Cisco Catalyst IW9165D Heavy Duty Access Point Configuration Guide, Release 26.1.x

Cisco Catalyst IW9165D Heavy Duty Access Point
Updated April 10, 2026

Topics included

1 Introduction.....5
Overview of the Access Point.....6
Determining image.....7
Convert the IW9165D AP between CAPWAP and URWB Modes.....8
Related Documentation.....9

2 Control and Provisioning of Wireless Access Points 11
Overview.....12
Provisioning certificates on Lightweight Access Points.....13
Understanding CAPWAP connectivity On AP.....14
Reset button settings.....15
Ethernet port usage on CAPWAP mode.....16
Indoor deployment.....16
Verify indoor deployment.....17
AP Radio Slot.....18
Supported fixed domains and country codes.....19
Radio antenna settings.....21
AFC support for 6 GHz standard power mode.....22
Verify AFC status on an AP.....23
Antenna disconnection detection.....23
Verify Antenna Disconnection Detection on an AP or AP Profile.....24
Troubleshooting.....25
GNSS.....25
Disable GNSS.....26
Enable GNSS.....26
Check the status of the GNSS module.....26
GNSS status and diagnostics.....26

1 Introduction

Topics:

- Overview of the Access Point
- Determining image
- Convert the IW9165D AP between CAPWAP and URWB Modes
- Related Documentation

Overview of the Access Point

This topic explains the Cisco Catalyst IW9165D Heavy Duty Access Point and Wireless Client, its supported modes, and key features for ultrareliable wireless connectivity in industrial environments.

The Cisco Catalyst IW9165D Heavy Duty Access Point and Wireless Client (IW9165D) is a robust wireless device designed to provide ultrareliable connectivity for moving vehicles and machines in industrial settings.

- Supports operation as Cisco Ultra-Reliable Wireless Backhaul (URWB) and CAPWAP modes, starting from specific software releases.
- Features a 2x2 Wi-Fi 6E design with options for internal and external antennas, simplifying wireless backhaul deployment.
- Does not support 2.4G radio or scan radio functionalities.

Supported Modes and Features of the IW9165D Access Point

The IW9165D access point can operate in multiple modes, each tailored for specific deployment scenarios and requirements.

- **Local mode** : The default mode where the AP serves clients, creating two CAPWAP tunnels (management and data) to the controller for central switching.
- **Flexconnect mode** : Data traffic is switched locally, not sent to the controller. The AP behaves like an autonomous AP but is managed by the controller and continues to function if the controller connection is lost.
- **Fabric mode** : The AP establishes a VxLAN tunnel (Access-Tunnel) to the fabric edge, preserving segmentation and inserting the SGT tag in the tunnel for secure connectivity.
- **Sniffer mode** : The AP captures and forwards all client packets on a given channel to a remote machine running packet analyzers such as Airopeek or Wireshark, including details like timestamp, signal strength, and packet size.

  > **Note**
  >
  > In sniffer mode, the server receiving the data must be on the same VLAN as the wireless controller management VLAN; otherwise, an error message is displayed.

- **Monitor mode** : The AP acts as a dedicated sensor for location-based services, rogue AP detection, and intrusion detection, without serving client data traffic.
- **Site Survey mode** : The AP GUI is enabled for configuring RF parameters during site survey investigations. For more information, see the Access Points Survey Mode section in the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide* .

Unsupported features for the IW9165D access point include:

- 2.4G radio, and
- Scan radio.

For more information about configuring the AP on the Wireless Controller, see the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide .

Typical Deployment of the IW9165D Access Point

The IW9165D can be deployed on moving vehicles such as automated guided vehicles (AGVs) in a factory, providing seamless wireless connectivity using URWB mode for high availability and low latency, or CAPWAP mode for integration with a wireless controller.

Determining image

This topic explains how to determine which software image your Catalyst IW9165D Access Point is running by using the CLI, and describes the different images available for CAPWAP and URWB modes.

The Catalyst IW9165D Access Point supports two wireless technologies—CAPWAP and URWB—on a single hardware platform, allowing you to switch images by updating the software without changing the hardware.

- CAPWAP and URWB are the two supported wireless modes.
- Each mode requires a specific software image: **ap1g6b-k9w8-xxx.tar** for CAPWAP and **ap1g6m-k9c1-xxx.tar** for URWB.
- The image can be determined using the **show version** command.

Software images and mode reference

Software images are stored under different folders on the same partition on IW9165D. You need to choose the image to boot up with according to the mode your AP is running, CAPWAP or URWB.

Table 1: IW9165D Software Images

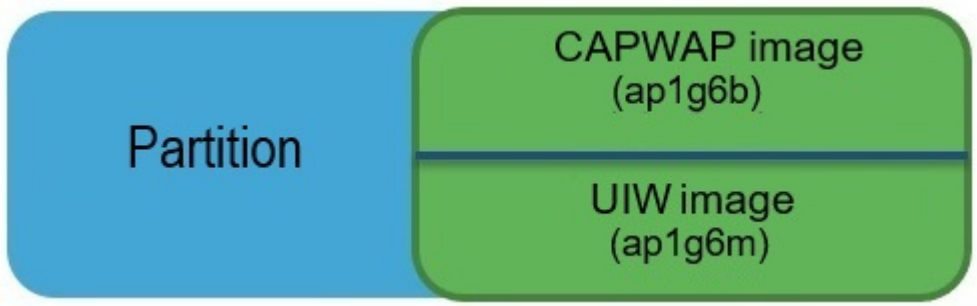
IW9165D Mode	Software Image	Description
CAPWAP	**ap1g6b-k9w8-xxx.tar**	Supports CAPWAP mode
URWB	Unified Industrial Wireless image **ap1g6m-k9c1-xxx.tar**	Supports URWB mode

Note

TIP: Select the correct image based on the desired operating mode of your access point.

This image shows the folder structure where software images are stored on the IW9165D:

Figure 1: IW9165D Software Image Folder Structure



Determining the running image using CLI

To determine the image that your IW9165D is running, use the **show version** command. The output will indicate the current image and mode:

- If the **show version** output displays **Cisco AP Software, (ap1g6b)** , it means the AP is running the CAPWAP image **ap1g6b-k9w8-xxx.tar** , which supports the CAPWAP mode.

```
Cisco AP Software, (ap1g6b), C9165, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2024 by Cisco Systems, Inc.
Compiled Tue Feb 20 23:04:29 GMT 2024
```

- If the **show version** output displays **Cisco AP Software (ap1g6m)** , it means the AP is running **ap1g6m-k9c1-xxx.tar** , which supports the Cisco URWB mode.

```
Cisco AP Software, (ap1g6m), C9165, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2024 by Cisco Systems, Inc.
Compiled Tue Feb 20 23:04:29 GMT 2024
```

Convert the IW9165D AP between CAPWAP and URWB Modes

Learn how to convert the IW9165D Access Point between CAPWAP and URWB modes using CLI commands. This procedure includes important prerequisites and cautions regarding device state and data loss.

This procedure describes how to change the operating mode of the IW9165D Access Point between CAPWAP and URWB. The device will reboot and start up in the selected mode after conversion.

1. Use the **configure boot mode urwb** command to convert from CAPWAP to URWB mode.

```
Device# configure boot mode urwb
```

   The access point reboots and starts up in URWB mode.

2. Use the **configure boot mode capwap** command to convert from URWB to CAPWAP mode.

```
Device# configure boot mode capwap
```

   - To convert the device from URWB to CAPWAP mode, the AP must be in offline mode.
   - To convert the AP to offline mode, use either the CLI method described inConfigure IW Service to offline mode using CLI the GUI method described in Configure IW Service to offline mode using GUI.
   - Image conversion performs a full factory reset which completely erases the configuration and data.

   The access point reboots and starts up in CAPWAP mode.

Related Documentation

This topic explains where to find related documentation for the Cisco Catalyst IW9165 Heavy Duty Series, including hardware, features, and configuration guides.

This topic provides links to additional documentation and guides relevant to the Cisco Catalyst IW9165 Heavy Duty Series.

To view all support information for the Cisco Catalyst IW9165 Heavy Duty Series, see https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9165d-heavy-duty-access-point/model.html .

In addition to the documentation available on the support page, you will need to refer to the following guides:

- For information about IW9165D hardware, see Cisco Catalyst IW9165D Heavy Duty Access Point Hardware Installation Guide.
- A full listing of the AP's features and specifications is provided in Cisco Catalyst IW9165 Series Data Sheet .
- For information about Cisco URWB mode configuration, see the relevant documents at:

  https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9165d-heavy-duty-access-point/model.html .
- For more information about the configuration on Cisco Catalyst 9800 Series Wireless Controllers, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide .

2 Control and Provisioning of Wireless Access Points

Topics:

- Overview
- Indoor deployment
- AFC support for 6 GHz standard power mode
- Verify AFC status on an AP
- Antenna disconnection detection
- Troubleshooting
- GNSS
- Disable GNSS
- Enable GNSS
- Check the status of the GNSS module
- GNSS status and diagnostics

Overview

Learn how the CAPWAP protocol enables wireless LAN controllers to manage multiple access points and secure communication between APs and controllers using DTLS encryption.

CAPWAP is an IEEE standard protocol that enables a wireless LAN controller to manage multiple APs. It also allows Wireless LAN Controllers (WLCs) to exchange control and data plane information over a secure communication tunnel.

- Operates at Layer 3 and requires IP addresses on both APs and WLCs.
- Establishes tunnels on UDP ports 5246 (control) and 5247 (data) for IPv4 and IPv6, with DTLS encryption for security.
- Allows centralized management of the wireless network and supports secure communication between APs and controllers.

CAPWAP Protocol

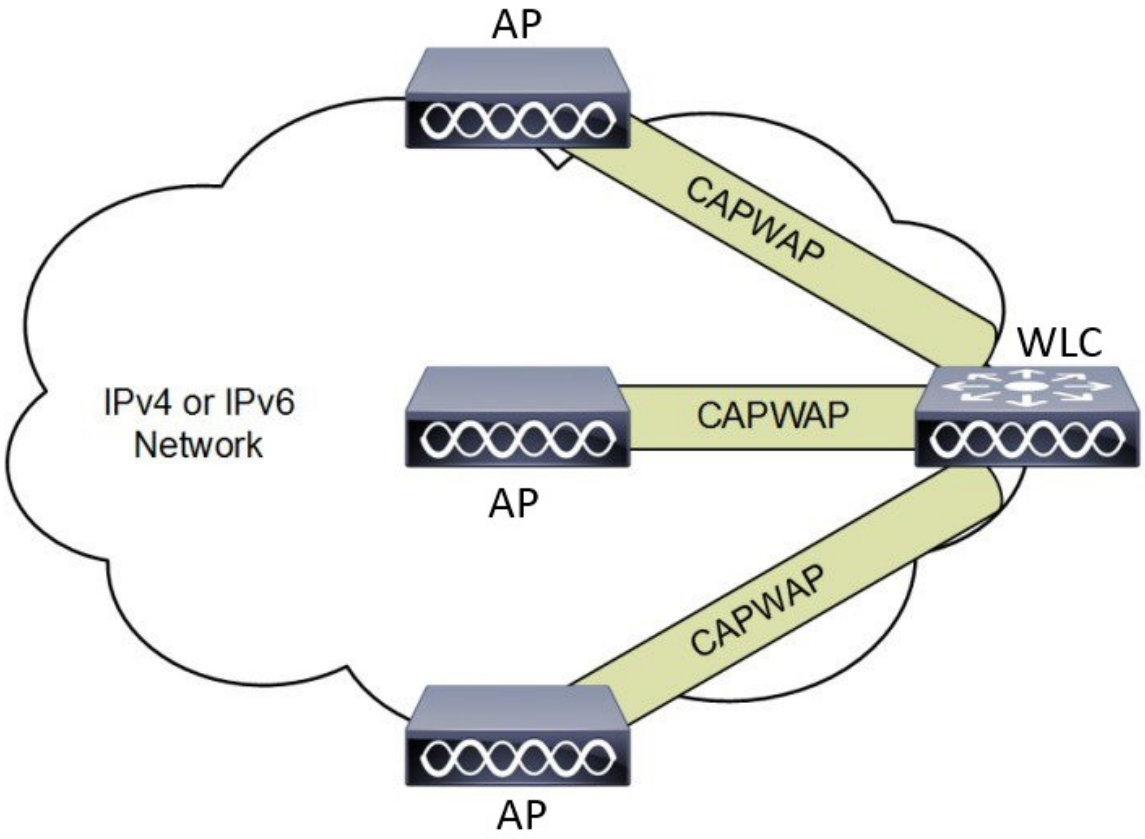
CAPWAP uses DTLS to secure the control channel, encrypting all management and control traffic between the AP and WLC. The data channel is disabled by default. To enable CAPWAP data encryption, a DTLS license is required on the WLC and additional configuration is necessary on the AP.

- DTLS ensures encrypted communication to prevent eavesdropping or tampering.
- If an AP does not support DTLS data encryption, only the control plane is secured.
- If an AP supports Data DTLS, it enables data DTLS after receiving configuration from the controller and performs a DTLS handshake on port 5247.
- All data traffic between the AP and controller is encrypted after successful DTLS session establishment.
- The IW9165E uses the IETF standard CAPWAP to communicate between the controller and other APs on the network.

CAPWAP APs Connected to a WLC

This figure shows CAPWAP APs connected to a wireless LAN controller, illustrating the secure communication tunnel established between the APs and the WLC using CAPWAP and DTLS encryption.

Figure 2: CAPWAP APs connected to a WLC



Provisioning certificates on Lightweight Access Points

This process describes the stages involved in provisioning a certificate on a Lightweight Access Point (LAP), including request, proxy, installation, and validation steps.

Certificate provisioning on a Lightweight Access Point (LAP) consists of several coordinated steps involving the LAP, controller, and certificate authority (CA).

The following actors and components participate in the certificate provisioning process:

- LAP: Initiates the certificate request and installs the signed certificate.
- Controller: Acts as a CA proxy and validates certificates during the JOIN process.
- CA: Signs the certificate request forwarded by the controller.

This process ensures secure communication by provisioning and validating device certificates on the LAP.

These stages describe the certificate provisioning workflow on a Lightweight Access Point (LAP):

1. **Certificate Request** : The LAP sends a certificate request to the controller to get a signed X.509 certificate.
2. **CA Proxy** : The controller acts as a CA proxy to facilitate the signing of the certificate request by the CA.
3. **Certificate Installation and Reboot** : Both the LSC CA and the LAP device certificates are installed in the LAP, and the system reboots automatically.
4. **JOIN Request** : After the reboot, the LAP sends the LSC device certificate to the controller as part of the JOIN request.
5. **JOIN Response and Validation** : The controller sends the new device certificate and validates the inbound LAP certificate with the new CA root certificate as part of the JOIN response.

Use LSC provisioning functionality to configure, authorize, and manage certificate enrollment with the existing PKI infrastructure for the controller and AP.

Understanding CAPWAP connectivity On AP

This topic explains how CAPWAP enables wireless access points (APs) to discover and securely connect to controllers, manage configuration and data, and operate in split or local MAC modes for efficient wireless network management.

CAPWAP (Control and Provisioning of Wireless Access Points) is a protocol that enables APs to discover, join, and communicate securely with wireless controllers, supporting both split and local MAC operation modes.

- Facilitates secure discovery and connection between APs and controllers using DTLS.
- Supports two operational modes: **Split MAC** and **Local MAC** .
- Enables centralized management of configuration, firmware, and user data traffic through control and data channels.

CAPWAP connectivity and operation details

CAPWAP connectivity involves a discovery phase, secure connection establishment, and management of AP configuration and data through dedicated channels.

- APs initiate a discovery phase by sending discovery request messages to locate a controller.
- Controllers respond with discovery responses, after which a secure DTLS connection is established.
- APs send CAPWAP join requests and receive join responses to complete the joining process.
- Controllers manage AP configuration, firmware, and control/data transactions post-join.

CAPWAP join process

This section describes the CAPWAP join process between an access point and a wireless LAN controller.

1. Enable CAPWAP on the AP.
2. AP sends discovery request to controller.
3. Controller replies with discovery response.
4. AP sends join request; controller sends join response.
5. Secure DTLS connection is established for CAPWAP control and data messages.

CAPWAP communication between the access point and the wireless LAN controller is established over two logical channels, each serving a distinct function:

- Control Channel: Used for configuration messages, image downloads, and client key exchanges. APs must acknowledge each message before sending the next.
- Data Channel: Used for encapsulation and tunneling of user data traffic between APs and WLCs, enabling centralized policy enforcement and QoS.

Table 2: CAPWAP Operation Modes Comparison

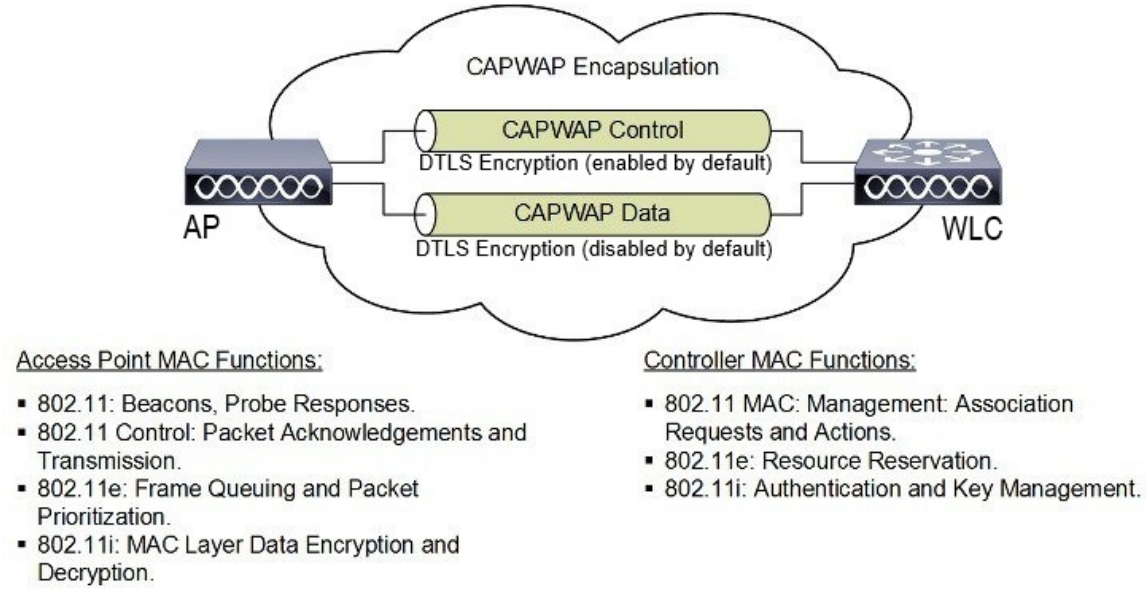
Attributes	Split MAC	Local MAC
MAC Function Distribution	802.11 protocol split between AP and WLC	All MAC functions performed at AP
Data Frame Handling	Encapsulated and exchanged between WLC and AP	Locally bridged or tunneled as Ethernet frames

Attributes	Split MAC	Local MAC
Management Frame Processing	Partially at AP, partially at WLC	Entirely at AP

Tip

In either mode, the AP processes Layer 2 wireless management frames locally before forwarding them to the controller.

Figure 3: Split MAC Architecture



Example: CAPWAP Join and Data Flow

For example, when a new AP is powered on, it sends a CAPWAP discovery request to locate a controller. After receiving a discovery response, the AP establishes a secure DTLS connection, sends a join request, and upon acceptance, the controller manages the AP's configuration and data traffic through CAPWAP channels.

Reset button settings

This topic explains the reset button settings for the IW9165E device, including the actions performed when the reset button is pressed for different durations and the device's LED behavior during reset.

The reset button on the IW9165E device allows users to perform different reset actions based on how long the button is pressed.

- Pressing the reset button for less than 20 seconds performs a full reset.
- Pressing the reset button for more than 20 seconds and less than 60 seconds performs a full factory reset (clears the FIPS flag).
- The LED turns blinking red after the boot loader receives the reset signal.

Reset button operation details

To perform a reset, ensure you press the device's reset button before powering on the device. The LED will indicate the reset status by turning blinking red after the boot loader receives the reset signal.

Ethernet port usage on CAPWAP mode

This topic explains the Ethernet port usage and internal port mapping rules for the Catalyst IW9165E in CAPWAP mode, including supported data rates and PoE standards.

The Catalyst IW9165E supports up to a 3.6 Gbps PHY data rate with two 2x2 multiple input and multiple output (MIMO) and two ethernet ports (2.5G mGig and 1G).

Catalyst IW9165E have below internal port mapping rules:

- Wired0 – One mGig (2.5 Gbps) ethernet ports with 802.3af, 802.3at, 802.3bt PoE support.

  Note

  The wired0 port is used as CAPWAP uplink port in the AP local/Flexconnect mode.

- Wired1 – 1Gig ethernet Lan Port.

  Note

  Starting from 17.14.1 release, RLAN feature is not supported in the wired1 port.

Indoor deployment

Learn how the indoor deployment mode for the IW9165E operates, including supported regulatory domains, default settings, and key considerations for access point deployment and frequency usage.

The indoor deployment mode for the IW9165E defines how the access point (AP) operates within supported regulatory domains, with specific default settings and frequency usage rules.

- Supports both indoor and outdoor deployment for regulatory domains -B (USA), -E (EU), -A (Canada), and -Z (Australia, New Zealand).
- By default, AP deployment mode is set to indoor.
- For the -B domain, outdoor and indoor frequencies are the same.

Support for 6G power modes

The following table summarizes the support for 6G power modes based on AP deployment and 6G deployment modes.

Table 3: Radio 6G power mode support table

AP Deployment Mode	6G Deployment Mode	Low Power Indoor support	Standard Power support
Indoor AP	Outdoor	No	Yes

> **Note**
>
> Outdoor mode can be used indoors, but indoor mode cannot be used outdoors because 5150–5350 MHz channels are indoor-only in -E countries.

For more information about configuring AP deployment mode on the Wireless Controller, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

Verify indoor deployment

Learn how to verify whether indoor deployment is enabled or disabled on the WLC and AP, and how to interpret the relevant CLI outputs.

This procedure describes how to verify whether the indoor deployment is enabled or not on the WLC and AP.

This procedure helps you determine the indoor deployment status on both the Wireless LAN Controller (WLC) and Access Point (AP).

1. Run the **show ap name** *ap-name* **config general | inc Indoor** command on the WLC.
   - When indoor mode is enabled, the show command provides the following output:

```
Device# show ap name ap-1 config general | inc Indoor
AP Indoor Mode          : Enabled
```

   - When indoor mode is disabled, the show command provides the following output:

```
Device# show ap name ap-1 config general | inc Indoor
AP Indoor Mode          : Disabled
```

2. Run the **show controllers Dot11Radio** *interface* command on the AP to check the indoor deployment status.
   - When indoor mode is enabled, the show command provides the following output:

```
Device# show controllers Dot11Radio 1
                                    …
Radio Info Summary:
 ======================
Radio: 5.0GHz
Carrier Set:  (-Ei)( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```

> **Note**
>
> In the command output, **-Ei** indicates the indoor mode is enabled.

- When indoor mode is disabled, the show command provides the following output:

```
Device# show controllers Dot11Radio 1
                                        …
Radio Info Summary:
 ======================
Radio: 5.0GHz
Carrier Set:  (-E)( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```

> **Note**
>
> In the command output, **-E** indicates that indoor mode is disabled.

The CLI output also shows the supported channels.

AP Radio Slot

This topic explains the AP Radio Slot feature in Cisco Catalyst IW9165E, including its dedicated Wi-Fi radios, dual-band switching capability, and the command used to switch between 5G and 6G bands.

The Cisco Catalyst IW9165E provides one dedicated 2x2 5GHz Wi-Fi radio and a Dual Band (XOR) radio that serves both 5 GHz and 6 GHz 2x2 radio bands.

- Supports dedicated 5GHz Wi-Fi radio and Dual Band (XOR) radio for 5 GHz and 6 GHz bands.
- Allows switching between 5G and 6G bands.
- Admin state is disabled by default; Slot 2 XOR radio is fixed to 5G by default.

AP Radio Slots

To switch between 5G and 6G bands on the Catalyst IW9165E, use the following CLI command:

- `ap name <ap-name> dot11 dual-band band 6ghz/5ghz`

> **Note**
>
> By default, admin state is disabled. Slot 2 XOR radio is fixed to 5G.

Table 4: AP Wi-Fi radio architecture modes

Mode	5 GHz Slot 1	5/6 GHz Slot 2
5G + 5G	5GHz 2x2:2SS (20/40/80 MHz)	5G 2x2:2SS (20/40/80/160 MHz)
5G + 6G	5GHz 2x2:2SS (20/40/80 MHz)	6G 2x2:2SS (20/40/80/160 MHz)

Supported fixed domains and country codes

This topic explains the fixed domain and country code support for Catalyst IW9165E access points, including supported domains and country codes for regulatory compliance.

The ROW regulatory domain simplifies the domain management of the manufacturing process for all the country codes that do not have a specific domain mapped.

Supported Fixed Domains

Domain	Country Codes
A	CA (Canada)
B	US (United States of America)

Domain	Country Codes
E	• AT (Austria) • AT (Austria) • BE (Belgium) • BG (Bulgaria) • HR (Croatia) • CY (Cyprus) • CZ (Czech Republic) • DK (Denmark) • EE (Estonia) • FI (Finland) • FR (France) • DE (Germany) • GR (Greece) • HU Hungary) • IS (Iceland) • IE (Ireland) • IT (Italy) • LV (Latvia) • LI (Liechtenstein) • LT (Lithuania) • LU (Luxembourg) • MT (Malta) • NL (Netherlands) • NO (Norway) • PL (Poland) • PT (Portugal) • RO (Romania) • SK (Slovak Republic) • SI (Slovenia) • ES (Spain) • SE (Sweden), and • CH (Switzerland).
F	ID (Indonesia)

Domain	Country Codes
Q	JP (Japan)
Z	• AU (Australia) and • NZ (New Zealand).

Catalyst IW9165 supported country codes (ROW)

Domain	Country Codes
ROW	• CL (Chile) • KR (Korea, Republic of) • GB (United Kingdom), and • VN (Vietnam).

Note

You are responsible for ensuring APs approval for use in your country. To verify approval and to identify the regulatory domain associated with a particular country. For more information, see Cisco Product Approval Status .

Radio antenna settings

This topic explains how to configure radio antenna settings for the Catalyst IW9165E, including supported antenna types, port assignments, and verification steps for Self Identifiable Antenna (SIA) compatibility.

The Catalyst IW9165E radio antenna settings define how external antennas are connected and configured for optimal wireless performance.

- The device supports four external antennas with RP-SMA (f) connectors.
- Radio 1 connects to antenna ports 1 and 2; Radio 2 connects to antenna ports 3 and 4.
- The IW9165E is compatible with Self Identifiable Antenna (SIA) antennas for the 6G band, with ports 1 and 3 supporting SIA antennas.

Supported antenna types and port assignments

The Catalyst IW9165E supports a range of external antennas and provides specific port assignments for each radio. SIA antennas are supported on select ports for the 6G band.

- Four external antennas with RP-SMA (f) connectors
- Radio 1: Antenna ports 1 and 2
- Radio 2: Antenna ports 3 and 4
- SIA antennas supported on ports 1 and 3 for the 6G band
- Compatible SIA antennas: IW-ANT-OMV-2567-N and IW-ANT-OMH-2567-N

Comparison of antenna gain values for each slot is shown in this table.

Table 5: Antenna gain (dBm)

5 GHz Slot 1	5 GHz Slot 2	6 GHz Slot 2
3 4 7 8 10 13 15	3 4 7 8 10 13 15	7

Note

A power cycle is mandatory after the first installation of the SIA antenna.

For more information on antennas, see the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Hardware Installation Guide .

This example demonstrates how to verify the SIA status on the controller using CLI commands. Run the **show ap config slots** <AP> command to display SIA information.

Device# show ap config slots AP2CF8.9B1C.CE78 Cisco AP Name : AP4C42.1E51.A144 Attributes for Slot 2 SIA Status : Present(RPTNC) SIA Product ID : IW-ANT-OMV-2567-N

AFC support for 6 GHz standard power mode

Learn how Automated Frequency Coordination (AFC) supports 6 GHz Standard Power mode on the Cisco Catalyst IW9165E, including operational requirements, power limitations, and deployment considerations.

The 6 GHz Standard Power mode is a regulatory-compliant operational mode for access points (APs) that requires coordination through an Automated Frequency Coordination (AFC) system.

- Standard Power APs must obtain available frequencies and power levels from the AFC system before operation.
- The AFC system determines allowable frequencies and maximum power based on regulatory body data (such as FCC for the U.S.).
- Transmission power is limited to a maximum of 36 dB EIRP, and APs are permitted in UNII-5 and UNII-7 bands in the -B (U.S) domain.

Standard power mode operation and deployment

The Cisco Catalyst IW9165E supports AFC 6 GHz Standard Power mode, enabling APs to operate in outdoor environments with regulatory compliance. The AFC system computes available frequencies and power, and coordinates AP operation to avoid interference.

Table 6: Radio 6 GHz Power Mode Support

AP Deployment Mode	6G Deployment Mode	Low-power Indoor Support	Standard Power Support
Indoor AP	Outdoor	No	Yes

Table 7: 6 GHz Target Power

Max Conducted per Path Power (SP/AFC)	Antenna Gain	Tx x Rx Chains	Max EIRP (SP/AFC)

20-80Mhz	160Mhz			
17 dBm	17 dBm	7 dBi	2x2	27 dBm

Verify AFC status on an AP

Learn how to verify the AFC request and response data, as well as the current operating power mode, on an AP using commands.

This procedure describes how to verify the AFC request and response data, as well as the current operating power mode, on an AP using commands.

1. Use the **show rrm afc** command to verify the AFC request and response data on the AP.

```
Device# show rrm afc

Location Type: 1
Deployment Type: 2
Height: 129
Uncertainty: 5
Height Type: 0
Request Status: 5
Request Status Timestamp: 2023-08-31T06:20:17Z
Request Id Sent: 5546388983266789933
Ellipse 1: longitude: -121.935066 latitude: 37.512830 major axis: 43 minor
axis:
9 orientation: 36.818100
AFC Response Request ID: 5546388983266789933
AFC Response Ruleset ID: US_47_CFR_PART_15_SUBPART_E
```

2. Use the **show controllers dot11Radio 2 | i Radio** command to verify the current operating power mode.

```
Device# show controllers dot11Radio 2 | i Radio
Dot11Radio2     Link encap:Ethernet  HWaddr 24:16:1B:F8:06:C0
Radio Info Summary:
Radio: 6.0GHz (SP)
```

Antenna disconnection detection

Learn how the Antenna Disconnection Detection feature monitors antenna integrity on access points to ensure optimal performance and reliability by identifying impaired or disconnected antennas.

Antenna Disconnection Detection is a feature that monitors the signal strength delta across antennas on an access point to identify impaired or disconnected antennas.

- Improves performance and reliability by using multiple antennas for better signal reception.
- Detects antenna issues based on signal strength differences exceeding a defined threshold for a specific duration.
- Notifies the system through IAPP messages and controller logs when an antenna issue is detected.

How Antenna Disconnection Detection Works

Multiple antennas on the transmitter and receiver of an access point (AP) enhance performance and reliability by selecting or combining the strongest signals. Detecting an impaired or physically broken antenna is critical to AP reliability.

The Antenna Disconnection Detection feature operates by monitoring the signal strength delta across the antennas on the receiver. If the delta exceeds a defined limit for a specific duration, the antenna is flagged as having issues.

- Improved reception through antenna diversity.
- Critical detection of antenna impairment or breakage.
- Automated notification via IAPP messages and controller logs.

For more information about configuring Antenna Disconnection Detection on the Wireless Controller, see Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide .

Verify Antenna Disconnection Detection on an AP or AP Profile

Learn how to verify the Antenna Disconnection Detection feature configuration on an access point (AP) or AP profile using CLI commands.

This procedure describes how to ensure that APs are operating with properly connected antennas. Verifying this configuration can help diagnose connectivity or coverage issues.

1. Use the **show ap name***ap-name* **config general** command to verify the configuration on an AP.

```
Conroller# show ap name AP4C42.1E51.A144 config general

Cisco AP Name   : AP4C42.1E51.A144
================================================
Cisco AP Identifier                              : 8c84.4292.f840
Country Code                                     : Multiple Countries :
US,CN,GB,HK,DE,IN,CZ,NZ
Regulatory Domain Allowed by Country             : 802.11bg:-ACE^
802.11a:-ABCDEHNSZ^   802.11 6GHz:-BEZ^
Radio Authority IDs                              : None
AP Country Code                                  : CZ  - Czech Republic
AP Regulatory Domain
802.11bg                                        : -E
802.11a                                         : -E
MAC Address                                      : 8c84.4292.f840
IP Address Configuration                         : DHCP
IP Address                                       : 9.9.33.3
IP Netmask                                       : 255.255.255.0
Gateway IP Address                               : 9.9.33.1
Fallback IP Address Being Used                   :
Domain                                           :
Name Server                                      :
CAPWAP Path MTU                                  : 1485
Capwap Active Window Size                        : 1
```

2. Use the **show ap profile name***ap-profile* **detailed** command to verify th detailed configuration parameters of a specific access point profile on the controller.

```
Controller# show ap profile name ap-profile detailed

AP Profile Name: ap-profile
.
.
.
AP broken antenna detection:
```

```
Status                                                  : ENABLED
RSSI threshold                                          : 40
Weak RSSI                                               : -80
Detection Time                                          : 120
```

Troubleshooting

Learn how to identify use cases and key considerations for understanding CAPWAP or LWAPP tunnel breaks between access points (APs) and the wireless controller, including references to additional troubleshooting resources.

The document provides use cases to understand the reason for the Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) tunnel break between Access Points (APs) and the Wireless Controller.

For more information, see Troubleshoot Access Point Disassociation from Controller

Note

There could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

Feedback request

Your input helps. A key aspect to improving these support documents is customer feedback. Note that these documents are owned and maintained by multiple teams within Cisco. If you find an issue specific to the document (unclear, confusing, information missing, etc):

- Provide feedback using the Feedback button located at the right panel of the corresponding article. The document owner will be notified, and will either update the article, or flag it for removal.
- Include information regarding the section, area, or issue you had with the document and what could be improved. Provide as much detail as possible.

Disclaimer and caution

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

GNSS

Introduces GNSS enhancements in Release 26.1.1, including controller-based enable or disable support and improved runtime status and diagnostic output.

Global Navigation Satellite System (GNSS) is a general term for satellite-based systems that provide positioning, navigation, and timing (PNT) services.

- GNSS provides positioning and navigation services anywhere on Earth.
- GNSS delivers position accuracy ranging from a few meters (standard) down to centimeters or millimeters.
- GNSS enables receivers to synchronize time to within billionths of a second, an essential requirement for telecom, power grids, and financial networks.

With Release 26.1.1, two GNSS enhancements are available: an option to enable or disable GNSS from the controller, and improved output for the **show gnss info** command, offering more detailed runtime status and diagnostics.

Disable GNSS

Explains how to dynamically disable GNSS on a specific access point to prevent inaccurate location reporting when satellite signals are weak.

From release 26.1.1, you can dynamically disable the GNSS service on a specific access point. This capability is especially useful when weak satellite signals could cause an AP to report inaccurate coordinates. By disabling GNSS in such cases, you can prevent incorrect location data from affecting the system and ensure the AP uses an alternative location source.

Use this procedure on the controller to disable the GNSS service.

Use the **ap name** *ap-name* **geolocation gnss shutdown** command to specify the AP and disable the GNSS service on that AP.

```
Device# ap name AP-BLR-01 geolocation gnss shutdown
```

The configuration persists across AP reboots.

Enable GNSS

Guides how to re-enable GNSS service on a specific access point from the controller using the appropriate geolocation command.

Use this procedure on the controller to enable the GNSS service.

Use the **ap name** *ap-name* **no geolocation gnss shutdown** command to specify the AP and enable the GNSS service on that AP.

```
Device# ap name AP-BLR-01 no geolocation gnss shutdown
```

Check the status of the GNSS module

Describes how to verify the administrative state of the GNSS module on an access point using the **show gnss info** command.

Starting with release 26.1.1, you can set the state of the GNSS module to administratively down. Use this procedure on the AP to check the status of the GNSS module.

Use the **show gnss info** command to view the status of the GNSS module.

```
Device# show gnss info

GNSS State Down
```

GNSS status and diagnostics

Explains the enhanced GNSS diagnostic output, including satellite details, signal quality, location data, fix status, accuracy, and uncertainty information.

The updated **show gnss info** command now includes more detailed runtime GNSS status and diagnostics including satellite distribution, signal quality, number of satellites, location, uncertainty ellipse and more.

A sample output is provided.

```
AP# show gnss info

GnssState: Started
ExternalAntenna: true
Fix: 3D-Fix ValidFix: true Time: 2022-01-01 00:01:01
Latitude: 37.4080 Longitude: -121.9530
HorAcc: 0 hDOP: 0.84
Uncertainty Ellipse:
 Major axis: 0 Minor axis: 0 Orientation: 0
Altitude MSL: 176.4 HAE: 0 VertAcc: 0
NumSat: 10
pDOP: 1.75 hDOP: 0.84 vDOP: 1.54 nDOP: 99.99 eDOP: 99.99 gDOP: 99.99 tDOP:
99.99
LastFixTime: 2022-01-01 00:01:00
SatelliteCount: 4

Const.    SatId CNO   Elev. Azim.
GPS       1     47    28    110
GPS       7     44    55    127
GPS       8     45    19    44
GPS       9     42    3     175

GNSS_PostProcessor:
Latitude: 37.4080 Longitude: -121.9530
HorAcc: 32.413618 hDOP: 18.628516
Uncertainty Ellipse:
 Major axis: 44.269861 Minor axis: 10.924539 Orientation: 141.70748
Altitude MSL: 360.78333 HAE: 0 VertAcc: 0

CiscoGNSS: N/A

Last Location Acquired:
Latitude: 37.4080 Longitude: -121.9530
HorAcc: 3.6618832 hDOP: 2.1045306
Uncertainty Ellipse:
 Major axis: 5.151356 Minor axis: 0.00035979961 Orientation: 146.63993
Altitude MSL: 310.9 HAE: 0 VertAcc: 0
Derivation Type: GNSS_PostProcessor
Time: 2025-10-05 01:28:46
```

© 2023-2025 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at 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/c/en/us/about/legal/trademarks.html. 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. (1721R)