Cisco Catalyst 9105AX Series Access Point Getting Started Guide

About this Guide

This guide provides instructions on how to install your Cisco Catalyst 9105AX series access point. It also contains mounting instructions and troubleshooting information along with links to resources that can help you configure your access point.

Note that the C9105AX series access point is referred to as the access point or the AP in this document.

About the Cisco Catalyst 9105AX Series Wireless Access Point

The Cisco Catalyst 9105AX series wireless access point is an advanced dual-band, dual-concurrent, enterprise 802.11ax (Wi-Fi 6) AP. This AP series has two models, both with integrated antennas only. The APs support 2x2:2 SS MU-MIMO applications and are designed to use both the 2.4 GHz and the 5 GHz bands.

Depending on the model, the AP can be mounted either on a wall or a ceiling. The AP supports full interoperability with leading 802.11ax and 802.11ac clients, along with a mixed deployment with other APs and controllers.

Cisco Catalyst 9105AX Series Wireless Access Point Features

A full listing of the AP's features and specifications are provided in the Cisco Catalyst 9105AX Series Access Point Data Sheet, at the following URL:

CCO URL to be added at FCS

The C9105AX series wireless AP is a wireless controller-based product and supports:

- Four dual-band integrated antennas on the 9105AX access point models (C9105AXI-*x* and C9105AXW-*x*)

Note The '*x*' in the model numbers represents the regulatory domain. For information on supported regulatory domains, see AP Model Numbers and Regulatory Domains, on page 4.

- Integrated internal antennas, omnidirectional in azimuth for both 2.4 GHz (peak gain 3dBi) and 5 GHz (peak gain 4dBi)
- Simultaneous 2x2 MIMO with 2 spatial streams for both 2.4 GHz and 5 GHz bands
- The following hardware external interfaces:
  - 1x100/1000/2500 Multigigabit Ethernet (RJ-45)
  - RS-232 Console Interface through RJ-45
  - Mode button (enables partial or full system configuration recovery)
  - USB 2.0 Port
  - One multi-color LED status indicator.
- Multiuser multiple-input multiple-output (MU-MIMO) technology with 2 spatial streams for downlink.
- Orthogonal Frequency Division Multiple Access (OFDMA)-based scheduling for both downlink and uplink
- Spatial Reuse (also known as BSS coloring) allows APs and their clients to differentiate between BSSs, thus permitting more simultaneous transmissions.
- New power savings mode called Target-Wakeup-Time (TWT), allows the client to stay asleep and wake up only at pre-scheduled (target) times to exchange data with the AP. This allows for significant energy savings for battery-operated devices.

- Cisco Digital Network Architecture (DNA) support enables Cisco Connected Mobile Experiences, Apple FastLane and Cisco Identity Services Engine.
- Cross-AP Noise Reduction, a Cisco innovation that enables APs to intelligently collaborate in real time about RF conditions so that users connect with optimized signal quality and performance.
- Optimized AP Roaming for ensuring that client devices associate with the AP in their coverage range that offers the fastest data rate available.
- Cisco CleanAir technology enhanced with 80-MHz channel support. CleanAir delivers proactive, high-speed spectrum intelligence across 20-, 40-, and 80-MHz-wide channels to combat performance problems arising from wireless interference.
- MIMO equalization capabilities, which optimize uplink performance and reliability by reducing the impact of signal fade.

The AP supports both Cisco Embedded Wireless Controller and lightweight deployments (using Cisco Wireless Controllers). The AP supports the following operating modes:

- Local—This is the default mode for the Cisco AP. In this mode, the AP serves clients.
- FlexConnect—FlexConnect mode for the Cisco AP.
- Monitor—This is the monitor-only mode for the Cisco AP.
- Sniffer—In the wireless sniffer mode, the AP starts sniffing the air on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). This includes information on the time stamp, signal strength, packet size, etc.

Note In the sniffer mode, the server to which the data is sent should be on the same VLAN as the wireless controller management VLAN, otherwise an error will be displayed.

- OEAP—This is the office extend mode for the Cisco AP.

AP Model Numbers and Regulatory Domains

Table 1: AP Model Numbers and Regulatory Domains

AP Type	Model Number	Details
Access Point for indoor environments, with internal antennas	C9105AXI-*x*	Dual-band, controller-based 802.11ax
	C9105AXW-*x*	Dual-band, controller-based 802.11ax, wallplate

You need to verify whether the AP model you have is approved for use in your country. To verify approval and to identify the regulatory domain that corresponds to a particular country, visit http://www.cisco.com/go/aironet/compliance. Not all regulatory domains have been approved. As and when they are approved, this compliance list will be updated.

Antennas and Radios

The C9105AX series access point configurations are:

- C9105AXI-*x*
- C9105AXW-*x*

Infrastructure APs (C9105AXI-*x*)

The C9105AXI AP has two internal dual-band antennas with a dedicated 2.4 GHz radio, a 5 GHz radio, and a dedicated 2.4 GHz IOT radio.

The AP can be mounted on a wall or a ceiling, and supports 2x2:2 SS MU-MIMO applications.

Wallplate APs (C9105AXW-*x*)

Like the C9105AXI APs, the C9105AXW-*x* access points have integrated antennas. They can be vertically mounted on a wall or on a standard junction box. Physical security is offered with the included Torx screw and the option to add a Kensington lock.

Safety Instructions

Translated versions of the following safety warnings are provided in the translated safety warnings document that is shipped with your access point. The translated warnings are also in the `Translated Safety Warnings for Cisco Catalyst Access Points`, which is available on Cisco.com.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Warning Read the installation instructions before using, installing or connecting the system to the power source.

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. To reduce risk of electric shock or fire, ensure that the protective device is rated not greater than:

20A, 240Vac

Warning To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Warning Ultimate disposal of this product should be handled according to all national laws and regulations.

Caution Statement CS-0440--Suitable for Use in Environment Air Spaces This equipment is suitable for use in environment air spaces (plenums) in accordance with Section 300.22 (C) of the National Electrical Code, and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, CSA C22.2. External power supply, power adapter and/or power injector, if provided, are not suitable installation in air spaces.

Unpacking

To unpack the access point, follow these steps:

Before you begin

The following accessories can be ordered separately from Cisco:

- AIR-AP-BRACKET-8= for ceiling mount installations
- AIR-AP-BRACKET-W4= for wall or electrical box installations
- Mid-span power injector AIR-PWRINJ6= when PoE is not available
- Spacer kit, includes spacer box, RJ-45 jumper cable, four M3.5x32 mounting screws, two #6-32x1.62" truss head machine screws, two M3x8 pan head mounting screws.
- Physical security kit AIR-SEC-50=, which includes 50 security screws used to secure the access point onto the wall-mounting bracket, 50 RJ-45 block-out plugs and 2 unlock keys for blocking physical access to the RJ45 Ethernet ports.
- Bracket Kit AIR-AP-BRACKET-W3, includes the mounting bracket, one M2x5.5 Torx security screw, two M3.5x32 pan head mounting screws, two #6-32x0.81" truss head machine-type mounting screws.

Procedure

Step 1 Unpack and remove the AP and the accessory kit (C9105AXW-KIT for wall or electrical box installations) from the shipping box.

Step 2 Return any packing material to the shipping container and save it for future use.

Step 3 Verify that you have received the items listed below. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.

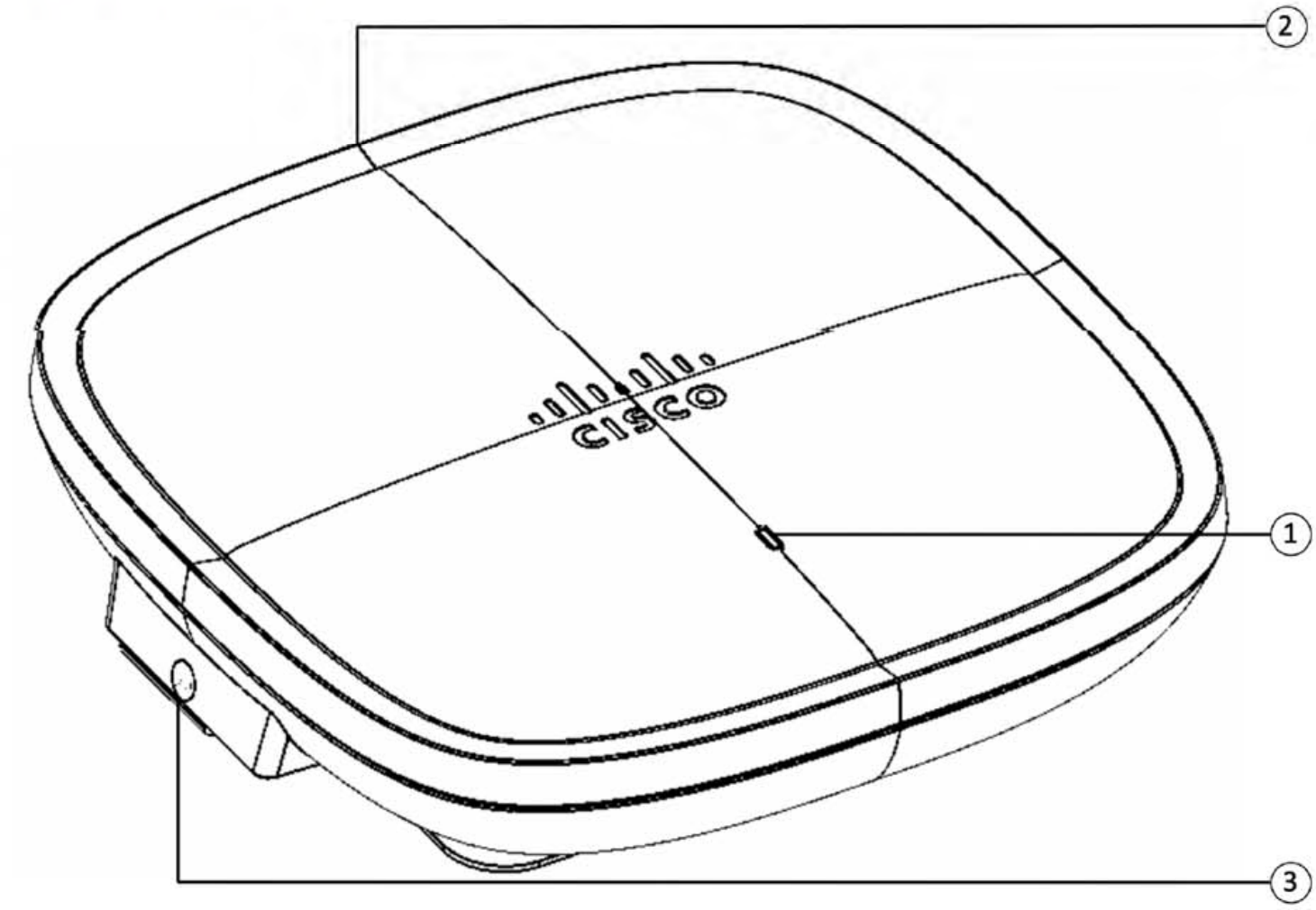
- The access point
- Mounting bracket

- For C9105AXI-*x*—AIR-AP-BRACKET-1= (default) or AIR-AP-BRACKET-2= (only if selected when you order the access point)
- For C9105AXW-*x*—AIR-AP-BRACKET-W3, and screws.

- Adjustable ceiling-rail clip (AIR-AP-T-RAIL-R or AIR-AP-T-RAIL-F) (selected when you order the access point)
- Torx security screw and mylar label to cover the screw (for C9105AXW-*x*).
- Power Injector AIR-PWRINJ6= (only if selected when you ordered the access point).

AP Views, Ports, and Connectors

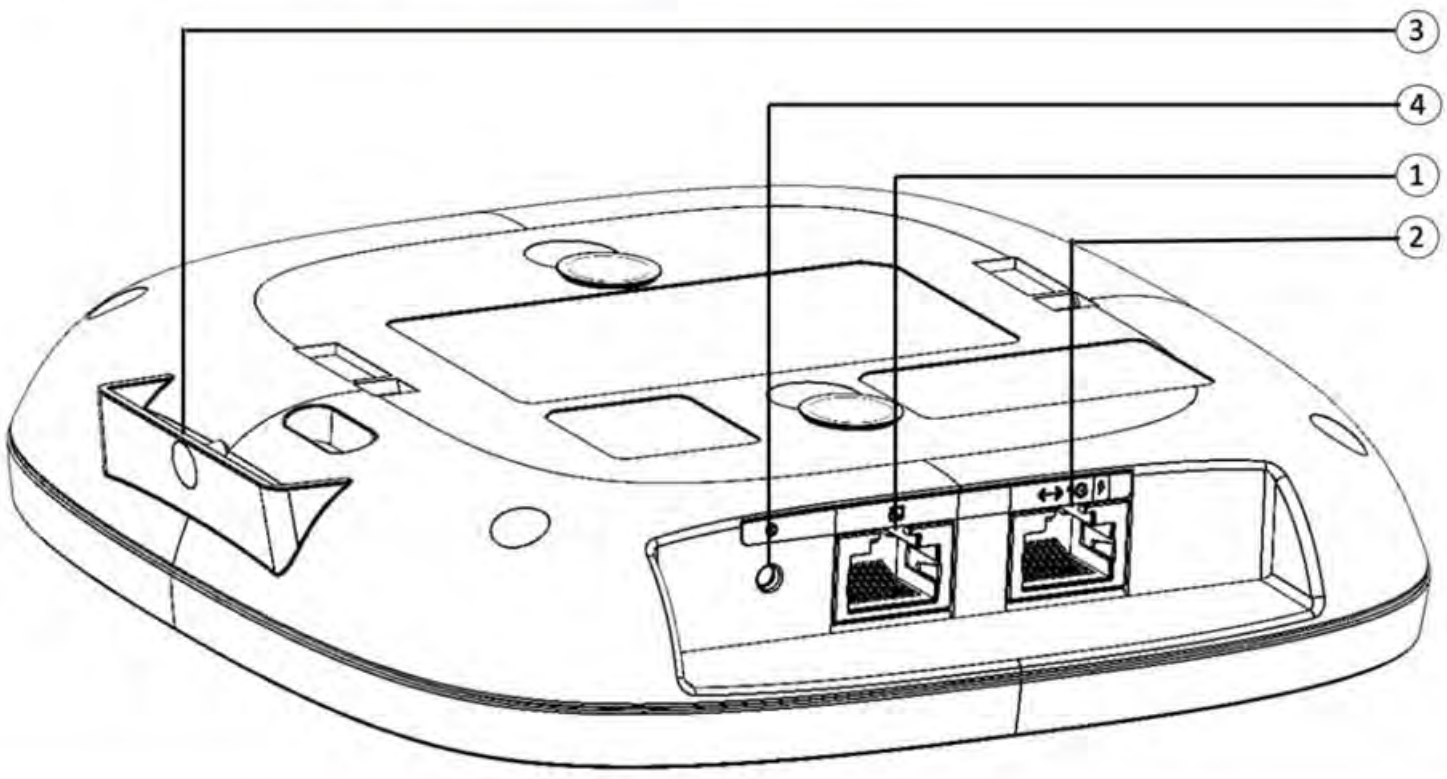
Figure 1: Face of the C9105AXI Model



1	Status LED[1]	3	USB 2.0 port
2	Location of the ports and connectors on the head of the AP.		

[1] For more information, see Checking the Access Point LEDs, on page 20 section.

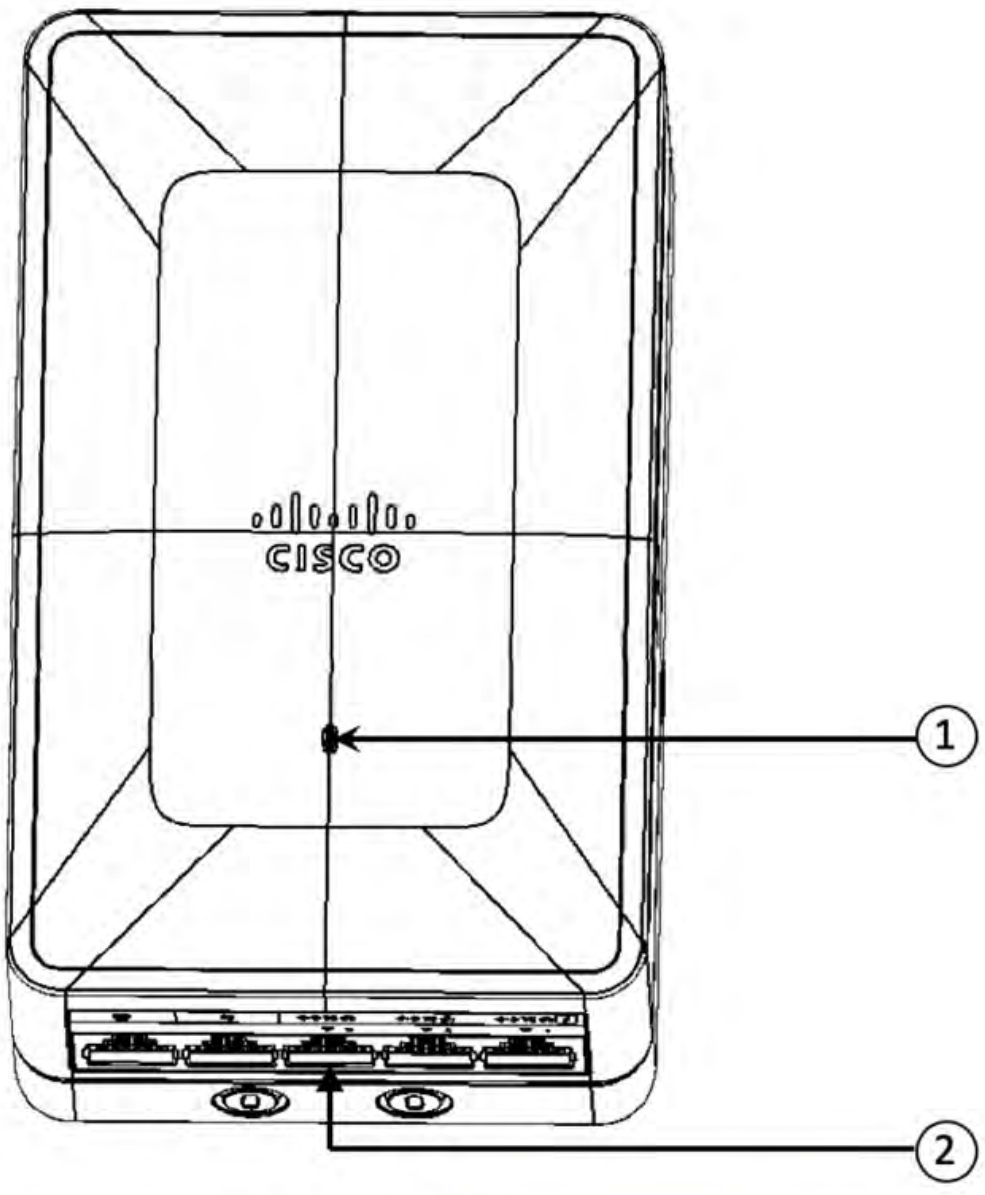
Figure 2: Ports and Connectors on the Head of the C9105AXI Model



1	RJ-45 console port	3	USB 2.0 port
2	PoE-In 1 GbE uplink port	4	Mode button[2]

[2] For information on how to use the Mode button, see Using the Mode Button, on page 21 section.

Figure 3: Face of the C9105AXW Model



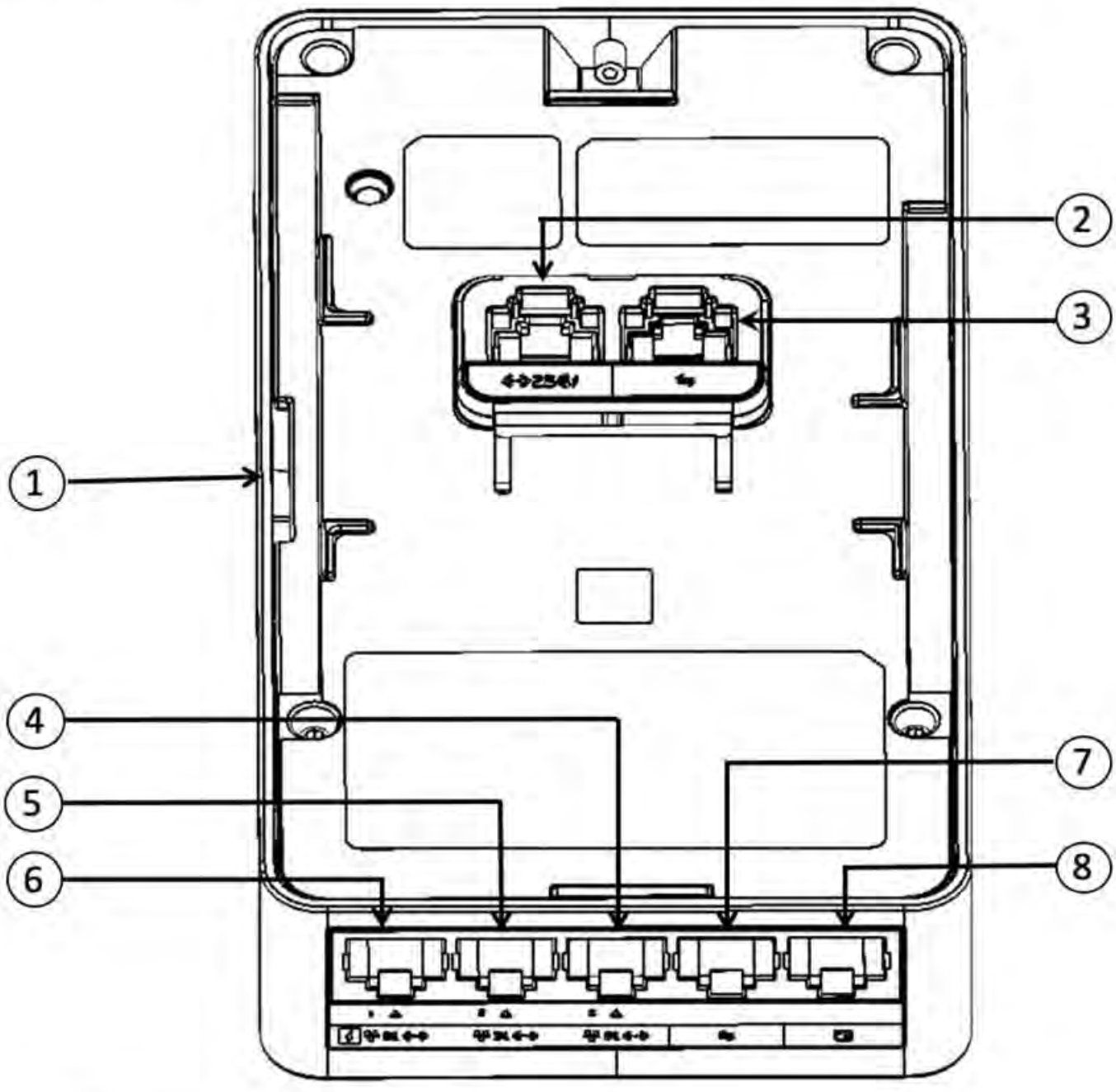
1	Location of the Status LED[3]	2	Ports and connectors on the base of the AP

[3] For more information, see Checking the Access Point LEDs, on page 20 section.

Note

- A physical security kit, which is sold separately, includes RJ-45 block-out plugs and two unlock keys using which you can restrict physical access to the Ethernet port.
- All the three LAN ports support Auto-MDIX. The interface automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately.

Figure 4: Ports and Connectors on the Base of the C9105AXW Model



1	Security screw, under mylar cover	5	1 GbE port (LAN port 2)

2	2.5GbE mGig uplink port This port supports: • Inline power capability • 10/100/1000/2500 capability. • Auto-MDIX (automatically support either straight through or crossover cables) • 802.3af/at power over the Ethernet interface	6	PSE (LAN port 1) This port provides 802.3af Power Sourcing Equipment (PSE) PoE-Out power on the LAN 1 Ethernet interface, when powered by 802.3at power.
3	Passive Pass-Through port. It is an RJ-45 port, from the back of the AP to the base of the AP.	7	Pass-Through port.
4	1 GbE port (LAN port 3)	8	RJ-45 console port

Preparing the AP for Installation

Before you mount and deploy your access point, we recommend that you perform a site survey (or use the site planning tool) to determine the best location to install your access point.

You should have the following information about your wireless network available:

- Access point locations
- Access point mounting options—on a wall or a ceiling only

Note You can mount the access point above a suspended ceiling but you must purchase additional mounting hardware: See Mounting the Access Point, on page 14 for additional information.

- Access point power options—802.3at (PoE+) (Cisco Power Injector AIR-PWRINJ6=), 802.3af (Cisco Power Injector AIR-PWRINJ5=), Cisco Universal PoE (Cisco UPOE), or hub (usually located in a wiring closet).

Note
- Access points mounted in a building's environmental airspace must be powered using PoE to comply with safety regulations.
- If AIR-PWRINJ5 is used, both the 2.4 GHz and 5 GHz radios will be reduced to 2x2 and Ethernet is downgraded to 1 GbE. The USB port will also be off.

Cisco recommends that you make a site map showing access point locations so that you can record the device MAC addresses from each location and return them to the person who is planning or managing your wireless network.

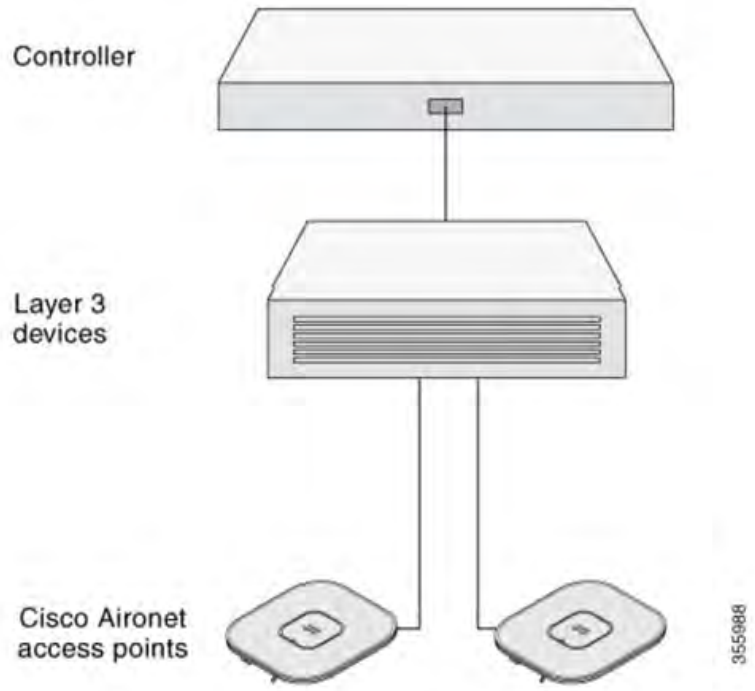
Installation Overview

Installing the access point involves the below operations:

Performing a Pre-Installation Configuration

The pre-installation configuration setup is illustrated in Figure 5: Pre-Installation Configuration Setup, on page 12.

Figure 5: Pre-Installation Configuration Setup



To perform pre-installation configuration, perform the following steps:

Before you begin

The following procedure ensures that your access point installation and initial operation go as expected. This procedure is optional.

Note Performing a pre-installation configuration is an optional procedure. If your network controller is properly configured, you can install your access point in its final location and connect it to the network from there. See the Deploying the Access Point on the Wireless Network, on page 20 for details.

Procedure

Step 1 Make sure that the Cisco Wireless Controller DS port is connected to the network. Use the procedure for CLI or web-browser interface as described in the appropriate Cisco Wireless Controller guide.

a) Make sure that access points have Layer 3 connectivity to the Cisco Wireless Controller Management and AP-Manager Interface.
b) Configure the switch to which your access point is to attach. See the Cisco Wireless Controller Configuration Guide for the release you are using. for additional information.
c) Set the Cisco Wireless Controller as the master so that new access points always join with it.
d) Make sure DHCP is enabled on the network. The access point must receive its IP address through DHCP.

Note An 802.11ax Cisco AP will be assigned an IP address from the DHCP server only if a default router (gateway) is configured on the DHCP server (enabling the AP to receive its gateway IP address) and the gateway ARP is resolved.

e) CAPWAP UDP ports must not be blocked in the network.
f) The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the Configuring DHCP Option 43 for more information.

Note The access point requires a gigabit Ethernet (GbE) link to prevent the Ethernet port from becoming a bottleneck for traffic because wireless traffic speeds exceed transmit speeds of a 10/100 Ethernet port.

Step 2 Apply power to the access point. See Grounding the Access Point, on page 19.

a) As the access point attempts to connect to the controller, the LEDs cycle through a green, red, and blue sequence, which can take up to 5 minutes.

Note If the access point remains in this mode for more than five minutes, the access point is unable to find the Master Cisco Wireless Controller. Check the connection between the access point and the Cisco Wireless Controller and be sure that they are on the same subnet.

b) If the access point shuts down, check the power source.
c) After the access point finds the Cisco Wireless Controller, it attempts to download the new operating system code if the access point code version differs from the Cisco Wireless Controller code version. While this is happening, the Status LED blinks blue.
d) If the operating system download is successful, the access point reboots.

Step 3 Configure the access point if required. Use the controller CLI, controller GUI, or Cisco Prime Infrastructure to customize the access-point-specific 802.11ax network settings.

Step 4 If the pre-installation configuration is successful, the Status LED is green indicating normal operation. Disconnect the access point and mount it at the location at which you intend to deploy it on the wireless network.

Step 5 If your AP does not indicate normal operation, turn it off and repeat the pre-installation configuration.

Note When you are installing a Layer 3 access point on a different subnet than the Cisco Wireless Controller, be sure that a DHCP server is reachable from the subnet on which you will be installing the access point, and that the subnet has a route back to the Cisco Wireless Controller. Also be sure that the route back to the Cisco Wireless Controller has destination UDP ports 5246 and 5247 open for CAPWAP communications. Ensure that the route back to the primary, secondary, and tertiary controller allows IP packet fragments. Finally, be sure that if address translation is used, that the access point and the Cisco Wireless Controller have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)

Mounting the Access Point

Mounting the C9105AXI-*x*

Cisco Catalyst 9105AX series access points can be mounted in several configurations – on a suspended ceiling, on a hard ceiling or wall, on an electrical or network box, and above a suspended ceiling.

Note When mounting the AP in the plenum air space or above a suspended ceiling, it should be mounted on a vertical wall or with the face of the AP (having the status LED) directed downwards.

For access point mounting instructions, go to the following URL:

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mounting/guide/apmount.html

The standard mounting hardware supported by the AP is listed in Table 2: Brackets and Clips for Mounting the AP, on page 14.

Table 2: Brackets and Clips for Mounting the AP

	Part Number	Description
Bracket	AIR-AP-BRACKET-8	Mounting bracket for ceiling and wall. See Figure 6: AIR-AP-BRACKET-8, on page 14
Clips	AIR-AP-T-RAIL-R	Ceiling Grid Clip (Recessed mounting) (This is the default option)
	AIR-AP-T-RAIL-F	Ceiling Grid Clip (Flush mounting)
	AIR-CHNL-ADAPTER	Optional adapter for channel-rail ceiling grid profile.

Figure 6: AIR-AP-BRACKET-8

Mounting the C9105AXW-*x*

The Cisco Catalyst C9105AXW-*x* access points can be mounted directly on the wall, to numerous global wall junction standards.

Table 3: C9105AXW-x Access Point Mounting Options

Type of Mounting	Mounting Bracket and Kit
Mounting the C9105AXW AP directly on a Wall, on page 14	AIR-AP-BRACKET-W4
Mounting the C9105AXW AP on an Electrical Junction Box, on page 16	AIR-AP-BRACKET-W4 C9105AXW-KIT spacer kit

Mounting the C9105AXW AP directly on a Wall

To mount the AP on a wall, follow these steps:

Procedure

Step 1 Fasten the wall-mount bracket (AIR-AP-BRACKET-W4) to the wall, using two M3.5X32mm screws. Ensure that the side having the **Mount Arrows Up** label is facing outwards, and the bracket is oriented vertically as indicated by the arrows. See Figure 11.

The wall-bracket dimensions are given in Figure 12.

Step 2 Connect the power and network cables to the AP.

If you are unable to connect a PoE cable to the port on the back of the AP, then:

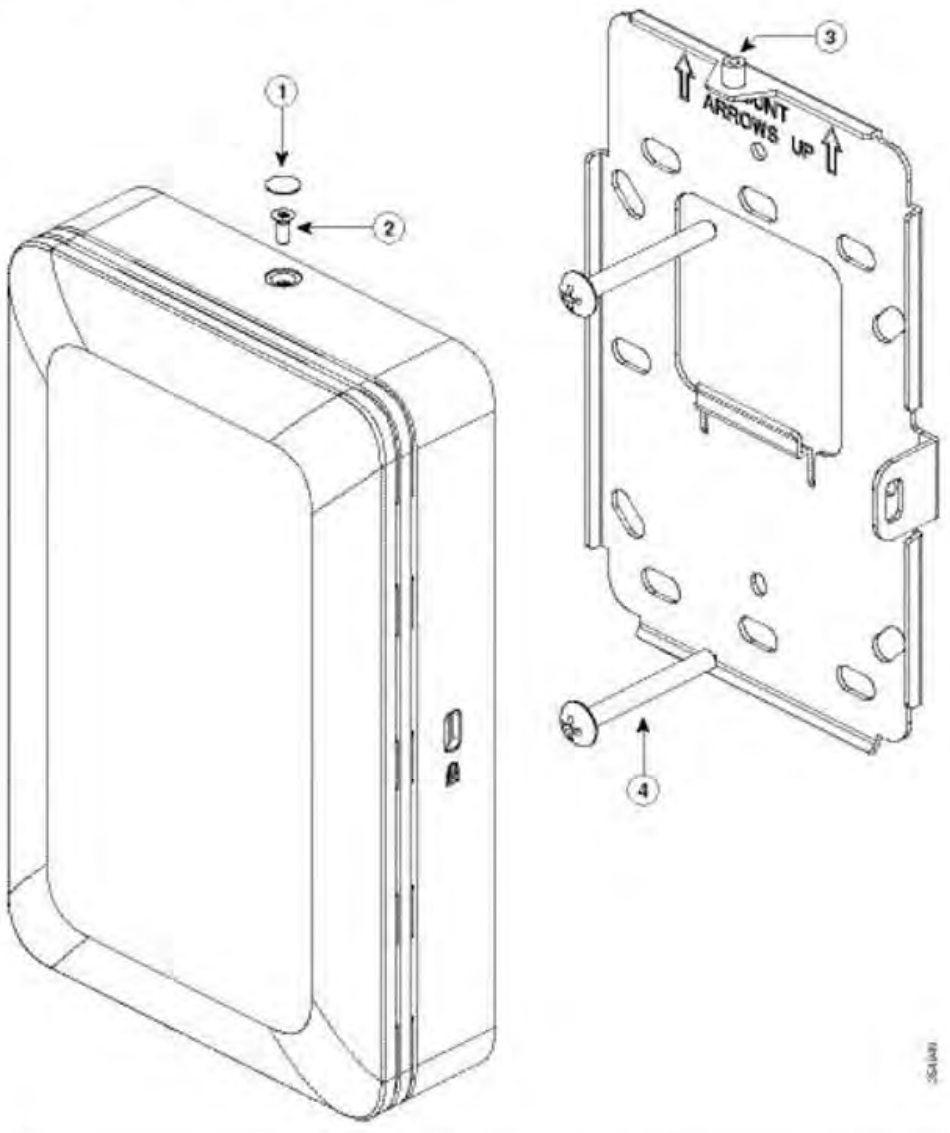
a) On the back of the AP, use an RJ45 jumper cable to connect the PoE port to the Pass-Through port. This jumper cable is available as part of the spacer kit C9105AXW-KIT.
b) Connect the PoE supply cable to the Pass-Through port on the base of the AP.

This connection sends power internally from the Pass-Through port on the base, to the Pass-Through port on the back, and then though the jumper cable into the PoE port on the back.

Step 3 Mount the AP onto the wall-mount bracket. For this, align the AP with the bracket and then offset the AP around ¼ inch above the bracket.

Step 4 Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label.

Figure 7: Mounting C9105AXW on a Wall



1	Mylar label for covering Torx security screw slot.	3	Screw hole on the wall-mount bracket for the security screw.
2	M2 x 5.5mm Torx security screw.	4	M3.5 x 32mm screws for fastening the bracket to the wall.

Mounting the C9105AXW AP on an Electrical Junction Box

To mount the AP on an electrical junction box, using a spacer box, follow these steps:

Procedure

Step 1 Fasten the wall-mount bracket (AIR-AP-BRACKET-W4) to the spacer box (C9105AXW-KIT=), using two M3X8mm pan head tapping screws. Ensure that the side having the **Mount Arrows Up** label facing outwards, and the bracket oriented vertically as indicated by the arrows. See Figure 9 and Figure 11.

The spacer box dimensions are given in Figure 10.

The wall-bracket dimensions are given in Figure 12.

Step 2 Fasten the wall-mount bracket and spacer box assembly to the electrical junction box, using two #6-32X1.62 inch machine screws. Ensure that the side having the **Mount Arrows Up** label is facing outwards, and the box is oriented vertically as indicated by the arrows.

Step 3 Connect the power and network cables to the AP.

If you are unable to connect a PoE cable to the port on the back of the AP, then:

a) On the back of the AP, use an RJ45 jumper cable to connect the PoE port to the Pass-Through port. This jumper cable is available as part of the spacer kit C9105AXW-KIT=.

b) Connect the PoE supply cable to the Pass-Through port on the base of the AP.

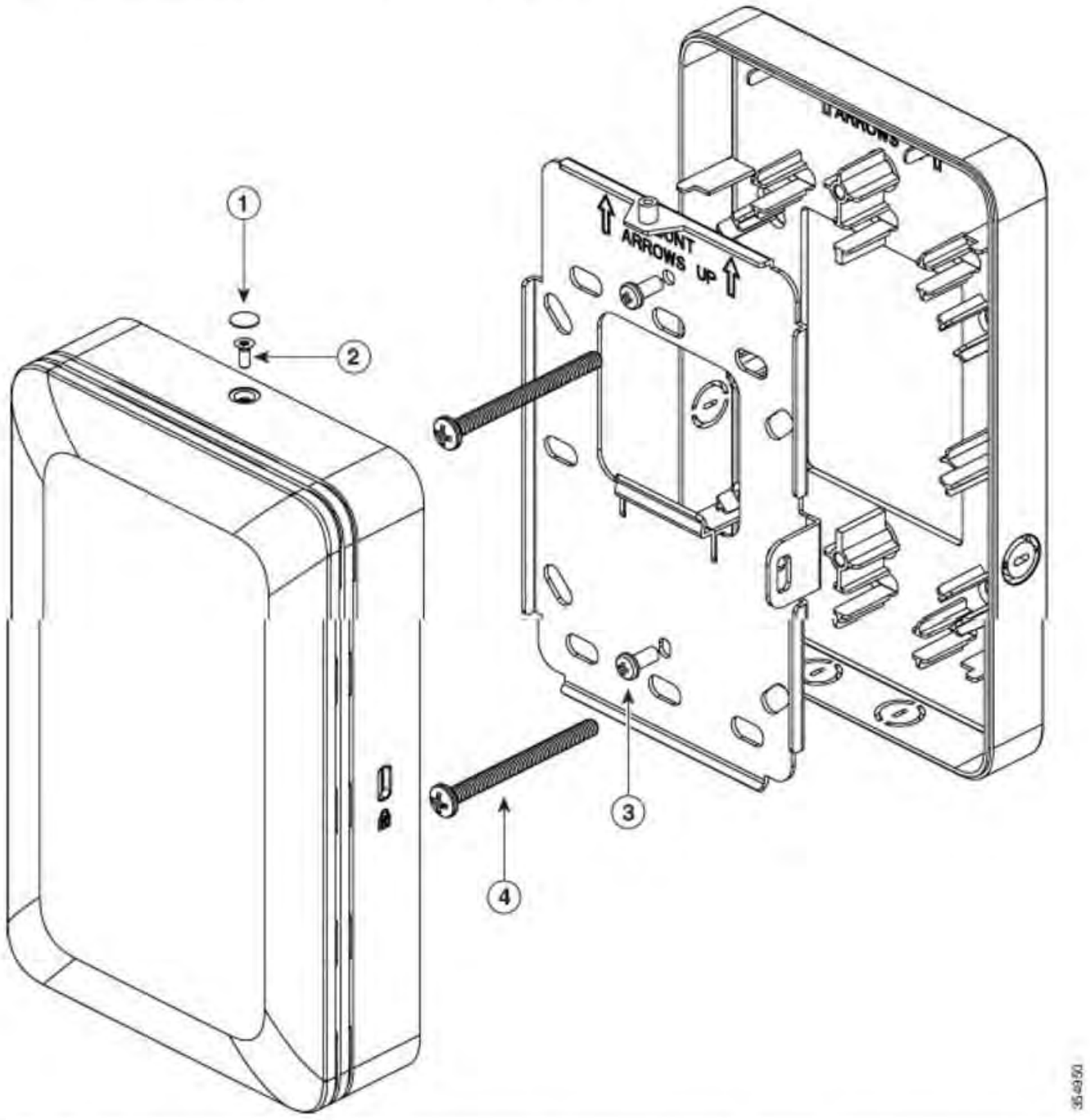
This connection sends power internally from the Pass-Through port on the base, to the Pass-Through port on the back, and then though the jumper cable into the PoE port on the back.

Note The punch-out holes on the spacer box (C9105AXW-KIT=) can be used for routing cables. However, an RJ45 connector will not fit through these holes. If this is required, you must first route a cable through the hole and then crimp an RJ45 connector on to the cable.

Step 4 Mount the AP onto the wall-mount bracket. For this, align the AP with the bracket and then offset the AP around ¼ inch above the bracket.

Step 5 Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label.

Figure 8: Mounting C9105AXW AP on an Electrical Junction Box using the Spacer



1	Mylar label for covering Torx security screw slot.	3	M3 x 8mm pan head tapping screws for fastening the wall-mount bracket to the spacer.
2	M2 x 5.5mm Torx security screw.	4	6-32 x 1.62inch screws for fastening the spacer-bracket assembly to the junction box.

Grounding the Access Point

Warning Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Grounding is not required for indoor installations.

Powering the Access Point

The AP can be powered only through Power-over-Ethernet (PoE) using the following:

- 802.3at (PoE+): Any 802.3at (30.0 W) compliant switch port or Cisco Power Injector AIR-PWRINJ6=
- 802.3af: Any 802.3af (15.4 W) compliant switch port or Cisco Power Injector AIR-PWRINJ5=

Note If 802.3af is used, the Ethernet will be downgraded to 1 GbE. Also, the PSE-In (LAN1) and USB ports will be off.

- 802.3bt: Any 802.3bt compliant switch port
- Cisco Universal PoE (Cisco UPOE)

Configuring and Deploying the Access Point

This section describes how to connect the access point to a controller. Because the configuration process takes place on the controller, see the Cisco Wireless Controller Configuration Guide for additional information.

The Controller Discovery Process

Note

- The controller must be running release 8.10.*x* or IOS-XE 17.3.*x* to support C9105AX access points. For more information, visit the access point data sheet available on Cisco.com at https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/guide-c07-742311.html.
- You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.
- Make sure that the controller is set to the current time. If the controller is set to a time that has already occurred, theaccess point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The access point supports these controller discovery processes:

- **Locally stored controller IP address discovery**—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see the Performing a Pre-Installation Configuration.

- **DHCP server discovery**—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the Configuring DHCP Option 43.
- **DNS discovery**—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Deploying the Access Point on the Wireless Network

After you have mounted the access point, follow these steps to deploy it on the wireless network.

Procedure

Step 1 Connect and power up the access point.

Step 2 Observe the access point LED.

For LED descriptions, see Checking the Access Point LEDs, on page 20.

a) When you power up the access point, it begins a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks sequentially green, red, and off. When the access point has joined a controller, the LED is chirping green if no clients are associated or green if one or more clients are associated.

b) If the LED is not on, the access point is most likely not receiving power.

c) If the LED blinks sequentially for more than 5 minutes, the access point is unable to find its primary, secondary, and tertiary Cisco Wireless Controller. Check the connection between the access point and the Cisco Wireless Controller, and be sure the access point and the Cisco Wireless Controller are either on the same subnet or that the access point has a route back to its primary, secondary, and tertiary Cisco Wireless Controller. Also, if the access point is not on the same subnet as the Cisco Wireless Controller, be sure that there is a properly configured DHCP server on the same subnet as the access point. See Configuring DHCP Option 43, on page 23 for additional information.

Step 3 Reconfigure the Cisco Wireless Controller so that it is not the master.

Note A master Cisco Wireless Controller should be used only for configuring access points and not in a working network.

Checking the Access Point LEDs

Depending on the access point type, the location of its status LED can be seen as shown in Figure 1: Face of the C9105AXI Model, on page 7 or Figure 3: Face of the C9105AXW Model, on page 9.

Note Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect. However, the intensity of the LED can be changed through the controller.

The access point status LED indicates various conditions which are described in the Table 4: LED Status Indications, on page 21 table below.

Table 4: LED Status Indications

Message Type	LED State	Message Meaning
Association status	Green	Normal operating condition, but no wireless client associated
	Blue	Normal operating condition, at least one wireless client association
Boot loader status	Green	Executing boot loader
Boot loader error	Blinking Green	Boot loader signing verification failure
Operating status	Blinking Blue	Software upgrade in progress
	Alternating between Green and Red	Discovery/join process in progress
	Cycling through Red-Off-Green-Off-Blue-Off	Access point location command invoked from controller web interface.
Access point operating system errors	Cycling through Blue-Red-Green-Off	General warning; insufficient inline power

Miscellaneous Usage and Configuration Guidelines

Using the Mode Button

Using the Mode button (see Figure 2: Ports and Connectors on the Head of the C9105AXI Model, on page 8) you can:

- Reset the AP to the default factory-shipped configuration.
- Clear the AP internal storage, including all configuration files.

To use the mode button, press, and keep pressed, the mode button on the access point during the AP boot cycle. Wait until the AP status LED changes to Blue. During this, the AP console shows a seconds counter, counting the number of seconds the mode button is pressed. Then:

- To reset the AP to the default factory-shipped configuration, keep the mode button pressed for less than 20 seconds. The AP configuration files are cleared.

  This resets all configuration settings to factory defaults, including passwords, the IP address, and the SSID.

- To clear the AP internal storage, including all configuration files and the regulatory domain configuration, keep the mode button pressed for more than 20 seconds, but less than 60 seconds.

The AP status LED changes from Blue to Red, and all the files in the AP storage directory are cleared.

If you keep the mode button pressed for more than 60 seconds, the mode button is assumed faulty and no changes are made.

Troubleshooting the Access Point to Cisco Controller Join Process

Note As specified in the *Cisco Wireless Solutions Software Compatibility Matrix*, ensure that your controller is running controller software release 8.10.*x* or IOS-XE 17.3.*x* or later to support C9105AX AP models.

Access points can fail to join a controller for many reasons: a RADIUS authorization is pending; self-signed certificates are not enabled on the controller; the access point and the controller regulatory domains don't match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point. Therefore, it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining problems without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to it and maintains information for any access points that have successfully joined it.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all syslog messages to IP address 255.255.255.255 by default.

You can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global syslog_server_IP_address** command. In this case, the controller sends the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific Cisco_AP syslog_server_IP_address** command. In this case, the controller sends the new specific syslog server IP address to the access point.

  The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.

  Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points and view the access point join information only from the controller CLI.

Important Information for Controller-based Deployments

Keep these guidelines in mind when you use C9105AX series access point:

- The access point can only communicate with Cisco wireless controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

Configuring DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling them to find and join a controller.

The following is a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Catalyst lightweight access points. For other DHCP server implementations, consult product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

The C9105AX series access point uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point DHCP Vendor Class Identifier (VCI) string (DHCP Option 43). The VCI string for the C9105AX series access point is:

```
Cisco AP C9105AX
```

The format of the TLV block is listed below:

- Type—0xf1 (decimal 241)
- Length—Number of controller IP addresses * 4
- Value—IP addresses of the WLC management interfaces listed sequentially in hex

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server, follow these steps:

Procedure

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
```

default-router <Default router>
dns-server <DNS Server>

Where:

<pool name> is the name of the DHCP pool, such as AP9105AX
<IP Network> is the network IP address where the controller resides, such as 10.0.15.1
<Netmask> is the subnet mask, such as 255.255.255.0
<Default router> is the IP address of the default router, such as 10.0.0.1
<DNS Server> is the IP address of the DNS server, such as 10.0.10.2

Step 3 Add the option 43 line using the following syntax:

option 43 hex <hex string>

The **hex string** is assembled by concatenating the TLV values shown below:

Type + Length + Value

Example

For example, suppose that there are two controllers with management interface IP addresses, **10.126.126.2** and **10.127.127.2**. The type is f1(hex). The length is 2 * 4 = 8 = 08 (hex). The IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string then yields f1080a7e7e020a7f7f02. The resulting Cisco IOS command added to the DHCP scope is `option 43 hex f1080a7e7e020a7f7f02`.

FAQs

Q. What is 802.11ax?

A. The IEEE 802.11ax standard, also known as the High-Efficiency Wireless (HEW) or Wi-Fi 6, builds off of the 802.11ac and delivers a better experience in typical environments, and a more predictable performance for advanced applications such as 4K or 8K video, high-density high-definition collaboration applications, all-wireless offices and Internet-of-Things (IoT). 802.11ax is designed to use both 2.4Ghz and the 5GHz bands, unlike prior standards.

Q. What is Flexible Radio Assignment?

A. The Flexible Radio Assignment (FRA) feature automatically detects when a high number of devices are connected to a network and changes the dual radios in the access point from 2.4 GHz/5 GHz to 5 GHz/5 GHz to serve more clients. The access point performs this function while still monitoring the network for security threats and RF Interference that may affect performance. Flexible Radio Assignment improves mobile user experience for high-density networks.

FRA has the different modes of operation:

- Default operating mode—Serving Clients on both 2.4 GHz and 5 GHz
- Dual 5 GHz Mode—Serving clients on both 5 GHz Radios
- Wireless Security Monitoring—Scanning both 2.4 GHz and 5 GHz for security threats while also serving 5 GHz clients

Q. What is Cisco Multigigabit Ethernet?

A. Cisco Multigigabit Ethernet (mGig) is a unique Cisco innovation also available in the Cisco Catalyst 9105AX series access point. With the increasing popularity of 802.11ax and new wireless applications, wireless devices now require more network bandwidth. Hence, there is a need for a technology that supports speeds higher than 1 Gbps on all cabling infrastructure. Cisco

Declarations of Conformity and Regulatory Information

This section provides declarations of conformity and regulatory information for the Cisco Catalyst 9105AX Series Access Points. You can find additional information at this URL:

http://www.cisco.com/go/aironet/compliance

Manufacturers Federal Communication Commission Declaration of Conformity Statement

Access Point Models	Certification Number
C9105AXI-B	LDK
C9105AXW-B	LDK

Manufacturer:

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Separation Distance		
MPE	Distance	Limite
0.35 mW/cm^2	. 20cm (7.9 inches)	1.00 mW/cm^2

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using the integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

VCCI Statement for Japan

Access Point Models :C9105AXI-Q

Warning	This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Guidelines for Operating Cisco Catalyst Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet access points in Japan. These guidelines are provided in both Japanese and English.

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。
1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：03-6434-6500

208697

JP Statement:

5GHz band (W52, W53): Indoor use only (except communicate to high power radio)

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: 03-6434-6500

Warning When installing the product, please use the provided or designated connection cables/power cables/AC adaptors/batteries. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the "UL" or "CSA" shown on the cord), not regulated with the subject law by showing "PSE" on the cord, for any other electrical devices than products designated by CISCO.

English Translation

When installing the product, please use the provided or designated connection cables/power cables/AC adaptors. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the “UL” shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have “PSE” shown on the code) is not limited to CISCO-designated products.

Industry Canada

Access Point Models	Certification Number
C1105AXI-A	2461B-
C9105AXI-A	2461B-

Canadian Compliance Statement

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Antenna Type	Antenna Gain	Antenna Impedance
IFA (Inverted-F antenna)	WiFi_1 ANT.≦ 4.89 WiFi_2 ANT.≦ ≦ 4.72 BLE ANT.≦ 2.30	50 ohms

Operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

La bande 5 150-5 250 MHz est réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Users are advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Les utilisateurs êtes avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Table 7: This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves

Separation Distance			
Frequency	**MPE**	**Distance**	**Limite**
2.4 GHz	2.07 W/m^2	20cm (7.9 inches)	5.4 W/m^2
5 GHz	3.52 W/m^2		9.76 W/m^2

Chinese Translation

Access Point Model: C9105AXI-T

低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

低功率射頻電機技術規範

4.7　無線資訊傳輸設備

4.7.5 在 5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

4.7.6 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

202591