Cisco CleanAir

Cisco ISE systems

A Cisco ISE system is a wireless spectrum management solution that

- proactively monitors and manages challenges caused by interference in a shared wireless spectrum
- uses Cisco CleanAir-enabled access points and controllers to detect and analyze native and foreign interference sources, and
- enables both manual and automated remediation to optimize wireless network operation.

Table 1: Feature history for CleanAir

Release	Feature	Feature Information
Cisco IOS XE 17.13.1	EDRRM Support for 6-GHz Band Radio	The Event-Driven Radio Resource Management (EDRRM) is enabled in the 6-GHz band radio of AP.

Components of Cisco ISE systems

Cisco CleanAir systems are comprised of several key hardware and software elements:

- Cisco CleanAir-**enabled APs**: These devices actively scan the wireless spectrum for all active transmitters.
- **Wireless controllers**: Cisco Catalyst 9800 Series Wireless Controller, , and .
- **Management platforms**: provide centralized management and visualization of spectrum and interference data forwarded by the controllers.

How Cisco CleanAir systems detect and respond to interference

1. **Always-On spectrum awareness**: Cisco ISE-enabled APs scan the industrial, scientific, and medical (ISM) bands, identifying and evaluating all radio devices that may cause interference.
2. **Unified control and interference intelligence**: The controller controls the access points and displays the interference devices.
3. **Actionable Insight for Every Interferer**: For every device operating in the unlicensed band, Cisco ISE provides information about what it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF so that you do not have to be an RF expert.

Benefits of Cisco ISE systems

- **Simplifies spectrum management**: Provides visibility into interference without requiring advanced RF expertise.
- **Improves network reliability**: Automatically detects and resolves issues affecting Wi-Fi performance.
- **Supports advanced WLAN services**: Ensures quality for voice over wireless and IEEE 802.11 operations by minimizing RF interference.

Wireless LAN systems use unlicensed 2.4-GHz and 5-GHz ISM bands, which are also shared by devices such as microwave ovens, cordless phones, and Bluetooth equipment. These non-Wi-Fi devices can disrupt network services including voice-over-wireless and IEEE 802.11 communications. Cisco CleanAir systems detect such interference and help mitigate its effects.

Cisco ISE-related terms

Table 2: Cisco CleanAir-related terms

Term	Description
AQI	Air Quality Index. The AQI indicates air quality based on RF interference. An AQI of zero is considered poor, and an AQI greater than eighty-five is considered good.
AQR	Air Quality Report. An AQR shows total interference from all sources, including major categories. The system sends an AQR every 15 minutes and every 30 seconds in Rapid mode.
DC	Duty Cycle. Indicates the percentage of time your device uses the channel.
EDRRM	Event-Driven RRM. When needed, EDRRM enables your access point to skip normal RRM intervals and immediately change channels.
IDR	Interference Device Reports that an AP sends to the controller .
ISI	Interference Severity Index. The ISI is an indicator of the severity of the interference.
RSSI	Received Signal Strength Indicator. RSSI measures the power in a received signal. It indicates the level detected by an access point from an interfering device.

Cisco CleanAir components

Summary

Cisco CleanAir technology uses a coordinated set of hardware and software components to detect, report, and address wireless interference. Each part of the system contributes to maintaining optimal air quality and reliable wireless performance.

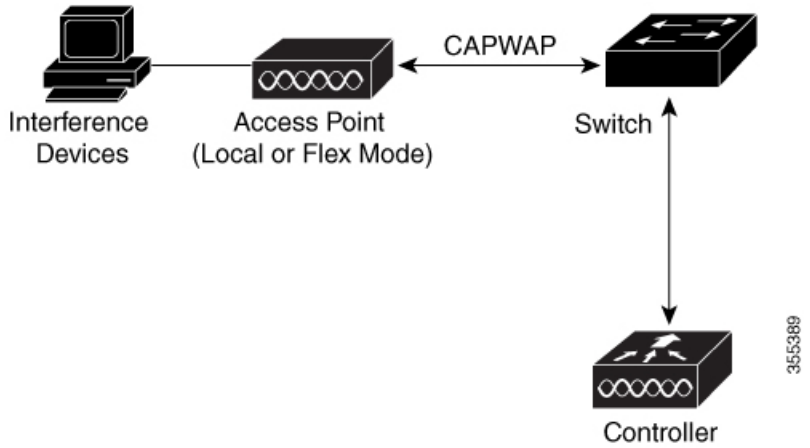
The key components involved in the process are:

- Cisco CleanAir-enabled AP: Collects information about Wi-Fi interference sources and processes it. The AP collects and sends the Air Quality Report (AQR) and Interference Device Report (IDR) to the controller .
- Controller: Controls and configures CleanAir-capable access points, collects and processes spectrum data, provides user interfaces (GUI and CLI), and detects, merges, and mitigates interference devices. The controller also detects, merges, and mitigates interference devices using RRM TPC and DCA For details, see Interference Device Merging.

CleanAir technology ensures wireless networks remain reliable by automatically detecting sources of interference and providing tools for administrators to analyze and respond to RF threats.

Workflow

Figure 1: Cisco CleanAir Solution



These stages describe the operation of Cisco CleanAir components in the system.

1. Configuration: Configures Cisco CleanAir capabilities on the APs.
2. Detection: Cisco CleanAir-enabled APs continuously scan the wireless environment for interference sources and assess air quality.
3. Reporting: APs generate reports such as Air Quality Reports (AQRs) and Interference Device Reports (IDRs), which summarize detected interference and air quality indexes.
4. Aggregation: Wireless controllers collect AQRs and IDRs from all APs, process the data, and store it in relevant databases.
5. Analysis and Response: Controllers use built-in mechanisms (like Radio Resource Management) to mitigate interference and maintain optimal RF conditions.

6. Advanced Services: MSE tracks interference devices over time and location, merges data from multiple controllers, and provides comprehensive threat detection with adaptive Wireless Intrusion Prevention System (WIPS).
7. Specialized Troubleshooting (optional): For in-depth RF analysis, an administrator can connect a CleanAir-enabled AP directly to a PC running Cisco Spectrum Expert.

Result

The Cisco CleanAir system delivers end-to-end automated detection, analysis, and mitigation of wireless interference, enabling proactive network management and high-quality wireless performance.

Difference between Wi-Fi chip-based RF Management and Cisco CleanAir

Feature	Wi-Fi Chip–Based RF Management	Cisco CleanAir
Noise identification	Reports broad, often vague RF noise without pinpointing sources	Precisely identifies interference type, source, potential impact to a WLAN
Noise measurement method	Relies on long-term averaging, which smooths out important details and reduces resolution of measurements	Captures real-time events with full granularity
Response style	Primarily reacts after interference is noticed	Enables proactive, context-aware mitigation allowing for intelligent, proactive decisions.
Transient interference handling	Averaging measurements reduces resolution of measurements, and disruptive signals do not appear to need mitigation.	Flags brief, spontaneous interference events immediately

Cisco CleanAir access points can detect and report severity of the interference .

Spectrum event-driven RRM is one such mitigation strategy.

Note Spectrum event-driven RRM can be triggered only by Cisco CleanAir-enabled access points in local mode.

Persistence interference

A persistent device avoidance is a wireless interference mitigation feature that

- identifies and continuously tracks intermittent interference sources such as microwave ovens,
- maintains channel avoidance for affected APs even if the interference is not constantly present, and
- automatically updates Radio Resource Management (RRM) whenever the interfering device or related access points are moved.

For example, if a microwave oven operates in a break room only for a few minutes at a time, Cisco CleanAir identifies the microwave as an interference source, locates the affected portion of the band

and APs most severely affected, and directs RRM to avoid those channels persistently. Even if the microwave is not active all day, the system maintains avoidance as long as the device is periodically detected. If you move either the microwave oven or the surrounding access points, the algorithm updates RRM automatically

Classes of persistent interference sources

Certain devices, once detected, are likely to remain in place and may cause ongoing interference. Cisco CleanAir can bias the affected channel in Radio Resource Management (RRM) so that CleanAir "remembers" the potential for interference. See Radio Resource Management White Paper.

These device classes qualify as persistent interference sources:

- Microwave ovens
- Outdoor Ethernet bridges
- WiMax fixed and mobile devices
- Motorola Canopy systems

Special case: Bluetooth devices

Bluetooth devices are detected and reported as interference only when actively transmitting. They often enter power-save modes, so interference may only be noticed during active streaming of data or voice.

Persistent devices detection

CleanAir-capable Monitor Mode AP collects information about persistent devices on all configured channels and store the information in controller . Local or Bridge mode AP detects interference devices on the serving channels only.

Persistent device avoidance

When a Persistent Device (PD) is detected in the CleanAir module, it is reported to the RRM module on the MA. This information is used in the channel selection by the subsequent EDRRM Event Driven RRM (ED-RRM) signal sent to the RRM module.

Spontaneous interference

Spontaneous interference is interference that appears suddenly on a network and may jam one or more channels. With Cisco CleanAir spectrum, event-driven RRM, you can set a threshold for air quality, abbreviated as AQ. If air quality drops below this threshold, the system immediately changes the affected AP's channel. Although most RF management systems avoid interference, they require time for information to spread before channels update. Cisco CleanAir uses AQ measurements to continually check the spectrum and can switch channels within **30 seconds**.

For example, if your AP detects interference from a device such as a video camera, it switches channels within **30 seconds** after the interference begins. Cisco CleanAir also helps you identify and locate the interference source so you can take permanent steps to resolve the issue later.

EDRRM and AQR update mode

An EDRRM and AQR update mode is a wireless network feature set that

- enables APs experiencing severe interference (“in distress”) to bypass normal RRM intervals and immediately change channels,
- requires CleanAir technology for monitoring and reporting classified interference devices, and
- provides fast action and remote configuration through control messages and local spectrum management.
- **EDRRM (Event Driven Radio Resource Management):** A function that allows an AP to react instantly to excessive interference by changing channels immediately instead of waiting for scheduled RRM intervals.
- **AQR (Air Quality Reporting) update mode**: A process by which CleanAir APs monitor air quality and report classified interference devices every 15 minutes; when interference causes substantial air quality degradation, EDRRM is triggered.

If a classified interference device severely degrades the air quality on an active channel, EDRRM triggers an immediate channel change so that no clients are stranded on an unusable channel.

Think of a city’s scheduled traffic lights as the normal RRM intervals, allowing cars (data) to move in an orderly, timed way. Normally, everyone waits for the green light, moving only at the set intervals. EDRRM is like having an emergency override for ambulances (APs in distress): if there’s a medical emergency (severe interference), the control center can change the lights to green immediately—regardless of the normal schedule—so the ambulance can take an alternate, clear route (new channel). Air Quality Reporting (AQR) acts like real-time traffic cameras detecting and reporting sudden blockages (classified interference devices) so that the emergency override can be triggered if road conditions (channel quality) deteriorate unexpectedly.

Restrictions for EDRRM and AQR update mode

- EDRRM is not enabled by default; you must first enable CleanAir and then enable EDRRM.
- If an interfering device is operating on an active channel and causes enough AQ degradation to trigger an EDRRM, then no clients will be able to use that channel or the AP. You must remove the AP from the channel.

Prerequisites for CleanAir

You can configure Cisco CleanAir only on CleanAir-enabled access points.

Only Cisco CleanAir-enabled access points in these access point modes can perform Cisco CleanAir spectrum monitoring:

- **Local** —In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only. An AP measures air quality and interference only when it is not transmitting Wi-Fi frames. When channel utilization is high, CleanAir detects less interference.
- **FlexConnect** —When a FlexConnect access point is connected to the controller , its Cisco CleanAir functionality is identical to local mode.
- **Monitor** —When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.
  - **All** —All channels

- **DCA** —Channel selection governed by the DCA list
- **Country** —All channels are legal within a regulatory domain

- **SE-Connect** : Use this mode to connect Spectrum Expert on a Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point and display detailed spectrum data. The application connects directly to the AP and bypasses the device. In SE-Connect mode, the AP does not provide Wi-Fi, RF, or spectrum data; it does not serve clients. Use this mode only for remote troubleshooting. You can have up to three active Spectrum Expert connections.

Only Cisco Catalyst 3850 and Switches can function as Mobility Agents.

Cisco Catalyst 3850 Switches, and Cisco 5760 Wireless LAN Controllers can function as Mobility Controllers.

Restrictions for CleanAir

Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor AP list. IDR clustering depends on the device 's ability to detect neighboring in-network APs. Correlating interference device detections from multiple APs is limited between monitor-mode APs.

-
- In the 4800 AP, slot 1 is dedicated to 5 GHz and cannot be moved to monitor mode. Slot 0 is an XOR slot and can be set to monitor mode, 2.4 GHz, or 5 GHz. Slot 2 is dedicated to monitor mode and will operate in 5 GHz. When AP monitor mode is enabled, slot 2 is disabled because a monitor radio is already available for both 2.4 and 5 GHz. The 3700 AP has dedicated 2.4 GHz (slot 0) and 5 GHz (slot 1) radios.

Do not connect APs in SE connect mode directly to any physical port on the controller.

CleanAir is not supported where the channel width is 160 MHz.

How to configure CleanAir

Enable CleanAir for the 2.4-GHz band (GUI)

Enable CleanAir on 2.4-GHz band radios for real-time interference detection.

Use this procedure to activate Cisco CleanAir technology on APs operating in the 2.4-GHz spectrum using the GUI.

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

Step 2 On the **CleanAir** window, click the **2.4 GHz Band** > **General** tab.

Step 3 Check the **Enable CleanAir** checkbox.

Step 4 Click **Apply**.

CleanAir is enabled on all selected 2.4-GHz radios, and spectrum analysis begins for those devices.

Enable CleanAir for the 2.4-GHz band (CLI)

Enable CleanAir technology on APs operating in the 2.4-GHz band radios for real-time interference detection using commands.

Procedure

Enable the CleanAir feature on the 802.11b network.

Example:

```
Device(config)#ap dot11 24ghz cleanair
Device(config)#no ap dot11 24ghz cleanair
```

Run the **no** form of this command to disable CleanAir on the 802.11b network.

CleanAir is enabled on all selected 2.4-GHz radios, and spectrum analysis begins for those devices.

Configure a CleanAir alarm for 2.4-GHz air-quality and devices (CLI)

Set up alarms that notify you when air quality drops or when certain device types are detected on the 2.4-GHz band using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the alarm for the threshold value for air-quality for all the 2.4-GHz devices.

Example:

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality threshold threshold_value
```

Add the **no** form of this command to disable the alarm.

Step 3 Configure the alarm for the 2.4-GHz devices using this command.

Example:

```
Device(config)# ap dot11 24ghz cleanair alarm device {bt-discovery | bt-link | canopy |
cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx |
video | wimax-fixed | wimax-mobile | xbox | zigbee}
```

Add the **no** form command to disable the alarm.

- bt-discovery: Bluetooth Discovery and bt-link: Bluetooth Link.
- canopy: Canopy devices and cont-tx: Continuous Transmitter.
- dect-like: Digital Enhanced Cordless Communication (DECT)-like phone and fh: 802.11 frequency hopping devices.
- inv: Devices using spectrally inverted WiFi signals and jammer: Jammer.
- mw-oven: Microwave oven and nonstd: Devices using non standard Wi-Fi channels.
- report: Interference device reporting and superag: 802.11 SuperAG devices.
- tdd-tx: TDD Transmitter and video: Video cameras.
- wimax-fixed: WiMax Fixed and wimax-mobile: WiMax Mobile.
- xbox: Xbox and zigbee: 802.15.4 devices.

Step 4 Return to the privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configure interference reporting for a 2.4-GHz device (GUI)

Configure which types of interference are detected by a 2.4-GHz device using the CleanAir GUI. This task guides you through selecting and applying specific interference types to monitor.

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

Step 2 Click the **2.4 GHz Band** tab.

Step 3 Choose the interference types and add them to the **Interference Types to detect** section.

These interference types are available:

- BLE Beacon: Bluetooth low energy beacon and Bluetooth Discovery.
- Bluetooth Link and Canopy.
- Continuous Transmitter and DECT-like Phone: Digital Enhanced Cordless Technology phone.
- 802.11 FH: 802.11 frequency hopping device and WiFi Inverted: Device using spectrally inverted Wi-Fi signals.
- Jammer and Microwave Oven.
- WiFi Invalid Channel: Device using nonstandard Wi-Fi channels and TDD Transmitter.
- Video Camera and SuperAG: 802.11 SuperAG device.

- WiMax Mobile and WiMax Fixed.
- 802.15.4, Microsoft Device and SI_FHSS.

Step 4 Click **Apply**.

Configure interference reporting for a 2.4-GHz device (CLI)

Configure a 2.4-GHz device to report interference using commands. This process enables devices to detect and provide information about various sources of wireless interference.

Procedure

Step 1 Configure the 2.4-GHz interference devices to report to the device using the command.

Example:

```
Device(config)# ap dot11 24ghz cleanair device {ble-beacon | bt-discovery | bt-link | canopy
 | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx
| video | wimax-fixed | wimax-mobile | xbox | zigbee | alarm}
```

Run the **no** form of this command to disable the configuration.

These are the list of the keyword descriptions:

- ble-beacon: Bluetooth low energy beacon.
- bt-discovery: Bluetooth discovery and bt-link: Bluetooth link.
- canopy: Canopy device and cont-tx: Continuous transmitter.
- dect-like: Digital Enhanced Cordless Communication-like phone and fh: 802.11-frequency hopping device.
- inv: Device using spectrally inverted Wi-Fi signals and jammer: Jammer.
- mw-oven: Microwave oven, nonstd: Device using nonstandard Wi-Fi channels and report: Interference device reporting.
- superag: 802.11 SuperAG device, tdd-tx: TDD transmitter and video: Video camera.
- wimax-fixed: WiMax Fixed and wimax-mobile: WiMax Mobile.
- microsoft xbox: Microsoft Xbox device and zigbee: 802.15.4 device.

Step 2 Return to the privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Enable CleanAir for the 5-GHz band (GUI)

Enable CleanAir to improve 5-GHz wireless interference detection and spectrum analysis using the GUI.

Perform this task when you need enhanced monitoring and automated mitigation of interference on 5-GHz wireless networks.

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

Step 2 On the **CleanAir** page, choose the **5 GHz Band** > **General** tab.

Step 3 Check the **Enable CleanAir** checkbox.

Step 4 Click **Apply**.

CleanAir is enabled for the 5-GHz band, enhancing the detection and mitigation of wireless interference.

Enable CleanAir for the 5-GHz band (CLI)

Enable the CleanAir feature to monitor and mitigate wireless interference on 5-GHz wireless networks using commands.

Procedure

Enable the CleanAir feature on a 802.11a network.

Example:

```
Device(config)# ap dot11 5ghz cleanair
```

Run the **no** form of this command to disable CleanAir on the 802.11a network.

CleanAir is enabled for the 5-GHz band, enhancing the detection and mitigation of wireless interference.

Configure interference reporting for a 5-GHz device (GUI)

Enable detection and reporting of selected interference types for better network performance.

Use this procedure when you need to monitor wireless interference on 5-GHz band devices using CleanAir technology.

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **CleanAir**.

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

Step 3 Choose the interference types and add them to the **Interference Types to detect** section.

These interference types are available:

- Canopy
- Continuous Transmitter
- DECT-like Phone—Digital Enhanced Cordless Technology phone
- 802.11 FH—802.11 frequency hopping device
- WiFi Inverted—Device using spectrally inverted Wi-Fi signals
- Jammer
- WiFi Invalid Channel—Device using nonstandard Wi-Fi channels
- SuperAG—802.11 SuperAG device
- TDD Transmitter
- WiMax Mobile
- WiMax Fixed
- Video Camera

Step 4 Click **Apply**.

Your 5-GHz device now detects and reports the selected interference types.

Configure interference reporting for a 5-GHz device (CLI)

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a 5-GHz interference device to report to the **ap dot11 5ghz cleanair device**{**canopy | cont-tx | dect-like | inv | jammer | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile**} command.

Example:

```
Device(config)#ap dot11 5ghz cleanair device canopy

Device(config)#ap dot11 5ghz cleanair device cont-tx

Device(config)#ap dot11 5ghz cleanair device dect-like

Device(config)#ap dot11 5ghz cleanair device inv

Device(config)#ap dot11 5ghz cleanair device jammer
```

```
Device(config)#ap dot11 5ghz cleanair device nonstd

Device(config)#ap dot11 5ghz cleanair device report
Device(config)#ap dot11 5ghz cleanair device superag
Device(config)#ap dot11 5ghz cleanair device tdd-tx
Device(config)#ap dot11 5ghz cleanair device video
Device(config)#ap dot11 5ghz cleanair device wimax-fixed
Device(config)#ap dot11 5ghz cleanair device wimax-mobile
Device(config)#ap dot11 5ghz cleanair device si_fhss
Device(config)#ap dot11 5ghz cleanair device alarm
```

Device. Run the **no** form of this command to disable interference device reporting.

This is a list of the keyword descriptions:

- **canopy**—Canopy device
- **cont-tx**—Continuous transmitter
- **dect-like**—Digital Enhanced Cordless Communication-like phone
- **fh**—802.11-frequency hopping device
- **inv**—Device using spectrally-inverted Wi-Fi signals
- **jammer**—Jammer
- **nonstd**—Device using nonstandard Wi-Fi channels
- **superag**—802.11 SuperAG device
- **tdd-tx**—TDD transmitter
- **video**—Video camera
- **wimax-fixed**—WiMax fixed
- **wimax-mobile**—WiMax mobile

Step 3 Return to the privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configure event driven RRM for a CleanAir event (GUI)

Configure event driven Radio Resource Management (RRM) to respond to CleanAir-detected interference.

Use this feature to optimize channel assignment automatically when a CleanAir-enabled access point detects significant interference.

Procedure

Step 1 Choose **Configuration** > **Radio Configurations** > **RRM**.
The **Radio Resource Management** window is displayed.

Step 2 Click the **DCA** tab.

Step 3 In the **Event Driven RRM** section, check the **EDRRM** check box to run RRM when CleanAir-enabled AP detects a significant level of interference.

Step 4 Configure the **Sensitivity Threshold** level at which RRM has to be invoked from the following options:

- **Low**: Represents a decreased sensitivity to changes in the environment and its value is set at 35.
- **Medium**: Represents medium sensitivity to changes in the environment at its value is set at 50.
- **High**: Represents increased sensitivity to changes in the environment at its value is set at 60.
- **Custom**: If you choose this option, you must specify a custom value in the **Custom Threshold** box.

Step 5 To configure rogue duty cycle, check the **Rogue Contribution** check box and then specify the **Rogue Duty-Cycle** in terms of percentage. The default value of rogue duty cycle is 80 percent.

Note
Rogue Contribution is a new component in ED-RRM functionality. It enables ED-RRM to respond to Rogue Channel Utilization, which operates independently from CleanAir metrics. Rogue Duty Cycle is derived from standard off-channel RRM metrics and triggers a channel change when neighboring rogue interference is detected. Since this process relies on RRM metrics rather than CleanAir, the timing depends on normal 180-second off-channel intervals, with a maximum delay of three minutes. Rogue Contribution is configured separately from CleanAir ED-RRM and is disabled by default. This feature allows each AP to respond to Wi-Fi interference originating outside the local network, with measurements taken at every individual AP.

Rogue Contribution is a new component in ED-RRM functionality. It enables ED-RRM to respond to detected Rogue Channel Utilization, which functions separately from CleanAir metrics.

Step 6 Save the configuration.

The controller now automatically triggers RRM based on CleanAir or optionally, rogue channel utilization events.

Configure EDRRM for a CleanAir event (CLI)

Enable automated, event-driven dynamic RRM adjustments in response to CleanAir events.

EDRRM allows the AP to adjust its channel management dynamically in response to detected interference or CleanAir events. This ensures better wireless performance and mitigation of interference.

Before you begin

Verify the AP supports CleanAir and EDRRM features.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# conf t
```

Run the **no** form of this command to disable EDRRM.

Step 2 Enable EDRRM CleanAir event.

Example:

```
Device (config)#ap dot11 24ghz rrm channel cleanair-event
```

```
Device(config)#no ap dot11 24ghz rrm channel cleanair-event
```

Run the **no** form of this command to disable EDRRM.

Step 3 Configure the EDRRM sensitivity of the CleanAir event.

Example:

```
Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

This a list of the keyword descriptions:

- Custom—Specifies custom sensitivity to non-Wi–Fi interference as indicated by the AQ value.
- High—Specifies the most sensitivity to non-Wi–Fi interference as indicated by the AQ value.
- Low—Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
- Medium—Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

EDRRM CleanAir event detection and response is enabled with your selected sensitivity, improving dynamic channel management during interference events.

CleanAir Pro scanning

CleanAir Pro scanning

A CleanAir Pro feature is a wireless monitoring capability that

- monitors and reports different categories of non-Wi-Fi interference across supported 2.4-GHz, 5-GHz, and 6-GHz band frequency bands
- generates detailed Interference Device Reports (IDRs) including interferer type, severity, and impacted channels, and

- calculates air quality (AQ) metrics for each dynamic channel assignment (DCA) channel to support intelligent channel management by the controller.

Table 3: Feature history for CleanAir Pro scanning

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.10.1	CleanAir Support for 6-GHz	The CleanAir is enabled in 6-GHz band radio of AP only if CleanAir is enabled globally in 6-GHz band in the controller and 6-GHz radio of individual AP. Cisco IOS XE Cupertino 17.9.1 supports 6-GHz only for spectral analysis on Cisco Catalyst Center. IDR and AQ are not supported for the 6-GHz band in Cisco IOS XE Cupertino 17.9.1.
Cisco IOS XE Cupertino 17.9.1	CleanAir Pro Scanning	The CleanAir Pro Scanning feature monitors and reports the different categories of non-Wi-Fi interference in the 2.4-GHz and 5-GHz bands.

Controller behavior for interferer and channel monitoring

The controller manages interferer information and channel selection using these methods:

- **Interferer database management**: The controller maintains a database of active interferers reported by each access point (AP) on the network.
- **Interferer merging**: If the same interferer is detected by multiple APs, the controller merges these records so the interferer is tracked as a single entity across the network.
- **Air quality tracking**: The controller monitors air quality metrics for each channel. These metrics are used during dynamic channel assignment (DCA) to select optimal channels for each AP.

Note The CleanAir Pro Scanning feature is applicable only for APs with CleanAir Pro-supported radios.

Channel-list configuration command keywords for CleanAir Pro scanning

CleanAir Pro Scanning scans channels in the slots or bands currently enabled on an AP. Here are certain commands used to enable scannig.

- **ap dot11 rrm monitor channel-list dca**: Scans only channels enabled under DCA.
- **ap dot11 rrm monitor channel-list country**: Scans all regulatory channels permitted in the site's country setting.

- **ap dot11 rrm monitor channel-list country all**: Scans every channel available to the radio, without regard to regulatory constraints.

Contents and event types in IDR

APs detect non-Wi-Fi interferers and report this data to the controller through Interference Device Report (IDR) such as

- duty cycle,
- Received Signal Strength Indicator (RSSI) in dBm, and
- a calculated Severity metric.

The controller receives IDR messages and uses event types to track the status of each interferer:

- **UP**: The interferer is first detected.
- **UPDT**: The interferer's status is updated.
- **DOWN**: The interferer is no longer observed.

The controller maintains a list of interferers along with the channels affected for each AP. Within an AP, interferers are merged if they share the same channel, RSSI, and device signature. Across multiple APs, a controller merges interferers reported as the same type.

These processes enable accurate tracking and consolidation of interferer data throughout the network.

Air quality index reports

The Air Quality Index (AQ) metric quantifies interference levels detected by each access point (AP) in a Cisco wireless network.

AQ calculation: AQ starts at 100 (optimal) for each AP and is decremented by the cumulative severity values of all detected interference sources.

Air Quality Metric Calculation

For example, if three Bluetooth devices are reported by an AP, each with a severity of two, this results in an overall cell AQ of 94 (2x3 BT = 6, 100 – 6 = AQ of 94).

Enable CleanAir Pro scan features (CLI)

Enable spectrum monitoring and interference detection across all supported wireless radios.

Use this procedure when you want to configure CleanAir Pro scanning and alarms on Cisco wireless devices using CLI.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the CleanAir features for the 2.4-GHz , 5-GHz, or 6-GHz radios using the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair** command.

Example:

```
Device(config)# ap dot11 24ghz cleanair
```

Step 3 Configure CleanAir alarm for air quality in the 2.4-GHz, 5-GHz, or 6-GHz radiosusing the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm air-quality** command.

Example:

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality
```

Step 4 Configure the air quality threshold value of CleanAir alarm in the 2.4-GHz , 5-GHz, or 6-GHz radios using the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm air-quality threshold** *threshold-value* command.

Example:

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality threshold 25
```

The valid range is between 1 and 100.

Step 5 Configure the continuous transmitter as the interference device CleanAir alarm in the 2.4-GHz , 5-GHz, or 6-GHz radios using the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm device cont-tx** command.

Example:

```
Device(config)# ap dot11 24ghz cleanair alarm device cont-tx
```

Step 6 Configure the air quality alarm on exceeding unclassified category severity using the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm unclassified** command.

Example:

```
Device(config)# ap dot11 24ghz cleanair alarm unclassified
```

Step 7 Configure the air quality alarm on exceeding unclassified category severity threshold using the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair alarm unclassified threshold** *threshold-value*command.

Example:

```
Device(config)# ap dot11 24ghz cleanair alarm unclassified threshold 15
```

The valid range is between 1 and 100.

Step 8 Configure continuous transmitter as the CleanAir interference device type using the **ap dot11** {**24ghz** | **5ghz** | **6ghz**} **cleanair device cont-tx** command.

Example:

```
Device(config)# ap dot11 24ghz cleanair device cont-tx
```

CleanAir Pro scan features are active, with alarms configured according to your settings.

Monitor CleanAir Pro statistics (GUI)

Review CleanAir Pro statistics for air quality, interference, and radio channels across your wireless network.

This task helps you assess wireless spectrum health, identify interference sources, and check air quality metrics for monitored access points.

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **CleanAir Statistics**.
The **CleanAir Statistics** window is displayed.

Step 2 Click the **2.4 GHz Band**, **5 GHz Band**, or **6 GHz Band** tab.
The **CleanAir Interference Devices** window is selected by default. You can monitor and detect the cluster IDs, the interferer type, severity, the affected channels, and so on, for the listed APs.

Step 3 Click the listed devices under the **CleanAir Interference Devices** tab to view the **CleanAir Interference Charts** that displays the **AQ Graph** and the **Interference Power**.

Step 4 Click the **Air Quality** tab to monitor the channel, the average and minimum AQ, number of interferers, the time at which the interference was detected, and the spectrum AP type.

Step 5 Click the **Worst Air Quality Report** tab to view the AQ report, with details of the AP that reported the worst AQ, the radio channel number with the worst-reported air quality, the minimum and the average AQ index, the interference device count, and the spectrum AP type.

You have reviewed CleanAir Pro statistics to monitor air quality, interference, and device-specific spectrum data across selected wireless bands.

Verify CleanAir Pro scanning details

To view the CleanAir Air Quality (AQ) data, run this command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair air-quality summary
```

To view the CleanAir Air Quality (AQ) worst data, run this command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair air-quality worst
```

To view the CleanAir device cluster information, run this command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair device cluster cluster-id
```

To view the CleanAir interferers of a device type, run this command:

```
Device# show ap dot11 {24ghz | 5ghz | 6ghz} cleanair device type
```

To view the CleanAir configuration for a specific AP, run this command:

```
Device# show ap name ap-name dot11 {24ghz | 5ghz | 6ghz} cleanair air-quality
Device# show ap name ap-name dot11 {24ghz | 5ghz | 6ghz} cleanair device
```

To view the continuous transmitter as the CleanAir interference device type, run this command:

```
Device# show ap dot11 6ghz cleanair device type cont-tx
```

Verify CleanAir parameters

You can verify CleanAir parameters using these commands:

Table 4: Commands for verifying CleanAir

Command Name	Description
show ap dot11 24ghz cleanair device type all	Displays all the CleanAir interferers for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type ble-beacon	Displays all the Bluetooth Low Energy (BLE) beacons for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type bt-discovery	Displays CleanAir interferers of type BT Discovery for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type bt-link	Displays CleanAir interferers of type BT Link for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type canopy	Displays CleanAir interferers of type Canopy for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type cont-tx	Displays CleanAir interferers of type Continuous transmitter for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type dect-like	Displays CleanAir interferers of type Digital Enhanced Cordless Telecommunications (DECT) Like for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type fh	Displays CleanAir interferers of type 802.11FH for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type inv	Displays CleanAir interferers of type Wi-Fi Inverted for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type jammer	Displays CleanAir interferers of type Jammer for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type mw-oven	Displays CleanAir interferers of type MW Oven for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type nonstd	Displays CleanAir interferers of type Wi-Fi inverted channel for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type superag	Displays CleanAir interferers of type SuperAG for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type tdd-tx	Displays CleanAir interferers of type TDD Transmit for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type video	Displays CleanAir interferers of type Video Camera for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type wimax-fixed	Displays CleanAir interferers of type WiMax Fixed for the 2.4-GHz band.

Configure air quality traps (CLI)

Set up SNMP traps so that you receive alerts when the air quality falls below a specified threshold.

Procedure

Step 1 Configure the trap **ciscoLwappSiAqLowSeverityHigh** to generate an alert when air quality goes beyond a given threshold.

On the controller GUI, navigate to **Configuration** > **Radio Configurations** > **Configuration** > **CleanAir** > **Trap configuration**.

The trap **ciscoLwappSiAqLowSeverityHigh** (OID: 1.3.6.1.4.1.9.9.513.1.6.1.0.5) is used to monitor air quality and generate alerts when the air quality index exceeds a specified threshold.

Step 2 Send the trap from the controller CLI. From the global configuration mode, enable SNMP traps for air quality index (AQI).

Example:

```
Device# snmp-server enable traps wireless SI
```

SNMP traps are configured, and the device sends alerts when air quality index thresholds are exceeded.

What to do next

Monitor SNMP alerts to ensure notifications are received as expected.

Monitor with CleanAir device clusters

A CleanAir device cluster is a spectrum monitoring feature that

- merges detections of the same interference device from multiple sensors into a single cluster,
- assigns and maintains a unique cluster ID for each device, and
- preserves device history by keeping cluster IDs active during temporary lapses in detection.

How CleanAir handles interference device monitoring

Some devices conserve power by limiting the transmit time until actually needed, which results in the spectrum sensor to stop detecting the device temporarily. This device is then correctly marked as down and removed from the spectrum database.

In cases when all the interferer detections for a specific device are reported, the cluster ID is kept alive for an extended period of time to prevent possible device-detection bouncing. If the same device is detected again, it is merged with the original cluster ID and the device-detection history is preserved.

Note You can configure Cisco CleanAir only on CleanAir-enabled APs.

: Bluetooth headset power management

Some Bluetooth headsets operate on battery power and employ methods to reduce power consumption, such as turning off the transmitter when not needed. Such devices can appear to come and go from the classification. To manage these devices, CleanAir keeps the cluster IDs for longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Configuration examples for CleanAir

This example shows how to enable CleanAir on the 2.4-GHz band and an AP operating in the channel:

```
Device#configure terminal
Device(config)#ap dot11 24ghz cleanair
Device(config)#exit
Device#ap name TAP1 dot11 24ghz cleanair
Device#end
```

This example shows how to enable an EDRRM CleanAir event in the 2.4-GHz band and configure high sensitivity to non-Wi–Fi interference:

```
Device#configure terminal
Device(config)#ap dot11 24ghz rrm channel cleanair-event
Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Device(config)#end
```

This example shows how to enable an AP in the monitor mode:

```
Device#ap name <ap-name> mode monitor
```

CleanAir FAQs

Q. Multiple access points detect the same interference device. However, the device shows them as separate clusters or different suspected devices clustered together. Why does this happen?

A. Access points must be RF neighbors for the device to consider merging the devices that are detected by these access points. An access point takes time to establish neighbor relationships. A few minutes after the device reboots or after there is a change in the RF group, and similar events, clustering will not be very accurate.

Q. How do I view neighbor access points?

A. To view neighbor access points, use the **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**} command.

This example shows how to display the neighbor access points:

```
Device#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                        :  -12 dBm on   1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0                        :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0                        :  -26 dBm on  11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0                        :  -24 dBm on   6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0                        :  -14 dBm on  11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0                        :  -31 dBm on   6 (10.10.0.5)
```

```
  AP 0CD9.96BA.5600 slot 0                              :  -44 dBm on   6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0                              :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. What are the AP debug commands available for CleanAir?

A. The AP debug commands for CleanAir are:

- **debug cleanair** {**bringup** | **event** | **logdebug** | **low** | **major** | **nsi** | **offchan**}
- **debug rrm** {**neighbor** | **off-channel** | **reports**}