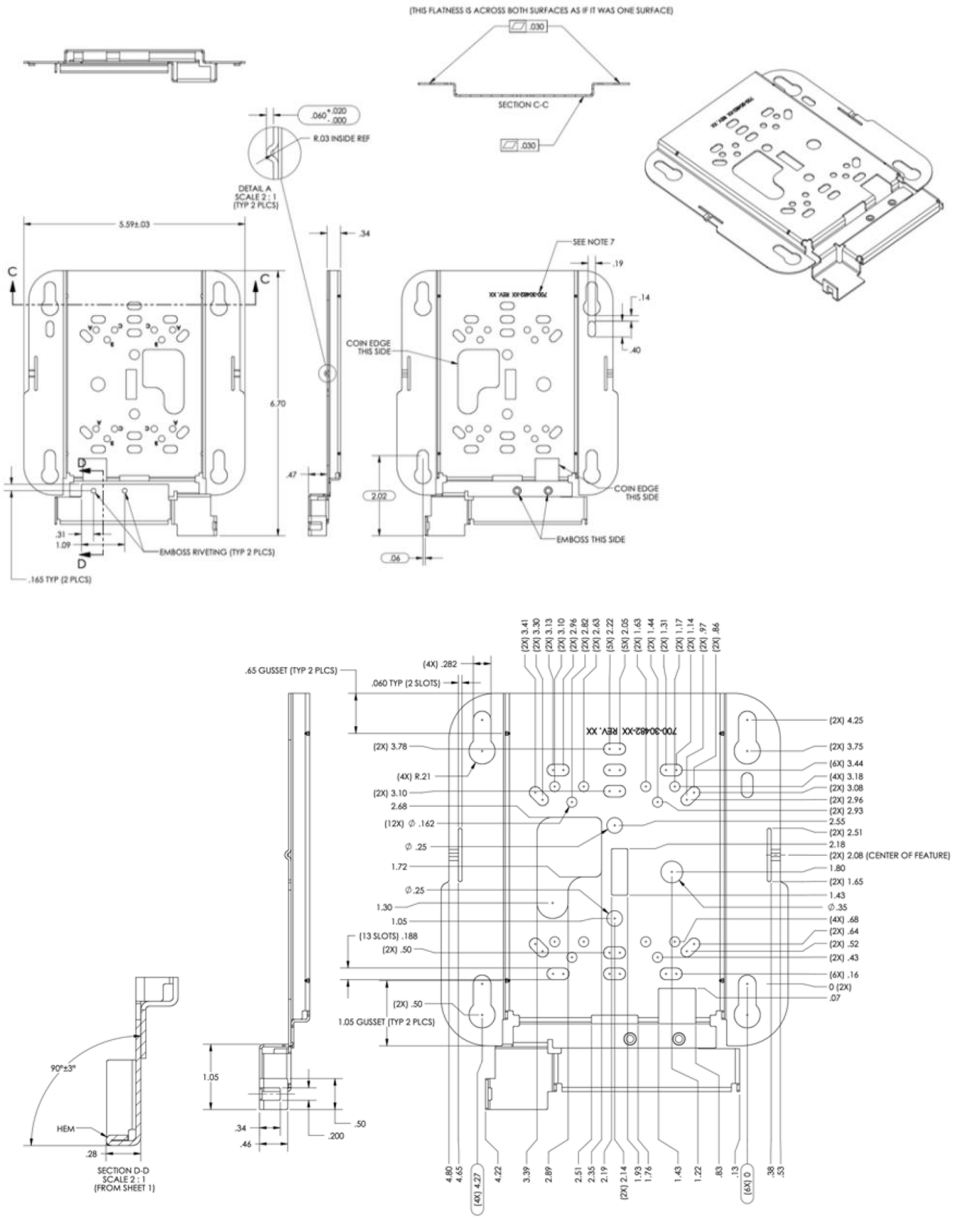
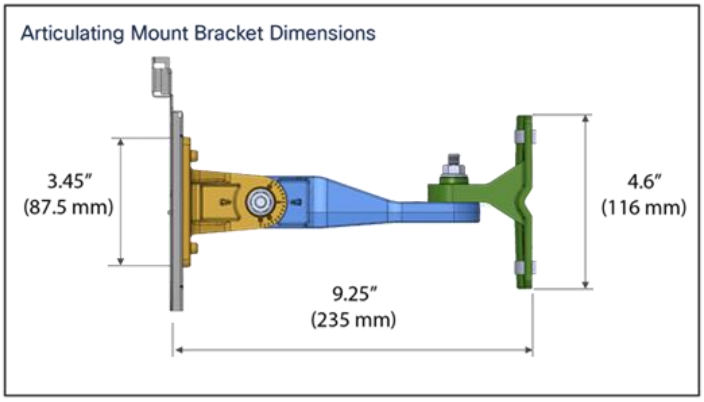


Figure 9. AIR-AP-BRACKET-2 Schematics

Figure 10. Articulating Mount Bracket



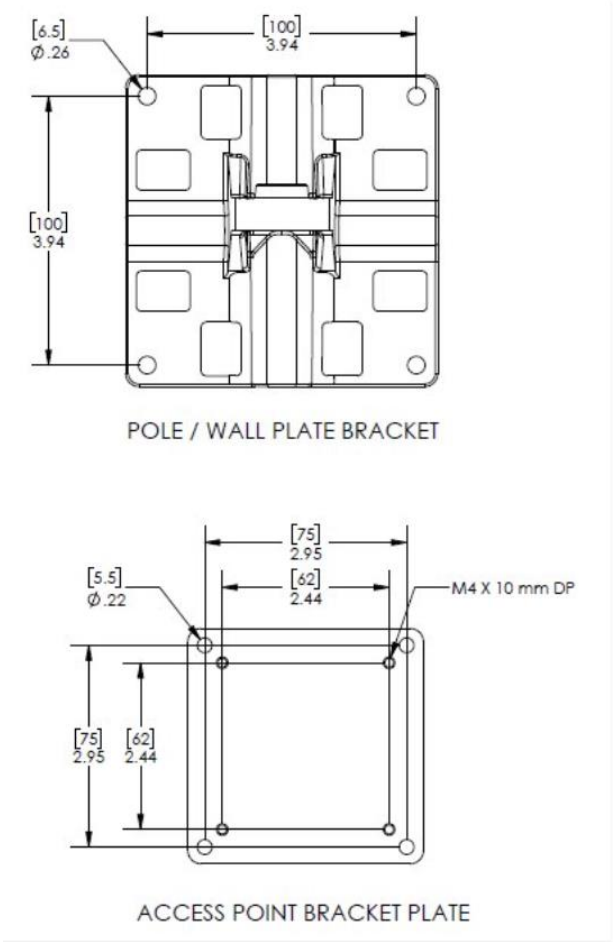


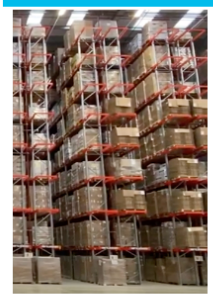
Figure 11. Articulating Mount Bracket Schematics

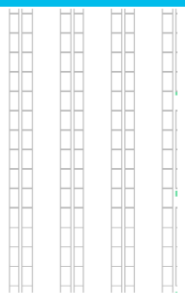
Use cases for CW9176D1

CW9176D1 is an ideal product for auditoriums and other places where focused connectivity is desired.

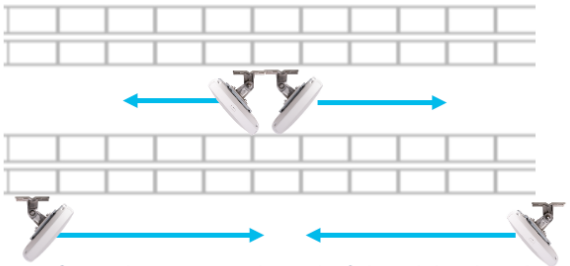
Use cases - Warehouse (High ceilings / long aisles)

Warehousing challenges
- High Ceilings
- Long aisles
- Stock material changes (seasonal)
- AP (distance to client) & mounting





Back-to-Back units in center of aisle covering long aisles (Ability to adjust tilt)

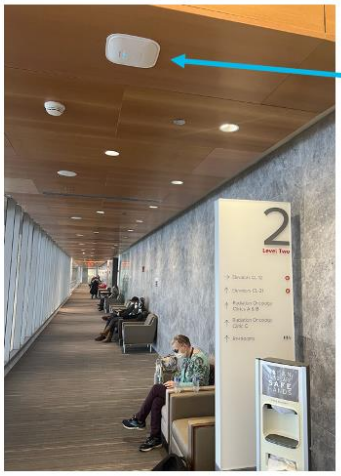


Or perhaps at each end of the aisle shooting down the aisle

Omni-directional pattern is problematic in these areas as AP should be directional and located high to avoid tow motors, changing stock material etc.

CW9176D1 is an ideal product for warehouse environment where focused connectivity is desired.

Use cases – Healthcare (long hallways)



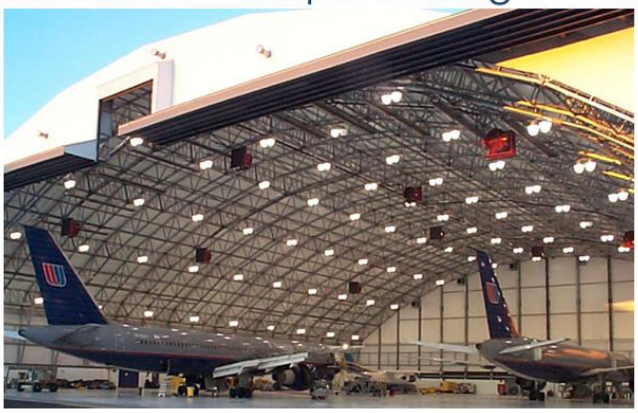
Long hallways are oftentimes handled with Omni-directional Access Points such as this Cisco Access Point flush mounted to a wooden ceiling.

When it becomes problematic or cost prohibitive to install multiple Access Points, a directional antenna unit can be installed on each end of the hallway assuming there are no metal doors or obstructions in the path

CW9176D1

CW9176D1 can be wall mounted instead of traditional ceiling mounted Access Points when the desire is to cover long hallways.

Use cases – Airport Hangars and Bus Garages



Conventional Omni-directional Access Points are not always compatible with high ceilings or areas with a lot of metal.

A directional AP can be mounted on the ceiling or wall allowing the RF energy to be focused where needed

Note: Conventional APs very high on the ceiling and in near proximity to each other, can cause Radio Resource Management (RRM) to hear the AP stronger than the clients. This can result in RRM to believe there is over coverage turning the RF power down on the Access Points causing issues. Directional Access Points help mitigate this issue

CW9176D1 can be used in areas with really high ceilings as the directional antenna can focus downward into a given area.

It is recommended when mounting Access Points to locate them as close to the users as possible, in the case of extremely high ceilings, Access Points with directional antenna arrays such as the CW9176D1 can improve the range of the client allowing the antenna to be mounted typically higher than the recommended distance of 10-15 Feet. Always be sure to test the connectivity during the installation process when the ceiling height exceeds 18 Ft.

Also, when co-locating units especially in close proximity, it is a good practice to test both units operating concurrently at heavy load (and then test each unit individually at heavy load) to verify the units are not interfering with each other. Whenever a unit is in close proximity of another unit (always try to space the operating channels <frequencies> as far apart as practical) verify any degradation that may occur is acceptable if not try reducing RF power or relocating the units. Anytime a unit is in very close proximity to another unit the potential of RF degradation (desense) can occur.

Cabling

The use of proper cable types will enhances the performance of the CW9176x. Since this AP has 5-Gbps ports, it is recommended to use either CAT6 or CAT 6a cable which support speeds of up to 10 Gbps. CAT 5e cables can still be used; however, the AP's performance may get degraded.

The table below lists the various cable types that can be used with the CW9176x.

Table 5. Cable Types Supported

Cable Type	Speeds	Maximum Length
CAT 5e	5 Gigabit	328 feet (100 meters)
CAT 6	1/2.5/5 Gigabit	330 feet (100 meters)
	10 Gigabit	164 feet (50 meters)
CAT 6a	10 Gigabit	330 feet (100 meters)

Power Over Ethernet

The following table depicts the radio, port, USB performance, and maximum power draw based on the AP's input power. For optimal performance, 803.2bt is required.

Note: It's recommended to use Cat 6 or Cat 6A cables for the best performance.

Table 6. PoE specifications for CW9176x on Cisco IOS XE 17.15.2

Power Source	Number of Spatial Streams	2.4 GHz Radio (Slot 0)	5 GHz Radio (Slot 1)	6 GHz Radio (Slot 3)	mGig Link Speed	USB	IoT/GPS/USB/Scan Radio
802.3 af (PoE)	NA	Disabled	Disabled	Disabled	1G	Disabled	Y
802.3 at (PoE+)	10	2x2	4x4	4x4	2.5G	Disabled	Y
802.3 bt (PoE++ / UPOE) (Class 6)	12	4x4	4x4	4x4	10G	Yes/9W	Y

Note: 2.5 Gig Ethernet Speed with 802.3at starting IOS-XE 17.15.3

Global Use AP

The CW9176x is a unified product, global use access point, that can be deployed with Cisco Catalyst 9800 Wireless LAN Controller (a.k.a Catalyst Management Mode) or cloud-based deployment with Meraki Wireless Stack (a.k.a Meraki Management Mode) anywhere in the world, where it's certified to use without the need for a regulatory domain specific SKU. This gives customers the flexibility and investment protection, when they decide to deploy the Access Point in any of the deployment model.

The CW9176x can discover the management mode based on the customer's intent by the presence of cloud connectivity and discovery options based on DHCP and DNS. Once the Access Point discovers the controller, it can obtain its country specific regulation through 1) GPS/GNSS based geo-location, 2) proximity based discovery or 3) through a regulatory activation file for air-gapped deployments.

Please refer to the Wi-Fi 7 Global Use AP deployment guide for a detailed explanation and configuration options to achieve the desired management mode discovery. <Link TBD >

Getting started with Wi-FI 7

The IEEE developed the 802.11be amendment (a.k.a "Extremely High Throughput") to the 802.11 standard, which the Wi-Fi alliance adopted the draft v3.0, as the basis for Wi-Fi 7 certification. The Wi-Fi 7 alliance planned to adopt a subset of features from the 802.11be amendment as part of their Release 1 certification, that was made available in January 2024. A second release with support for incremental set of features is planned for Release 2 certification, slated for December of 2025.

Wi-Fi 7 offers many enhancements that will benefit enterprises, as well as end users by increasing speeds up to four times compared to Wi-Fi 6. In addition, it offers super low latency, more robust connection, higher spectral efficiency, better interference mitigation, more power-saving techniques, better roaming experience, and increased security.

Wi-Fi 7 in essence, brings in the following features.

- 4096 QAM (a.k.a 4K-QAM) – encodes the number of bits in a sub-carrier to 12 bits, in contrast to 10 bits encoded in a sub-carrier for 1024 QAM in Wi-Fi 6. This introduces two new MCS rates MCS 12 and 13. 4K QAM helps upto 20% higher data transmission rates. This is an ***optional*** feature for Wi-Fi 7 certification.
- 320 MHz Channel Width (at 6 GHz) – The max channel width is doubled to 320 MHz when compared to 160 MHz in Wi-Fi 6. With 1200 MHz spectrum space available in the 6 GHz band, it's possible to achieve 3x 320 MHz wide channels. This is an ***optional*** feature for Wi-Fi 7 certification.
- Multi-link operation (a.k.a MLO) – enables aggregation of multiple bands or channels. With MLO, the Wi-Fi 7 Access Point and Client devices can can associate and simultaneously exchange traffic on multiple bands (or multiple channels in the same band if the access point has a dual 5 GHz radio). The distribution of traffic on different bands, help achieve higher throughput, reduced latency and improves reliability. This is a ***mandatory*** feature for Wi-Fi 7 certification.
- Preamble Puncturing – allows access points to 'carve out' or 'puncture' a portion of channel width that is affected by interference, resulting in the remaining channel being used for data transmission. This ensures optimal Wi-Fi performance especially when there is interference.This is a ***mandatory*** feature for Wi-Fi 7 certification.
- Multiple Resource Unit (a.k.a MRU) – improves the OFDMA technology (that was introduced in 802.11ax amendment/Wi-Fi 6). OFDMA allows sub-carriers in a channel bandwidth to be grouped into smaller portions called "Resource Units," (RUs). These individual RUs are assigned to different stations, which allows access points to serve them simultaneously during uplink and downlink transmissions. In Wi-Fi 6, access points assign only a single RU to each wireless client. Wi-Fi 7 allows multiple resource units (MRUs) to be assigned to each wireless client. MRUs enhance spectral efficiency and interference mitigation. This is a ***mandatory*** feature for Wi-Fi 7 certification.

The next sections details the configuration steps needed to enable 802.11be and the other features.

Enable 11be

In the Cisco Catalyst 9800 controller GUI, navigate to **Configurations > Radio Configurations > High Throughput**, and choose **Enable 11be** for the bands where 802.11be is needed, and click **Apply**.

Note:

1. It is recommended to enable this for all the bands.
2. If 802.11be is enabled, MLO gets enabled too. This MLO setting is not independent and of the 802.11be configuration..

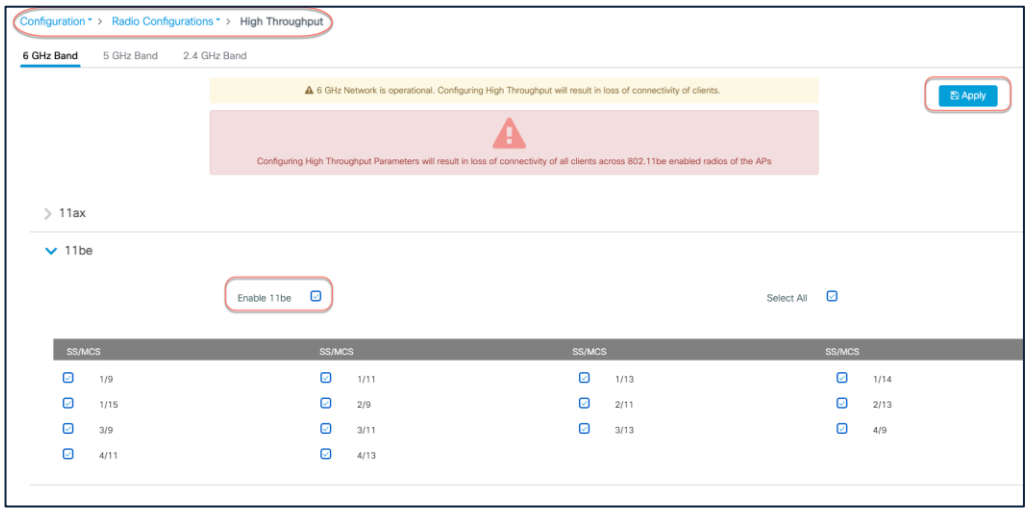


Figure 12. Enable 11be for different bands in the Cisco Catalyst 9800 controller GUI

320 MHz

The channel width for the 6 GHz band, could be set to a maximum of 320 MHz in DBS channel width, for RRM to issue out a 320 MHz channel width, when its algorithm finds it conducive to issue a larger channel width.

From **Configuration > Tags & Profiles > RF/Radio**, edit the 6 GHz RF Profile to include 320 MHz as the max channel width.

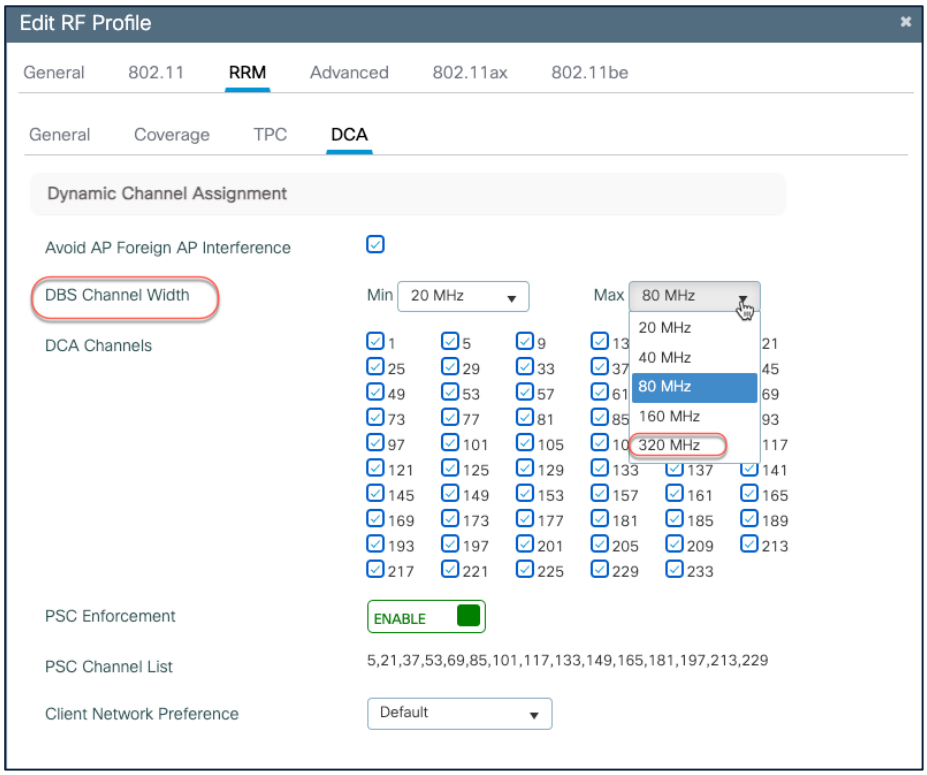


Figure 13. Update RF Profile to Set DBS Channel Width in the Cisco Catalyst 9800 controller GUI

A specific AP could be statically configured for 320 MHz on the access point configuration page.

Navigate to **Configuration > Wireless > Access Points > 6 GHz Radios**, select the AP, change the RF channel assignment to Custom and select 320 MHz as the channel width.

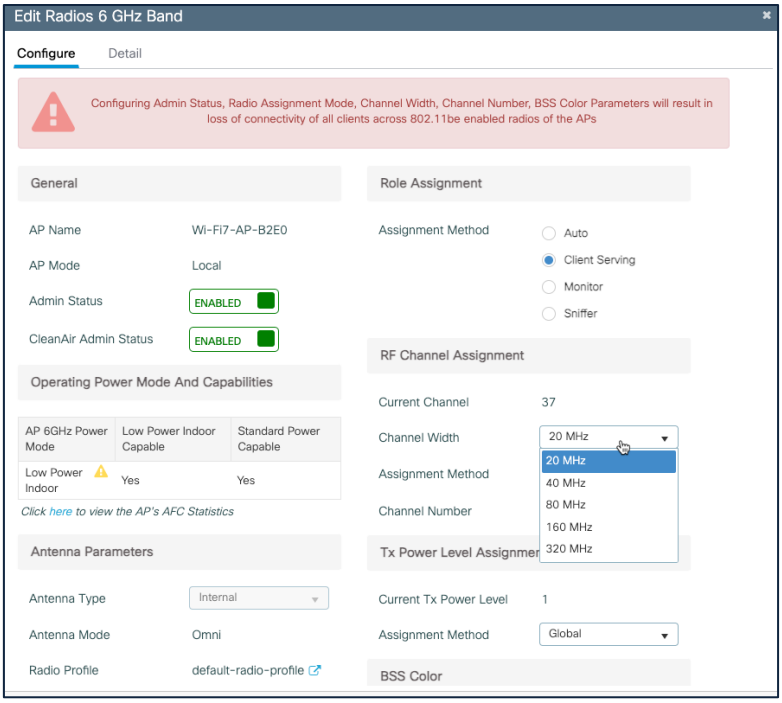


Figure 14. Set RF Channel Width in the Cisco Catalyst 9800 controller GUI

Preamble Puncturing

Preamble puncturing is supported for 80 MHz or higher channel widths. For an 80 MHz, only 20 MHz is allowed to the punctured. The following table lists the allowed preamble puncturing options.

Table 7. Software Interoperability

Channel Width	Allowed Puncturing
20 and 40 MHz	Puncturing not allowed
80 MHz	20 MHz
160 MHz	20 or 40 MHz
320 MHz	40, 80 or 40 + 80 MHz

To enable Preamble Puncturing, navigate to **Configuration > Tags & Profiles > RF/Radio** > edit the **RF Profile** of the 5 GHz and 6 GHz bands and enable **Preamble Puncturing** under the 802.11be tab.

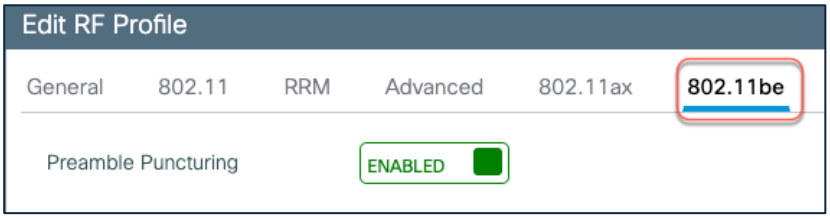


Figure 15. Edit RF Profile to Enable Preamble Puncturing in the Cisco Catalyst 9800 controller GUI

Security

Wi-Fi 7 mandates the support for WPA3 and Enhanced Open (based on OWE) along with Protected Management Frame (PMF) for the clients to operate in 802.11be data rates and features like MLO. There are new AKMs (AKM 24 and 25) added for WPA3-Personal. Additionally, Wi-Fi 7 requires beacon protection for both the AP and the Wireless Clients. With MLO, security needs to be established across all the links of a multi-link association. The security requirements is to mainly make the Wi-Fi networks more secure and protect against cyberattacks.

The following table lists the security requirements for Wi-Fi 7 and comparison with previous Wi-Fi generations.

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

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

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

WLAN Design Considerations

The security requirements for Wi-Fi 7 may necessitate a design change of the WLANs in the current deployment. There are a few options that the customer can consider, while implementing Wi-Fi 7.

Option 1 – Reconfigure the existing WLANs to WPA3/Enhanced Open, along with the required AKMs and Ciphers – i.e. one SSID for all radio policies. While this makes the WLAN most secure, there are practical difficulties in implementation, as many existing clients may not support WPA3 and PMF.

Option 2 – Add new SSIDs with the new security requirement for Wi-Fi 7 and have the newer clients associate to this SSID. This is an easy and flexible approach. The downside to this is maintaining additional SSIDs.

Option 3 – Migrate the SSIDs to Transition Mode – OWE Transition and WPA3 Transition. This is a conservative approach, taking one step to make the WLANs more secure and allowing newer clients with WPA3 security and older clients with WPA2 security to co-exist.

In the below section, you can find the configuration details for Option 3.

Open Security

Requirements for Wi-Fi 7: OWE, AKM 18, Cipher CCMP128 or GCMP 256.

Recommendation: Configure OWE Transition.

Configure two SSIDs.

SSID #1 with OWE, Broadcast disabled. Select WPA3 as the security, with AKM as OWE and Cipher as CCMP128 and GCMP256. Attach to all radio policies.

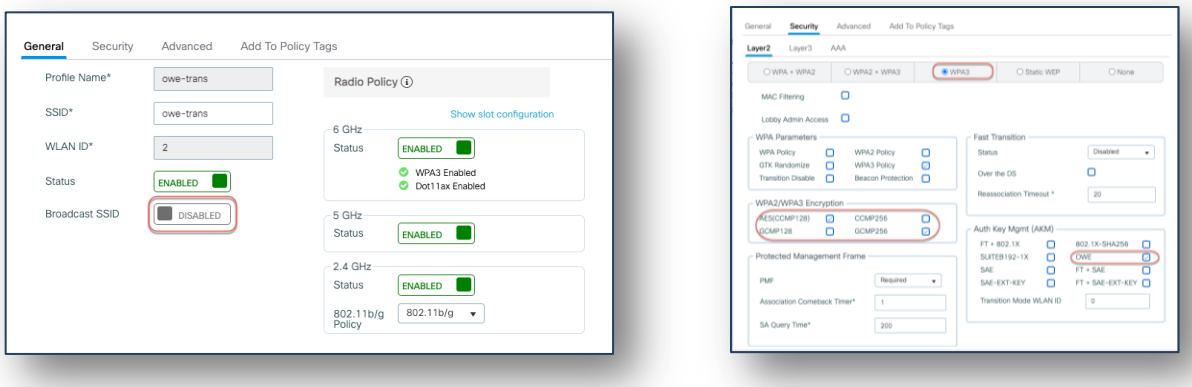


Figure 16. Configure OWE SSID with Broadcast Disabled and WPA3 security in the Cisco Catalyst 9800 controller GUI

SSID #2 with Open, Broadcast enabled. Select Open as the security and map this WLAN to the OWE WLAN created above (SSID #1). Attach the radio policy to 2.4 and 5 GHz.

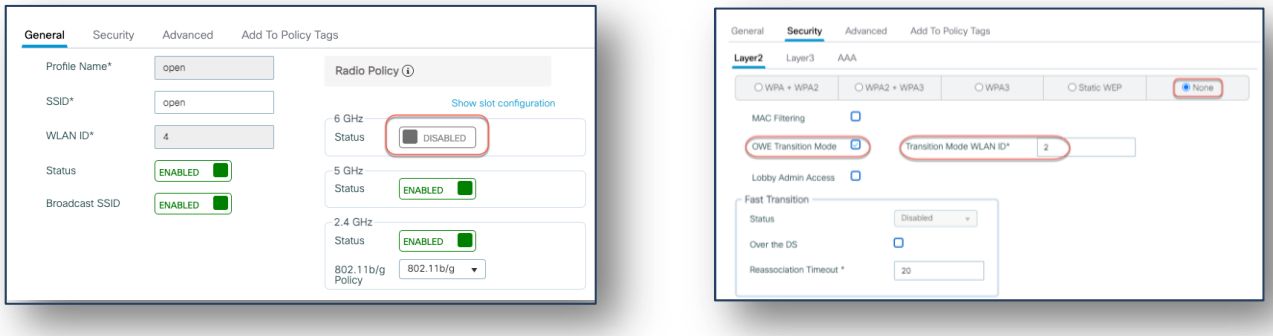


Figure 17. Configure Open SSID and Broadcast Enabled in the Cisco Catalyst 9800 controller GUI

Older clients connect with “open” security on 2.4 or 5 GHz bands. Newer Wi-Fi 7 clients connect with “OWE” security on 2.4/5/6 GHz and can perform Multi-link operation (MLO).

Note: Very old clients with outdated drivers may have difficulty in associating to OWE Transition Mode. It’s highly recommended to update the drivers and test the clients in the environment.

WPA2/WPA3 Personal Security

Requirements for Wi-Fi 7: AKM 24 or 25, Cipher CCMP128 or GCMP 256.

Recommendation: Configure WPA3 Transition (WPA2 + WPA3 Mixed Mode).

Configure the SSID to be WPA2 + WPA3 security type. Select AKM as PSK, SAE and SAE-EXT-KEY. Cipher as CCM128 and GCMP256. PMF as Optional. Use the same password.

Note: If FT is enabled, select FT+PSK, FT+SAE and FT+SAE-EXT-KEY.

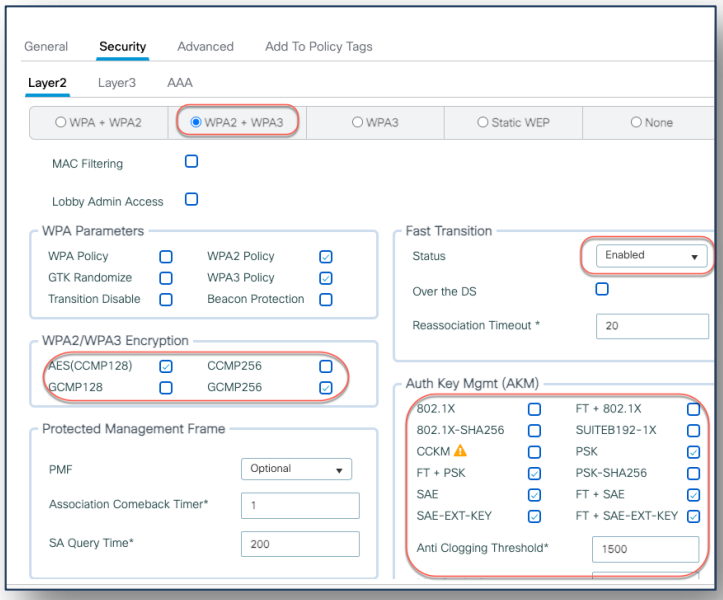


Figure 18. Configure WPA3 Transition (WPA2+WPA3 mixed mode) in the Cisco Catalyst 9800 controller GUI

Wi-Fi 7 clients connect with WPA3/SAE-EXT-KEY or WPA3/FT-SAE-EXT-KEY with PMF

Wi-Fi 6E clients connect with WPA3/SAE or WPA3/FT-SAE with PMF

Wi-Fi 6 clients that support WPA3 connect with WPA3/SAE or WPA3/FT-SAE with PMF in 2.4 /5 GHz bands.

Note:

1. Wi-Fi 7 needs AKM 24 or 25 as per specification. The initial clients in the market seem to negotiate 11be rates/MLO even with AKM 8 & 9. This may change in the future, when client driver implementation gets stricter.
2. If very old clients that still use WPA1 are present in the network, then the recommendation is to have those clients in a separate SSID.

WPA2/WPA3 Enterprise Security

Requirements for Wi-Fi 7 : AKM 3 or 5, Cipher CCMP128 (For most common deployments)

Recommendation : Configure WPA3 Transition (WPA2 + WPA3 Mixed Mode).

Configure the SSID to be WPA2 + WPA3 security type. Select AKM as 802.1x-SHA256 and 802.1x.

Note: If FT is enabled, select AKM as FT+802.1x.

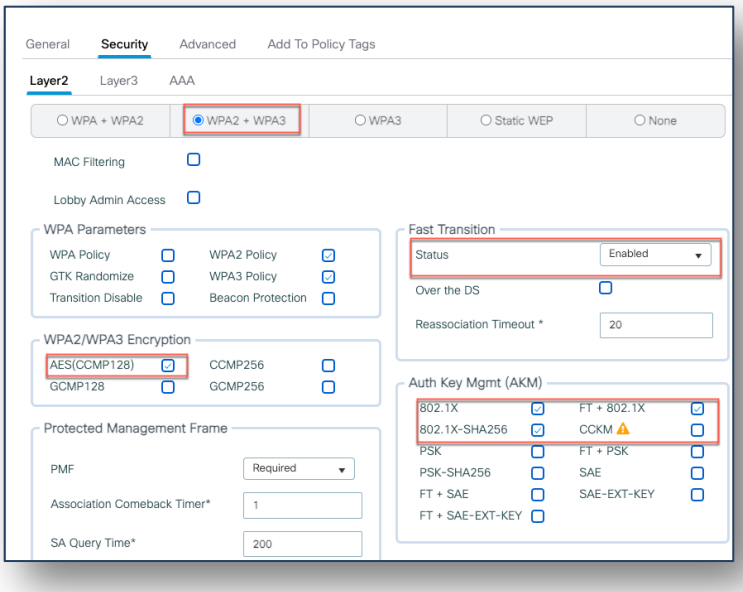


Figure 19. Configure WPA3 Transition (WPA2+WPA3 mixed mode) in the Cisco Catalyst 9800 controller GUI

On the client side that support WPA3, configure WPA3 Enterprise. Wi-Fi 7 clients will use the settings to connect to any band with MLO. For Wi-Fi 6E clients, they will prefer connecting to 6 GHz band and Wi-Fi 6 clients will connect to 5 or 2.4 GHz band. For clients that don't support WPA3, configure a WPA2 profile.

Note: Very old clients with outdated drivers may have difficulty in associating to WPA3 Transition Mode. It's highly recommended to update the drivers and test the clients in the environment.

Viewing Clients

The Cisco Catalyst 9800 GUI now displays the MLO capability and client statistics. From the main dashboard or **Monitoring > Clients**, select a client listed in the Protocol column as "11be (MLO)".

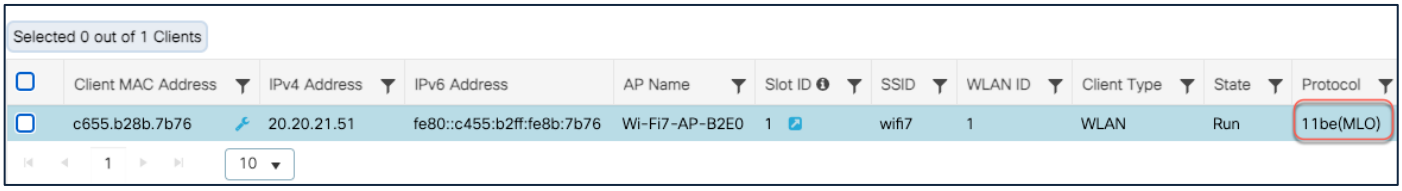


Figure 20. View Client Statistics in the Cisco Catalyst 9800 controller GUI

In the 360 View, the client's MLO capability is indicated along with the number of radio slots it is associated to. In the example below, the client is associated to 2 radio slots.

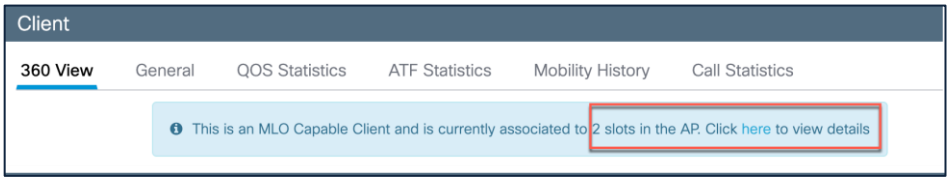


Figure 21. View Client's MLO Capability and Associated Radio Slots in the Cisco Catalyst 9800 controller GUI

Click on the link to view the details, client propertis, security information and client statistics.

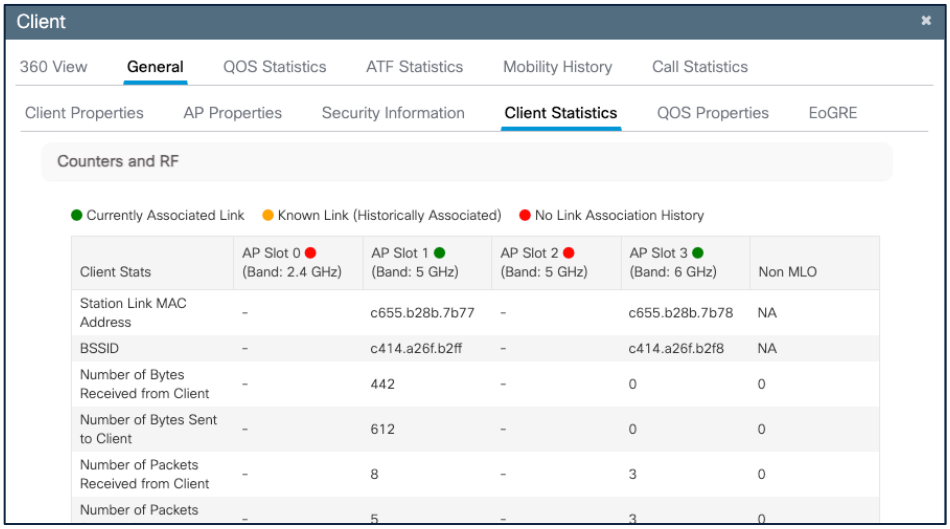
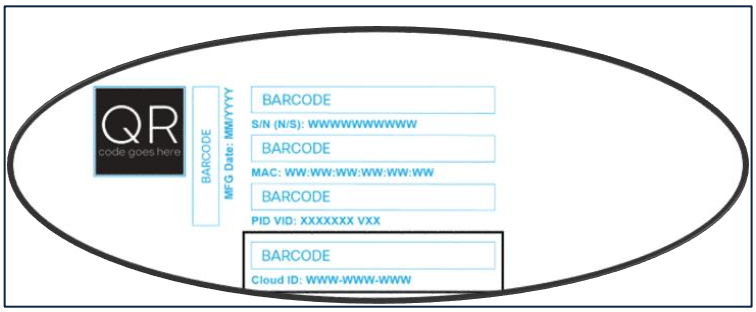


Figure 22. View Client Statistics in the Cisco Catalyst 9800 controller GUI

Migration between Management Modes

The Cisco Wireless CW9176x is a Global Use, Unified Product and can convert from the Cisco Catalyst management mode to the Meraki management mode and vice versa. This Unified Product gives you the flexibility of being deployed in a Catalyst 9800 WLC based deployment or cloud based Meraki deployment. It also provides investment protection for the future in case you want to switch between the two management options anytime from Day 1 to Day N.

Starting with Wi-Fi 7 Access Points, the Meraki Serial Number has been renamed to "Cloud ID". There is no functional change to how this was used in the previous generation product.

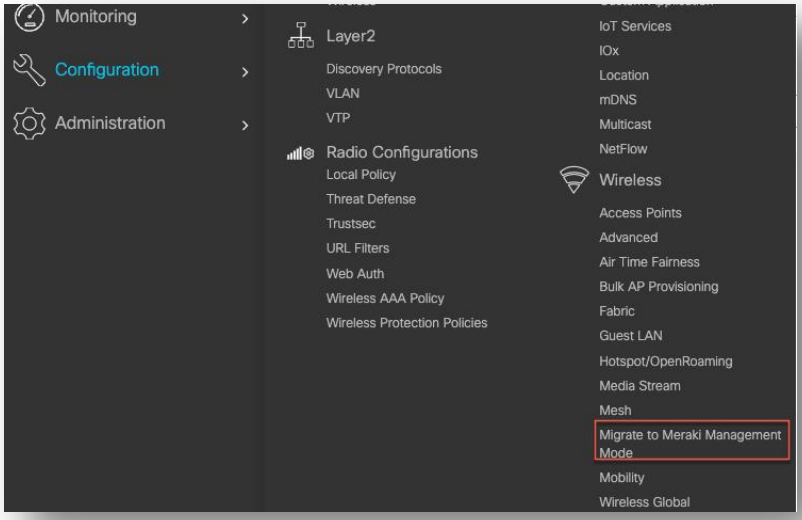


Conversion Process

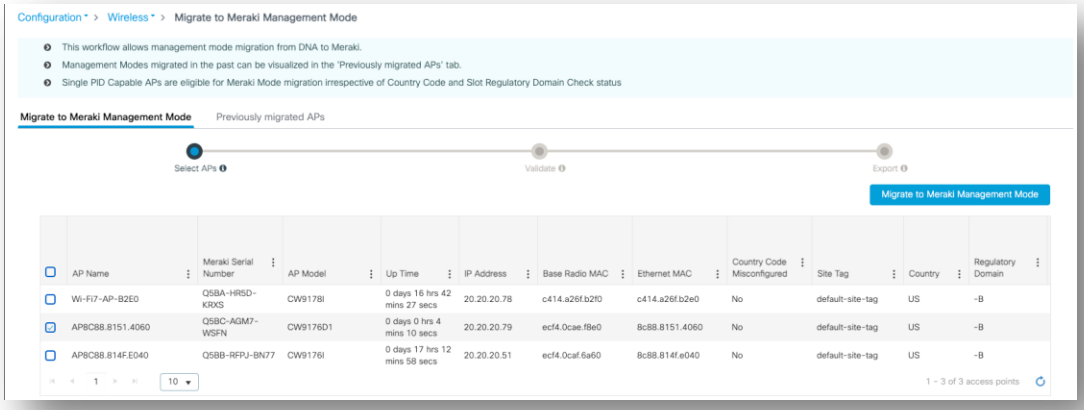
The CW9176x can be converted from Catalyst Management Mode to Meraki Management Mode through a simple work flow in C9800 WLC UI.

The following are the step to perform the conversion process.

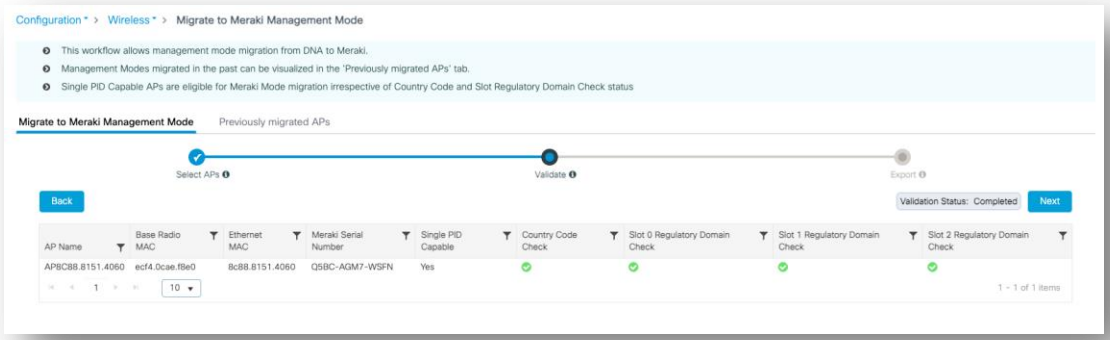
1. Start the conversion workflow from Configuration → Wireless → Migrate to Meraki Management Mode.



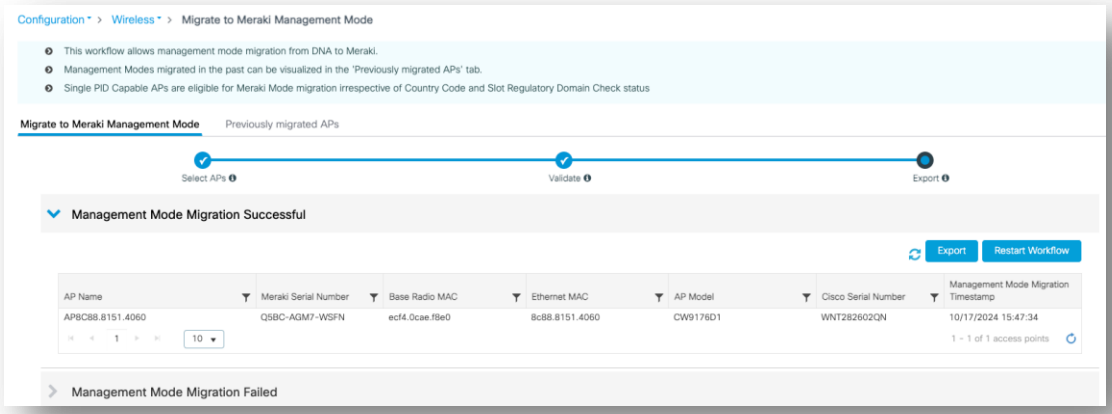
2. Select the APs you want to convert and click Migrate to Meraki Management Mode.



3. The controller will then validate the APs. Select Next.

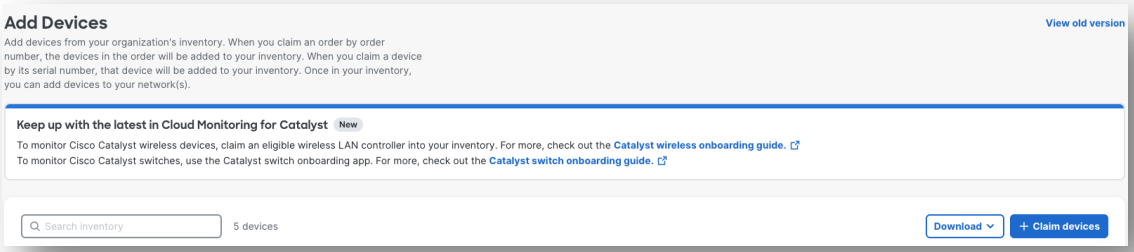


4. Confirm the change on the selected Access Points.

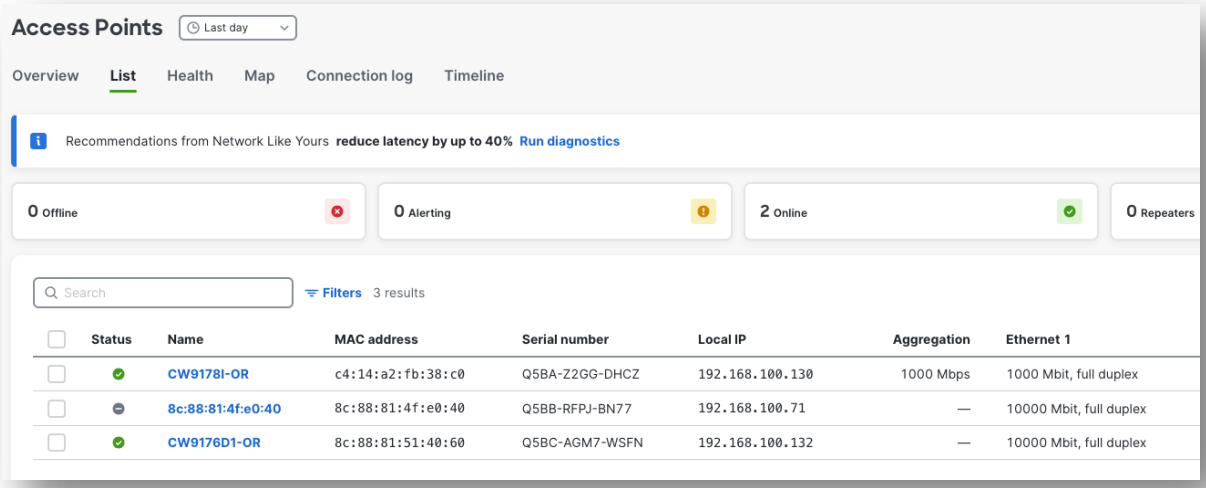


5. Export or download the data to be copied to Meraki Dashboard. The data can be exported in multiple formats – Serial Number, JSON or Export to Meraki Dashboard.

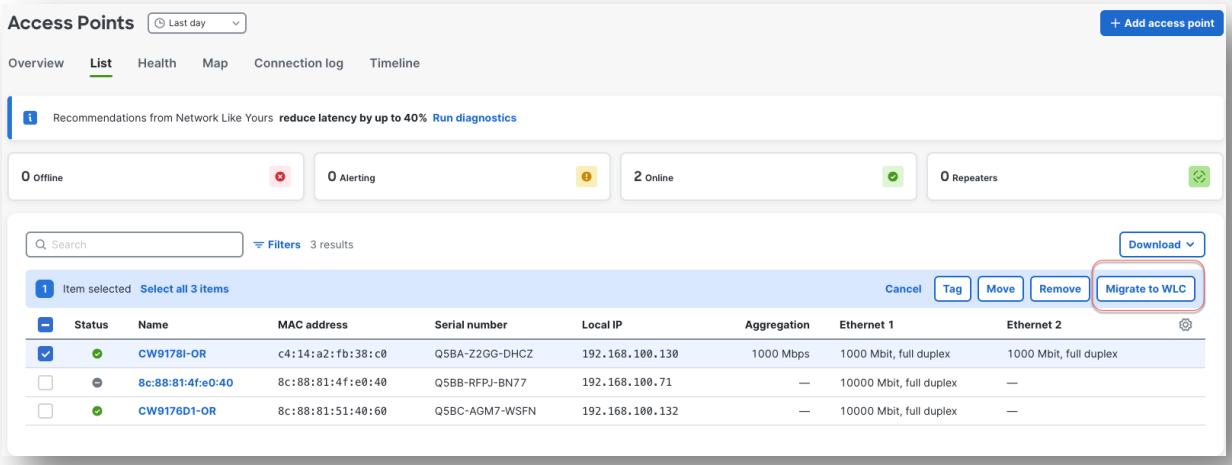
6. Add devices in Meraki Dashboard. Follow the Meraki Claim process.



7. Once devices and claimed, the AP will appear in the dashboard in few minutes.



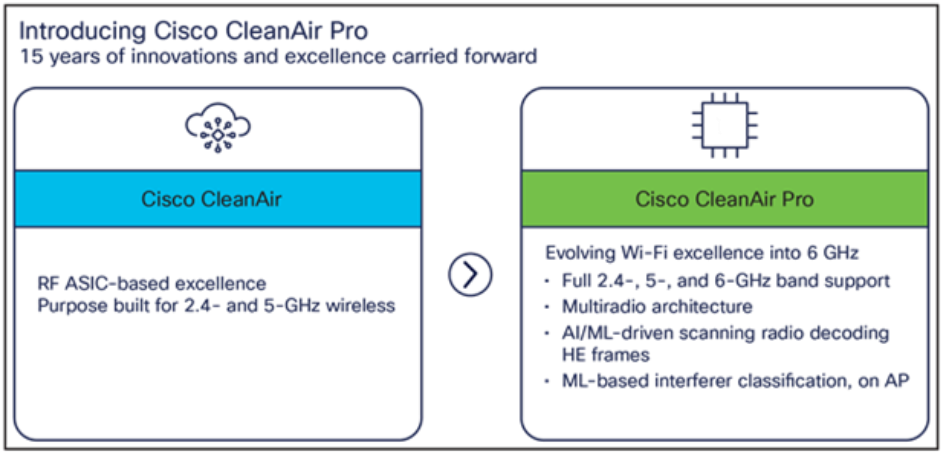
8. To convert an AP from Meraki Management Mode to Catalyst Management Mode, select the AP that you want to migrate and click on “Migrate to WLC”.



Cisco CleanAir Pro

Wi-Fi 6E added 6 GHz spectrum for unlicensed use of Wi-Fi, 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® (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 features work in conjunction with the AI/ML-driven scanning radio, CleanAir Pro also works with the Catalyst 9176x APs' serving radios. Unlike previous generations of APs, CleanAir Pro can even decode extremely high throughput (EHT, 802.11be) frames, which is crucial since Wi-Fi 7 EHT 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 Catalyst Center.



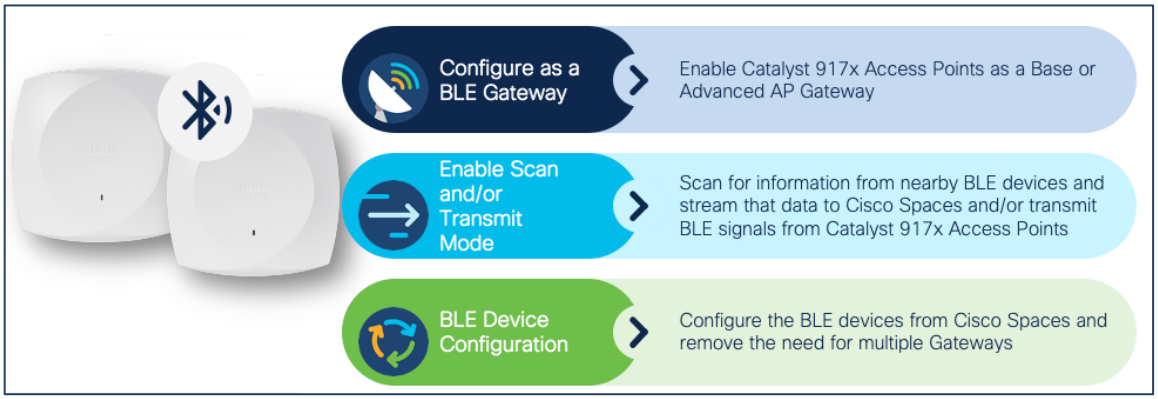
Internet of Things Integration

IoT Services with Cisco Spaces

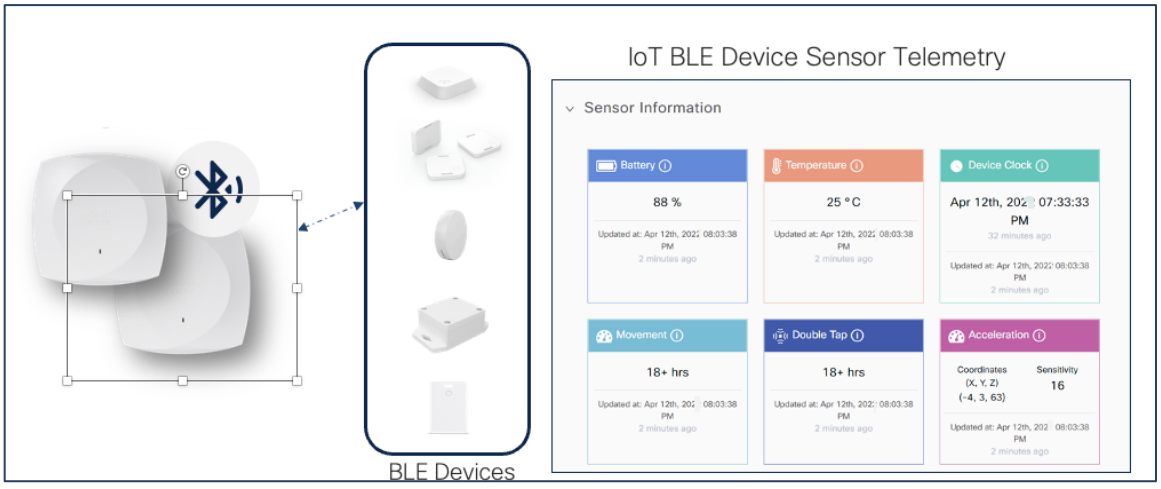
The Catalyst CW9176x have a built-in IoT radio that can be used in conjunction with the IoT Services platform service in Cisco Spaces. IoT Services is designed to enable management of Internet of Things (IoT) devices across vendors, form factors, and technology protocols.

Within IoT Services, you can enable a CW9176x 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.

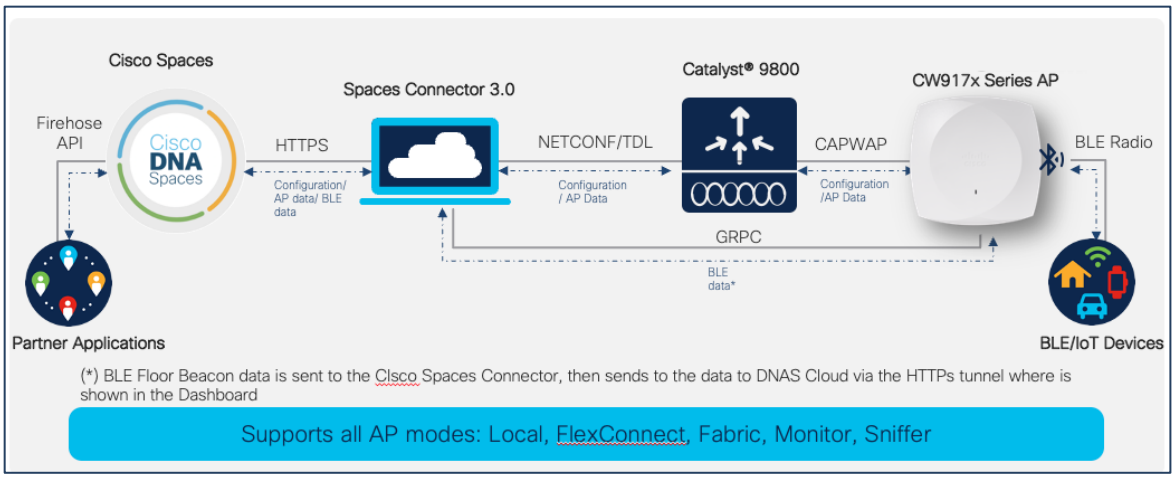
The CW9176x can manage and configure wireless IoT devices if you enable the Advanced AP Gateway feature, which installs a Cisco IOx application on the access point. This saves the user the trouble of having several gateways across different vendors.



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



The figure below depicts how BLE data is sent from the Cisco Wireless CW9176x to Cisco Spaces.



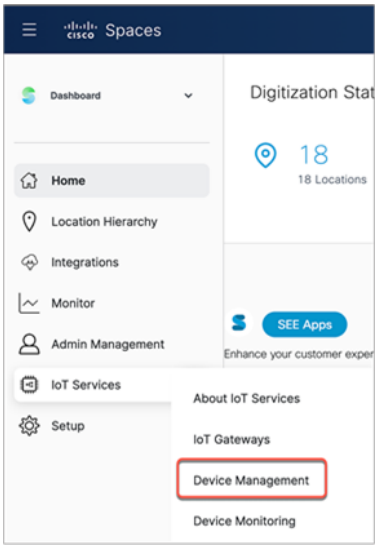
The built-in IoT radio require Cisco Spaces and IoT Services to be configured. Please use the following guides for configuring Cisco Spaces and IoT Services.

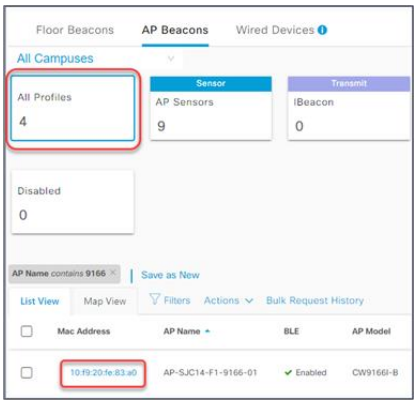
https://www.cisco.com/c/en/us/td/docs/wireless/spaces/config-guide/ciscospaces-configuration-guide.html

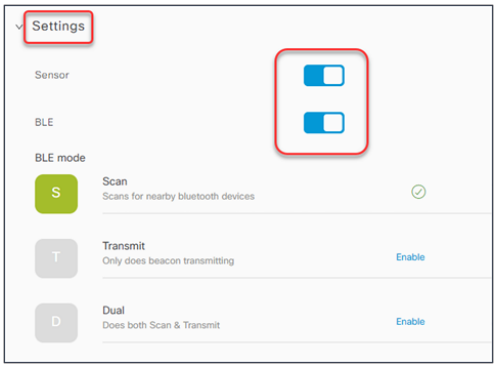
https://www.cisco.com/c/en/us/td/docs/wireless/cisco-dna-spaces/iot-services/b_iot_services.html

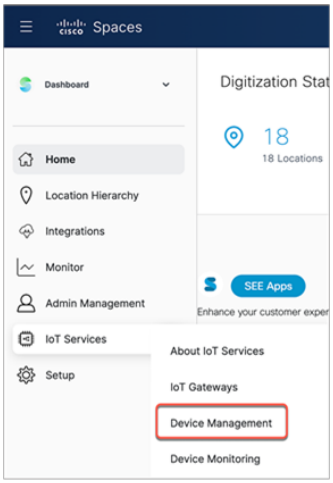
To enable the IoT radio or environmental sensors in Cisco Spaces, go to the specific access point in IoT Services in Cisco Spaces and select the feature to turn on or bulk-enable each feature in the AP Beacons page.

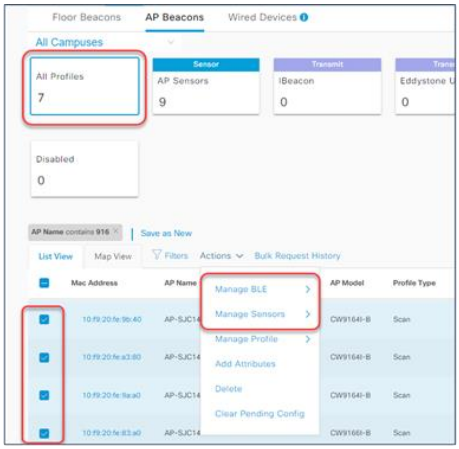
The figures below depict how to enable or disable the IoT radio or environmental sensors on Cisco Spaces through a specific access point.











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

Site Survey Mode

The Cisco Wireless CW9176x supports Site Survey mode. 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 and allowing wireless clients to join via an internal Dynamic Host Configuration Protocol (DHCP) pool. Site Survey mode provides all the control needed to configure and conduct a site survey. 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 CW9176x 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.

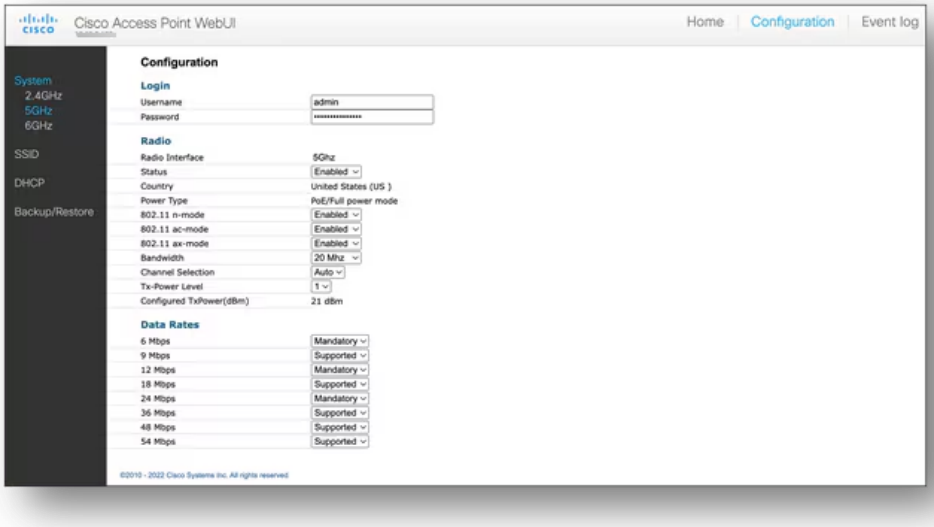


Figure 23. View RF Metrics for AP in Site Survey Mode

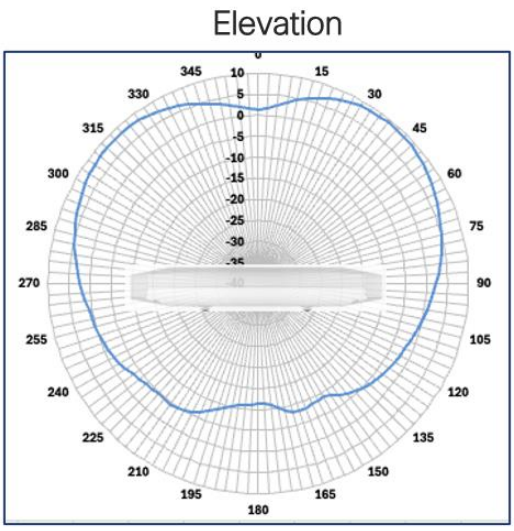
The steps below describe how to convert a CW9176x AP into Site Survey mode:

1. Change the AP to Site Survey mode. Enter command “ap site-survey”
2. After booting up, the AP is automatically assigned a static IP of 10.0.23.1.
3. The AP will start broadcasting the C9178_site_survey SSID with open/OWE security.
4. Connect your wireless client with the C9178_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. Enter command “ap capwap”

Note:

1. If an AP is converted to Site Survey mode while connected to a WLC, it will disjoin and go into standalone mode.
2. For the above mentioned Site Survey functionality, the AP should have joined a Catalyst 9800 WLC atleast once. When the AP is in Day 0 mode, the CLI to convert the AP to Site Survey mode is not present.
3. The AP carries over the country code configured, while it was connected to the Catalyst 9800 WLC.

Antenna Patterns (9176I)



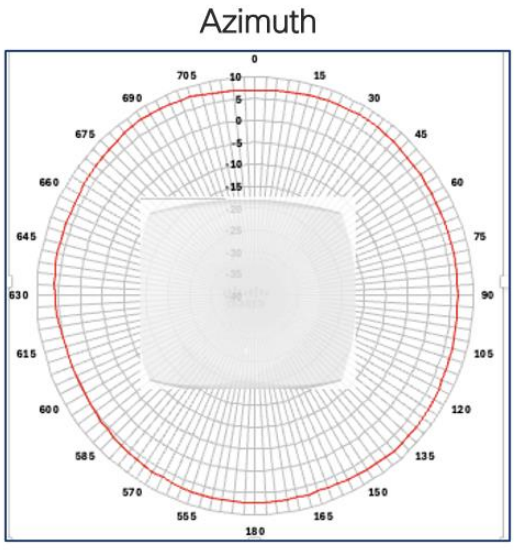


Figure 24. Dual Band Radio (2.4 GHz) Antenna Patterns

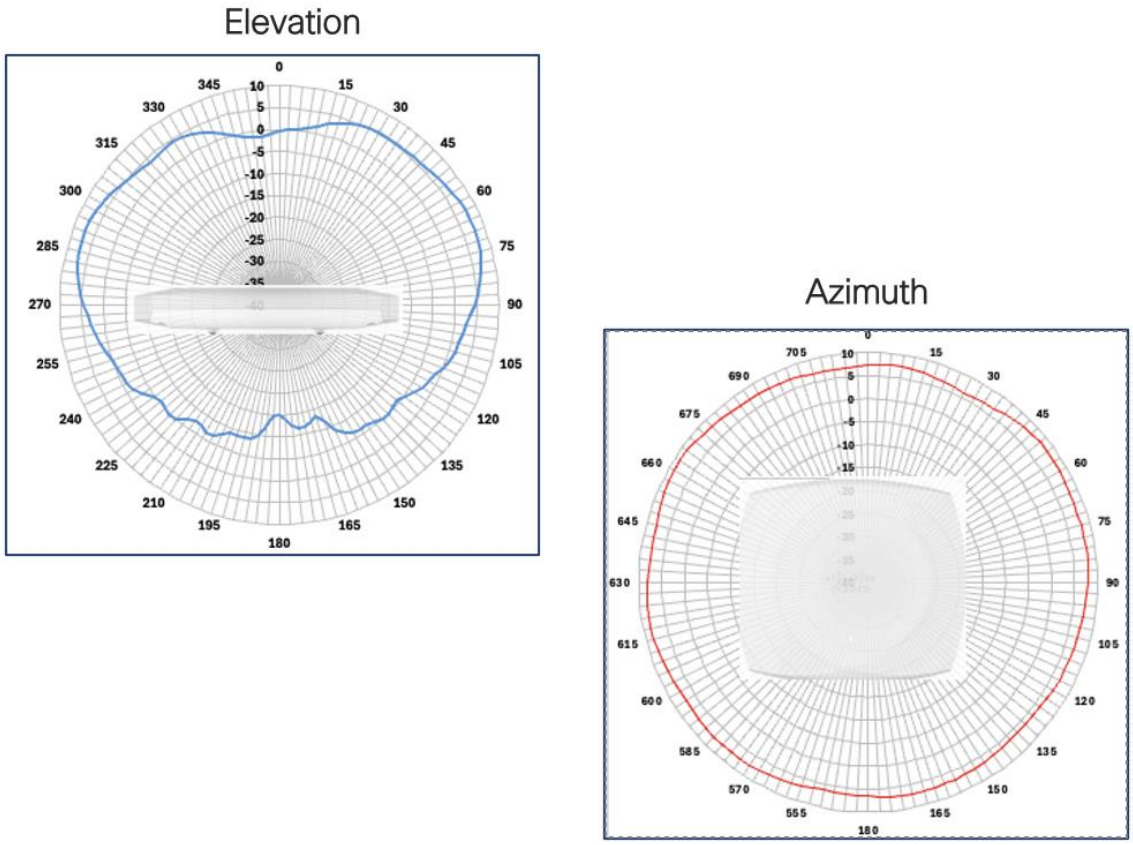


Figure 25. Dual Band Radio (5 GHz) Antenna Patterns

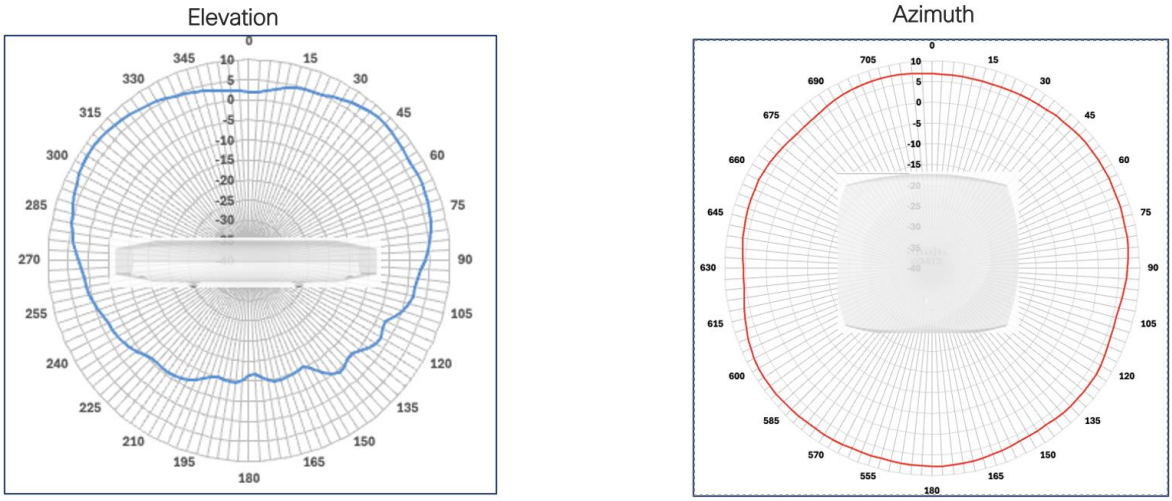


Figure 26. 5GHz Radio (Slot 2) Antenna Patterns

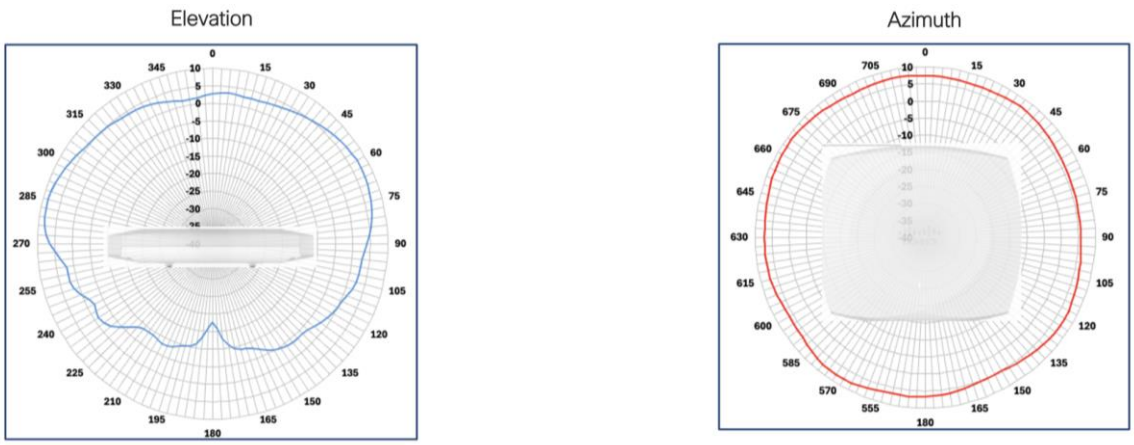


Figure 27. 6GHz Radio Antenna Patterns

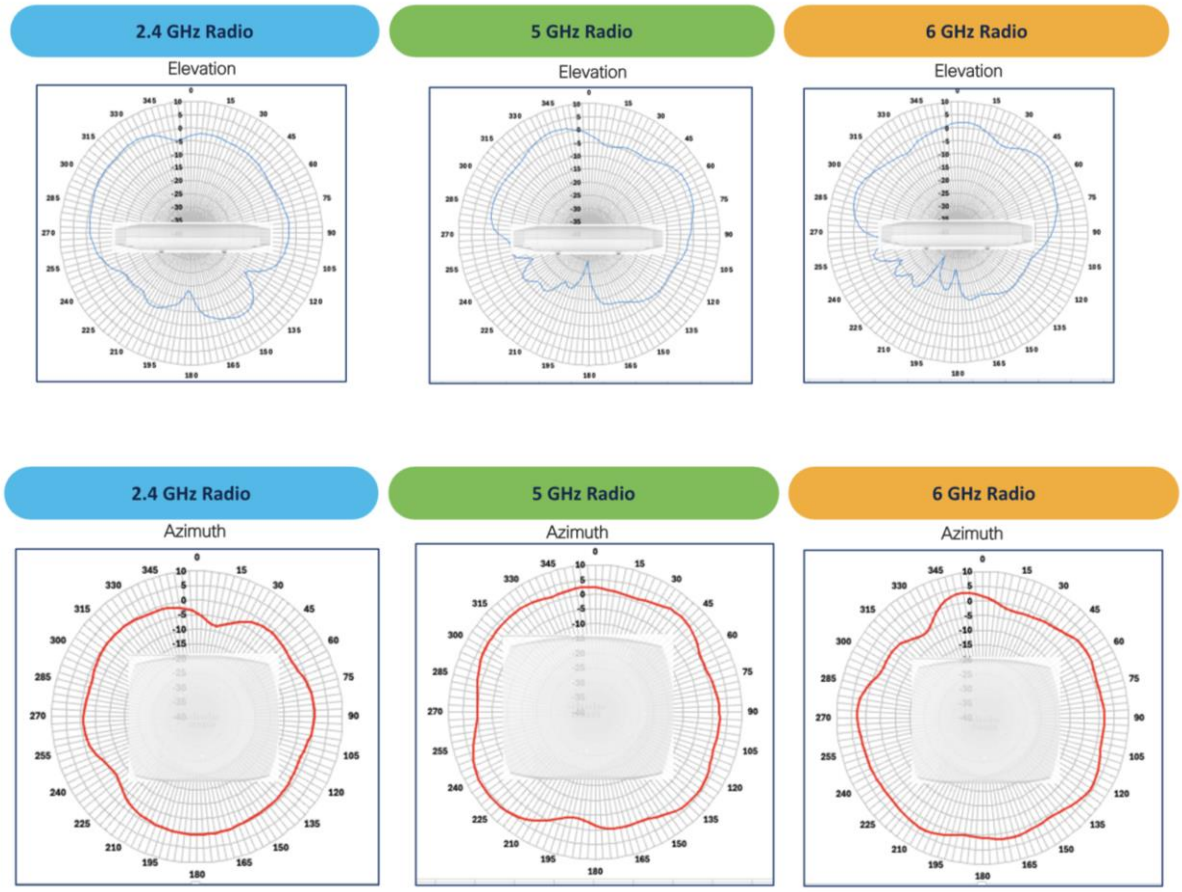


Figure 28. AI/ML-Driven Scanning Radio Antenna Patterns

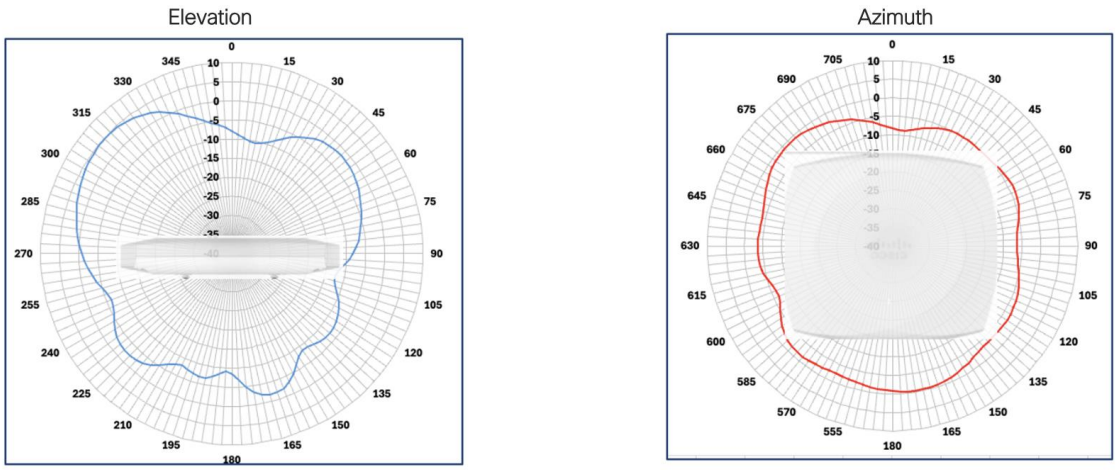


Figure 29. IoT Radio Antenna Patterns

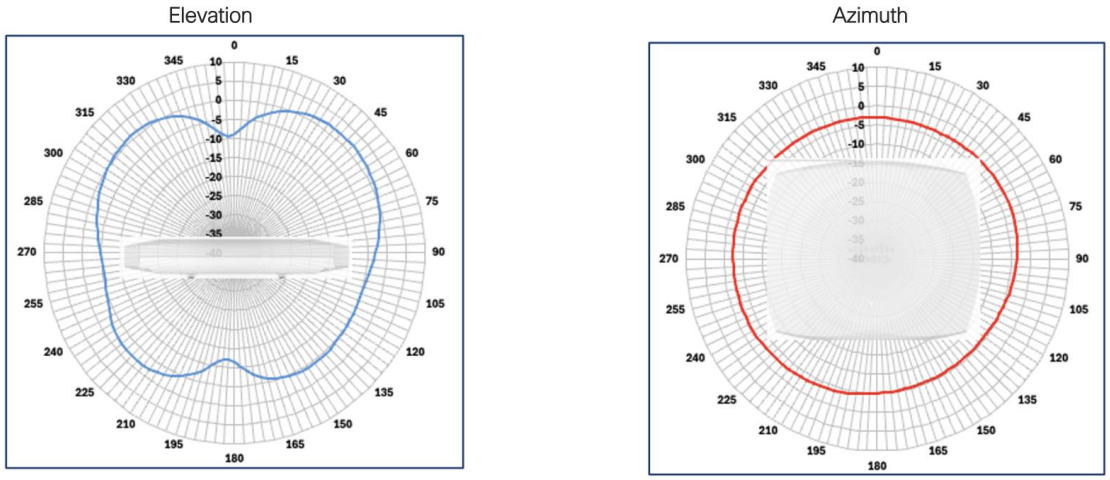


Figure 30. GNSS Antenna Patterns

Antenna Patterns (9176D1)

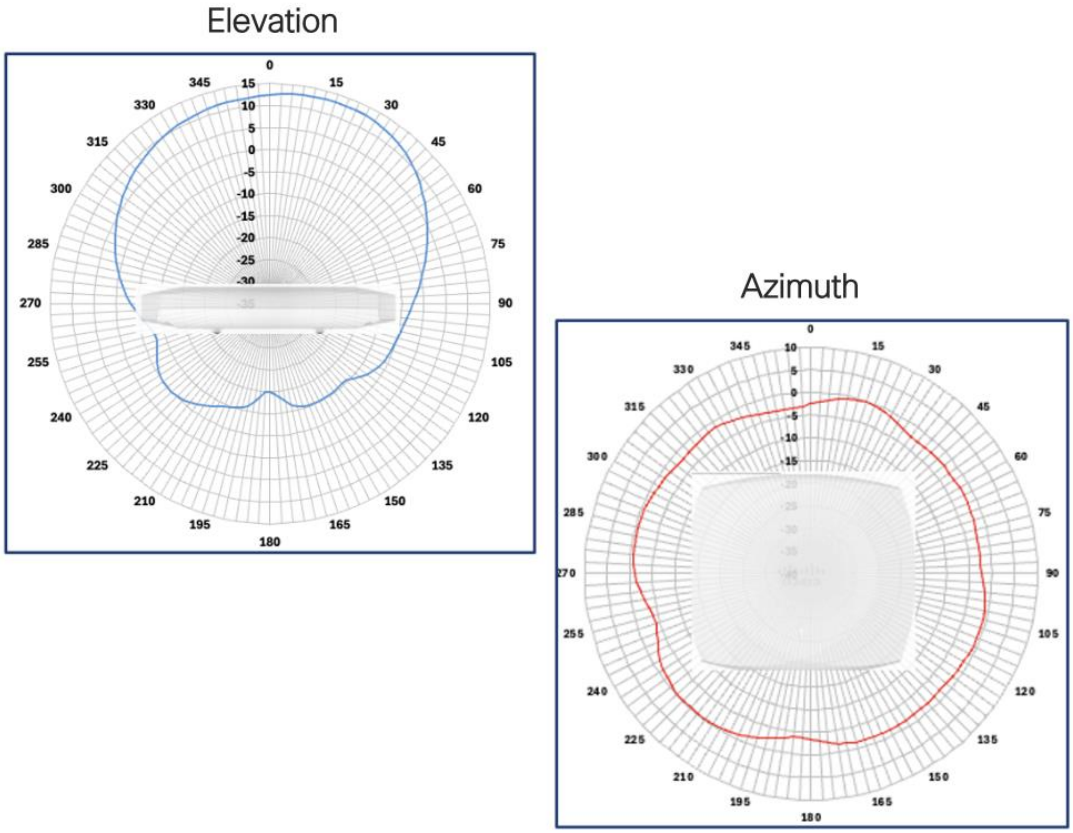


Figure 31. Dual Band Radio (2.4 GHz) Antenna Patterns

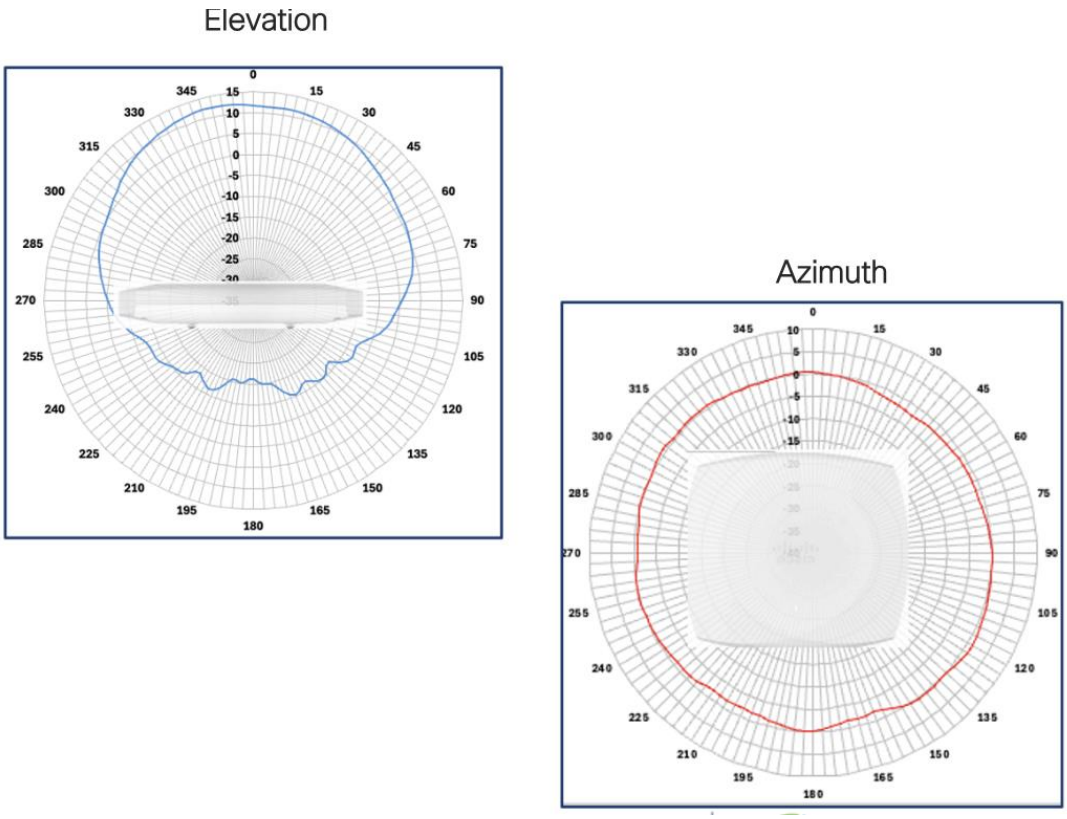


Figure 32. Dual Band Radio (5 GHz) Antenna Patterns

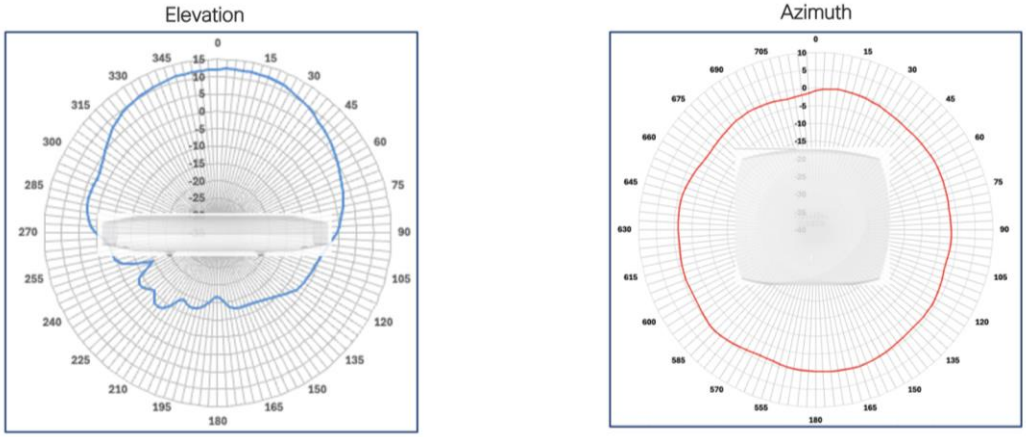


Figure 33. 5GHz Radio (Slot 2) Antenna Patterns

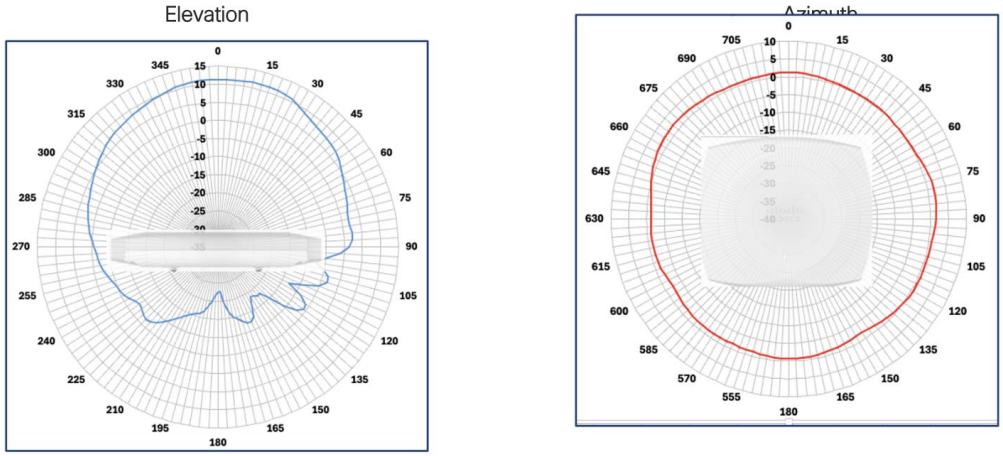


Figure 34. 6GHz Radio Antenna Patterns

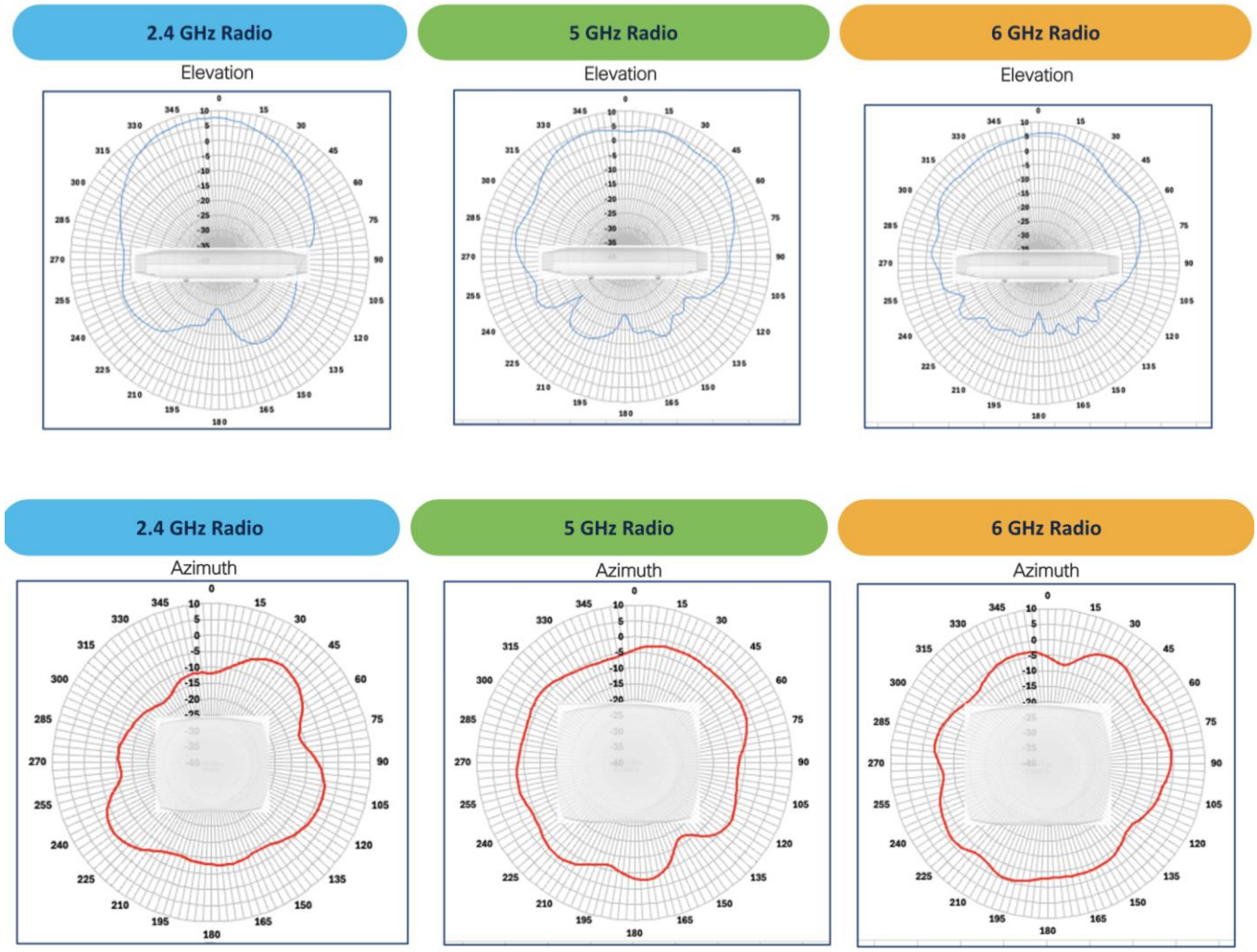


Figure 35. AI/ML-Driven Scanning Radio Antenna Patterns

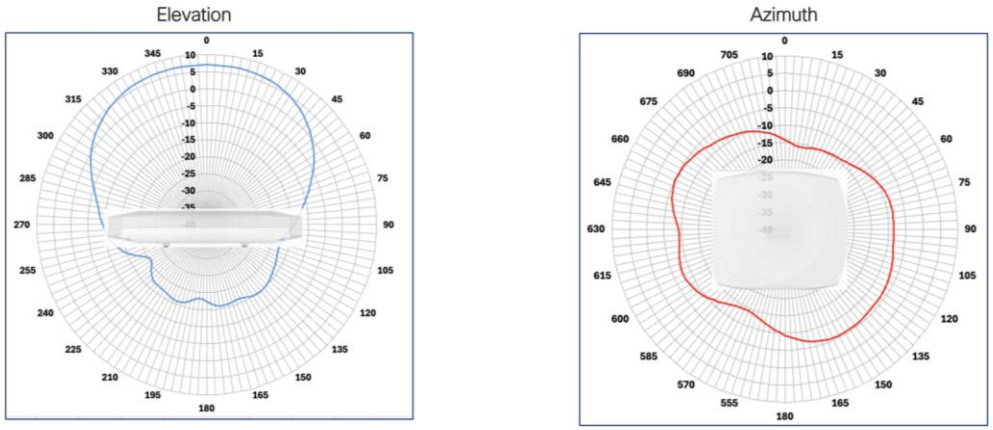


Figure 36. IoT Radio Antenna Patterns

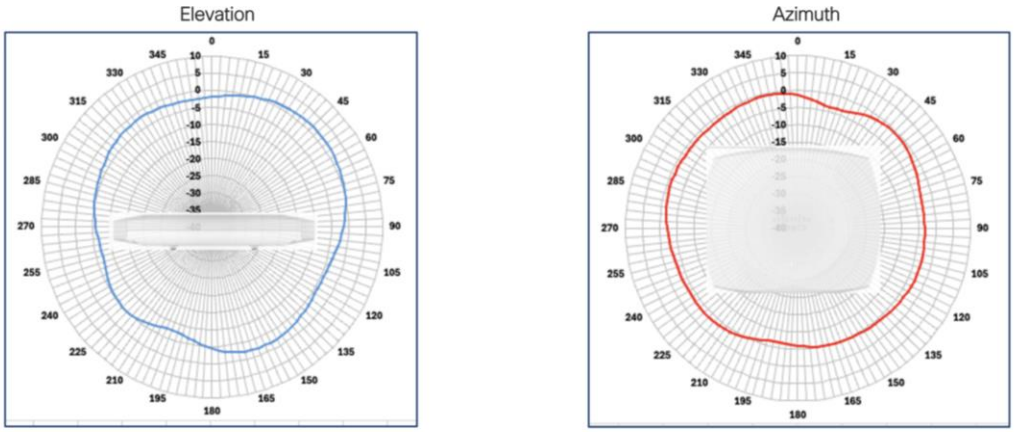


Figure 37. GNSS Antenna Patterns

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**.