AP Configuration

Feature History for Configuring the Access Point Console

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature History for Configuring the Access Point Console

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	Configuring the Access Point Console	This feature allows you to configure the Access Point (AP) console from the controller. In Cisco IOS XE Cupertino 17.8.x and earlier releases, the AP console could be disabled from the controller, only by enabling the Federal Information Processing Standard (FIPS) mode or the Common Criteria (CC) mode.

Information About Configuring the Access Point Console

From Cisco IOS XE Cupertino 17.9.1 onwards, a new option (a configuration knob) is introduced to enable the Access Point console from the controller, which is independent of the FIPS mode or the high-security

mode (CC mode). (Until Cisco IOS XE Cupertino 17.8.1, the console was enabled by default). This configuration knob can be activated through the controller GUI and CLI.

Console enablement is isolated from the FIPS mode and is configured through the AP join profile. In the CC mode, the console and SSH are disabled. When you enable the CC mode, it overrides the AP console configurations, if any, done from the AP profile.

Configuring the AP Console (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 In the **Management** tab, in the **Telnet/SSH Configuration** section, check the **Serial Console** check box.

Step 3 Click **Apply to Device**.

Configuring the AP Console (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP profile and enters AP profile configuration mode.
Step 3	**[no] console** **Example:** `Device(config-ap-profile)# console`	Enables the AP serial console port. Use the **no** form of this command to disable the AP serial console port.

Verifying the AP Console Status

To verify the AP console status from the controller, run the following command:

```
Device# show ap config general | include ap-Name | console
Cisco AP Name : CiscoAP
================================================

Cisco AP Identifier : 6XXX.bXXX.aXXX
```

```
Country Code : US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-AB 802.11 6GHz:-B
AP Country Code : US - United States
AP Regulatory Domain
802.11bg : -A
802.11a : -B
MAC Address : 6XXX.bXXX.0XXX
IP Address Configuration : DHCP
IP Address : 30.30.30.26
IP Netmask : 255.255.255.0
Gateway IP Address : 30.30.30.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Capwap Active Window Size : 1
Telnet State : Disabled
CPU Type : ARMv8 Processor rev 4 (v8l)
Memory Type : DDR3
Memory Size : 1752064 KB
SSH State : Enabled
Serial Console State : Enabled
```

Information About AP Audit Configuration

The AP Audit Configuration feature helps to detect wireless service synchronization issues between the controller and an AP. In Cisco IOS XE Amsterdam, Release 17.3.1, two methods are implemented to support AP audit configuration.

- Config Checker: This functionality helps in auditing the application of wireless policies during the AP join phase. Any discrepancies at this stage is reported on the controller. This is a built-in functionality and you cannot disable the same. When you try to configure any of the AP attributes such as name, IP address, controller information, tag, mode, radio mode, and radio admin state, the AP parses the CAPWAP payload configuration from the controller and reports errors detected back to the controller with proper code. If a discrepancy is detected, the controller flags errors using the syslog.
- Config Audit: This functionality helps to perform periodic comparison of operational states between an AP and the controller after the AP join phase and while the corresponding AP is still connected. Discrepancies, if any, are reported immediately on the controller. The consolidated report is available at the controller anytime. This functionality is disabled by default. The periodic auditing interval is a configurable parameter.

  Use the **ap audit-report** command to enable and configure audit report parameters. When triggered, AP sends configurations from the database to the controller, and the controller compares the configurations against the current configuration. If a discrepancy is detected, the controller flags the error using the syslog.

Restrictions for AP Audit Configuration

- Config checker alerts are available only through the syslog.
- IOS AP is not supported.

- The audit reports are not synchronized from the active to the standby controller. After SSO, they are not readily available until the next reporting interval of the already-connected APs.
- The audit reports are not available when an AP is in standalone mode.
- This feature is supported only on APs in FlexConnect mode.

Configure AP Audit Parameters (CLI)

The AP Audit Configuration feature helps you compare the operational states between an AP and the controller. The AP sends state view details to the controller, and the controller compares it with what it perceives as the AP state. This feature is disabled by default.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap audit-report enable** **Example:** `Device(config)# ap audit-report enable`	Enables audit reporting.
Step 3	**ap audit-report interval** *interval* **Example:** `Device(config)# ap audit-report interval 1300`	Configures AP audit reporting interval. The default value for interval is 1440 minutes. The valid range is from 10 to 43200.

Verifying AP Audit Report Summary

To verify the AP audit report summary, use the **ap audit-report summary** command:

```
Device# show ap audit-report summary
WTP Mac                   Radio                  Wlan                IPv4 Acl
IPv6 Acl       Last Report Time
------------------------------------------------------------------------------------------
1880.90fd.6b40   OUT_OF_SYNC    OUT_OF_SYNC    IN_SYNC        IN_SYNC        01/01/1970
05:30:00 IST
```

Verifying AP Audit Report Detail

To verify an AP audit report's details, use the **show ap name ap-name audit-report detail** command:

```
Device# show ap name Cisco-AP audit-report detail
Cisco AP Name   : Cisco-AP
================================================
 IPV4 ACL Audit Report Status     : IN_SYNC
```

```
IPV6 ACL Audit Report Status     : IN_SYNC

Radio Audit Report Status        : IN_SYNC

WLAN Audit Report Status         :
Slot-id  Wlan-id  Vlan           State          SSID           Auth-Type      Other-Flag
-------------------------------------------------------------------------------------
0        4        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC
1        4        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC

bh-csr1#show ap audit-report summary
WTP-Mac          Radio          Wlan           IPv4-Acl       IPv6-Acl       Last-Report-Time
-------------------------------------------------------------------------------------------------
4001.7aca.5140   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:17:39 IST
4001.7aca.5a60   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:18:25 IST
7070.8b23.a1a0   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:18:29 IST
a0f8.49dc.9460   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:16:43 IST
a0f8.49dc.96e0   IN_SYNC        IN_SYNC        IN_SYNC        IN_SYNC        06/22/2020
13:17:55 IST
```

2.4-GHz Radio Support

Configuring 2.4-GHz Radio Support for the Specified Slot Number

Before you begin

Note The term *802.11b radio* or *2.4-GHz radio* will be used interchangeably.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 24ghz slot 0 SI** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI`	Enables Spectrum Intelligence (SI) for the dedicated 2.4-GHz radio hosted on slot 0 for a specific access point. For more information, *Spectrum Intelligence* section in this guide. Here, **0** refers to the Slot ID.
Step 3	**ap name** *ap-name* **dot11 24ghz slot 0 antenna** {**ext-ant-gain** *antenna_gain_value* | **selection** [**internal** | **external**]}	Configures 802.11b antenna hosted on slot 0 for a specific access point.

	Command or Action	Purpose
	Example: `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 antenna selection internal`	• **ext-ant-gain**: Configures the 802.11b external antenna gain. *antenna_gain_value*- Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295. • **selection**: Configures the 802.11b antenna selection (internal or external). **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.
Step 4	**ap name** *ap-name* **dot11 24ghz slot 0 beamforming** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming`	Configures beamforming for the 2.4-GHz radio hosted on slot 0 for a specific access point.
Step 5	**ap name** *ap-name* **dot11 24ghz slot 0 channel** {*channel_number* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto`	Configures advanced 802.11 channel assignment parameters for the 2.4-GHz radio hosted on slot 0 for a specific access point.
Step 6	**ap name** *ap-name* **dot11 24ghz slot 0 cleanair** **Example:**	Enables CleanAir for 802.11b radio hosted on slot 0 for a specific access point.

	Command or Action	Purpose
	`Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair`	
Step 7	**ap name** *ap-name* **dot11 24ghz slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A`	Configures 802.11n antenna for 2.4-GHz radio hosted on slot 0 for a specific access point. Here, **A**: Is the antenna port A. **B**: Is the antenna port B. **C**: Is the antenna port C. **D**: Is the antenna port D.
Step 8	**ap name** *ap-name* **dot11 24ghz slot 0 shutdown** **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown`	Disables 802.11b radio hosted on slot 0 for a specific access point.
Step 9	**ap name** *ap-name* **dot11 24ghz slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 txpower auto`	Configures transmit power level for 802.11b radio hosted on slot 0 for a specific access point. • *tx_power_level*: Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**: Enables auto-RF.

5-GHz Radio Support

Configuring 5-GHz Radio Support for the Specified Slot Number

Before you begin

Note The term *802.11a radio* or *5-GHz radio* will be used interchangeably in this document.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **dot11 5ghz slot 1 SI** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 SI`	Enables Spectrum Intelligence (SI) for the dedicated 5-GHz radio hosted on slot 1 for a specific access point. Here, **1** refers to the Slot ID.
Step 3	**ap name** *ap-name* **dot11 5ghz slot 1 antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna ext-ant-gain`	Configures external antenna gain for 802.11a radios for a specific access point hosted on slot 1. *antenna_gain_value*—Refers to the external antenna gain value in multiples of .5 dBi units. The valid range is from 0 to 4294967295. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.
Step 4	**ap name** *ap-name* **dot11 5ghz slot 1 antenna mode** [**omni** | **sectorA** | **sectorB**] **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna mode sectorA`	Configures the antenna mode for 802.11a radios for a specific access point hosted on slot 1.
Step 5	**ap name** *ap-name* **dot11 5ghz slot 1 antenna selection** [**internal** | **external**] **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna selection internal`	Configures the antenna selection for 802.11a radios for a specific access point hosted on slot 1.

	Command or Action	Purpose
Step 6	**ap name** *ap-name* **dot11 5ghz slot 1 beamforming** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 beamforming`	Configures beamforming for the 5-GHz radio hosted on slot 1 for a specific access point.
Step 7	**ap name** *ap-name* **dot11 5ghz slot 1 channel** {*channel_number* | **auto** | **width** [**20** | **40** | **80** | **160**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 channel auto`	Configures advanced 802.11 channel assignment parameters for the 5-GHz radio hosted on slot 1 for a specific access point. Here, *channel_number*- Refers to the channel number. The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 5ghz slot 1 cleanair** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 cleanair`	Enables CleanAir for 802.11a radio hosted on slot 1 for a given or specific access point.
Step 9	**ap name** *ap-name* **dot11 5ghz slot 1 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 dot11n antenna A`	Configures 802.11n for 5-GHz radio hosted on slot 1 for a specific access point. Here, **A**- Is the antenna port A. **B**- Is the antenna port B. **C**- Is the antenna port C. **D**- Is the antenna port D.
Step 10	**ap name** *ap-name* **dot11 5ghz slot 1 rrm channel** *channel* **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 rrm channel 2`	Is another way of changing the channel hosted on slot 1 for a specific access point. Here, *channel*- Refers to the new channel created using 802.11h channel announcement. The valid range is from 1 to 173, provided 173 is a valid channel in the country where the access point is deployed.
Step 11	**ap name** *ap-name* **dot11 5ghz slot 1 shutdown** **Example:** `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 shutdown`	Disables 802.11a radio hosted on slot 1 for a specific access point.
Step 12	**ap name** *ap-name* **dot11 5ghz slot 1 txpower** {*tx_power_level* | **auto**} **Example:**	Configures 802.11a radio hosted on slot 1 for a specific access point.

	Command or Action	Purpose
	`Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto`	• *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.

6-GHz Radio Support

Configuring 6-GHz Radio Support for the Specified Slot Number

Before you begin

Static channel must be set before changing the channel width.

As there are no external antenna APs, as by regulatory requirements, antennas have to be captive (internal always) for 6-GHz.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 6ghz slot 3 antenna port** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 antenna port A`	Configures the antenna port for 802.11 6-Ghz radios for a specific access point. Here, **A**: Is the antenna port A. **B**: Is the antenna port B. **C**: Is the antenna port C. **D**: Is the antenna port D.
Step 3	**ap name** *ap-name* **dot11 6ghz slot 3 antenna selection** [**internal** | **external**] **Example:**	Configures the antenna selection, either internal or external, for 802.11 6-Ghz radios for a specific access point.

	Command or Action	Purpose
	`Device# ap name Cisco-AP dot11 6ghz slot 1 antenna selection internal`	**Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model. • Cisco Catalyst 9120E and 9130E APs support self-identifying antennas (SIA). Cisco Catalyst 9115E APs do not support SIA antennas. Although Cisco Catalyst 9115E APs work with SIA antennas, the APs do not auto-detect SIA antennas nor add the correct external gain.
Step 4	**ap name** *ap-name* **dot11 6ghz slot 3 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 channel auto`	Configures advanced 802.11 channel assignment parameters for the 6-GHz radio hosted on slot 3 for a specific access point. Here, *channel_number*: Refers to the channel number. The valid range is from 1 to 233.
Step 5	**ap name** *ap-name* **dot11 6ghz slot 3 dot11ax bss-color** {*bss-color-number* | **auto**} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 dot11ax bss-color auto`	Enables basic service set (BSS) color for 802.11 6-Ghz radio for a given or specific access point. Here, *bss-color-number*: Refers to the BSS color number. The valid range is from 1 to 63.
Step 6	**ap name** *ap-name* **dot11 6ghz slot 3 radio role** {**auto** | **manual** {**client-serving** | **monitor** | **sniffer**}} **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 radio role auto`	Configures the 802.11 6-Ghz radio role, which is either **auto** or **manual**.
Step 7	**ap name** *ap-name* **dot11 6ghz slot 3 rrm channel** *channel* **Example:**	Configures a new channel using 802.11h channel announcement. Here,

	Command or Action	Purpose
	`Device# ap name Cisco-AP dot11 6ghz slot 3 rrm channel 1`	*channel*: Refers to the new channel created using 802.11h channel announcement. The valid range is from 1 to 233.
Step 8	**ap name** *ap-name* **dot11 6ghz slot 3 shutdown** **Example:** `Device# ap name Cisco-AP dot11 6ghz slot 3 shutdown`	Disables the 802.11 6-Ghz radio on the Cisco AP.
Step 9	**ap name** *ap-name* **dot11 6ghz slot 3 txpower** {*tx_power_level* | **auto**} **Example:** `# ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto`	Configures 802.11 6-Ghz Tx power level. • *tx_power_level*: Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**: Enables auto-RF.

Information About Dual-Band Radio Support

The Dual-Band (XOR) radio in Cisco 2800, 3800, 4800, and the 9120 series AP models offer the ability to serve 2.4–GHz or 5–GHz bands or passively monitor both the bands on the same AP. These APs can be configured to serve clients in 2.4–GHz and 5–GHz bands, or serially scan both 2.4–GHz and 5–GHz bands on the flexible radio while the main 5–GHz radio serves clients.

Cisco Catalyst Wireless 9166 AP (CW9166) now has XOR function for a dual 5-GHz 4x4 or 5-GHz 4x4 and 6-GHz 4x4 radios. These radios can also be configured as client serving, monitor or as a sniffer interface like the earlier XOR radios.

Note For all countries that do not support 6-GHz spectrum for use of Wi-Fi, when the Cisco Catalyst Wireless 9166I AP operates as dual 5-GHz, the 5-GHz channels will be locked on both the radios even if slot 2 is disabled or set up for monitoring.

Cisco APs models up and through the Cisco 9120 APs are designed to support dual 5–GHz band operations with the *i* model supporting a dedicated Macro/Micro architecture and the *e* and *p* models supporting Macro/Macro. The CW9166I supports Macro/Macro cell.

When a radio moves between bands (from 2.4-GHz to 5-GHz and vice versa), clients need to be steered to get an optimal distribution across radios. When an AP has two radios in the 5–GHz band, client steering algorithms contained in the Flexible Radio Assignment (FRA) algorithm are used to steer a client between the same band co-resident radios.

The XOR radio support can be steered manually or automatically:

- Manual steering of a band on a radio—The band on the XOR radio can only be changed manually.
- Automatic client and band steering on the radios is managed by the FRA feature that monitors and changes the band configurations as per site requirements.

Note RF measurement will not run when a static channel is configured on slot 1. Due to this, the dual band radio slot 0 will move only with 5–GHz radio and not to the monitor mode.

When slot 1 radio is disabled, RF measurement will not run, and the dual band radio slot 0 will be only on 2.4–GHz radio.

Note Only one of the 5-GHz radios can operate in the UNII band (100 - 144), due to an AP limitation to keep the power budget within the regulatory limit.

Configuring Default XOR Radio Support

Before you begin

Note The default radio points to the XOR radio hosted on slot 0.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* **Example:** `Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	Configures the 802.11 dual-band antenna on a specific Cisco access point. *antenna_gain_value*: The valid range is from 0 to 40.
Step 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** **Example:** `Device# ap name ap-name dot11 dual-band shutdown`	Shuts down the default dual-band radio on a specific Cisco access point. Use the **no** form of the command to enable the radio.
Step 4	**ap name** *ap-name* **dot11 dual-band role manual client-serving** **Example:** `Device# ap name ap-name dot11 dual-band role manual client-serving`	Switches to client–serving mode on the Cisco access point.

	Command or Action	Purpose
Step 5	**ap name** *ap-name* **dot11 dual-band band 24ghz** **Example:** `Device# ap name ap-name dot11 dual-band band 24ghz`	Switches to 2.4-GHz radio band.
Step 6	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} **Example:** `Device# ap name ap-name dot11 dual-band txpower 2`	Configures the transmit power for the radio on a specific Cisco access point. **Note** When an FRA-capable radio (slot 0 on 9120 AP[for instance]) is set to Auto, you cannot configure static channel and Txpower on this radio. If you want to configure static channel and Txpower on this radio, you will need to change the radio role to Manual Client-Serving mode. This note is not applicable for Cisco Catalyst Wireless 9166 AP (CW9166).
Step 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* **Example:** `Device# ap name ap-name dot11 dual-band channel 2`	Enters the channel for the dual band. *channel-number*—The valid range is from 1 to 173.
Step 8	**ap name** *ap-name* **dot11 dual-band channel auto** **Example:** `Device# ap name ap-name dot11 dual-band channel auto`	Enables the auto channel assignment for the dual-band.
Step 9	**ap name** *ap-name* **dot11 dual-band channel width**{**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} **Example:** `Device# ap name ap-name dot11 dual-band channel width 20 MHz`	Chooses the channel width for the dual band.
Step 10	**ap name** *ap-name* **dot11 dual-band cleanair** **Example:** `Device# ap name ap-name dot11 dual-band cleanair`	Enables the Cisco CleanAir feature on the dual-band radio.
Step 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz | 5 GMHz**} **Example:**	Selects a band for the Cisco CleanAir feature. Use the **no** form of this command to disable the Cisco CleanAir feature.

	Command or Action	Purpose
	`Device# ap name ap-name dot11 dual-band cleanair band 5 GHz` `Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`	
Step 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name ap-name dot11 dual-band dot11n antenna A`	Configures the 802.11n dual-band parameters for a specific access point.
Step 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** **Example:** `Device# show ap name ap-name auto-rf dot11 dual-band`	Displays the auto-RF information for the Cisco access point.
Step 14	**show ap name** *ap-name* **wlan dot11 dual-band** **Example:** `Device# show ap name ap-name wlan dot11 dual-band`	Displays the list of BSSIDs for the Cisco access point.

Configuring XOR Radio Support for the Specified Slot Number (GUI)

Procedure

Step 1 Click **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** section, select the AP for which you want to configure dual-band radios.

The AP name, MAC address, CleanAir capability and slot information for the AP are displayed. If the Hyperlocation method is HALO, the antenna PID and antenna design information are also displayed.

Step 3 Click **Configure**.

Step 4 In the **General** tab, set the **Admin Status** as required.

Step 5 Set the **CleanAir Admin Status** field to Enable or Disable.

Step 6 Click **Update & Apply to Device**.

Configuring XOR Radio Support for the Specified Slot Number

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	Configures dual-band antenna for the XOR radio hosted on slot 0 for a specific access point. *external_antenna_gain_value* - Is the external antenna gain value in multiples of .5 dBi unit. The valid range is from 0 to 40. **Note** • For APs supporting self-identifying antennas (SIA), the gain depends on the antenna, and not on the AP model. The gain is learned by the AP and there is no need for controller configuration. • For APs that do not support SIA, the APs send the antenna gain in the configuration payload, where the default antenna gain depends on the AP model.
Step 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	Configures current band for the XOR radio hosted on slot 0 for a specific access point.
Step 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	Configures dual-band channel for the XOR radio hosted on slot 0 for a specific access point. *channel_number*- The valid range is from 1 to 165.
Step 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	Enables CleanAir features for dual-band radios hosted on slot 0 for a specific access point.

	Command or Action	Purpose
Step 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	Configures 802.11n dual-band parameters hosted on slot 0 for a specific access point. Here, **A**- Enables antenna port A. **B**- Enables antenna port B. **C**- Enables antenna port C. **D**- Enables antenna port D.
Step 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	Configures dual-band role for the XOR radio hosted on slot 0 for a specific access point. The following are the dual-band roles: • **auto**- Refers to the automatic radio role selection. • **manual**- Refers to the manual radio role selection.

Step 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`
		Disables dual-band radio hosted on slot 0 for a specific access point.
		Use the **no** form of this command to enable the dual-band radio.

Step 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} **Example:** `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	Configures dual-band transmit power for XOR radio hosted on slot 0 for a specific access point. • *tx_power_level*- Is the transmit power level in dBm. The valid range is from 1 to 8. • **auto**- Enables auto-RF.

Receiver Only Dual-Band Radio Support

Information About Receiver Only Dual-Band Radio Support

This feature configures the dual-band Rx-only radio features for an access point with dual-band radios.

This dual-band Rx-only radio is dedicated for Analytics, Hyperlocation, Wireless Security Monitoring, and BLE AoA*.

This radio will always continue to serve in monitor mode, therefore, you will not be able to make any channel and *tx-rx* configurations on the 3rd radio.

Configuring Receiver Only Dual-Band Parameters for Access Points

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.

Step 3 In the **General** tab, enable the **CleanAir** toggle button.

Step 4 Click **Update & Apply to Device**.

Enabling CleanAir with Receiver Only Dual-Band Radio on a Cisco Access Point

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

Step 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 cleanair band** {**24Ghz** | **5Ghz**}
	Example:
	`Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 cleanair band 24Ghz`
	`Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 cleanair band 24Ghz`
		Enables CleanAir with receiver only (Rx-only) dual-band radio on a specific access point.
		Here, 2 refers to the slot ID.
		Use the **no** form of this command to disable CleanAir.

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 In the **Dual-Band Radios** settings, click the AP for which you want to configure the dual-band radios.

Step 3 In the **General** tab, disable the **CleanAir Status** toggle button.

Step 4 Click **Update & Apply to Device**.

Disabling Receiver Only Dual-Band Radio on a Cisco Access Point

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.

Step 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 shutdown**
	Example:
	`Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 shutdown`
	`Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 shutdown`
		Disables receiver only dual-band radio on a specific Cisco access point.
		Here, 2 refers to the slot ID.
		Use the **no** form of this command to enable receiver only dual-band radio.

Configuring Client Steering (CLI)

Before you begin

Enable Cisco CleanAir on the corresponding dual-band radio.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless macro-micro steering transition-threshold balancing-window** *number-of-clients(0-65535)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold balancing-window 10`	Configures the micro-macro client load–balancing window for a set number of clients.
Step 4	**wireless macro-micro steering transition-threshold client count** *number-of-clients(0-65535)*	Configures the macro-micro client parameters for a minimum client count for transition.

	Command or Action	Purpose
	Example: `Device(config)# wireless macro-micro steering transition-threshold client count 10`	
Step 5	**wireless macro-micro steering transition-threshold macro-to-micro** *RSSI-in-dBm(–128—0)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold macro-to-micro -100`	Configures the macro–to–micro transition RSSI.
Step 6	**wireless macro-micro steering transition-threshold micro-to-macro** *RSSI-in-dBm(–128—0)* **Example:** `Device(config)# wireless macro-micro steering transition-threshold micro-to-macro -110`	Configures the micro–to–macro transition RSSI.
Step 7	**wireless macro-micro steering probe-suppression aggressiveness** *number-of-cycles(–128—0)* **Example:** `Device(config)# wireless macro-micro steering probe-suppression aggressiveness -110`	Configures the number of probe cycles to be suppressed.
Step 8	**wireless macro-micro steering probe-suppression hysteresis** *RSSI-in-dBm* **Example:** `Device(config)# wireless macro-micro steering probe-suppression hysteresis -5`	Configures the macro-to-micro probe in RSSI. The range is between –6 to –3.
Step 9	**wireless macro-micro steering probe-suppression probe-only** **Example:** `Device(config)# wireless macro-micro steering probe-suppression probe-only`	Enables probe suppression mode.
Step 10	**wireless macro-micro steering probe-suppression probe-auth** **Example:** `Device(config)# wireless macro-micro steering probe-suppression probe-auth`	Enables probe and single authentication suppression mode.

	Command or Action	Purpose
Step 11	**show wireless client steering** **Example:** `Device# show wireless client steering`	Displays the wireless client steering information.

Verifying Cisco Access Points with Dual-Band Radios

To verify the access points with dual-band radios, use the following command:

```
Device# show ap dot11 dual-band summary

AP Name Subband Radio      Mac   Status Channel Power Level Slot ID Mode
-------------------------------------------------------------------------------
4800   All 3890.a5e6.f360 Enabled (40)* *1/8     (22 dBm)      0   Sensor
4800   All 3890.a5e6.f360 Enabled N/A    N/A       2               Monitor
```

Information About OFDMA Support for 11ax Access Points

The Cisco Catalyst 9100 series access points are the next generation WiFi 802.11ax access point, which is ideal for high-density high-definition applications.

The IEEE 802.11ax protocol aims to improve user experience and network performance in high density deployments for both 2.4 GHz and 5 GHz. The 802.11ax APs supports transmission or reception to more than one client simultaneously using Orthogonal Frequency Division Multiplexing (OFDMA).

The IEEE 802.11ax supports uplink MU-MIMO and also adds OFDMA for multiple users in the uplink and downlink. All the users in IEEE 802.11ax OFDMA have the same time allocations and it ends at the same time. In MU-MIMO and OFDMA, multiple stations (STAs) either simultaneously transmit to a single STA or simultaneously receive from a single STA independent data streams over the same radio frequencies.

Supported Modes on 11ax Access Points

The following AP modes are supported:

- Local mode
- Flex-connect mode
- Bridge mode
- Flex+Mesh mode

Configuring 11AX (GUI)

You can configure 11ax for the frequencies, 5 GHz and 2.4 GHz.

Procedure

Step 1 Choose **Configuration > Radio Configurations > High Throughput**.

Step 2 Click the **5 GHz Band** tab.

a) Expand the **11ax** section.
b) Select the **Enable 11ax** and **Multiple Bssid** check boxes, if required.
c) Check either the **Select All** check box to configure all the data rates or select the desired options from the available data rates list.

Step 3 Click the **2.4 GHz Band** tab.

a) Expand the **11ax** section.
b) Select the **Enable 11ax** and **Multiple Bssid** check boxes, if required.
c) Check either the **Select All** check box to configure all the data rates or select the desired options from the available data rates list.

Configuring Channel Width

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap dot11** { **24ghz** | **5ghz** } **rrm channel dca chan-width 160** **Example:** `Device(config)# ap dot11 5ghz rrm channel dca chan-width 160`	Configures channel width for 802.11 radios as 160. Use the **no** form of the command to disable the configuration. **Note** Cisco Catalyst 9115 and C9120 series APs do not support 80+80 channel width. Cisco Catalyst 9117 series APs do not support OFDMA in 160 channel width.
Step 3	**ap dot11** { **24ghz** | **5ghz** } **rf-profile** *profile-name* **Example:** `Device(config)# ap dot11 5ghz rf-profile ax-profile`	Configures an RF profile and enters RF profile configuration mode.
Step 4	**channel chan-width 160** **Example:** `Device(config-rf-profile)# channel chan-width 160`	Configures the RF profile DCA channel width.

Configuring 802.11ax Radio Parameters (GUI)

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **5 GHz Band** > **11ax**.

Step 2 Check or uncheck the **Enable 11 n** check box.

Step 3 Check the check boxes for the desired MCS/(data rate) or to select all of them, check the **Select All** check box.

Step 4 Click **Apply**.

Step 5 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **2.4 GHz Band** > **11ax**.

Step 6 Check or uncheck the **Enable 11 n** check box.

Step 7 Check the check boxes for the desired MCS/(data rate) or to select all of them, check the **Select All** check box.

Step 8 Click **Apply**.

Step 9 Choose **Configuration** > **Wireless** > **Access Points**.

Step 10 Click the Access Point.

Step 11 In the **Edit AP** dialog box, enable the **LED State** toggle button and choose the LED brightness level from the **LED Brightness Level** drop-down list.

Step 12 Click **Update and Apply to Device**.

Configuring 802.11ax Radio Parameters (CLI)

Follow the procedure given below to configure radio parameters:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**ap dot11** { **24ghz** | **5ghz** | **6ghz** } **dot11ax** **Example:** `Device(config)# ap dot11 6ghz dot11ax`	Configures 802.11 6GHz dot11ax parameters. Use the **no** form of the command to disable the configuration.
Step 3	**ap dot11** { **24ghz** | **5ghz** | **6ghz** } **dot11ax mcs tx index** *index* **spatial-stream** *spatial-stream-value* **Example:**	Enables the 11ax 2.4-Ghz, 5-Ghz, or 6-Ghz band modulation and coding scheme (MCS) transmission rates.

	Command or Action	Purpose
	`Device(config)# ap dot11 5ghz dot11ax mcs tx index 11 spatial-stream 8`	
Step 4	**ap led-brightness** *brightness-level* **Example:** `Device(config)# ap led-brightness 6`	(Optional) Configures the led brightness level.

Setting up the 802.11ax Radio Parameters

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **led-brightness-level** *brightness-level* **Example:** `Device# ap name ax-ap led-brightness-level 6`	Configures the led brightness level.
Step 3	**ap name** *ap-name***dot11** { **24ghz** | **5ghz** } **dot11n antenna** *antenna-port* **Example:** `Device# ap name ap1 dot11 5ghz dot11n antenna A`	Configures the 802.11n - 5 GHz antenna selection. Use the **no** form of the command to disable the configuration.
Step 4	**ap name** *ap-name* **dot11** { **24ghz** | **5ghz** } **channel width** *channel-width* **Example:** `Device# ap name ap1 dot11 5ghz channel width 160`	Configures 802.11 channel width.
Step 5	**ap name** *ap-name* **dot11** { **24ghz** | **5ghz** } **secondary-80** *channel-num* **Example:** `Device# ap name ap1 dot11 5ghz secondary-80 12`	Configures the advanced 802.11 secondary 80Mhz channel assignment parameters.

Configuring OFDMA on a WLAN

Note For Cisco Catalyst 9115 and 9120 series APs, the configuration given below are per radio, and not per WLAN. This feature remains enabled on the controller, if it is enabled on any of the WLANs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 2	**wlan** *wlan1* **Example:** `Device(config)# wlan wlan1`	Enters the WLAN configuration mode.
Step 3	**dot11ax** *downlink-ofdma* **Example:** `Device(config-wlan)# dot11ax downlink-ofdma`	Enables the downlink connection that uses the OFDMA technology. Use the **no** form of the command to disable the configuration.
Step 4	**dot11ax** *uplink-ofdma* **Example:** `Device(config-wlan)# dot11ax uplink-ofdma`	Enables the uplink connection that uses the OFDMA technology .
Step 5	**dot11ax** *downlink-mumimo* **Example:** `Device(config-wlan)# dot11ax downlink-mumimo`	Enables the downlink connection that uses the MUMIMO technology.
Step 6	**dot11ax** *uplink-mumimo* **Example:** `Device(config-wlan)# dot11ax uplink-mumimo`	Enables the uplink connection that uses the MUMIMO technology.
Step 7	**dot11ax** *twt-broadcast-support* **Example:** `Device (config-wlan)# dot11ax twt-broadcast-support`	Enables the TWT broadcast support operation.

Verifying Channel Width

To verify the channel width and other channel information, use the following **show** commands:

```
Device# show ap dot11 5ghz summary

AP Name             Mac Address       Slot    Admin State  Oper State  Channel    Width
 Txpwr
-------------------------------------------------------------------------------------------------
AP80e0.1d75.6954    80e0.1d7a.7620     1       Enabled      Up          (52)*      160
  1(*)

Device# show ap dot11 dual-band summary

AP Name        Subband    Radio Mac        Status     Channel    Power Level  Slot ID
   Mode
-------------------------------------------------------------------------------------------------
kartl28021mi    All       002a.1058.38a0    Enabled   (52)*      (1)*            1
   REAP

Device# show ap name <ap-name> channel

802.11b/g Current Channel                       : 11
Slot ID                                         : 0
Allowed Channel List                            : 1,2,3,4,5,6,7,8,9,10,11
802.11a Current Channel ..................... 52  (160 MHz)
Slot ID                                         : 1
Allowed Channel List                            :
36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,149,153,157,161,165

Device# show ap name <ap-name> config slot <slot-num>
.
.
.
Phy OFDM Parameters
              Configuration                             : Automatic
              Current Channel                           : 52
              Extension Channel                         : No Extension
              Channel Width                             : 160 MHz
             Allowed Channel List                       :
36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140,149,153,157,161,165
             TI Threshold                               : 0

Device# show ap dot11 5ghz channel
.
.
.
  DCA Sensitivity Level                     : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width              : 160 MHz
  DCA Minimum Energy Limit                  : -95 dBm
.
.
.

Device# show ap rf-profile name <name> detail
.
.
.
Unused Channel List              : 165
DCA Bandwidth                    :  160 MHz
DCA Foreign AP Contribution      : Enabled
.
```

.
.

Verifying Client Details

To verify the client information, use the following **show** commands:

```
Device# show wireless client mac-address <mac-address> detail


Client MAC Address : a886.ddb2.05e9
Client IPv4 Address : 169.254.175.214
Client IPv6 Addresses : fe80::b510:a381:8099:4747
                        2009:300:300:57:4007:6abb:2c9a:61e2
Client Username: N/A
Voice Client Type   : Unknown
AP MAC Address : c025.5c55.e400
AP Name: APe4c7.22b2.948e
Device Type: N/A
Device Version: N/A
AP slot : 0
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 1
Wireless LAN Name: SSS_OPEN
BSSID : c025.5c55.e406
Connected For : 23 seconds
Protocol : 802.11ax - 5 GHz
Channel : 8
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 86400 sec (Remaining time: 86378 sec)

.
.
.
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                          WLAN  State             Protocol Method
  Role
-------------------------------------------------------------------------------------------------
a886.ddb2.05e9 APe4c7.22b2.948e                 1     Run               11ax(5) None
 Local


Device# show wireless stats client detail


Total Number of Clients : 1

Protocol Statistics

---------------------------------------------------------------------------
Protocol            Client Count
 802.11b              : 0
```

```
 802.11g             : 0
 802.11a             : 0
 802.11n-2.4GHz      : 0
 802.11n-5 GHz       : 0
 802.11ac            : 0
 802.11ax-5 GHz      : 0
 802.11ax-2.4 GHz    : 0
 802.11ax-6 GHz      : 1
```

Verifying Radio Configuration

To verify the radio configuration information, use the following **show** commands:

```
Device# show ap dot11 5ghz network

802.11a Network                             : Enabled
.
.
.
802.11ax                                    : Enabled
  DynamicFrag                               : Enabled
  MultiBssid                                : Disabled
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1               : Disabled
  MCS  9, Spatial Streams = 1               : Disabled
  MCS 11, Spatial Streams = 1               : Disabled
  MCS  7, Spatial Streams = 2               : Supported
  MCS  9, Spatial Streams = 2               : Supported
  MCS 11, Spatial Streams = 2               : Supported
  MCS  7, Spatial Streams = 3               : Supported
  MCS  9, Spatial Streams = 3               : Disabled
  MCS 11, Spatial Streams = 3               : Disabled
  MCS  7, Spatial Streams = 4               : Supported
  MCS  9, Spatial Streams = 4               : Supported
  MCS 11, Spatial Streams = 4               : Supported
  MCS  7, Spatial Streams = 5               : Supported
  MCS  9, Spatial Streams = 5               : Supported
  MCS 11, Spatial Streams = 5               : Supported
  MCS  7, Spatial Streams = 6               : Supported
  MCS  9, Spatial Streams = 6               : Supported
  MCS 11, Spatial Streams = 6               : Supported
  MCS  7, Spatial Streams = 7               : Supported
  MCS  9, Spatial Streams = 7               : Supported
  MCS 11, Spatial Streams = 7               : Supported
  MCS  7, Spatial Streams = 8               : Supported
  MCS  9, Spatial Streams = 8               : Supported
  MCS 11, Spatial Streams = 8               : Supported
Beacon Interval                             : 100
.
.
.
Maximum Number of Clients per AP Radio      : 200

Device# show ap dot11 24ghz network

802.11b Network                             : Enabled
.
.
.
802.11axSupport..................................... Enabled
      dynamicFrag.............................. Disabled
      multiBssid............................... Disabled
```

```
802.11ax                                  : Enabled
  DynamicFrag                             : Enabled
  MultiBssid                              : Enabled
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1             : Supported
  MCS  9, Spatial Streams = 1             : Supported
  MCS 11, Spatial Streams = 1             : Supported
  MCS  7, Spatial Streams = 2             : Supported
  MCS  9, Spatial Streams = 2             : Supported
  MCS 11, Spatial Streams = 2             : Supported
  MCS  7, Spatial Streams = 3             : Supported
  MCS  9, Spatial Streams = 3             : Supported
  MCS 11, Spatial Streams = 3             : Supported
  MCS  7, Spatial Streams = 4             : Disabled
  MCS  9, Spatial Streams = 4             : Disabled
  MCS 11, Spatial Streams = 4             : Disabled
Beacon Interval                           : 100
.
.
.
Maximum Number of Clients per AP Radio    : 200
```

```
Device# show ap dot11 6ghz network
802.11 6Ghz Network                       : Enabled
802.11ax                                  : Enabled
.
.
.
802.11ax MCS Settings:
  MCS  7, Spatial Streams = 1             : Supported
  MCS  9, Spatial Streams = 1             : Supported
  MCS 11, Spatial Streams = 1             : Supported
  MCS  7, Spatial Streams = 2             : Supported
  MCS  9, Spatial Streams = 2             : Supported
  MCS 11, Spatial Streams = 2             : Supported
  MCS  7, Spatial Streams = 3             : Supported
  MCS  9, Spatial Streams = 3             : Supported
  MCS 11, Spatial Streams = 3             : Supported
  MCS  7, Spatial Streams = 4             : Supported
  MCS  9, Spatial Streams = 4             : Supported
  MCS 11, Spatial Streams = 4             : Supported
Beacon Interval                           : 95
.
.
.
Maximum Number of Clients per AP Radio    : 200
WiFi to Cellular RSSI Threshold           : -85 dbm
Client Network Preference                 : default
```

```
#show wlan id 1
WLAN Profile Name     : wlanon66
================================================
Identifier                                    : 1
Description                                   :
Network Name (SSID)                           : wlanon66
Status                                        : Enabled
Broadcast SSID                                : Enabled
Advertise-Apname                              : Enabled
Universal AP Admin                            : Disabled
Max Associated Clients per WLAN               : 0
Max Associated Clients per AP per WLAN        : 0
Max Associated Clients per AP Radio per WLAN  : 200
OKC                                           : Enabled
Number of Active Clients                      : 0
CHD per WLAN                                  : Enabled
```

```
WMM                                             : Allowed
WiFi Direct Policy                              : Disabled
.
.
.
Operational State of Radio Bands
    2.4ghz                                      : UP
    5ghz                                        : UP
    6ghz                                        : DOWN (Required config: Disable WPA2 and
Enable WPA3 & dot11ax)
DTIM period for 802.11a radio                   :
DTIM period for 802.11b radio                   :
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Mac Filter Override Authorization list name     : Disabled
Accounting list name                            :
802.1x authentication list name                 : Disabled
802.1x authorization list name                  : Disabled
Security
    802.11 Authentication                       : Open System
.
.
.
802.11ac MU-MIMO                                : Enabled
802.11ax parameters
    802.11ax Operation Status                   : Enabled
    OFDMA Downlink                              : Enabled
    OFDMA Uplink                                : Enabled
    MU-MIMO Downlink                            : Enabled
    MU-MIMO Uplink                              : Enabled
    BSS Target Wake Up Time                     : Enabled
    BSS Target Wake Up Time Broadcast Support   : Enabled
.
.
.
```

Note For 6-GHz radio, the 802.11ax parameters are taken from the multi BSSID profile tagged to the corresponding 6-GHz RF profile of the AP. So, the WLAN dot11ax parameters are overridden by multi BSSID profile parameters in the case of 6-GHz. There are no changes for 2.4 and 5-GHz band WLANs. They continue to use the WLAN parameters for 802.11ax.

```
Device# show ap led-brightness-level summary

AP Name                          LED Brightness level
------------------------------------------------------
AP00FC.BA01.CC00                 Not Supported
AP70DF.2FA2.72EE                 8
AP7069.5A74.6678                 2
APb838.6159.e184                 Not Supported
```

Information About Cisco Flexible Antenna Port

The presence of multiple antennas on the transmitters and the receivers of access points (APs), results in better performance and reliability of the APs. Multiple antennas improve reception through the selection of stronger signals or a combination of individual signals, at the receiver. You can configure the antenna ports to be used in the APs as either dual-band antennas or as single-band antennas to optimize radio coverage.

- Dual-band antenna mode: APs operate in both the 2.4-GHz and 5-GHz bandwidth with all the four antennas—A, B, C, and D. An example of a dual-band antenna mode AP is the Cisco Industrial Wireless 3702 AP.
- Single-band antenna mode: Among the APs, antennas A and B operate in the 2.4-GHz bandwidth, and the antennas C and D operate in the 5-GHz bandwidth. An example of a single-band antenna mode AP is the Cisco Catalyst Industrial Wireless 6300 AP.

Configuring a Cisco Flexible Antenna Port (GUI)

Procedure

Step 1 Choose **Configuration > Wireless > Access Points**.

Step 2 Click **AP Name**.

Step 3 Click the **Advanced** tab.

Step 4 From the **Antenna Mode** drop-down list, choose the antenna mode.

Step 5 Click **Apply & Update**.

Configuring a Cisco Flexible Antenna Port (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **antenna-band-mode** {**dual** | **single**} **Example:** `Device# ap name ap-name antenna-brand-mode single`	Configures antenna band mode as single or dual.

Verifying Flexible Antenna Port Configuration

The following is a sample output of the **show ap name** *ap_name* **config general** command that shows the bands selected on a specific AP:

```
Device# show ap name APXXXX.31XX.83XX config general
Cisco AP Name   : APXXXX.31XX.83XX
================================================
Cisco AP Identifier                             : b4de.312e.00c0
Country Code                                    : Multiple Countries : US,IN
Regulatory Domain Allowed by Country   : 802.11bg:-A   802.11a:-ABDN

AP Submode                                      : Not Configured
Antenna Band Mode                               : Dual
```

The following is a sample output of the **show ap name** *ap_name* **config slot 0** command that shows the bands selected on a specific AP with dual-band mode enabled:

```
Device# show ap name APXXXX.31XX.83XX config slot 0 | sec 802.11n Antennas
    802.11n Antennas
      A                                       : ENABLED
      B                                       : ENABLED
      C                                       : ENABLED
      D                                       : ENABLED

    802.11n Antennas
      MIMO                                    : x
      Tx                                      : Unknown
      Rx                                      : Unknown
```

The following is a sample output of the **show ap name** *ap_name* **config slot 1** command that shows the bands selected on a specific AP with single-band mode enabled:

```
Device# show ap name APXXXX.31XX.83XX config slot 1 | sec 802.11n Antennas
    802.11n Antennas
      A                                       : DISABLED
      B                                       : DISABLED
      C                                       : ENABLED
      D                                       : ENABLED

    802.11n Antennas
      MIMO                                    : x
      Tx                                      : Unknown
      Rx                                      : Unknown
```

Feature History for Environmental Sensors in Access Points

This table provides release and related information for the feature explained in this module.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 2: Feature History for Environmental Sensors on Access Points

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	Environmental Sensors in Access Points	The Environmental Sensors in Access Points feature helps you collect real-time environmental data, such as, air quality, temperature, and humidity, from the environmental sensors that are embedded in the Cisco Catalyst 9136 Series Access Points.
Cisco IOS XE Cupertino 17.9.1	Environmental Sensors in Access Points	This feature is supported on Cisco Catalyst Wireless 9166I Series Access Points.

Information About Environmental Sensors in Access Points

You can collect real-time environmental data, such as, air quality, temperature, and humidity, from the environmental sensors that are embedded in the Cisco Catalyst 9136 Series Access Points, and make this data

available to customers and partners through the Cisco Spaces solution. You can disable, enable, and configure the scan interval of the sensors from the Cisco Catalyst 9800 Series Wireless Controller CLIs.

Note From Cisco IOS XE Cupertino 17.8.1, this feature is supported on Cisco Catalyst 9136 Series APs.

In Cisco IOS XE Cupertino 17.9.1, air quality, temperature, and humidity are supported on Cisco Catalyst Wireless 9166I Series Access Points.

Currently, two sensors are added to Cisco Catalyst 9136 Series APs:

- Total volatile organic compounds (TVOC) air quality sensor
- Combined Temperature and Humidity sensor

Use Cases

The following are the use cases for the environmental sensors in APs:

- In the healthcare industry, environmental sensors help reduce wastage and spoilage of pharmaceuticals by maintaining a consistent environment.
- In the hospitality industry, environmental sensors help improve customer experience by monitoring the air quality of a room.
- In the retail industry, these sensors prevent spoilage of products.

Configuring Environmental Sensors in an AP Profile (CLI)

To configure the environmental sensor in the Cisco Catalyst 9800 Series Wireless Controllers under an AP profile, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures an AP profile.
Step 3	**sensor environment air-quality** **Example:**	Configures AP environmental air quality sensor. Enters AP sensor configuration mode.

	Command or Action	Purpose
	`Device(config-ap-profile)# sensor environment air-quality`	
Step 4	**no shutdown** **Example:** `Device(config-ap-sensor)# no shutdown`	Enables the AP air quality sensor configuration.
Step 5	**sensor environment temperature** **Example:** `Device(config-ap-profile)# sensor environment temperature`	Configures AP environmental temperature sensor. Enters AP sensor configuration mode.
Step 6	**no shutdown** **Example:** `Device(config-ap-sensor)# no shutdown`	Enables the AP temperature sensor configuration.
Step 7	**sampling** *data-sampling-interval* **Example:** `Device(config-ap-sensor)# sampling 200`	Configures data sampling interval, in seconds. The valid range is between 5 and 3600. The default value is 5. Use the **no** form of this command to set the data sampling interval to the default time of 5.
Step 8	**exit** **Example:** `Device(config-ap-sensor)# exit`	Exits the sub mode.

Configuring Environment Sensors in Privileged EXEC Mode (CLI)

To disable the sensor on an AP that might be sending invalid data (an AP near an air vent or near a coffee machine), you can disable the sensor by running the corresponding commands in the privileged EXEC mode of the Cisco Catalyst 9800 Series Wireless Controllers.

Note For a sensor to be operational in the **Up** state, both, the AP profile configuration state and the AP administrative state should be enabled. If any of the two is disabled, the sensor operational status will stay **Down**.

To disable and enable the admin state of the sensor, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter the password if prompted.

	Command or Action	Purpose
Step 2	**ap name** *ap-name* **sensor environment**{**air-quality** | **temperature**} **shutdown** **Example:** `Device# ap name CiscoAP sensor environment air-quality shutdown`	Disables the sensor admin state of the AP.
Step 3	**ap name** *ap-name* **no sensor environment**{**air-quality** | **temperature**} **shutdown** **Example:** `Device# ap name CiscoAP no sensor environment air-quality shutdown`	Enables the sensor admin state of the AP.

Verifying the AP Sensor Status

To verify the status of the AP sensors, run the following command:

```
Device# show ap sensor status
AP Name                          MAC-address          Sensor-type      Config-State
Admin-State      Oper-Status     Sampling-Interval
-------------------------------------------------------------------------------------
Cisco.1DBC                        xxxx.xxxx.xxx1       Air-quality      Disabled
Enabled          Down            5
Cisco.1DBC                        xxxx.xxxx.xxx2       Temperature      Disabled
Enabled          Down            5
Cisco.1E24                        xxxx.xxxx.xxx3       Air-quality      Disabled
Enabled          Down            5
Cisco.1E24                        xxxx.xxxx.xxx4       Temperature      Disabled
Enabled          Down            5
```

Information About CAPWAP LAG Support

Link aggregation (LAG) simplifies controller configuration because you no longer require to configure primary and secondary ports for each interface. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

The CAPWAP LAG support feature is applicable for access points that support multiple ethernet ports for CAPWAP.

The 11AC APs with dual ethernet ports require the CAPWAP AP LAG support for data channel.

Cisco Aironet 1850, 2800, and 3800 Series APs' second Ethernet port is used as a link aggregation port, by default. It is possible to use this LAG port as an RLAN port when LAG is disabled.

The following APs use LAG port as an RLAN port:

- 1852E
- 1852I

- 2802E
- 2802I
- 3802E
- 3802I
- 3802P
- 9136I

Note The CAPWAP LAG feature is not supported on Cisco Catalyst 9176I and Cisco Catalyst 9176D1 APs.

Restrictions for CAPWAP LAG Support

- APs must be specifically enabled for CAPWAP AP LAG support.
- CAPWAP data does not support IPv6.
- Data DTLS must not be enabled when LAG is enabled.
- APs behind NAT and PAT are not supported.

Enabling CAPWAP LAG Support on Controller (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Wireless Global**.
Step 2 Check the **AP LAG Mode** check box.
Step 3 Click **Apply**.

Enabling CAPWAP LAG Support on Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap lag support** **Example:** `Device(config)# ap lag support`	Enables CAPWAP LAG support on the controller. **Note** After executing this command, you get to view the following warning statement: *Changing the lag support will cause all the APs to disconnect.* Thus, all APs with LAG capability reboots and joins the enabled CAPWAP LAG.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enabling CAPWAP LAG Globally on Controller

If the CAPWAP LAG is enabled globally on the controller, the following occurs:

- AP joins the controller.
- AP exchanges its CAPWAP support.
- LAG mode starts, if LAG is enabled on AP.

Disabling CAPWAP LAG Globally on Controller

If the CAPWAP LAG is disabled globally on the controller, the following occurs:

- AP joins the controller.
- AP exchanges its CAPWAP support.
- AP LAG config is sent to AP, if LAG is already enabled on AP.
- AP reboots.
- AP joins back with the disabled LAG.

Enabling CAPWAP LAG for an AP Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click **Add**.

Step 3 Under the **General** tab, enter the **Name** of the AP Profile and check the **LAG Mode** check box to set the CAPWAP LAG for the AP profile.

Step 4 Click **Apply to Device**.

Enabling CAPWAP LAG for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters AP profile configuration mode. **Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**lag** **Example:** `Device(config-ap-profile)# lag`	Enables CAPWAP LAG for an AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Disabling CAPWAP LAG for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:**	Configures an AP profile and enters AP profile configuration mode.

	Command or Action	Purpose
	`Device(config)# ap profile xyz-ap-profile`	**Note** When you delete a named profile, the APs associated with that profile will not revert to the default profile.
Step 3	**no lag** **Example:** `Device(config-ap-profile)# no lag`	Disables CAPWAP LAG for an AP profile.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Disabling CAPWAP LAG Support on Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**no ap lag support** **Example:** `Device(config)# no ap lag support`	Disables CAPWAP LAG support on the controller . **Note** All APs with LAG capability reboots and joins the disabled CAPWAP LAG.
Step 3	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying CAPWAP LAG Support Configurations

To verify the global LAG status for all Cisco APs, use the following command:

```
Device# show ap lag-mode
AP Lag-Mode Support Enabled
```

To verify the AP LAG configuration status, use the following command:

```
Device# show ap name <ap-name> config general
Cisco AP Identifier : 0008.3291.6360
Country Code : US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-AB
```

```
AP Country Code : US - United States
::
AP Lag Configuration Status : Enabled/Disabled
Has AP negotiated lag based on AP capability and per AP config.
```

Feature History for CAPWAP Message Aggregation

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 3: Feature History for CAPWAP Message Aggregation

Release	Feature	Feature Information
Cisco IOS XE 17.14.1	CAPWAP Message Aggregation	The CAPWAP Message Aggregation feature aggregates the CAPWAP control messages of the same type waiting in the queue to be transmitted to the AP.

Information About CAPWAP Message Aggregation

The CAPWAP Message Aggregation feature aggregates the CAPWAP control messages to be sent to APs. When APs are busy processing packets, the messages to be sent to the APs are stored in the controller. When you enable the feature, if the last message type in the queue and the current message type are the same, the CAPWAP messages are aggregated and capped at Maximum Transmission Unit (MTU). This improves the performance of the system.

Guidelines

- Applicable to all AP modes.
- The CAPWAP Message Aggregation feature is disabled by default.

Use Case

Flex deployment use case: You can expect a round-trip delay when packets are sent over wide area network (WAN) in Flex deployments. With the CAPWAP message aggregation, the round-trip time reduces significantly. Also, the client join and client roam are faster.

Configuring CAPWAP Message Aggregation (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile default-ap-profile`	Configures an AP profile and enters the AP profile configuration mode.
Step 3	**capwap aggregation** **Example:** `Device(config-ap-profile)# capwap aggregation`	Enables CAPWAP message aggregation. This feature is disabled by default.
Step 4	**end** **Example:** `Device(config-ap-profile)# end`	Exits configuration mode and returns to privileged EXEC mode.

Verifying CAPWAP Message Aggregation

To view the total number of aggregated CAPWAP control packets for the controller, use the following command:

```
Device# show wireless stats ap packet

Packet stats

Capwap Control Packets Received* : 11183016
Capwap Data Keep Alive Packets Received : 160399
Capwap Data DOT1X EAP Packets Received: 549
Capwap Data DOT1X Mgmt Packets Received: 6003
Capwap Data DOT1X Key Type Packets Received: 0
Capwap Data DOT1X Control Packets Received: 0
Capwap Data ARP Packets Received: 0
Capwap Data IP Packets Received: 0
Capwap Data IPV6 Packets Received: 0
Capwap Data RRM Packets Received: 0
Capwap Data DHCP Packets Received: 0
Capwap Data RFID Packets Received: 0
Capwap Data IAPP Packets Received: 2531939
Capwap Dgram Input Errors : 0
Capwap Discovery Packets Received : 22299
Capwap Discovery Dgram Input Errors : 0
Aggregated Capwap Control Packets Sent: 119337
**** Note: Capwap control packets exclude discovery/primary discovery packets ****
```

To verify the status of the CAPWAP message aggregation feature, use the following command:

```
Device# show ap profile name default-ap-profile detailed
AP Profile Name               : default-ap-profile
Description                   : default custom profile
Country code                  : Not configured
Stats Timer                   : 180
Link Latency                  : ENABLED
Data Encryption               : DISABLED
LED State                     : ENABLED
NTP server                    : 0.0.0.0
```

```
NTP Authentication            : DISABLED
Jumbo MTU                     : ENABLED
24ghz Report Interval         : 90
5ghz Report Interval          : 90
bssid stats status            : ENABLED
bssid stats frqncy interval   : 120
bssid neighbor stats status   : ENABLED
bssid neighbor stats interval : 120
CAPWAP Control Aggregation    : ENABLED
```

Configuring Bulk AP Provisioning

Bulk AP provisioning allows you to configure multiple AP parameters for more than one AP at a time. You can configure AP parameters such as admin status and floor location, geolocation parameters, and high availability parameters.

Procedure

Step 1 Navigate to the **Configuration** > **Wireless** > **Bulk AP Provisioning** page.

You can view the current tasks along with its status.

Step 2 Click **Start a workflow to create an AP Provisioning task** to start a new bulk AP provisioning task.

Step 3 In the **Select AP** page, configure the following:

a) Change the name of the task.
b) Select the APs you wish to provision.
c) Click **Next**.

Step 4 In the **Select Parameters** page, configure the following as required:

a) Change the admin status by clicking on the drop-down list.
b) Enter the location.
c) Enter the above ground level height in meters. The range is from -100 to 1000.
d) Enter the tolerance as uncertainty height in meters. The range is from 0 to 100.
e) Enter the cable length in meters. The range is from 1 to 100. The default is 10.

We recommend that you keep the default value of 10 meters with the Cisco provided external antenna.

Note This option is available on selected models that support adding an external antenna.

f) Enter the floor ID.
g) Enter the name and management IP address of the primary, secondary, and tertiary controller.
h) Click **Next**.

Step 5 In the **Summary** page, click **Apply** after confirming the changes.

You can view changes in the task status from its provisioning to completion. On clicking the task, you can view the count of the configurations that were applied and not applied on each of the selected APs.