Configuring Cisco CleanAir

This section describes how to configure Cisco CleanAir on a controller and an access point. It contains the following sections:

- Information About CleanAir, page 1
- Guidelines and Limitations, page 4
- Configuring Cisco CleanAir, page 5
- Monitoring the Interference Devices, page 12
- Information About Spectrum Expert Connection, page 19
- Related Documents, page 21
- Feature History of CleanAir, page 22

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. CleanAir provides spectrum management and RF visibility.

A Cisco CleanAir system consists of CleanAir-enabled access points, Cisco Wireless LAN Controllers, and Cisco Prime Infrastructure. These access points collect information about all 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 Cisco WLC. The Cisco WLC controls the access points, collects spectrum data, and forwards information to Cisco Prime Infrastructure or a Cisco mobility services engine (MSE) upon request.

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.

CleanAir is supported on mesh AP backhaul at a 5-GHz radio of mesh. You can enable CleanAir on backhaul radios and can provide report interference details and air quality.

Role of the Cisco Wireless LAN Controller in a Cisco CleanAir System

The Cisco WLC 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. The Air Quality Report (AQR) contains information about the total interference from all identified sources represented by the 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 enables you to take action in cases where the interference due to unclassified interfering devices is more.
- 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.

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 interferences 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 Cisco WLC 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 stores the information in the Cisco WLC. 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 Cisco WLC to provide 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, thus enhancing 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 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 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.

- 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 Cisco 2500 Series Controllers.
- Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.

Configuring Cisco CleanAir

This section describes how to configure Cisco CleanAir on a controller and an access point. It contains the following sections:

Configuring Cisco CleanAir on the Controller

This section contains the following topics:

- Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (GUI), on page 5
- Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (CLI), on page 7

Configuring Cisco CleanAir on the Cisco Wireless LAN 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.

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 Cisco WLC 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 Cisco WLC 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 Cisco WLC. 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 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 Cisco WLC 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 Cisco WLC 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 Alarm Threshold (1 to 100)** that you want to set. An alarm is generated when the air quality reaches a threshold value. The default is 35. Valid range is from 1 and 100.

d) 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 threshond specified in the **AQI Alarm Threshold**.

Unclassified interferences are interferences that are detected but do not correspond to any of the identifiable interference types.

e) Enter the **Threshold for Unclassified category trap (1 to 99)**. Enter a value from 1 and 99. The default is 20. This is the severity index threshold for an unclassified interference category.

f) Select the **Enable Interference Type Trap** check box to trigger interferer alarms when the Cisco WLC detects specified device types, or unselect it to disable this feature. The default value is selected

g) 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 Cisco WLC 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**.

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, click **Change Settings**. The **802.11a (or 802.11b) > RRM > Dynamic Channel Assignment (DCA)** page appears.

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. 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.

e) Click **Apply**.

Step 9 Click **Save Configuration**.

Configuring Cisco CleanAir on the Cisco Wireless LAN Controller (CLI)

Step 1 Configure Cisco CleanAir functionality on the 802.11 network by entering this command:
config {**802.11a** | **802.11b**} **cleanair** {**enable** | **disable**} *all*

If you disable this feature, the Cisco WLC does not receive any spectrum data. The default value is enable.

Step 2 Enable CleanAir on all associated access points in a network:
config {**802.11a** | **802.11b**} **cleanair enable network**

You can enable CleanAir on a 5-GHz radio of mesh access points.

Step 3 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* 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)

Note Access points that are associated to the Cisco WLC 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 Cisco WLC or Prime Infrastructure. Filtering allows the system to resume normal performance levels.

Step 4 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 5 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 6 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 7 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 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 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 8 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 9 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 10 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 11 Enable persistent devices propagation by entering this command:
config advanced {**802.11a** | **802.11b**} **channel pda-prop** {**enable** | **disable**}

Step 12 Save your changes by entering this command:
save config

Step 13 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 14 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

Configuring Cisco CleanAir on an Access Point (GUI)

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.

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**.

Step 5 Click **Save Configuration**.

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 of Configuring Cisco CleanAir on an Access Point (GUI), on page 11 for descriptions of the spectrum management operation states and the possible error codes for the spectrum sensor state.

Monitoring the Interference Devices

This section describes how to monitor the interference devices of the 802.11a/n and 802.11b/g/n radio bands using the controller GUI or CLI.

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/n > Interference Devices** to open the CleanAir > Interference Devices page.
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.

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.

  Select 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**.
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*

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.

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*

Note No more than 25 interferers can be detected by a Cisco AP.

Detecting Persistent Sources of Interference

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*

Monitoring Persistent Devices (GUI)

To monitor persistent devices on a specific access point using the Cisco WLC 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*

Information similar to the following appears:

```
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 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 the Air Quality of Radio Bands

This section describes how to monitor the air quality of the 802.11a/n and 802.11b/g/n radio bands using both the Cisco WLC GUI and CLI.

Monitoring the Air Quality of Radio Bands (GUI)

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

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**

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*

Monitoring the Worst Air Quality of Radio Bands (GUI)

Step 1 Choose **Monitor** > **Cisco CleanAir** >**Worst Air-Quality** to open the **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 802.11 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 802.11 radio band.

Step 2 See 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 802.11 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**

Viewing the 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**

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

See the air quality information for a specific access point on the 802.11 radio band by entering this command:

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

Viewing the 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*

- 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 *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)

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 About 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 Prime Infrastructure or by manually launching it from the Cisco WLC. This section provides instructions for the latter.

Configuring Spectrum Expert (GUI)

Before You Begin

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

Step 2 Configure the access point for SE-Connect mode using the Cisco WLC 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 Cisco WLC 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 for 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 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 3 On the Windows PC, access the Cisco Software Center from this URL:
http://www.cisco.com/cisco/software/navigator.html

Step 4 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 5 Run the Spectrum Expert application on the PC.

Step 6 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 On the Cisco WLC GUI, the NSI key appears in the Network Spectrum Interface Key field (below the Port Number field) on the All APs > Details for page. To view the NSI key from the Cisco WLC CLI, enter the **show ap config** {**802.11a** | **802.11b**} *Cisco_AP* command.

When an access point in SE-Connect mode joins a Cisco WLC, it sends a Spectrum Capabilities notification message, and the Cisco WLC responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the Cisco WLC for use in NSI authentication. The Cisco WLC 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 Cisco WLC GUI shows the number of Spectrum Expert applications that are currently connected to the access point radio.

Step 7 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 8 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Related Documents

Related Topic	Document Title
• Cisco Prime Infrastructure Reports on CleanAir • To initiate a Spectrum Expert connection using Cisco Prime Infrastructure	Cisco Prime Infrastructure Configuration Guide URL: http://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html
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 of CleanAir

This table lists the release history for this feature.

Table 1: Feature History for 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.