



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, on page 1](#)
- [Monitoring the Interference Device \(GUI\), on page 1](#)
- [Monitoring the Interference Device \(CLI\), on page 3](#)
- [Monitoring Persistent Devices \(GUI\), on page 5](#)
- [Monitoring Persistent Devices \(CLI\), on page 5](#)
- [Monitoring the Air Quality of Radio Bands, on page 6](#)

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
```

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

- **802.11a**
- **802.11-inv**—A device using spectrally inverted Wi-Fi signals

- **802.11-nonstd**—A device using nonstandard Wi-Fi channels
 - **canopy**—A canopy bridge device
 - **cont-tx**—A continuous transmitter
 - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
 - **jammer**—A jamming device
 - **superag**—An 802.11 SuperAG device
 - **tdd-tx**—A time division duplex (TDD) transmitter
 - **video**—A video device
 - **wimax-fixed**—A WiMAX fixed device
 - **wimax-mobile**—A WiMAX mobile device
- **802.11b**
 - **bt-link**—A Bluetooth link device
 - **bt-discovery**—A Bluetooth discovery device
 - **ble-beacon**—A BLE beacon device
 - **mw-oven**—A microwave oven device
 - **802.11-fh**—An 802.11 frequency-hopping device
 - **802.15.4**—An 802.15.4 device
 - **tdd-tx**—A time division duplex (TDD) transmitter
 - **jammer**—A jamming device
 - **cont-tx**—A continuous transmitter
 - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
 - **video**—A video device
 - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
 - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
 - **superag**—An 802.11 SuperAG device
 - **canopy**—A canopy bridge device
 - **wimax-mobile**—A WiMAX mobile device
 - **wimax-fixed**—A WiMAX fixed device
 - **msft-xbox**—A Microsoft Xbox device

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)

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 is displayed.

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_1572_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 2020

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 controller 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 (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
```

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:

- **802.11a**
 - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
 - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
 - **canopy**—A canopy bridge device
 - **cont-tx**—A continuous transmitter

- **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
 - **jammer**—A jamming device
 - **superag**—An 802.11 SuperAG device
 - **tdd-tx**—A time division duplex (TDD) transmitter
 - **video**—A video device
 - **wimax-fixed**—A WiMAX fixed device
 - **wimax-mobile**—A WiMAX mobile device
- **802.11b**
- **bt-link**—A Bluetooth link device
 - **bt-discovery**—A Bluetooth discovery device
 - **ble-beacon**—A BLE beacon device
 - **mw-oven**—A microwave oven device
 - **802.11-fh**—An 802.11 frequency-hopping device
 - **802.15.4**—An 802.15.4 device
 - **tdd-tx**—A time division duplex (TDD) transmitter
 - **jammer**—A jamming device
 - **cont-tx**—A continuous transmitter
 - **dect-like**—A digital enhanced cordless communication (DECT)-compatible phone
 - **video**—A video device
 - **802.11-inv**—A device using spectrally inverted Wi-Fi signals
 - **802.11-nonstd**—A device using nonstandard Wi-Fi channels
 - **superag**—An 802.11 SuperAG device
 - **canopy**—A canopy bridge device
 - **wimax-mobile**—A WiMAX mobile device
 - **wimax-fixed**—A WiMAX fixed device
 - **msft-xbox**—A Microsoft Xbox device

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
```

