



Configuring Cisco CleanAir

This chapter contains the following sections:

- [Information About CleanAir, page 14-1](#)
- [Guidelines and Limitations, page 14-4](#)
- [Configuring Cisco CleanAir, page 14-5](#)
- [Monitoring the Interference Devices, page 14-14](#)
- [Monitoring the Air Quality of Radio Bands, page 14-19](#)
- [Configuring a Spectrum Expert Connection, page 14-24](#)
- [Additional References, page 14-26](#)
- [Feature History for Configuring CleanAir, page 14-27](#)

Information About CleanAir

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

A Cisco CleanAir system consists of CleanAir-enabled access points, controllers, and WCS. These access points 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 controller. The controller controls the access points, collects spectrum data, and forwards information to WCS or a Cisco mobility services engine (MSE) upon request. The controller provides a local user interface to configure basic CleanAir features and display basic spectrum information. WCS provides an advanced user interface for configuring Cisco CleanAir features, displaying information, and keeping records. The MSE is optional for the basic feature set but required for advanced features such as tracking the location of non-Wi-Fi interference devices.

For every device operating in the unlicensed band, Cisco CleanAir tells you 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 so that you do not have to be an RF expert.

Wireless LAN systems operate in unlicensed 2.4- 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 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 into the Cisco Unified Wireless Network addresses this problem of radio frequency (RF) interference.

Role of the Controller in a Cisco CleanAir System

The controller 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 air quality reports from the access point and stores them in the air quality database. Air Quality Report (AQR) 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 WCS and the MSE.

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.

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.

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 controller 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 Devices Propagation

Persistent device information that is detected by local or monitor mode access points is propagated to the neighboring access points connected to the same controller. This provides better chance of handling and avoiding persistent devices. Persistent device detected by the CleanAir-enabled access point is propagated to neighboring non-CleanAir access points, which enhances channel selection quality.

Guidelines and Limitations

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.
- **FlexConnect**—When a FlexConnect access point is connected to the controller, its Cisco CleanAir functionality is identical to local mode.
- **Monitor**—When Cisco CleanAir is enabled in monitor mode, the access point provides air quality and interference detection reports for all monitored channels.

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**

Suppose you have two APs, one in the FlexConnect mode and the other in the monitor mode. Also suppose that you have created a profile enabling EAP attack against 802.1x auth. The Airmagnet (AM) tool, which can generate different types of attacks, fails to generate any attack even if you have provided valid AP MAC and STA MAC addresses. But if the AP MAC and STA MAC addresses in the AM tool are swapped, that is, the AP MAC address is specified in the STA MAC field and the STA MAC address is specified in the AP MAC field, then the tool is able to generate attacks, which the AP in the Monitor mode is also able to detect.

**Note**

The access point does not participate in AQ HeatMap in WCS.

- **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 controller. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the controller. In addition to performing spectrum intelligence, an access point can provide other. See the [“Configuring a Spectrum Expert Connection” section on page 14-24](#) for instructions on establishing a Spectrum Expert console connection.
- 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 controller’s ability to detect neighboring in-network access points. Correlating interference device detections from multiple access points is limited between monitor-mode access points.

- Spectrum Expert (SE) Connect functionality is supported for local, flexconnect, bridge, and monitor modes. The access point provides spectrum information to Spectrum Expert only for the current channel(s). For local, FlexConnect, and bridge modes, the spectrum data is available for the current active channel(s) and for the monitor mode, the common monitored channel list is available. The access point continues to send AQ (Air Quality) and IDR (Interference Device Reports) reports to the controller 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.
- Controllers have limitations on the number of monitor mode AP's that they can support. This is because, a monitor mode AP saves data for all the channels.
- Do not connect access points in SE connect mode directly to any physical port on the 2500 Series Controller.
- Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.

Configuring Cisco CleanAir

This section contains the following topics:

- [Configuring Cisco CleanAir on the Controller, page 14-5](#)
- [Configuring Cisco CleanAir on an Access Point, page 14-11](#)

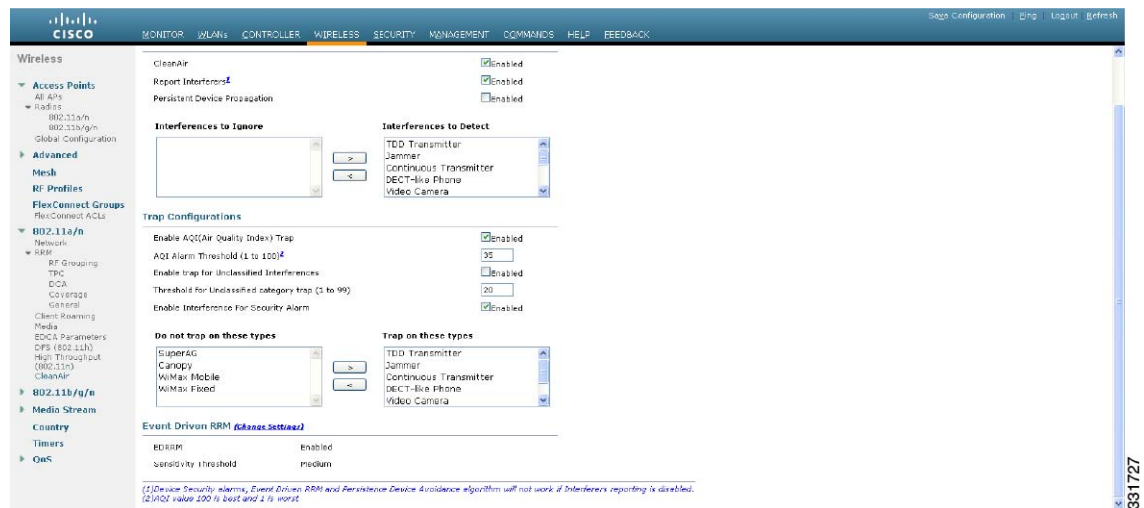
Configuring Cisco CleanAir on the Controller

This section contains the following topics:

- [Configuring Cisco CleanAir on the Controller \(GUI\), page 14-5](#)
- [Configuring Cisco CleanAir on the Controller \(CLI\), page 14-8](#)

Configuring Cisco CleanAir on the Controller (GUI)

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

Figure 14-1 802.11a (or 802.11b) > CleanAir

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 controller from detecting spectrum interference. By default, the value is not selected.

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 controller from reporting interferers. The default value is selected.



Note Device Security alarms, Event Driven RRM, and 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 controller. Persistent interferers are present at a 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 possible sources of interference that you can choose are as follows:

- **Bluetooth Paging Inquiry**—A Bluetooth discovery (802.11b/g/n only)
- **Bluetooth Sco Acl**—A Bluetooth link (802.11b/g/n only)
- **Generic DECT**—A digital enhanced cordless communication (DECT)-compatible phone
- **Generic TDD**—A time division duplex (TDD) transmitter
- **Generic Waveform**—A continuous transmitter
- **Jammer**—A jamming device
- **Microwave**—A microwave oven (802.11b/g/n only)
- **Canopy**—A canopy bridge device
- **Spectrum 802.11 FH**—An 802.11 frequency-hopping device (802.11b/g/n only)

- **Spectrum 802.11 inverted**—A device using spectrally inverted Wi-Fi signals
- **Spectrum 802.11 non std channel**—A device using nonstandard Wi-Fi channels
- **Spectrum 802.11 SuperG**—An 802.11 SuperAG device
- **Spectrum 802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **Video Camera**—An analog video camera
- **WiMAX Fixed**—A WiMAX fixed device (802.11a/n only)
- **WiMAX Mobile**—A WiMAX mobile device (802.11a/n only)
- **XBox**—A Microsoft Xbox (802.11b/g/n only)

**Note**

Access points that are associated to the controller 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 controller or WCS. 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.
- Enter the **AQI Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality falls below the configured threshold value. The default is 35. The valid range is from 1 and 100.
- Select the **Enable trap for Unclassified Interferences** check box to enable the AQI alarm to be generated upon detection of unclassified interference beyond the severity threshold specified in the **AQI Alarm Threshold**. Unclassified interferences are interferences that are detected but do not correspond to any of the identifiable interference types.
- Enter the **Threshold for Unclassified category trap (1 to 99)**. The valid range is from 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.
- c. Select the **Enable Interference Type Trap** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
- d. 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 controller to send an alarm when it detects a jamming device, select the **Enable Interference Type Trap** check box and move the jamming device to the Trap on These Types box.

Step 7 Click **Apply** to commit your changes.

- 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:
- 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.
 - If you want to change the current status of event-driven RRM or the sensitivity level, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page appears.
 - 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.
 - 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 and the corresponding AQ index falls below the threshold level, RRM initiates a local channel assignment and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

If you selected the EDRRM sensitivity threshold as custom, you must set a threshold value in the Custom Sensitivity Threshold field. The default sensitivity is 35.

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

The default value is Medium.
 - Click **Apply** to commit your changes.
- Step 9** Click **Save Configuration** to save your changes.
-

Configuring Cisco CleanAir on the Controller (CLI)

- Step 1** Configure Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network by entering this command:
- ```
config {802.11a | 802.11b} cleanair {enable | disable} all
```
- If you disable this feature, the controller does not receive any spectrum data. The default value is enable.
- Step 2** Configure interference detection and specify sources of interference that need to be detected by the Cisco CleanAir system by entering this command:
- ```
config {802.11a | 802.11b} cleanair device {enable | disable} type
```
- where you choose the *type* is one of the following:
- 802.11-fh**—An 802.11 frequency-hopping device (802.11b/g/n only)
 - 802.11-inv**—A device using spectrally inverted Wi-Fi signals
 - 802.11-nonstd**—A device using nonstandard Wi-Fi channels
 - 802.15.4**—An 802.15.4 device (802.11b/g/n only)
 - all**—All interference device types (this is the default value)
 - bt-discovery**—A bluetooth discovery (802.11b/g/n only)
 - bt-link**—A bluetooth link (802.11b/g/n only)
 - canopy**—A canopy device

- **cont-tx**—A continuous transmitter
- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A **microwave oven** (802.11b/g/n only)
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video camera**—An analog video camera
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)



Note Access points that are associated to the controller send interference reports only for the interference types specified in this command. This functionality allows you to filter out interferers that may be flooding the network and causing performance problems for the controller or WCS. Filtering allows the system to resume normal performance levels.

Step 3 Configure the triggering of air quality alarms by entering this command:

config {802.11a | 802.11b} cleanair alarm air-quality {enable | disable}

The default value is enabled.

Step 4 Specify the threshold at which you want the air quality alarm to be triggered by entering this command:

config {802.11a | 802.11b} cleanair alarm air-quality threshold *threshold*

where *threshold* is a value between 1 and 100 (inclusive). 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.

Step 5 Enable the triggering of interferer alarms by entering this command:

config {802.11a | 802.11b} cleanair alarm device {enable | disable}

The default value is enable.

Step 6 Specify sources of interference that trigger alarms by entering this command:

config {802.11a | 802.11b} cleanair alarm device *type* {enable | disable}

where you choose *type* as one of the following:

- **802.11-fh**—An 802.11 frequency-hopping device (802.11b/g/n only)
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals
- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
- **802.15.4**—An 802.15.4 device (802.11b/g/n only)
- **all**—All interference device types (this is the default value)
- **bt-discovery**—A Bluetooth discovery (802.11b/g/n only)
- **bt-link**—A Bluetooth link (802.11b/g/n only)
- **canopy**—A canopy device
- **cont-tx**—A continuous transmitter

- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- **jammer**—A jamming device
- **mw-oven**—A **microwave oven** (802.11b/g/n only)
- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video camera**—An analog video camera
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)

Step 7 Configure the triggering of air quality alarms for unclassified devices by entering this command:

```
config {802.11a | 802.11b} cleanair alarm unclassified {enable | disable}
```

Step 8 Specify the threshold at which you want the air quality alarm to be triggered for unclassified devices by entering this command:

```
config {802.11a | 802.11b} cleanair alarm unclassified threshold threshold
```

where *threshold* is a value from 1 and 99 (inclusive). 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.

Step 9 Trigger spectrum event-driven radio resource management (RRM) to run when a Cisco CleanAir-enabled access point detects a significant level of interference by entering these commands:

- **config advanced {802.11a | 802.11b} channel cleanair-event {enable | disable}**—Enables or disables spectrum event-driven RRM. The default value is disabled.
- **config advanced {802.11a | 802.11b} channel cleanair-event sensitivity {low | medium | high | custom}**—Specifies the threshold at which you want RRM to be triggered. When the interference level 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. Low represents a decreased sensitivity to changes in the environment while high represents an increased sensitivity. You can also set the sensitivity to a custom level of your choice. The default value is medium.
- **config advanced {802.11a | 802.11b} channel cleanair-event sensitivity threshold *thresholdvalue***—If you set the threshold sensitivity as custom, you must set a custom threshold value. The default is 35.

Step 10 Enable persistent devices propagation by entering this command:

```
config advanced {802.11a | 802.11b} channel pda-prop {enable | disable}
```

Step 11 Save your changes by entering this command:

```
save config
```

Step 12 See the Cisco CleanAir configuration for the 802.11a/n or 802.11b/g/n network by entering this command:

```
show {802.11a | 802.11b} cleanair config
```

Information similar to the following appears:

```
(Cisco Controller) >show 802.11a cleanair config
```

```
Clean Air Solution..... Disabled
Air Quality Settings:
```

```

Air Quality Reporting..... Enabled
Air Quality Reporting Period (min)..... 15
Air Quality Alarms..... Enabled
  Air Quality Alarm Threshold..... 35
  Unclassified Interference..... Disabled
  Unclassified Severity Threshold..... 20
Interference Device Settings:
  Interference Device Reporting..... Enabled
  Interference Device Types:
    TDD Transmitter..... Enabled
    Jammer..... Enabled
    Continuous Transmitter..... Enabled
    DECT-like Phone..... Enabled
    Video Camera..... Enabled
    WiFi Inverted..... Enabled
    WiFi Invalid Channel..... Enabled
    SuperAG..... Enabled
    Canopy..... Enabled
    WiMax Mobile..... Enabled
    WiMax Fixed..... Enabled
Interference Device Alarms..... Enabled
  Interference Device Types Triggering Alarms:
    TDD Transmitter..... Disabled
    Jammer..... Enabled
    Continuous Transmitter..... Disabled
    DECT-like Phone..... Disabled
    Video Camera..... Disabled
    WiFi Inverted..... Enabled
    WiFi Invalid Channel..... Enabled
    SuperAG..... Disabled
    Canopy..... Disabled
    WiMax Mobile..... Disabled
    WiMax Fixed..... Disabled
Additional Clean Air Settings:
  CleanAir ED-RRM State..... Disabled
  CleanAir ED-RRM Sensitivity..... Medium
  CleanAir ED-RRM Custom Threshold..... 50
  CleanAir Persistent Devices state..... Disabled
  CleanAir Persistent Device Propagation..... Enabled

```

- Step 13** See the spectrum event-driven RRM configuration for the 802.11a/n or 802.11b/g/n network by entering this command:

show advanced {802.11a | 802.11b} channel

Information similar to the following appears:

```

Automatic Channel Assignment
Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds [startup]
Anchor time (Hour of the day)..... 0
Channel Update Contribution..... SNI
CleanAir Event-driven RRM option..... Enabled
CleanAir Event-driven RRM sensitivity..... Medium

```

Configuring Cisco CleanAir on an Access Point

This section contains the following topics:

- [Configuring Cisco CleanAir on an Access Point \(GUI\), page 14-12](#)

- [Configuring Cisco CleanAir on an Access Point \(CLI\), page 14-13](#)

Configuring Cisco CleanAir on an Access Point (GUI)

To configure Cisco CleanAir functionality for a specific access point using the controller GUI, follow these steps:

- Step 1** Choose **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.

Figure 14-2 802.11a/n Cisco APs > Configure Page

The screenshot shows the Cisco Wireless Controller GUI. The left sidebar has a tree view with 'Wireless' expanded, showing 'Access Points' > 'Radios' > '802.11a/n'. The main content area is titled '802.11a/n Cisco APs > Configure'. It contains several configuration sections:

- General:** AP Name (aphep_ap_1142), Admin Status (Enable), Operational Status (UP), Slot # (1).
- 11n Parameters:** 11n Supported (Yes), ClientLink (checkbox).
- CleanAir:** CleanAir Capable (No), CleanAir Admin Status (Disable).
- Antenna Parameters:** Antenna Type (Internal), Antenna (A, B, C) with Rx and Tx checkboxes.
- RF Channel Assignment:** Current Channel (153), Channel Width (40 MHz), Assignment Method (Global/Custom).
- Tx Power Level Assignment:** Current Tx Power Level (4), Assignment Method (Global/Custom).
- Performance Profile:** View and edit Performance Profile for this AP.

- Step 2** Hover your cursor over the blue drop-down arrow for the desired access point and click **Configure**. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure 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 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.

The Number of Spectrum Expert Connections text box shows the number of Spectrum Expert applications that are currently connected to the access point radio. Up to three active connections are possible.

- Step 4** Click **Apply** to commit your changes.
- Step 5** Click **Save Configuration** to save your changes.
- Step 6** Click **Back** to return to the 802.11a/n (or 802.11b/g/n) Radios page.

Step 7 View the Cisco CleanAir status for each access point radio by looking at the CleanAir Status text box on the 802.11a/n (or 802.11b/g/n) Radios page.

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.



Note

You can create a filter to make the 802.11a/n Radios page or the 802.11b/g/n Radios page show only access point radios that have a specific Cisco CleanAir status (such as UP, DOWN, ERROR, or N/A). This feature is especially useful if your list of access point radios spans multiple pages, preventing you from viewing them all at once. To create a filter, click **Change Filter** to open the Search AP dialog box, select one or more of the CleanAir Status check boxes, and click **Find**. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, CleanAir Status: UP).

Configuring Cisco CleanAir on an Access Point (CLI)

Step 1 Configure Cisco CleanAir functionality for a specific access point by entering this command:

```
config {802.11a | 802.11b} cleanair {enable | disable} Cisco_AP
```

Step 2 Save your changes by entering this command:

```
save config
```

Step 3 See the Cisco CleanAir configuration for a specific access point on the 802.11a/n or 802.11b/g/n network by entering this command:

```
show ap config {802.11a | 802.11b} Cisco_AP
```

Information similar to the following appears:

```
Cisco AP Identifier..... 0
Cisco AP Name..... CISCO_AP3500
...
Spectrum Management Information
  Spectrum Management Capable..... Yes
  Spectrum Management Admin State..... Enabled
  Spectrum Management Operation State..... Up
  Rapid Update Mode..... Disabled
  Spectrum Expert connection..... Disabled
  Spectrum Sensor State..... Configured (Error code = 0)
```



Note

See [Step 7](#) in the “[Configuring Cisco CleanAir on an Access Point \(GUI\)](#)” section for descriptions of the spectrum management operation states and the possible error codes for the spectrum sensor state.

Monitoring the Interference Devices

This section contains the following topics:

- [Prerequisites for Monitoring the Interference Devices, page 14-14](#)
- [Monitoring the Interference Device \(GUI\), page 14-14](#)
- [Monitoring the Interference Device \(CLI\), page 14-16](#)
- [Monitoring Persistent Devices \(GUI\), page 14-18](#)
- [Monitoring Persistent Devices \(CLI\), page 14-18](#)

Prerequisites for Monitoring the Interference Devices

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

Monitoring the Interference Device (GUI)

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

Figure 14-3 *CleanAir > Interference Device Page*

CISCO										
MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK										
Monitor	802.11b/g/n Cisco APs > Interference Devices									Entries 1 - 14 of 14
Summary	Current Filter: None [Change Filter] [Clear Filter]									
Access Points										
Cisco CleanAir										
802.11a/n										
Interference Devices										
Air Quality Report										
802.11b/g/n										
Interference Devices										
Air Quality Report										
Worst Air-Quality Report										
Statistics										
CDP										
Rogues										
Clients										
Multicast										
	AP Name	Radio Slot#	Interferer Type	Affected Channel	Detected Time	Severity	Duty Cycle (%)	RSSI	DevID	Cluster
	AP1-L	0	Xbox	1,2,3,4,5,6,7,8,9,10,11	Mon May 17 11:56:40 2010	5	10	-54	0xf001	73:79:8
	AP1-L	0	802.11FH	1,5,6,7,8,9	Mon May 17 11:56:44 2010	1	1	-41	0xf002	73:79:8
	AP1-L	0	SuperAG	1,2,3,4,5,6,7,8,9,10,11	Mon May 17 12:44:17 2010	1	1	-33	0xf007	73:79:8
	AP1-L	0	DECT phone	1,2,3,4,5,6,7,8,9,10,11	Mon May 17 12:51:32 2010	2	3	-44	0xf008	73:79:8
	AP3-L	0	Xbox	11	Mon May 17 12:51:29 2010	3	1	-60	0x4009	73:79:8
	AP3-L	0	802.11FH	11	Mon May 17 22:51:59 2010	1	1	-44	0x4011	73:79:8
	AP3-L	0	DECT phone	11	Tue May 18 00:36:37 2010	2	1	-46	0x4012	73:79:8
	AP2-Z	0	DECT phone	1	Mon May 17 12:01:52 2010	2	1	-44	0x5008	73:79:8
	AP2-Z	0	Xbox	1	Mon May 17 12:51:26 2010	2	1	-68	0x500a	73:79:8
	AP2-Z	0	802.11FH	1	Tue May 18 00:14:20 2010	1	1	-44	0x500e	73:79:8
	AP7-Z	0	Xbox	6	Mon May 17 12:11:42 2010	3	1	-64	0x2005	73:79:8
	AP7-Z	0	DECT phone	6	Mon May 17 12:11:50 2010	2	1	-49	0x2006	73:79:8

This page shows the following information:

- **AP Name**—The name of the access point where the interference device is detected.
- **Radio Slot #**—Slot where the radio is installed.
- **Interferer Type**—Type of the interferer.
- **Affected Channel**—Channel that the device affects.
- **Detected Time**—Time at which the interference was detected.
- **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.

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.

Step 2 Click **Change Filter** to display the information about interference devices based on a particular criteria.

Step 3 Click **Clear Filter** to remove the filter and display the entire access point list.

You can create a filter to display the list of interference devices that are based on the following filtering parameters:

- **Cluster ID**—To filter based on the Cluster ID, select the check box and enter the Cluster ID in the text box next to this field.
- **AP Name**—To filter based on the access point name, select the check box and enter the access point name in the text box next to this field.
- **Interferer Type**—To filter based on the type of the interference device, select the check box and select the interferer device from the options.

Choose one of the interferer devices:

- **BT Link**
- **MW Oven**
- **802.11 FH**
- **BT Discovery**
- **TDD Transmit**
- **Jammer**
- **Continuous TX**
- **DECT Phone**
- **Video Camera**
- **802.15.4**
- **WiFi Inverted**
- **WiFi Inv. Ch**
- **SuperAG**
- **Canopy**
- **XBox**
- **WiMax Mobile**
- **WiMax Fixed**

- **WiFi ACI**
- **Unclassified**
- Activity Channels
- Severity
- Duty Cycle (%)
- RSSI

Step 4 Click **Find** to commit your changes.

The current filter parameters are displayed in the Current Filter field.

Monitoring the Interference Device (CLI)

This section describes the commands that you can use to monitor the interference devices for the 802.11a/n or 802.11b/g/n radio band.

Detecting Interferers by an Access Point

See information for all of the interferers detected by a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

show {802.11a | 802.11b} cleanair device ap *Cisco_AP*

Information similar to the following appears:

DC = Duty Cycle (%)

ISI = Interference Severity Index (1-Low Interference, 100-High Interference)

RSSI = Received Signal Strength Index (dBm)

DevID = Device ID

No	ClusterID	DevID	Type	AP Name	ISI	RSSI	DC	Channel
1	c2:f7:40:00:00:03	0x8001	DECT phone	CISCO_AP3500	1	-43	3	149,153,157,161
3	c2:f7:40:00:00:03	0x8005	Canopy	CISCO_AP3500	2	-62	2	153,157,161,165

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 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 longer and they are remerged into a single record upon detection. This process smoothens the user records and accurately represents the device history.

Detecting Interferers by Device Type

See information for all of the interferers of a specific device type on the 802.11a/n or 802.11b/g/n radio band by entering this command:

show {802.11a | 802.11b} cleanair device type type

Information similar to the following appears:

DC = Duty Cycle (%)
 ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
 RSSI = Received Signal Strength Index (dBm)
 DevID = Device ID
 * indicates cluster center device

No	ClusterID	DevID	Type	AP Name	ISI	RSSI	DC	Channel
1	b4:f7:40:00:00:03	0x4185	DECT-like (26)	CISCO_AP35001	-58	3	153,157,161,165	

Detecting Persistent Sources of Interference

View a list of persistent sources of interference for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

show ap auto-rf {802.11a | 802.11b} Cisco_AP

Information similar to the following appears:

```

Number Of Slots..... 2
AP Name..... AP1-L
MAC Address..... c4:7d:4f:3a:07:1e
  Slot ID..... 1
  Radio Type..... RADIO_TYPE_80211a
  Sub-band Type..... All
Noise Information
  Noise Profile..... PASSED
  Channel 34..... -97 dBm
  Channel 36..... -90 dBm
  Channel 38..... -97 dBm
Interference Information
  Interference Profile..... PASSED
  Channel 34..... -128 dBm @ 0 % busy
  Channel 36..... -128 dBm @ 0 % busy
  Channel 38..... -128 dBm @ 0 % busy
  Channel 40..... -128 dBm @ 0 % busy
Load Information
  Load Profile..... PASSED
  Receive Utilization..... 0 %
  Transmit Utilization..... 0 %
  Channel Utilization..... 0 %
  Attached Clients..... 0 clients
Coverage Information
  Coverage Profile..... PASSED
  Failed Clients..... 0 clients
Client Signal Strengths
  RSSI -100 dbm..... 0 clients
  RSSI -92 dbm..... 0 clients
  RSSI -84 dbm..... 0 clients
Client Signal To Noise Ratios
  SNR 0 dB..... 0 clients
  SNR 5 dB..... 0 clients
  SNR 10 dB..... 0 clients
  SNR 15 dB..... 0 clients
Nearby APs

```

```

AP c4:7d:4f:52:cf:a0 slot 1..... -36 dBm on 149 (10.10.10.27)
AP c4:7d:4f:53:1b:50 slot 1..... -10 dBm on 149 (10.10.10.27)
Radar Information
Channel Assignment Information
Current Channel Average Energy..... unknown
Previous Channel Average Energy..... unknown
Channel Change Count..... 0
Last Channel Change Time..... Mon May 17 11:56:32 2010
Recommended Best Channel..... 149
RF Parameter Recommendations
Power Level..... 7
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346
Antenna Pattern..... 0

Persistent Interference Devices
Classtype Channel DC (%) RSSI (dBm) Last Update Time
-----
Canopy 149 4 -63 Tue May 18 03:21:16 2010
All third party trademarks are the property of their respective owners.

```

Monitoring Persistent Devices (GUI)

To monitor persistent devices on a specific access point using the controller GUI:

Choose **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. Hover your cursor over the blue drop-down arrow for the desired access point and click **Detail**. The 802.11a/n (or 802.11b/g/n) AP Interfaces > Detail page appears.

This page displays the details of the access points along with the list of persistent devices detected by this access point. Details of the persistent devices is displayed under the Persistent Devices section.

The following information for each persistent device is available:

Class Type—The class type of the persistent device.

Channel—Channel this device is affecting.

DC(%)—Duty cycle (in percentage) of the persistent device.

RSSI(dBm)—RSSI indicator of the persistent device.

Last Seen Time—Timestamp when the device was last active.

Monitoring Persistent Devices (CLI)

To view the list of persistent devices using the CLI, use the following command:

show ap auto-rf {802.11a | 802.11b} ap_name

```

Number Of Slots..... 2
AP Name..... AP_1142_MAP
MAC Address..... c4:7d:4f:3a:35:38
Slot ID..... 1
Radio Type..... RADIO_TYPE_80211a
Sub-band Type..... All
Noise Information
. . .
. . .
Power Level..... 1
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346

```

```

Antenna Pattern..... 0

Persistent Interference Devices
Class Type                Channel  DC (%)  RSSI (dBm)  Last Update Time
-----
Video Camera              149      100    -34         Tue Nov  8 10:06:25 2011

```

The following information for each persistent device is available:

- **Class Type**—The class type of the persistent device.
- **Channel**—Channel on which this device is affecting.
- **DC(%)**—Duty cycle (in percentage) of the persistent device.
- **RSSI(dBm)**—RSSI indicator of the persistent device.
- **Last Updated Time**—Timestamp when the device was last active.

Monitoring the Air Quality of Radio Bands

This section contains the following topics:

- [Monitoring the Air Quality of Radio Bands \(GUI\), page 14-19](#)
- [Monitoring the Air Quality of Radio Bands \(CLI\), page 14-20](#)
- [Monitoring the Worst Air Quality of Radio Bands \(GUI\), page 14-21](#)
- [Monitoring the Air Quality of Radio Bands \(CLI\), page 14-20](#)

Monitoring the Air Quality of Radio Bands (GUI)

To monitor the air quality of radio bands using the controller GUI, follow this step:

Choose **Monitor > Cisco CleanAir > 802.11a/n or 802.11b/g > Air Quality Report** to open the CleanAir > Air Quality Report page.

Figure 14-4 CleanAir > Air Quality Report Page

AP Name	Radio Slot#	Channel	Average AQ	Minimum AQ	Interferer	DFS
ZEST	1	48	98	98	0	No
ZEST	1	60	99	99	0	No

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

- **AP Name**—The name of the access point that reported the worst air quality for the 802.11a/n or 802.11b/g/n radio band.
- **Radio Slot**—The slot number where the radio is installed.
- **Channel**—The radio channel where the air quality is monitored.
- **Minimum AQ**—The minimum air quality for this radio channel.
- **Average AQ**—The average air quality for this radio channel.
- **Interferer**—The number of interferers detected by the radios on the 802.11a/n or 802.11b/g/n radio band.
- **DFS**—Dynamic Frequency Selection. This indicates if DFS is enabled or not.

Monitoring the Air Quality of Radio Bands (CLI)

This section describes the commands that you can use to monitor the air quality of the 802.11a/n or 802.11b/g/n radio band.

Viewing a Summary of the Air Quality

See a summary of the air quality for the 802.11a/n or 802.11b/g/n radio band by entering this command:

show {802.11a | 802.11b} cleanair air-quality summary

Information similar to the following appears:

AQ = Air Quality

DFS = Dynamic Frequency Selection

AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
CISCO_AP3500	36	95	70	0	
CISCO_AP3500	40	93	75	0	
CISCO_AP3500	44	95	80	0	
CISCO_AP3500	48	97	75	0	
CISCO_AP3500	52	98	80	0	
...					

Viewing Air Quality for all Access Points on a Radio Band

See information for the 802.11a/n or 802.11b/g/n access point with the air quality by entering this command:

show {802.11a | 802.11b} cleanair air-quality

Information similar to the following appears:

AQ = Air Quality

DFS = Dynamic Frequency Selection

AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
CISCO_AP3500	1	83	57	3	5

Viewing Air Quality for an Access Point on a Radio Band

See air quality information for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show {802.11a | 802.11b} cleanair air-quality Cisco_AP
```

Information similar to the following appears:

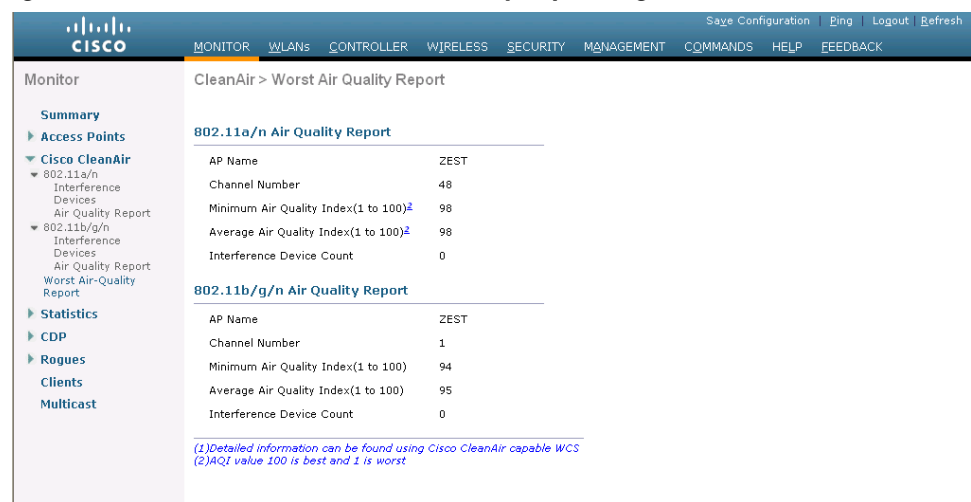
```
Slot Channel Avg AQ Min AQ Total Power (dBm) Total Duty Cycle (%)
-----
1 140 100 100 -89 0

Interferer Power (dBm) Interferer Duty Cycle (%) Interferers DFS
-----
-128 0 0
```

Monitoring the Worst Air Quality of Radio Bands (GUI)

- Step 1** Choose **Monitor > Cisco CleanAir > 802.11b/g > Worst Air-Quality** to open the CleanAir > Worst Air Quality Report page.

Figure 14-5 CleanAir > Worst Air Quality Report Page



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

- **AP Name**—The name of the access point that reported the worst air quality for the 802.11a/n or 802.11b/g/n radio band.
- **Channel Number**—The radio channel with the worst reported air quality.
- **Minimum Air Quality Index(1 to 100)**—The minimum air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Average Air Quality Index(1 to 100)**—The average air quality for this radio channel. An air quality index (AQI) value of 100 is the best, and 1 is the worst.
- **Interference Device Count**—The number of interferers detected by the radios on the 802.11a/n or 802.11b/g/n radio band.

Step 2 View a list of persistent sources of interference for a specific access point radio as follows:

- a. **Choose 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.
- b. Hover your cursor over the blue drop-down arrow for the desired access point radio and click **CleanAir-RRM**. The 802.11a/n (or 802.11b/g/n) Cisco APs > *Access Point Name* > Persistent Devices page appears. This page lists the device types of persistent sources of interference detected by this access point radio. It also shows the channel on which the interference was detected, the percentage of time that the interferer was active (duty cycle), the received signal strength (RSSI) of the interferer, and the day and time when the interferer was last detected.

Monitoring the Worst Air Quality of Radio Bands (CLI)

This section describes the commands that you can use to monitor the air quality of the 802.11a/n or 802.11b/g/n radio band.

Viewing a Summary of the Air Quality (CLI)

See a summary of the air quality for the 802.11a/n or 802.11b/g/n radio band by entering this command:

show {802.11a | 802.11b} cleanair air-quality summary

Information similar to the following appears:

AQ = Air Quality

DFS = Dynamic Frequency Selection

AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
CISCO_AP3500	36	95	70	0	
CISCO_AP3500	40	93	75	0	
CISCO_AP3500	44	95	80	0	
CISCO_AP3500	48	97	75	0	
CISCO_AP3500	52	98	80	0	
...					

Viewing Worst Air Quality Information for all Access Points on a Radio Band (CLI)

See information for the 802.11a/n or 802.11b/g/n access point with the worst air quality by entering this command:

show {802.11a | 802.11b} cleanair air-quality worst

Information similar to the following appears:

AQ = Air Quality

DFS = Dynamic Frequency Selection

AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
CISCO_AP3500	1	83	57	3	5

Viewing Air Quality for an Access Point on a Radio Band (CLI)

See air quality information for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

show {802.11a | 802.11b} cleanair air-quality Cisco_AP

Information similar to the following appears:

```
Slot Channel Avg AQ  Min AQ  Total Power (dBm) Total Duty Cycle (%)
-----
1      140      100    100      -89              0

Interferer Power (dBm) Interferer Duty Cycle (%) Interferers DFS
-----
-128                  0              0
```

Viewing Air Quality for an Access Point by Device Type (CLI)

- See information for all of the interferers detected by a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

show {802.11a | 802.11b} cleanair device ap Cisco_AP

Information similar to the following appears:

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI = Received Signal Strength Index (dBm)
DevID = Device ID
```

No	ClusterID	DevID	Type	AP Name	ISI	RSSI	DC	Channel
1	c2:f7:40:00:00:03	0x8001	DECT phone	CISCO_AP3500	1	-43	3	149,153,157,161
3	c2:f7:40:00:00:03	0x8005	Canopy	CISCO_AP3500	2	-62	2	153,157,161,165

- See information for all of the interferers of a specific device type on the 802.11a/n or 802.11b/g/n radio band by entering this command:

show {802.11a | 802.11b} cleanair device type type

where you choose the *type* as one of the following:

- 802.11-fh**—An 802.11 frequency-hopping device (802.11b/g/n only)
- 802.11-inv**—A device using spectrally inverted Wi-Fi signals
- 802.11-nonstd**—A device using nonstandard Wi-Fi channels
- 802.15.4**—An 802.15.4 device (802.11b/g/n only)
- all**—All interference device types (this is the default value)
- bt-discovery**—A bluetooth discovery (802.11b/g/n only)
- bt-link**—A bluetooth link (802.11b/g/n only)
- canopy**—A canopy bridge device
- cont-tx**—A continuous transmitter
- dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
- jammer**—A jamming device
- mw-oven**—A microwave oven (802.11b/g/n only)

- **superag**—An 802.11 SuperAG device
- **tdd-tx**—A time division duplex (TDD) transmitter
- **video camera**—An analog video camera
- **wimax-fixed**—A WiMAX fixed device
- **wimax-mobile**—A WiMAX mobile device
- **xbox**—A Microsoft Xbox (802.11b/g/n only)

Information similar to the following appears:

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI = Received Signal Strength Index (dBm)
DevID = Device ID
      * indicates cluster center device
```

No	ClusterID	DevID	Type	AP Name	ISI	RSSI	DC	Channel
1	b4:f7:40:00:00:03	0x4185	DECT-like	(26) CISCO_AP35001	-58	3	153,157,161,165	

Detecting Persistent Sources of Interference (CLI)

See a list of persistent sources of interference for a specific access point on the 802.11a/n or 802.11b/g/n radio band by entering this command:

```
show ap auto-rf {802.11a | 802.11b} Cisco_AP
```

Information similar to the following appears:

```
Number Of Slots..... 2
AP Name..... CISCO_AP3500
...
Persistent Interferers
  Classtype              Channel  DC (%)  RSSI (dBm)  Last Update Time
-----
  802.11FH               149     3      -58         Thu Jan 1 00:20:34 2009
  Radar                  153     2      -81         Thu Jan 1 00:20:35 2009
  Continuous Transmitter 157     2      -62         Thu Jan 1 00:20:36 2009
  ...
All third party trademarks are the property of their respective owners.
```

Configuring a Spectrum Expert Connection

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 Spectrum Expert application (referred to as a *Spectrum Expert console*). You can initiate the Spectrum Expert connection semi-automatically from WCS or by manually launching it from the controller. This section provides instructions for the latter.

To configure a Spectrum Expert, follow these steps:

- Step 1** 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.
- Step 2** Make sure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.
- Step 3** Configure the access point for SE-Connect mode using the controller GUI or CLI.



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.

- If you are using the controller GUI, follow these steps:
 - a. Choose **Wireless > Access Points > All APs** to open the All APs page.
 - b. Click the name of the desired access point to open the All APs > Details page.
 - c. 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.
 - d. Click **Apply** to commit your changes.
 - e. Click **OK** when prompted to reboot the access point.
- If you are using the controller CLI, follow these steps:
 - a. To configure the access point for SE-Connect mode, enter this command:

```
config ap mode se-connect Cisco_AP
```

- b. When prompted to reboot the access point, enter **Y**.

- c. To verify the SE-Connect configuration status for the access point, enter this command:

```
show ap config {802.11a | 802.11b} Cisco_AP
```

Information similar to the following appears:

```
Cisco AP Identifier..... 0
Cisco AP Name..... CISCO_AP3500
...
Spectrum Management Information
  Spectrum Management Capable..... Yes
  Spectrum Management Admin State..... Enabled
  Spectrum Management Operation State..... Up
  Rapid Update Mode..... Disabled
  Spectrum Expert connection..... Enabled
  Spectrum Sensor State..... Configured (Error code = 0)
```

- Step 4** On the Windows PC, access the Cisco Software Center from this URL:
<http://www.cisco.com/cisco/software/navigator.html>
- Step 5** Click **Product > Wireless > Cisco Spectrum Intelligence > Cisco Spectrum Expert > Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.0 executable (*.exe) file.
- Step 6** Run the Spectrum Expert application on the PC.

- Step 7** 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.



Note 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.



Note To view the NSI key from the controller CLI, enter the **show ap config {802.11a | 802.11b} Cisco_AP** command. To view the NSI key from the controller GUI, choose **Wireless > Access Points > All APs** to open the All APs page. Click the name of the desired access point to open the All APs > Details page. The NSI key appears in the General tab.

When an access point in SE-Connect mode joins a controller, it sends a Spectrum Capabilities notification message, and the controller responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the controller for use in NSI authentication. The controller 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. The Number of Spectrum Expert Connections text box on the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page of the controller GUI shows the number of Spectrum Expert applications that are currently connected to the access point radio.

- Step 8** 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 9** Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Additional References

For additional information related to configuring CleanAir, see the following sections:

Related Documents

Related Topic	Document Title
Cisco WCS Reports on CleanAir	Cisco Wireless Control System Configuration Guide URL: http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html
To initiate a Spectrum Expert connection using WCS	Cisco Wireless Control System Configuration Guide
Using Spectrum Expert	Cisco Spectrum Expert Users Guide, Release 4.0 URL: http://www.cisco.com/en/US/products/ps9393/products_user_guide_list.html

Feature History for Configuring CleanAir

Table 14-1 lists the release history for this feature.

Table 14-1 Feature History for Configuring CleanAir

Feature Name	Releases	Feature Information
Cluster ID	7.0.116.0	Cluster identification number that uniquely identifies the type of the devices.
CleanAir	7.0.98.0	CleanAir enables you to identify and track non-Wi-Fi sources of interference, adjust your network configuration for optimal performance, identify threats from malicious devices, and allow your WLAN to coexist with other wireless devices.

