Cisco CleanAir

- Prerequisites for CleanAir, on page 1
- Restrictions for CleanAir, on page 2
- Information About Cisco CleanAir, on page 2
- How to Configure CleanAir, on page 7
- Configuring Cisco CleanAir using the Controller GUI, on page 15
- Configuring Cisco Spectrum Expert, on page 15
- Verifying CleanAir Parameters, on page 17
- Configuration Examples for CleanAir, on page 19
- CleanAir FAQs, on page 20
- Additional References, on page 22

Prerequisites for CleanAir

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

Only Cisco CleanAir-enabled access points using the following 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.
- Monitor—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

  The following options are available:

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

  Note The access point does not participate in AQ HeatMap in Prime Infrastructure.

- SE-Connect—This mode enables a user to connect a Spectrum Expert application running on an external Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point in order to display and

analyze detailed spectrum data. The Spectrum Expert application connects directly to the access point, bypassing the device. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the device. All CleanAir system functionality is suspended while the AP is in this mode, and no clients are served. This mode is intended for remote troubleshooting only. Up to three active Spectrum Expert connections are possible.

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 access point list. IDR clustering depends on the device's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- Monitor Mode access point in slot 2 operates at 2.4 GHz only.
- We recommend a ratio of 1 monitor-mode access point for every 5 local-mode access points; this can vary based on the network design and expert guidance for best coverage.
- Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.
- CleanAir is not supported wherein the channel width is 160 MHz.

Information About Cisco CleanAir

Cisco CleanAir is a solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of a shared spectrum (both native devices and foreign interferers). It also enables the network to act upon this information. For example, you can manually remove the interfering device, or the system can automatically change the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points, Cisco Wireless LAN Controllers, and Cisco Prime Infrastructure. These access points collect information about all the devices that operate in the industrial, scientific, and medical (ISM) bands, identify and evaluate the information as a potential interference source, and forward it to the controller. The controller controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure or a Cisco mobility services engine (MSE) upon request.

Any networking configurations can be performed only on the mobility controller, configurations cannot be performed in the MA mode. However, any radio level CleanAir configurations can be done using mobility anchor.

For every device operating in the unlicensed band, Cisco CleanAir provides information about what it is, where it is, how it is impacting your wireless network, and what actions you or your network should take. It simplifies RF.

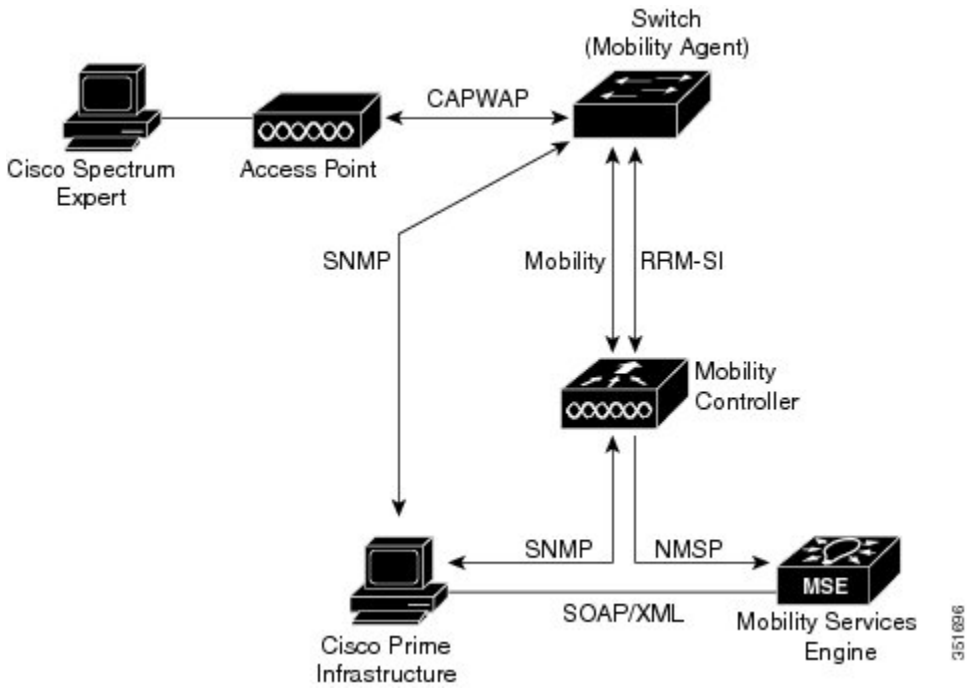
Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices, such as microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations.

Some of the most advanced WLAN services, such as voice-over-wireless and IEEE 802.11n radio communications, might be significantly impaired by the interference caused by other legal users of the ISM bands. The integration of Cisco CleanAir functionality addresses this problem of RF interference.

Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and device. Cisco Prime Infrastructure (PI), Mobility Services Engine (MSE) and Cisco Spectrum Expert are optional system components. Cisco PI and MSE provide user interfaces for advanced spectrum capabilities such as historic charts, tracking interference devices, location services and impact analysis.

Figure 1: Cisco CleanAir Solution



An access point equipped with Cisco CleanAir technology collects information about non-Wi-Fi interference sources, processes it, and forwards it to the MA. The access point sends the Air Quality Report (AQR) and Interference Device Report (IDR) to the controller.

The mobility controller (MC) controls and configures CleanAir-capable access points, and collects and processes spectrum data, and provides it to the PI and/or the MSE. The MC provides local user interfaces (GUI and CLI) to configure basic CleanAir features and services and display current spectrum information. The MC also detects, merges, and mitigates interference devices using RRM TPC and DCM. For details, see Interference Device Merging.

Cisco PI provides advanced user interfaces for CleanAir that include feature enabling and configuration, consolidated display information, historic AQ records and reporting engines. PI also shows charts of interference devices, AQ trends, and alerts.

Cisco MSE is required for location and historic tracking of interference devices, and provides coordination and consolidation of interference reports across multiple controllers. MSE also provides adaptive Wireless Intrusion Prevention System (WIPS) service that provides comprehensive over-the-air threat detection, location and mitigation. MSE also merges all the interference data.

To obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer, you can configure a Cisco CleanAir-enabled access point to connect directly to a Microsoft Windows XP or Vista PC running the Cisco Spectrum Expert application.

The device performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (CLI, and SNMP) for configuring Cisco CleanAir features and retrieving data.
- Displays spectrum data.
- Collects and processes AQRs from the access point and stores them in the air quality database. AQRs contain information about the total interference from all the identified sources represented by the Air Quality Index (AQI) and the summary for the most severe interference categories. The CleanAir system can also include unclassified interference information under per-interference type reports that enable you to take action in scenarios where interference because of unclassified interfering devices is more.
- Collects and processes IDRs from the access point and stores them in the interference device database.
- Forwards spectrum data to Prime Infrastructure and the MSE.

Note In Cisco Catalyst 9800 Series Wireless Controller, when Cisco CleanAir is disabled, both CleanAir and Air Quality reporting are disabled. In spite of this, Air Quality is still populated.

Cisco CleanAir-Related Terms

Table 1: CleanAir-Related Terms

Term	Decription
AQI	Air Quality Index. The AQI is an indicator of air quality, based on the air pollutants. An AQI of 0 is bad and an AQI > 85 is good.
AQR	Air Quality Report. AQRs contain information about total interference from all the identified sources represented by AQI and the summary of the most severe interference categories. AQRs are sent every 15 minutes to the Mobility Controller and every 30 seconds in the Rapid mode.
DC	Duty Cycle. Percentage of time that the channel is utilized by a device.
EDRRM	Event-Driven RRM. EDRRM allows an access point in distress to bypass normal RRM intervals and immediately change channels.
IDR	Interference Device Reports that an access point sends to the controller.
ISI	Interference Severity Index. The ISI is an indicator of the severity of the interference.
MA	Mobility Agent. An MA is either an access switch that has a wireless module running on it or an MC with an internal MA running on it. An MA is the wireless component that maintains client mobility state machine for a mobile client that is connected to an access point to the device that the MA is running on.
MC	Mobility Controller. An MC provides mobility management services for inter-peer group roaming events. The MC provides a central point of contact for management and sends the configuration to all the mobility agents under its sub-domain of their mobility configuration, peer group membership and list of members.

Term	Decription
RSSI	Received Signal Strength Indicator. RSSI is a measurement of the power present in a received radio signal. It is the power at which an access point sees the interferer device.

Interference Types that Cisco CleanAir can Detect

Cisco CleanAir can detect interference, report on the location and severity of the interference, and recommend different mitigation strategies. Two such mitigation strategies are persistent device avoidance and spectrum event-driven RRM.

Wi-Fi chip-based RF management systems share these characteristics:

- Any RF energy that cannot be identified as a Wi-Fi signal is reported as noise.
- Noise measurements that are used to assign a channel plan tend to be averaged over a period of time to avoid instability or rapid changes that can be disruptive to certain client devices.
- Averaging measurements reduces the resolution of the measurement. As such, a signal that disrupts clients might not look like it needs to be mitigated after averaging.
- All RF management systems available today are reactive in nature.

Cisco CleanAir is different and can positively identify not only the source of the noise but also its location and potential impact to a WLAN. Having this information allows you to consider the noise within the context of the network and make intelligent and, where possible, proactive decisions. For CleanAir, two types of interference events are common:

- Persistent interference
- Spontaneous interference

Persistent interference events are created by devices that are stationary in nature and have intermittent but largely repeatable patterns of interference. For example, consider the case of a microwave oven located in a break room. Such a device might be active for only 1 or 2 minutes at a time. When operating, however, it can be disruptive to the performance of the wireless network and associated clients. Using Cisco CleanAir, you can positively identify the device as a microwave oven rather than indiscriminate noise. You can also determine exactly which part of the band is affected by the device, and because you can locate it, you can understand which access points are most severely affected. You can then use this information to direct RRM in selecting a channel plan that avoids this source of interference for the access points within its range. Because this interference is not active for a large portion of the day, existing RF management applications might attempt to again change the channels of the affected access points. Persistent device avoidance is unique, however, in that it remains in effect as long as the source of interference is periodically detected to refresh the persistent status. The Cisco CleanAir system knows that the microwave oven exists and includes it in all future planning. If you move either the microwave oven or the surrounding access points, the algorithm updates RRM automatically.

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

Note All the APs using qualcomm atheros chipset sends air-quality as 100 percent even if the radios detect interference.

Spontaneous interference is interference that appears suddenly on a network, perhaps jamming a channel or a range of channels completely. The Cisco CleanAir spectrum event-driven RRM feature allows you to set a threshold for air quality (AQ) which, if exceeded, triggers an immediate channel change for the affected access point. Most RF management systems can avoid interference, but this information takes time to propagate through the system. Cisco CleanAir relies on AQ measurements to continuously evaluate the spectrum and can trigger a move within 30 seconds. For example, if an access point detects interference from a video camera, it can recover by changing channels within 30 seconds of the camera becoming active. Cisco CleanAir also identifies and locates the source of interference so that more permanent mitigation of the device can be performed at a later time.

In the case of Bluetooth devices, Cisco CleanAir-enabled access points can detect and report interference only if the devices are actively transmitting. Bluetooth devices have extensive power-save modes. For example, interference can be detected when data or voice is being streamed between the connected devices.

Interference Device Merging

The Interference Devices (ID) messages are processed on a Mobility Controller (MC). The Mobility Anchor (MA) forwards the ID messages from APs and hence they are processed on the MC. The MC has visibility of the neighbor information across APs connected to different MAs.

ID merging logic requires AP neighbor information. Neighbor information is obtained from the RRM module. This api only gives neighbor information to the APs directly connected to MC.

Currently the AP neighbor list on MA is synced to MC once every 3 minutes; hence the AP neighbor list obtained by this api could be at most 3 mins old. This delay results in delay in merging of Devices as they are discovered. The subsequent periodic merge will pick up the updated neighbor information and merge is performed

Persistent Devices

Some interference devices such as outdoor bridges and Microwave Ovens only transmit when needed. These devices can cause significant interference to the local WLAN due to short duration and periodic operation remain largely undetected by normal RF management metrics. With CleanAir the RRM DCA algorithm can detect, measure, register and remember the impact and adjust the DCA algorithm. This minimizes the use of channels affected by the persistent devices in the channel plan local to the interference source. Cisco CleanAir detects and stores the persistent device information in the device and this information is used to mitigate interfering channels.

Persistent Devices Detection

CleanAir-capable Monitor Mode access point collects information about persistent devices on all configured channels and store the information in controller. Local/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.

EDRRM and AQR Update Mode

EDRRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AQ and reports the AQ every 15 minutes. AQ only reports classified interference devices. The key benefit of EDRRM is very fast action time. 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 access point. You must remove the access point from the channel. EDRRM is not enabled by default, you must first enable CleanAir and then enable EDRRM.

AQRs are only available on the MC. The mode configuration and timers are held in Radio Control Block (RCB) on MA (for APs connected to MA). There is no change to the current API available for EMS/NMS. No change is required for directly connected APs as RCB (spectrum config and timers) is available locally. For remote APs (APs connected to MA), three new control messages are added. These three messages are for enable, restart timer and disable rapid update mode for a given AP MAC address and slot.

CleanAir High Availability

CleanAir configuration (network and radio) is stateful during the switchover. On the MC, Embedded Instrumentation Core (EICORE) provides the sync on network configurations across active and standby nodes. The radio configurations are synced using the HA Infrastructure. The CleanAir configurations on MA are pulled from the MC upon joining. The network configuration is not stored in the EICORE on MA, hence it is synced using HA Infrastructure.

CleanAir Data (AQ and IDR) reports are not stateful, that is, the standby and active nodes are not synced. On switchover, the APs send the reports to the current active slot. The RRM Client (HA Infra Client) is used for CleanAir HA sync.

How to Configure CleanAir

Enabling CleanAir for the 2.4-GHz Band (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz cleanair**
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 24ghz cleanair**
	Example:
	`Device(config)#ap dot11 24ghz cleanair`
	`Device(config)#no ap dot11 24ghz cleanair`
		Enables the CleanAir feature on the 802.11b network. Run the **no** form of this command to disable CleanAir on the 802.11b network.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value*
3. **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** }
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Device(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50`	Configures the alarm for the threshold value for air-quality for all the 2.4-GHz devices. Add the **no** form of this command to disable the alarm.
Step 3	**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** }	Configures the alarm for the 2.4-GHz devices. Add the **no** form command to disable the alarm. • **bt-discovery**—Bluetooth Discovery.

	Command or Action	Purpose
	Example: `Device(config)#ap dot11 24ghz cleanair alarm device canopy`	• **bt-link**—Bluetooth Link. • **canopy**—Canopy devices. • **cont-tx**—Continuous Transmitter. • **dect-like**—Digital Enhanced Cordless Communication (DECT)-like phone. • **fh**—802.11 frequency hopping devices. • **inv**—Devices using spectrally inverted WiFi signals. • **jammer**—Jammer. • **mw-oven**—Microwave oven. • **nonstd**—Devices using non standard Wi-Fi channels. • **report**—Interference device reporting. • **superag**—802.11 SuperAG devices. • **tdd-tx**—TDD Transmitter. • **video**—Video cameras. • **wimax-fixed**—WiMax Fixed. • **wimax-mobile**—WiMax Mobile. • **xbox**—Xbox. • **zigbee**—802.15.4 devices.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Interference Reporting for a 2.4-GHz Device (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 24ghz cleanair 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** }
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 24ghz cleanair 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** }
	Example:
	`Device(config)# ap dot11 24ghz cleanair device bt-discovery`
	`Device(config)# ap dot11 24ghz cleanair device bt-link`
	`Device(config)# ap dot11 24ghz cleanair device canopy`
	`Device(config)# ap dot11 24ghz cleanair device cont-tx`
	`Device(config)# ap dot11 24ghz cleanair device dect-like`
	`Device(config)# ap dot11 24ghz cleanair device fh`
	`Device(config)# ap dot11 24ghz cleanair device inv`
	`Device(config)# ap dot11 24ghz cleanair device jammer`
	`Device(config)# ap dot11 24ghz cleanair device mw-oven`
	`Device(config)# ap dot11 24ghz cleanair device nonstd`
	`Device(config)# ap dot11 24ghz cleanair device report`
	`Device(config)# ap dot11 24ghz cleanair device superag`
	`Device(config)# ap dot11 24ghz cleanair device tdd-tx`
	`Device(config)# ap dot11 24ghz cleanair device video`
	`Device(config)# ap dot11 24ghz cleanair device wimax-fixed`
	`Device(config)# ap dot11 24ghz cleanair device`
		Configures the 2.4-GHz interference devices to report to the device. Run the **no** form of this command to disable the configuration.
		The following is a list of the keyword descriptions:
		• **bt-discovery**—Bluetooth discovery
		• **bt-link**—Bluetooth link
		• **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
		• **mw-oven**—Microwave oven
		• **nonstd**—Device using nonstandard Wi-Fi channels
		• **report**—no description
		• **superag**—802.11 SuperAG device
		• **tdd-tx**—TDD transmitter
		• **video**—Video camera
		• **wimax-fixed**—WiMax Fixed
		• **wimax-mobile**—WiMax Mobile
		• **xbox**—Xbox device
		• **zigbee**—802.15.4 device

	Command or Action	Purpose

	wimax-mobile
	
	`Device(config)# ap dot11 24ghz cleanair device xbox`
	
	`Device(config)# ap dot11 24ghz cleanair device zigbee`	

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 CleanAir for the 5-GHz Band (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz cleanair**
3. **end**

DETAILED STEPS

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

Step 2	**ap dot11 5ghz cleanair**
	Example:
	`Device(config)#ap dot11 5ghz cleanair`
	
	`Device(config)#no ap dot11 5ghz cleanair`
		Enables the CleanAir feature on a 802.11a network. Run the **no** form of this command to disable CleanAir on the 802.11a network.

Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value*
3. **ap dot11 5ghz cleanair alarm device**{**canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Device(config)#ap dot11 5ghz cleanair alarm air-quality threshold 50`	Configures the alarm for the threshold value for air-quality for all the 5-GHz devices. Add the **No** form of the command to disable the alarm.
Step 3	**ap dot11 5ghz cleanair alarm device**{**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **report** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**} **Example:** `Device(config)#ap dot11 5ghz cleanair alarm device`	Configures the alarm for the 5-GHz devices. Add the **no** form of the command to disable the alarm. • **canopy**—Canopy devices. • **cont-tx**—Continuous Transmitter. • **dect-like**—Digital Enhanced Cordless Communication (DECT) like phone. • **fh**—802.11 frequency hopping devices. • **inv**—Devices using spectrally inverted WiFi signals. • **jammer**—Jammer. • **nonstd**—Devices using non-standard WiFi channels. • **radar**—Radars. • **report**—Interference device reporting. • **superag**—802.11 SuperAG devices. • **tdd-tx**—TDD Transmitter. • **video**—Video cameras. • **wimax-fixed**—WiMax Fixed. • **wimax-mobile**—WiMax Mobile.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Interference Reporting for a 5-GHz Device (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11 5ghz cleanair device**{**canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile**}
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair device**{**canopy	cont-tx	dect-like	inv	jammer	nonstd	radar	report	superag	tdd-tx	video	wimax-fixed	wimax-mobile**} **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 radar` `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`	Configures a 5-GHz interference device to report to the device. Run the **no** form of this command to disable interference device reporting. The following 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 • **radar**—Radars • **report**—Interference device reporting • **superag**—802.11 SuperAG device • **tdd-tx**—TDD transmitter • **video**—Video camera • **wimax-fixed**—WiMax fixed • **wimax-mobile**—WiMax mobile

	Command or Action	Purpose
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring EDRRM for a CleanAir Event (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event**
3. **ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high | low | medium**}]
4. **end**

DETAILED STEPS

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

Step 2	**ap dot11** {**24ghz**	**5ghz**} **rrm channel cleanair-event**
		Example:
		`Device(config)#ap dot11 24ghz rrm channel cleanair-event`
		`Device(config)#no ap dot11 24ghz rrm channel cleanair-event`
			Enables EDRRM CleanAir event. Run the **no** form of this command to disable EDRRM.

Step 3	**ap dot11** {**24ghz**	**5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high	low	medium**}] **Example:** `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures the EDRRM sensitivity of the CleanAir event. The following is a list of the keyword descriptions: • **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.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Persistent Device Avoidance

SUMMARY STEPS

1. **configure terminal**
2. **ap dot11** {**24ghz** | **5ghz**} **rrm channel device**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz**	**5ghz**} **rrm channel device** **Example:** `Device(config)#ap dot11 24ghz rrm channel device`	Enables the persistent non Wi–Fi device avoidance in the 802.11 channel assignment. Add the **no** form of the command to disable the persistent device avoidance.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Cisco CleanAir using the Controller GUI

Configuring Cisco Spectrum Expert

Configuring Spectrum Expert (CLI)

Before you begin

- Spectrum Expert (Windows XP laptop client) and access point should be pingable, otherwise; it will not work.
- Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.
- The access point must be a TCP server listening on ports 37540 for 2.4-GHz and 37550 for 5-GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.
- You can view the NSI key from the device CLI by using the **show ap name** *ap_name* **config dot11** {**24ghz** | **5ghz**} command.

Step 1 To configure the access point for SE-Connect mode, enter this command:

ap name *ap_name* **mode se-connect**

Example:

```
Device#ap name Cisco_AP3500 mode se-connect
```

Step 2 When prompted to reboot the access point, enter **Y**.

Step 3 To view the NSI key for the access point, enter this command:

show ap name *ap_name* **config dot11** {**24ghz** | **5ghz**}

Example:

```
Device#show ap name Cisco_AP3500 config dot11 24ghz

<snippet>
CleanAir Management Information
    CleanAir Capable                          : Yes
    CleanAir Management Admin State           : Enabled
    CleanAir Management Operation State       : Up
    CleanAir NSI Key                          : 274F1F9B1A5206683FAF57D87BFFBC9B
    CleanAir Sensor State                     : Configured

<snippet>
```

What to do next

On the Windows PC, download Cisco Spectrum Expert:

- Access the Cisco Software Center from this URL: http://www.cisco.com/cisco/software/navigator.html
- Click **Product > Wireless > Cisco Spectrum Intelligence** > **Cisco Spectrum Expert** > **Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.1.11 executable (*.exe) file.
- Run the Spectrum Expert application on the PC.
- When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

  When an access point in SE-Connect mode joins a device, it sends a Spectrum Capabilities notification message, and the device responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the device for use in NSI authentication. The device generates one key per access point, which the access point stores until it is rebooted.

  Note You can establish up to three Spectrum Expert console connections per access point radio.

- Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.

- Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Verifying CleanAir Parameters

You can verify CleanAir parameters using the following commands:

Table 2: Commands for verifying CleanAir

Command Name	Description
show ap dot11 24ghz cleanair air-quality summary	Displays CleanAir AQ data for the 2.4-GHz band.
show ap dot11 24ghz cleanair air-quality worst	Displays CleanAir AQ worst data for the 2.4-GHz band.
show ap dot11 24ghz cleanair config	Displays CleanAir configuration for the 2.4-GHz band.
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 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 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 persistent	Displays CleanAir interferers of type Persistent for the 2.4-GHz band.

Command Name	Description
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.
show ap dot11 24ghz cleanair device type wimax-mobile	Displays CleanAir interferers of type WiMax Mobile for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type xbox	Displays CleanAir interferers of type Xbox for the 2.4-GHz band.
show ap dot11 24ghz cleanair device type zigbee	Displays CleanAir interferers of type Zigbee for the 2.4-GHz band.
show ap dot11 5ghz cleanair air-quality summary	Displays CleanAir AQ data for the 5-GHz band.
show ap dot11 5ghz cleanair air-quality worst	Displays CleanAir AQ worst data for the 5-GHz band.
show ap dot11 5ghz cleanair config	Displays CleanAir configuration for the 5-GHz band.
show ap dot11 5ghz cleanair device type all	Displays all the CleanAir interferers for the 5-GHz band.
show ap dot11 5ghz cleanair device type canopy	Displays CleanAir interferers of type Canopy for the 5-GHz band.
show ap dot11 5ghz cleanair device type cont-tx	Displays CleanAir interferers of type Continuous TX for the 5-GHz band.
show ap dot11 5ghz cleanair device type dect-like	Displays CleanAir interferers of type DECT Like for the 5-GHz band.
show ap dot11 5ghz cleanair device type inv	Displays CleanAir interferers of type Wi-Fi Inverted for the 5-GHz band.
show ap dot11 5ghz cleanair device type jammer	Displays CleanAir interferers of type Jammer for the 5-GHz band.
show ap dot11 5ghz cleanair device type nonstd	Displays CleanAir interferers of type Wi-Fi inverted channel for the 5-GHz band.
show ap dot11 5ghz cleanair device type persistent	Displays CleanAir interferers of type Persistent for the 5-GHz band.
show ap dot11 5ghz cleanair device type superag	Displays CleanAir interferers of type SuperAG for the 5-GHz band.

Command Name	Description
show ap dot11 5ghz cleanair device type tdd-tx	Displays CleanAir interferers of type TDD Transmit for the 5-GHz band.
show ap dot11 5ghz cleanair device type video	Displays CleanAir interferers of type Video Camera for the 5-GHz band.
show ap dot11 5ghz cleanair device type wimax-fixed	Displays CleanAir interferers of type WiMax Fixed for the 5-GHz band.
show ap dot11 5ghz cleanair device type wimax-mobile	Displays CleanAir interferers of type WiMax Mobile for the 5-GHz band.

Monitoring Interference Devices

When a CleanAir-enabled access point detects interference devices, detections of the same device from multiple sensors are merged together to create clusters. Each cluster is given a unique ID. 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. Such a device is correctly 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.

For example, some bluetooth headsets operate on battery power. These devices employ methods to reduce power consumption, such as turning off the transmitter when not actually 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 access point 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
```

Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices: Example

This example shows how to configure a CleanAir Alarm for 2.4-GHz Air-Quality threshold of 50 dBm and an Xbox device:

```
Device#configure terminal
Device(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50
Device(config)#ap dot11 24ghz cleanair alarm device xbox
Device(config)#end
```

Configuring Interference Reporting for 5-GHz Devices: Example

This example shows how to configure interference reporting for 5-GHz devices:

```
Device#configure terminal
Device(config)#ap dot11 5ghz cleanair alarm device xbox
Device(config)#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
```

Configuring Persistent Device Avoidance: Example

This example shows how to enable persistent non Wi–Fi device avoidance in the 2.4-GHz band:

```
Device#configure terminal
Device(config)#ap dot11 24ghz rrm channel device
Device(config)#end
```

Configuring an Access Point for SE-Connect Mode: Example

This example shows how to configure an access point in the SE-Connect mode:

```
Device#ap name Cisco_AP3500 mode se-connect
```

CleanAir FAQs

Q. How do I check if my MC is up?

A. To check if the MC is up, use the command: **show wireless mobility summary**.

This example shows how to display the mobility summary:

```
Device#show wireless mobility summary

Mobility Controller Summary:
Mobility Role                                 : Mobility Controller
Mobility Protocol Port                        : 16666
Mobility Group Name                           : MG-AK
Mobility Oracle                               : Disabled
Mobility Oracle IP Address                    : 0.0.0.0
DTLS Mode                                     : Enabled
Mobility Domain ID for 802.11r                : 0x39b2
Mobility Keepalive Interval                   : 10
Mobility Keepalive Count                      : 3
Mobility Control Message DSCP Value           : 48
Mobility Domain Member Count                  : 2
Link Status is Control Link Status : Data Link Status
Controllers configured in the Mobility Domain:
IP              Public IP        Group Name       Multicast IP     Link Status
------------------------------------------------------------------------------
```

```
9.6.136.10       -                MG-AK           0.0.0.0          UP   : UP
```

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. Can I merge two monitor-mode access points using a device?

A. No, you cannot merge two monitor-mode access points using a device. You can merge the monitor mode access points only using MSE.

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 debug commands available for CleanAir?

A. The debug commands for CleanAir are:

- **debug cleanair** {**all** | **error** | **event** | **internal-event** | **nmsp** | **packet**}
- **debug rrm** {**all** | **channel** | **detail** | **error** | **group** | **ha** | **manager** | **message** | **packet** | **power** | **prealarm** | **profile** | **radar** | **rf-change** | **scale** | **spectrum**}

Q. Why are CleanAir Alarms not generated for interferer devices?

A. Verify that the access points are CleanAir-capable and CleanAir is enabled both on the access point and the device.

Q. Can the Cisco Catalyst 3850 and 3650 Series Switches function as a Mobility Agent (MA)?

A. Yes, the Cisco Catalyst 3850 and 3650 Series Switches can function as an MA.

Q. Are CleanAir configurations available on the MA?

A. From Release 3.3 SE, CleanAir configurations are available on the MA. You can use the following two CleanAir commands on the MA:

- **show ap dot11 5ghz cleanair config**

- **show ap dot11 24ghz cleanair config**

Additional References

Related Documents

Related Topic	Document Title
CleanAir commands and their details	*CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)*
High Availability configurations	*High Availability Configuration Guide, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*
High Availability commands and their details	*High Availability Command Reference, Cisco IOS XE Release 3SE (Cisco 5700 Series Wireless Controllers)*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support