Configuring Cisco CleanAir

- Finding Feature Information, on page 1
- Prerequisites for CleanAir, on page 1
- Restrictions for CleanAir, on page 2
- Information About CleanAir, on page 3
- How to Configure CleanAir, on page 8
- Configuring Cisco CleanAir using the Controller GUI, on page 16
- Configuring Cisco Spectrum Expert, on page 18
- Monitoring CleanAir Parameters, on page 21
- Configuration Examples for Configuring CleanAir, on page 25
- CleanAir FAQs, on page 26
- Additional References, on page 28

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

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 channel 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 switch. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the switch. 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.
- Only Cisco Catalyst 3850 and Switches can function as a Mobility Agent.
- Cisco Catalyst 3850 Switches and Cisco 5760 Wireless LAN Controllers can function as Mobility Controllers.

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 8
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 8
Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Enabling CleanAir for 5-GHz Band, on page 11
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 12
Configuring Interference Reporting for 5-GHz devices, on page 13

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 switch's ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.
- SE-connect is an access point mode similar to local mode or monitor mode. The access point provides spectrum information to Spectrum Expert only for the current channel(s). The spectrum data is available for the current active channel(s) and the common monitored channel list is available. The access point continues to send AQ (Air Quality) and IDR (Interference Device Reports) reports to the switch and perform normal activities according to the current mode. Sniffer and rogue detections access point modes are incompatible with all types of CleanAir spectrum monitoring.
- Local Mode access point—Serves WLAN clients with the time slicing off-channel scanning and listens for 50 ms on each channel, and scans configurable feature scanning for all/country/DCA channels.
- Monitor Mode access point—Does not serve WLAN clients and are dedicated to scanning only. These access points listen for 1.2 s on each channel, and scans all channels.

- Cisco recommends a ratio of 1 monitor mode access point for every 5 local mode access points, this may also 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.

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 8
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 8
Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Enabling CleanAir for 5-GHz Band, on page 11
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 12
Configuring Interference Reporting for 5-GHz devices, on page 13

Information About CleanAir

Cisco CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. All of the users of the shared spectrum can be seen (both native devices and foreign interferers). It also enables the network to act upon this information. For example, the interfering device can be manually removed or the system can automatically change the channel away from the interference.

A Cisco CleanAir system consists of CleanAir-enabled access points, wireless controller modules, mobility controllers, mobility anchors and next generation switches. The access points join the mobility controller directly or through the mobility anchor. They collect information about all 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 switch. The switch controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure (PI) 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 tells what it is, where it is, how it is impacting the wireless network, and what actions should be taken. It simplifies RF.

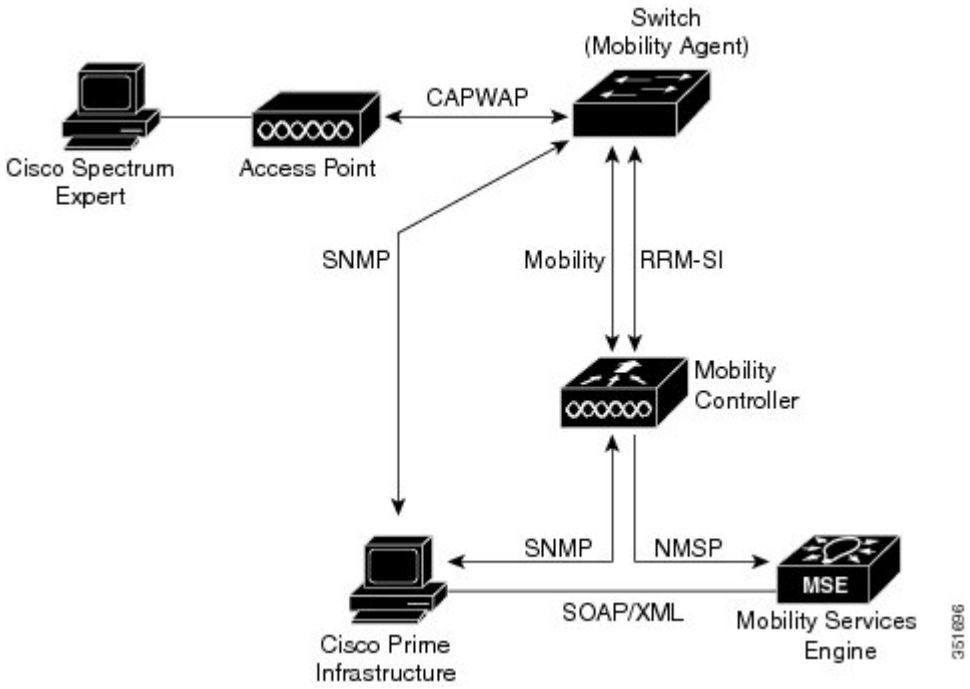
Wireless LAN systems operate in unlicensed 2.4-GHz and 5-GHz ISM bands. Many devices like microwave ovens, cordless phones, and Bluetooth devices also operate in these bands and can negatively affect the Wi-Fi operations.

Some of the most advanced WLAN services, such as voice over wireless and IEEE 802.11n radio communications, could 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 radio frequency (RF) interference.

Cisco CleanAir Components

The basic Cisco CleanAir architecture consists of Cisco CleanAir-enabled APs and switch. 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 AQR and IDR reports to the controller.

The mobility controller (MC) controls and configures CleanAir-capable access points, 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 does detection, merging and mitigation of interference devices using RRM TPC and DCM. For details on Interference Device Merging, see Interference Device Merging, on page 6.

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 switch performs the following tasks in a Cisco CleanAir system:

- Configures Cisco CleanAir capabilities on the access point.
- Provides interfaces (GUI, 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 contains information about the total interference from all identified sources represented by Air Quality Index (AQI) and summary for the most severe interference categories. The CleanAir system can also

include unclassified interference information under per interference type reports which enable you to take action in cases where the interference due to unclassified interfering devices is frequent.

- Collects and processes Interference Device Reports (IDRs) from the access point and stores them in the interference device database.
- Forwards spectrum data to Prime Infrastructure and the MSE.

Terms Used in Cisco CleanAir

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 the total interference from all identified sources represented by AQI and 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	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 the 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.
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. New

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.

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) that, 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 switch 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.

Related Topics

Configuring EDRRM for CleanAir-Events, on page 15

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 Infrastructre. 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 2.4-GHz Band

SUMMARY STEPS

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

DETAILED STEPS

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

Step 2	**ap dot11 24ghz cleanair**
	Example:
	`Switch(config)#ap dot11 24ghz cleanair`
	`Switch(config)#no ap dot11 24ghz cleanair`
		Enables the CleanAir feature on 802.11b network. Add **no** in the command to disable CleanAir on the 802.11b network.

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

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions for CleanAir, on page 2
CleanAir FAQs, on page 26

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:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Switch(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** } **Example:** `Switch(config)#ap dot11 24ghz cleanair alarm device canopy`	Configures the alarm for the 2.4-GHz devices. Add the **no** form command to disable the alarm. • **bt-discovery**—Bluetooth Discovery. • **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.

	Command or Action	Purpose
		• **zigbee**—802.15.4 devices.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions for CleanAir, on page 2
CleanAir FAQs, on page 26

Configuring Interference Reporting for 2.4-GHz Devices

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:** `Switch# 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:** `Switch(config)# ap dot11 24ghz cleanair device bt-discovery` `Switch(config)# ap dot11 24ghz cleanair device bt-link` `Switch(config)# ap dot11 24ghz cleanair device canopy` `Switch(config)# ap dot11 24ghz cleanair device cont-tx` `Switch(config)# ap dot11 24ghz cleanair device dect-like`	Configures the 2.4 GHz interference devices to report to the switch. Use the **no** form of this command to disable the configuration. • **bt-discovery**—Bluetooth Discovery • **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

	Command or Action	Purpose

	`Switch(config)# ap dot11 24ghz cleanair device fh`
	`Switch(config)# ap dot11 24ghz cleanair device inv`
	`Switch(config)# ap dot11 24ghz cleanair device jammer`
	`Switch(config)# ap dot11 24ghz cleanair device mw-oven`
	`Switch(config)# ap dot11 24ghz cleanair device nonstd`
	`Switch(config)# ap dot11 24ghz cleanair device report`
	`Switch(config)# ap dot11 24ghz cleanair device superag`
	`Switch(config)# ap dot11 24ghz cleanair device tdd-tx`
	`Switch(config)# ap dot11 24ghz cleanair device video`
	`Switch(config)# ap dot11 24ghz cleanair device wimax-fixed`
	`Switch(config)# ap dot11 24ghz cleanair device wimax-mobile`
	`Switch(config)# ap dot11 24ghz cleanair device xbox`
	`Switch(config)# ap dot11 24ghz cleanair device zigbee`
		• **nonstd**- Devices using non-standard WiFi channels
		• **report**- no description
		• **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 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions for CleanAir, on page 2
CleanAir FAQs, on page 26
Monitoring the Interference Devices (GUI), on page 24

Enabling CleanAir for 5-GHz Band

SUMMARY STEPS

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

DETAILED STEPS

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

Step 2	**ap dot11 5ghz cleanair**
	Example:
	`Switch(config)#ap dot11 5ghz cleanair`
	`Switch(config)#no ap dot11 5ghz cleanair`
		Enables the CleanAir feature on 802.11a network. Add **no** in the command to disable CleanAir on the 802.11a network.

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

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions for CleanAir, on page 2
CleanAir FAQs, on page 26

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:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11 5ghz cleanair alarm air-quality threshold** *threshold_value* **Example:** `Switch(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.

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

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions for CleanAir, on page 2
CleanAir FAQs, on page 26

Configuring Interference Reporting for 5-GHz devices

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:** `Switch# 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:
	`Switch(config)#ap dot11 5ghz cleanair device canopy`
	`Switch(config)#ap dot11 5ghz cleanair device cont-tx`
	`Switch(config)#ap dot11 5ghz cleanair device dect-like`
	`Switch(config)#ap dot11 5ghz cleanair device inv`
	`Switch(config)#ap dot11 5ghz cleanair device jammer`
	`Switch(config)#ap dot11 5ghz cleanair device nonstd`
	`Switch(config)#ap dot11 5ghz cleanair device radar`
	`Switch(config)#ap dot11 5ghz cleanair device report`
	`Switch(config)#ap dot11 5ghz cleanair device superag`
	`Switch(config)#ap dot11 5ghz cleanair device tdd-tx`
	`Switch(config)#ap dot11 5ghz cleanair device video`
	`Switch(config)#ap dot11 5ghz cleanair device wimax-fixed`
	`Switch(config)#ap dot11 5ghz cleanair device wimax-mobile`
		Configures the 5-GHz interference devices to report to the switch. Add the **no** form of the command to disable interference device reporting.
		• **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 3	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

Prerequisites for CleanAir, on page 1
Restrictions for CleanAir, on page 2
CleanAir FAQs, on page 26
Monitoring the Interference Devices (GUI), on page 24

Configuring EDRRM for CleanAir-Events

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:** `Switch# configure terminal`	Enters global configuration mode.

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

Step 3	**ap dot11** {**24ghz**	**5ghz**} **rrm channel cleanair-event** [**sensitivity** {**high**	**low**	**medium**}] **Example:** `Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	Configures the EDRRM sensitivity of cleanair-event. • **High**—Specifies the most sensitivity to non Wi–Fi interference as indicated by the air quality (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:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

EDRRM and AQR Update Mode, on page 7

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:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**ap dot11** {**24ghz**	**5ghz**} **rrm channel device** **Example:** `Switch(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:** `Switch(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 CleanAir on the Cisco Wireless LAN Controller (GUI)

Step 1 Choose **Configuration > Wireless** > **802.11a/n or 802.11b/g/n > CleanAir** to open the **802.11a (or 802.11b) > CleanAir** page.

Step 2 Select the **CleanAir** check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or unselect it to prevent the switch from detecting spectrum interference. By default, the Cisco CleanAir is disabled.

Step 3 Select the **Report Interferers** check box to enable the Cisco CleanAir system to report any detected sources of interference, or unselect it to prevent the switch from reporting interferers. The default value is selected.

Note Device Security alarms, Event Driven RRM, and the Persistence Device Avoidance algorithm do not work if Report Interferers are disabled.

Step 4 Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables you to propagate information about persistent devices to the neighboring access points connected to the same switch. Persistent interferers are present at the location and interfere with the WLAN operations even if they are not detectable at all times.

Step 5 Ensure that any sources of interference that need to be detected and reported by the Cisco CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferences to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are detected. The sources of interference that you can choose depend on the type of radio, 802.11a/n/ac or 802.11b/g/n, and are as follows:

- **802.11 FH**—A 802.11 FH device

- **802.15.4**—A 802.15.4 or ZigBee device
- **Continuous Transmitter**—A continuous transmitter
- **Bluetooth Discovery**—A Bluetooth device
- **DECT-like Phone**—A digital enhanced cordless communication (DECT)-compatible phone
- **Microsoft**—A Microsoft device
- **SuperAG**—A 802.11a/g SuperAG device
- **Microwave Phone**—A microwave phone
- **Jammer**—A jamming device
- **Canopy**—A canopy bridge device
- **TDD Transmitter**—A time division duplex (TDD) transmitter device
- **Video Camera**—An analog video camera
- **WiFi Invalid Channel**—A WiFi invalid channel
- **WiFi Inverted**—A device using spectrally inverted Wi-Fi signals (I and Q signals of the RF signal are inverted)
- **WiMAX Fixed**—A WiMAX fixed device (802.11a/n only)
- **WiMAX Mobile**—A WiMAX mobile device (802.11a/n only)

Note Access points that are associated to the switch send interference reports only for the interferers that appear in the Interferences to Detect box. This functionality allows you to filter out interferers that you do not want as well as any that may be flooding the network and causing performance problems for the switch or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 6 Configure Cisco CleanAir alarms as follows:

a) Select the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.

b) If you selected the **Enable AQI Trap** check box in *Step a*, enter a value between 1 and 100 (inclusive) in the AQI Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

c) Enter the AQI threshold in the **AQI Alarm Threshold** text box. An alarm is generated when the air quality reaches a threshold value. The default is 35. The range is from 1 and 100.

d) Select the **Enable Interference For Security Alarm** check box to trigger interferer alarms when the switch detects specified device types, or unselect it to disable this feature. The default value is selected

e) Make sure that any sources of interference that need to trigger interferer alarms appear in the **Trap on These Types** box and any that do not need to trigger interferer alarms appear in the **Do Not Trap on These Types** box. Use the **>** and **<** buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

For example, if you want the switch to send an alarm when it detects a jamming device, select the **Enable Interference For Security Alarm** check box and move the jamming device to the **Trap on These Types** box.

Step 7 Click **Apply**.

Step 8 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference as follows:

a) Look at the **EDRRM** field to see the current status of spectrum event-driven RRM and, if enabled, the Sensitivity Threshold field to see the threshold level at which event-driven RRM is invoked.

b) If you want to change the current status of event-driven RRM or the sensitivity level, go to the **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page.

c) Select the **EDRRM** check box to trigger RRM to run when an access point detects a certain level of interference, or unselect it to disable this feature. The default value is selected.

d) If you selected the **EDRRM** check box in *Step c*, choose **Low**, **Medium**, **High** , or **Custom** from the Sensitivity Threshold drop-down list to specify the threshold at which you want RRM to be triggered. When the interference for the access point rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. EDRRM prevents the access point from returning to the original channel for three hours after the event.

High—Represents an increased sensitivity to changes in the environment.

Custom—Allows you to set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

Low—Represents a decreased sensitivity to changes in the environment.

The EDRRM AQ threshold value for low sensitivity is 35, medium sensitivity is 50, and high sensitivity is 60.

e) Click **Apply**.

Step 9 Click **Save Configuration**.

Configuring Cisco CleanAir on an Access Point (GUI)

Step 1 Choose **Configuration > Wireless** > **Access Points > Radios > 802.11a/n or 802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page.

Step 2 Select the check box adjacent to the desired access point and click **Configure**. The 802.11a/n (or 802.11b/g/n) Radios page appears.

The **CleanAir Capable** field shows whether this access point can support CleanAir functionality. If it can, go to the next step to enable or disable CleanAir for this access point. If the access point cannot support CleanAir functionality, you cannot enable CleanAir for this access point.

Note By default, the Cisco CleanAir functionality is enabled on the radios.

Step 3 Enable Cisco CleanAir functionality for this access point by choosing **Enable** from the CleanAir Admin Status drop-down list. To disable CleanAir functionality for this access point, choose **Disable**. The default value is Enable. This setting overrides the global CleanAir configuration for this access point.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Cisco Spectrum Expert

Configuring Spectrum Expert (GUI)

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 switch CLI by using the **show ap name** *ap_name* **config dot11** {**24ghz** | **5ghz**} command.

Step 1 Ensure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Note The SE-Connect mode is set for the entire access point, not just a single radio. However, the Spectrum Expert console connects to a single radio at a time.

Step 2 Choose **Configuration** > **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 3 Click the name of the desired access point to open the All APs > Details page.

Step 4 Choose **SE-Connect** from the AP Mode drop-down list. This mode is available only for access points that are capable of supporting Cisco CleanAir functionality. For the SE-Connect mode to appear as an available option, the access point must have at least one spectrum-capable radio in the Enable state.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **OK** when prompted to reboot the access point.

Step 7 On the Windows PC, access the Cisco Software Center from this URL:

http://www.cisco.com/cisco/software/navigator.html

Step 8 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.

Step 9 Run the Spectrum Expert application on the PC.

Step 10 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 switch, it sends a Spectrum Capabilities notification message, and the switch responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the switch for NSI authentication. The switch 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.

Step 11 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.

Step 12 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

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 switch 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:

```
Switch#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:

```
Switch#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 switch, it sends a Spectrum Capabilities notification message, and the switch responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the switch for use in NSI authentication. The switch 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.

Monitoring CleanAir Parameters

You can monitor CleanAir parameters using the following commands:

Table 2: Commands for Monitoring CleanAir

Commands	Description
show ap dot11 24ghz cleanair air-quality summary	Displays CleanAir Air Quality (AQ) data for 2.4-GHz band
show ap dot11 24ghz cleanair air-quality worst	Displays CleanAir Air Quality (AQ) worst data for 2.4-GHz band
show ap dot11 24ghz cleanair config	Displays CleanAir Configuration for 2.4-GHz band
show ap dot11 24ghz cleanair device type all	Displays all CleanAir Interferers for 2.4-GHz band
show ap dot11 24ghz cleanair device type bt-discovery	Displays CleanAir Interferers of type BT Discovery for 2.4-GHz band
show ap dot11 24ghz cleanair device type bt-link	Displays CleanAir Interferers of type BT Link for 2.4-GHz band
show ap dot11 24ghz cleanair device type canopy	Displays CleanAir Interferers of type Canopy for 2.4-GHz band
show ap dot11 24ghz cleanair device type cont-tx	Displays CleanAir Interferers of type Continuous transmitter for 2.4-GHz band
show ap dot11 24ghz cleanair device type dect-like	Displays CleanAir Interferers of type DECT Like for 2.4-GHz band

Commands	Description
show ap dot11 24ghz cleanair device type fh	Displays CleanAir Interferers of type 802.11FH for 2.4-GHz band
show ap dot11 24ghz cleanair device type inv	Displays CleanAir Interferers of type WiFi Inverted for 2.4-GHz band
show ap dot11 24ghz cleanair device type jammer	Displays CleanAir Interferers of type Jammer for 2.4-GHz band
show ap dot11 24ghz cleanair device type mw-oven	Displays CleanAir Interferers of type MW Oven for 2.4-GHz band
show ap dot11 24ghz cleanair device type nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 2.4-GHz band
show ap dot11 24ghz cleanair device type persistent	Displays CleanAir Interferers of type Persistent for 2.4-GHz band
show ap dot11 24ghz cleanair device type superag	Displays CleanAir Interferers of type SuperAG for 2.4-GHz band
show ap dot11 24ghz cleanair device type tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 2.4-GHz band
show ap dot11 24ghz cleanair device type video	Displays CleanAir Interferers of type Video Camera for 2.4-GHz band
show ap dot11 24ghz cleanair device type wimax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 2.4-GHz band
show ap dot11 24ghz cleanair device type wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 2.4-GHz band
show ap dot11 24ghz cleanair device type xbox	Displays CleanAir Interferers of type Xbox for 2.4-GHz band
show ap dot11 24ghz cleanair device type zigbee	Displays CleanAir Interferers of type zigbee for 2.4-GHz band
show ap dot11 5ghz cleanair air-quality summary	Displays CleanAir Air Quality (AQ) data for 5-GHz band
show ap dot11 5ghz cleanair air-quality worst	Displays CleanAir Air Quality (AQ) worst data for 5-GHz band
show ap dot11 5ghz cleanair config	Displays CleanAir Configuration for 5-GHz band
show ap dot11 5ghz cleanair device type all	Displays all CleanAir Interferers for 5-GHz band
show ap dot11 5ghz cleanair device type canopy	Displays CleanAir Interferers of type Canopy for 5-GHz band
show ap dot11 5ghz cleanair device type cont-tx	Displays CleanAir Interferers of type Continuous TX for 5-GHz band

Commands	Description
show ap dot11 5ghz cleanair device type dect-like	Displays CleanAir Interferers of type DECT Like for 5-GHz band
show ap dot11 5ghz cleanair device type inv	Displays CleanAir Interferers of type WiFi Inverted for 5-GHz band
show ap dot11 5ghz cleanair device type jammer	Displays CleanAir Interferers of type Jammer for 5-GHz band
show ap dot11 5ghz cleanair device type nonstd	Displays CleanAir Interferers of type WiFi Inv. Ch for 5-GHz band
show ap dot11 5ghz cleanair device type persistent	Displays CleanAir Interferers of type Persistent for 5-GHz band
show ap dot11 5ghz cleanair device type superag	Displays CleanAir Interferers of type SuperAG for 5-GHz band
show ap dot11 5ghz cleanair device type tdd-tx	Displays CleanAir Interferers of type TDD Transmit for 5-GHz band
show ap dot11 5ghz cleanair device type video	Displays CleanAir Interferers of type Video Camera for 5-GHz band
show ap dot11 5ghz cleanair device type wimax-fixed	Displays CleanAir Interferers of type WiMax Fixed for 5-GHz band
show ap dot11 5ghz cleanair device type wimax-mobile	Displays CleanAir Interferers of type WiMax Mobile for 5-GHz band

You can also check the CleanAir status of the access points using the switch GUI:

Choose **Monitor** > **Wireless** > **Access Points** > **802.11 a/n/ac**or **802.11 b/g/n**.

The **Radios** page is displayed showing a list of access points that are associated with the switch. You can see the CleanAir Admin and CleanAir Status.

The Cisco CleanAir status is one of the following:

- **UP**—The spectrum sensor for the access point radio is currently operational (error code 0).
- **DOWN**—The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled (error code 8). To correct this error, enable the radio.
- **ERROR**—The spectrum sensor for the access point radio has crashed (error code 128), making CleanAir monitoring nonoperational for this radio. If this error occurs, reboot the access point. If the error continues to appear, you might want to disable Cisco CleanAir functionality on the radio.
- **N/A**—This access point radio is not capable of supporting Cisco CleanAir functionality.

Monitoring the 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 temporarily stop detecting the device. This device is then correctly marked as down. A down device is correctly removed from the spectrum database. In cases when all the interferer detections for a specific devices 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 longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Monitoring the Interference Devices (GUI)

Before you begin

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

Step 1 Choose **Monitor > Interferers > Cisco CleanAir > 802.11a/n or 802.11b/g/n > Interference Devices** to open the Cisco APs > Interference Devices page.

This page shows the following information:

- **AP Name**—The name of the access point where the interference device is detected.
- **Interferer Type**—Type of the interferer.
- **Affected Channel**—Channel that the device affects.
- **Severity**—Severity index of the interfering device.
- **Duty Cycle (%)**—Proportion of time during which the interfering device was active.
- **RSSI**—Receive signal strength indicator (RSSI) of the access point.
- **DevID**—Device identification number that uniquely identified the interfering device.
- **ClusterID**—Cluster identification number that uniquely identifies the type of the devices.

Step 2 Click the **Filter** icon or choose the **Quick Filter** option from the Show drop-down list to display the information about interference devices based on a particular criteria.

Related Topics

Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Configuring Interference Reporting for 5-GHz devices, on page 13

Monitoring the Worst Air Quality of Radio Bands (GUI)

Choose **Monitor** > **Cisco CleanAir** > **Worst Air-Quality** to open the Air Quality Report page.

This page shows the air quality of both the 802.11a/n and 802.11b/g/n radio bands. This page displays the following information:

- **AP Name**—Name of the access point that reported the worst air quality for the 802.11 radio band.
- **Channel Number**—Radio channel with the worst reported air quality.
- **Minimum Air Quality Index**—Minimum air quality for this radio channel. The range is from 1 to 100. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Average Air Quality Index**—Average air quality for this radio channel. The range is from 1 to 100. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Interference Device Count**—Number of interferers detected by the radios on the 802.11 radio band.

Configuration Examples for Configuring CleanAir

Enabling CleanAir on 2.4-GHz Band and an Access Point: Example

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

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair
Switch(config)#exit
Switch#ap name TAP1 dot11 24ghz cleanair
Switch#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:

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

Configuring Interference Reporting for 5-GHz Devices: Example

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

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

Configuring EDRRM for CleanAir-Events: Example

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:

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

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel device
Switch(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:

```
Switch#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:

```
Switch#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 switch shows them as separate clusters or different suspected devices clustered together. Why does this happen?

A. Access points must be RF neighbors for the switch to consider the merging of devices that are detected by these access points. The access point takes time to establish neighbor relationships. A few minutes

after the switch reboots or 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 switch?

A. No, you cannot merge two monitor mode access points using a switch. 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 command: **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**}

This example shows how to display the neighbor access points:

```
Switch#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 switch.

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

A. Yes, the Cisco Catalyst 3850 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**

Related Topics

Enabling CleanAir for 2.4-GHz Band, on page 8
Configuring a CleanAir Alarm for 2.4-GHz Air-Quality and Devices, on page 8
Configuring Interference Reporting for 2.4-GHz Devices, on page 10
Enabling CleanAir for 5-GHz Band, on page 11
Configuring a CleanAir Alarm for 5-GHz Air-Quality and Devices, on page 12
Configuring Interference Reporting for 5-GHz devices, on page 13

Additional References

Related Documents

Related Topic	Document Title
CleanAir commands and their details	*CleanAir Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 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 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