Wireless Quality of Service

CleanAir

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.

Detecting Interferers by an Access Point

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.

Prerequisites for CleanAir

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

Only Cisco CleanAir-enabled access points using the following access point modes can perform Cisco CleanAir spectrum monitoring:

- Local—In this mode, each Cisco CleanAir-enabled access point radio provides air quality and interference detection reports for the current operating channel only.
- 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. All CleanAir system functionality is suspended while the AP is in this mode, and no clients are served. This mode is intended for remote troubleshooting only. Up to three active Spectrum Expert connections are possible.

Restrictions on CleanAir

- Access points in monitor mode do not transmit Wi-Fi traffic or 802.11 packets. They are excluded from radio resource management (RRM) planning and are not included in the neighbor access point list. IDR clustering depends on the 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.
- Monitor Mode access point in slot 2 operates at 2.4 GHz only.
- Cisco recommends a ratio of 1 monitor mode access point for every 5 local mode access points, this may also vary based on the network design and expert guidance for best coverage.
- Do not connect access points in SE connect mode directly to any physical port on Cisco 2500 Series Cisco WLCs.
- Spectrum Expert (Windows XP laptop client) and AP should be pingable, otherwise; it will not work.

Configuring Cisco CleanAir on the Controller

Configuring Cisco CleanAir on Cisco WLC (GUI)

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

Step 2 Check the **CleanAir** check box to enable Cisco CleanAir functionality on the 802.11a/n or 802.11b/g/n network, or uncheck it to prevent the Cisco WLC from detecting spectrum interference. By default, this feature is in disabled state.

Step 3 Check the **Report Interferers** check box to enable the Cisco CleanAir system to report any detected sources of interference, or uncheck it to prevent the Cisco WLC from reporting interferers. By default, this feature is in enabled state.

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

Step 4 Check 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 APs 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. 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/ac only)
- **WiMAX Mobile—**A WiMAX mobile device (802.11a/n/ac only)
- **XBox—**A Microsoft Xbox (802.11b/g/n only)

Note When you include BLE Beacon in the **Interferences to Detect** list, the 2.4GHz serving radio periodically goes off channel for a scan.

Note APs 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) Check the **Enable AQI (Air Quality Index) Trap** check box to enable the triggering of air quality alarms, or uncheck the box to disable this feature. By default, this feature is in enabled state.

b) If you checked the **Enable AQI Trap** check box in *Step a*, enter a value between 1 and 100 (inclusive) in the **AQI Alarm Threshold** field 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) Check 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** field. 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) Check the **Enable Interference Type Trap** check box to trigger interferer alarms when the Cisco WLC detects specified device types, or uncheck it to disable this feature. By default, this feature is in enabled state.

g) Ensure 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. 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, check 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 AP 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 is displayed.

c) Check the **EDRRM** check box to trigger RRM to run when an AP detects a certain level of interference, or uncheck it to disable this feature. By default, this feature is in enabled state.

d) If you checked 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 AP rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected AP 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) To configure rogue duty cycle, check the **Rogue Contribution** check box and then specify the **Rogue Duty-Cycle** in terms of percentage. The default value of **Rogue Duty-Cycle** is 80%.
f) Save the configuration.

Configuring Cisco CleanAir on Cisco WLC (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. By default, this feature is in disabled state.

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 Configure and monitor Interference Awareness by entering the following commands:

- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event** {**enable** | **disable**}
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution** {**enable** | **disable**}
- **config advanced** {**802.11a** | **802.11b**} **channel cleanair-event rogue-contribution duty-cycle** *value*
- **show** {**802.11a** | **802.11b**} **cleanair config**
- **debug airewave-director profile enable**
- **debug airewave-director channel enable**

Step 12 Enable persistent devices propagation by entering this command:
config advanced {**802.11a** | **802.11b**} **channel pda-prop** {**enable** | **disable**}

Step 13 Save your changes by entering this command:
save config

Step 14 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 15 See the spectrum event-driven RRM configuration for the 802.11a/n/ac 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/ac or 802.11b/g/n** to open the 802.11a/n/ac (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/ac (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/ac (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/ac (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/ac 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/ac 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/ac 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 12 for descriptions of the spectrum management operation states and the possible error codes for the spectrum sensor state.

Monitoring Interference Devices

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/ac 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/ac 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/ac 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/ac or 802.11b/g/n** to open the 802.11a/n/ac (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/ac (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/ac 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/ac 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/ac 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/ac 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/ac 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/ac 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/ac 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/ac 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/ac 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/ac 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/ac** or **802.11b/g/n** to open the 802.11a/n/ac (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/ac (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/ac 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/ac 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/ac 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/ac or 802.11b/g/n radio band by entering this command:

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

Media and EDCA

Aggressive Load Balancing

Information About Configuring Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

Note Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. The code 17 indicates that the AP is busy. The AP does not respond with an association response bearing 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is exceeded, and another less busy AP heard the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

Note Voice Client does not authenticate when delay is configured more than 300 ms. To avoid this configure a Central-Auth, Local Switching WLAN with CCKM, configure a Pagent Router between AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN and try associating the voice client

Passive scanning clients will be able to associate to an AP irrespective of whether load balancing is enabled or not.

Note Cisco 600 Series OfficeExtend Access Points do not support client load balancing.

With the 7.4 release, FlexConnect access points do support client load balancing.

You can configure the controller to analyze the WAN interface utilization of neighboring APs and then load balance the clients across the lightly loaded APs. You can configure this by defining a load balancing threshold. By defining the threshold, you can measure the WAN interface utilization percentage. For example, a threshold value of 50 triggers the load balancing upon detecting utilization of 50% or more on an AP-WAN interface.

Note For a FlexConnect AP the association is locally handled. The load-balancing decisions are taken at the Cisco WLC. A FlexConnect AP initially responds to the client before knowing the result of calculations at the Cisco WLC. Load-balancing doesn't take effect when the FlexConnect AP is in standalone mode.

FlexConnect AP does not send (re)association response with status 17 for Load-Balancing as Local mode APs do; instead, it first sends (re)association with status 0 (success) and then deauth with reason 5.

Configuring Aggressive Load Balancing (GUI)

Step 1 Choose **Wireless** > **Advanced** > **Load Balancing** to open the Load Balancing page.

Step 2 In the Client Window Size text box, enter a value between 1 and 20.
The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing window + client associations on AP with the lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 3 In the Maximum Denial Count text box, enter a value between 0 and 10.
The denial count sets the maximum number of association denials during load balancing.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 To enable or disable aggressive load balancing on specific WLANs, do the following:

a) Choose **WLANs** > **WLAN ID**. The WLANs > Edit page appears.

b) In the **Advanced** tab, select or unselect the **Client Load Balancing** check box.
c) Click **Apply**.
d) Click **Save Configuration**.

Configuring Aggressive Load Balancing (CLI)

Step 1 Set the client window for aggressive load balancing by entering this command:
config load-balancing window *client_count*

You can enter a value between 0 and 20 for the *client_count* parameter.

Step 2 Set the denial count for load balancing by entering this command:
config load-balancing denial *denial_count*

You can enter a value between 1 and 10 for the *denial_count* parameter.

Step 3 Save your changes by entering this command:
save config

Step 4 Enable or disable aggressive load balancing on specific WLANs by entering this command:
config wlan load-balance allow {**enable** | **disable**} *wlan_ID*

You can enter a value between 1 and 512 for *wlan_ID* parameter.

Step 5 Verify your settings by entering this command:
show load-balancing

Step 6 Save your changes by entering this command:
save config

Step 7 Configure the load balance mode on a WLAN by entering this command:
config wlan load-balance mode {*client-count* | *uplink-usage*} *wlan-id*

This feature requires the AP to upload its uplink usage statistics to the controller periodically. Check these statistics by entering this command:

show ap stats system *cisco-AP*

Media Session and Snooping

Information About Media Session Snooping and Reporting

This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the controller and Cisco Prime Infrastructure. You can enable or disable Voice over IP (VoIP) snooping and reporting for each WLAN.

When you enable VoIP Media Session Aware (MSA) snooping, the access point radios that advertise this WLAN look for SIP voice packets that comply with SIP RFC 3261. They do not look for non-RFC 3261-compliant SIP voice packets or Skinny Call Control Protocol (SCCP) voice packets. Any SIP packets destined to or originating from port number 5060 (the standard SIP signaling port) are considered for further inspection. The access points track when Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, are already on an active call, or are in the process of ending a call. Upstream packet classification for both client types occurs at the access point. Downstream packet classification occurs at the controller for WMM clients and at the access point for non-WMM clients. The access points notify the controller and Cisco Prime Infrastructure of any major call events, such as call establishment, termination, and failure.

The controller provides detailed information for VoIP MSA calls. For failed calls, the controller generates a trap log with a timestamp and the reason for failure (in the GUI) and an error code (in the CLI) to aid in troubleshooting. For successful calls, the controller shows the number and duration of calls for usage tracking purposes. Cisco Prime Infrastructure displays failed VoIP call information in the Events page.

Restrictions for Media Session Snooping and Reporting

Controller software release 6.0 or later releases support Voice over IP (VoIP) Media Session Aware (MSA) snooping and reporting.

Configuring Media Session Snooping (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure media session snooping.

Step 3 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 4 Under Voice, select the **Media Session Snooping** check box to enable media session snooping or unselect it to disable this feature. The default value is unselected.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Step 7 See the VoIP statistics for your access point radios as follows:

a) Choose **Monitor** > **Access Points** > **Radios** > **802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.

b) Scroll to the right and click the **Detail** link for the access point for which you want to view VoIP statistics. The **Radio > Statistics** page appears.
The VoIP Stats section shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the controller.

Step 8 Choose **Management** > **SNMP** > **Trap Logs** to see the traps generated for failed calls. The Trap Logs page appears. For example, log 0 in the figure shows that a call failed. The log provides the date and time of the call, a description of the failure, and the reason why the failure occurred.

Configuring Media Session Snooping (CLI)

Step 1 Enable or disable VoIP snooping for a particular WLAN by entering this command:
config wlan call-snoop {**enable** | **disable**} *wlan_id*

Step 2 Save your changes by entering this command:
save config

Step 3 See the status of media session snooping on a particular WLAN by entering this command:
show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
...
 FlexConnect Local Switching....................... Disabled
    FlexConnect Learn IP Address..................... Enabled
    Infrastructure MFP protection.............. Enabled (Global Infrastructure MFP
Disabled)
 Client MFP..................................... Optional
    Tkip MIC Countermeasure Hold-down Timer....... 60
Call Snooping.................................... Enabled
```

Step 4 See the call information for an MSA client when media session snooping is enabled and the call is active by entering this command:
show call-control client callInfo *client_MAC_address*

Information similar to the following appears:

```
Uplink IP/port..................................... 192.11.1.71 / 23870
Downlonk IP/port................................... 192.12.1.47 / 2070
UP................................................. 6
Calling Party...................................... sip:1054
Called Party....................................... sip:1000
Call ID............................................ 58635b00-850161b7-14853-1501a8
Number of calls for given client is.............. 1
```

Step 5 See the metrics for successful calls or the traps generated for failed calls by entering this command:
show call-control ap {**802.11a** | **802.11b**} *Cisco_AP* {**metrics** | **traps**}

Information similar to the following appears when you enter **show call-control ap** {**802.11a** | **802.11b**} *Cisco_AP* **metrics**:

```
Total Call Duration in Seconds.................. 120
Number of Calls................................. 10
```

Information similar to the following appears when you enter **show call-control ap** {**802.11a** | **802.11b**} *Cisco_AP* **traps**:

```
Number of traps sent in one min.................. 2
Last SIP error code.............................. 404
Last sent trap timestamp..................... Jun 20 10:05:06
```

To aid in troubleshooting, the output of this command shows an error code for any failed calls. This table explains the possible error codes for failed calls.

Table 1: Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotallowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.
406	notAcceptabl	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header text box sent in the request.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time, if it could not determine the location of the user in time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.

Error Code	Integer	Description
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header text box.
480	temporarilyNotAvailable	The callee's end system was contacted successfully, but the callee is currently unavailable.
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header text box with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.

Error Code	Integer	Description
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

Note If you experience any problems with media session snooping, enter the **debug call-control** {**all** | **event**} {**enable** | **disable**} command to debug all media session snooping messages or events.

QoS Enhanced BSS

Prerequisites for Using QoS Enhanced BSS on Cisco 7921 and 7920 Wireless IP Phones

Follow these guidelines to use Cisco 7921 and 7920 Wireless IP Phones with controllers:

- Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11b dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The 7921 or 7920 phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- Both the 7921 and 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7921 or 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7921 or 7920.
- For standalone 7921 phones, load-based CAC must be enabled, and the WMM Policy must be set to Required on the WLAN.
- The controller supports traffic classification (TCLAS) coming from 7921 phones using firmware version 1.1.1. This feature ensures proper classification of voice streams to the 7921 phones.

- When using a 7921 phone with the 802.11a radio of a 1242 series access point, set the 24-Mbps data rate to Supported and choose a lower Mandatory data rate (such as 12 Mbps). Otherwise, the phone might experience poor voice quality.

Information About QoS Enhanced BSS

The QoS Enhanced Basis Service Set (QBSS) information element (IE) enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7921 or 7920 phone uses the QBSS value to determine if they should associate to another access point. You can enable QBSS in these two modes:

- Wi-Fi Multimedia (WMM) mode, which supports devices that meet the 802.11E QBSS standard (such as Cisco 7921 IP Phones)
- 7920 support mode, which supports Cisco 7920 IP Phones on your 802.11b/g network

  The 7920 support mode has two options:

  - Support for 7920 phones that require call admission control (CAC) to be configured on and advertised by the client device (these are typically older 7920 phones)
  - Support for 7920 phones that require CAC to be configured on and advertised by the access point (these are typically newer 7920 phones)

    When access point-controlled CAC is enabled, the access point sends out a Cisco proprietary CAC Information Element (IE) and does not send out the standard QBSS IE.

Restrictions for QoS Enhanced BSS

- The OEAP 600 Series access points do not support CAC.
- QBSS is disabled by default.
- 7920 phones are non-WMM phones with limited CAC functionality. The phones look at the channel utilization of the access point to which they are associated and compare that to a threshold that is beaconed by the access point. If the channel utilization is less than the threshold, the 7920 places a call. In contrast, 7921 phones are full-fledged WMM phones that use traffic specifications (TSPECs) to gain access to the voice queue before placing a phone call. The 7921 phones work well with load-based CAC, which uses the percentage of the channel set aside for voice and tries to limit the calls accordingly.

  Because 7921 phones support WMM and 7920 phones do not, capacity and voice quality problems can arise if you do not properly configure both phones when they are used in a mixed environment. To enable both 7921 and 7920 phones to co-exist on the same network, make sure that load-based CAC and 7920 AP CAC are both enabled on the controller and the WMM Policy is set to Allowed. These settings become particularly important if you have many more 7920 users than 7921 users.
- We recommend that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, if the handset is refused at its first reassociation attempt.

Configuring QBSS (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure WMM mode.

Step 3 When the **WLANs > Edit** page appears, choose the **QoS** tab to open the **WLANs > Edit (Qos)** page.

Step 4 From the WMM Policy drop-down list, choose one of the following options, depending on whether you want to enable WMM mode for 7921 phones and other devices that meet the WMM standard:

- **Disabled—**Disables WMM on the WLAN. This is the default value.
- **Allowed—**Allows client devices to use WMM on the WLAN.
- **Required—**Requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5 Select the **7920 AP CAC** check box if you want to enable 7920 support mode for phones that require access point-controlled CAC. The default value is unselected.

Step 6 Select the **7920 Client CAC** check box if you want to enable 7920 support mode for phones that require client-controlled CAC. The default value is unselected.

Note You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

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

Step 8 Click **Save Configuration** to save your changes.

Configuring QBSS (CLI)

Step 1 Determine the ID number of the WLAN to which you want to add QBSS support by entering this command:
show wlan summary

Step 2 Disable the WLAN by entering this command:
config wlan disable *wlan_id*

Step 3 Configure WMM mode for 7921 phones and other devices that meet the WMM standard by entering this command:
config wlan wmm {**disabled** | **allowed** | **required**} *wlan_id*

where

- **disabled** disables WMM mode on the WLAN.
- **allowed** allows client devices to use WMM on the WLAN.
- **required** requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 4 Enable or disable 7920 support mode for phones that require client-controlled CAC by entering this command:
config wlan 7920-support client-cac-limit {**enable** | **disable**} *wlan_id*

Note You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Step 5 Enable or disable 7920 support mode for phones that require access point-controlled CAC by entering this command:
config wlan 7920-support ap-cac-limit {**enable** | **disable**} *wlan_id*

Step 6 Reenable the WLAN by entering this command:
config wlan enable *wlan_id*

Step 7 Save your changes by entering this command:
save config

Step 8 Verify that the WLAN is enabled and the Dot11-Phone Mode (7920) text box is configured for compact mode by entering this command:
show wlan *wlan_id*

Reanchoring of Roaming Voice Clients

Information About Reanchoring of Roaming Voice Clients

You can allow voice clients to get anchored on the best suited and nearest available controller, which is useful when intercontroller roaming occurs. By using this feature, you can avoid the use of tunnels to carry traffic between the foreign controller and the anchor controller and remove unnecessary traffic from the network.

The ongoing call during roaming is not affected and can continue without any problem. The traffic passes through proper tunnels that are established between the foreign controller and the anchor controller. Disassociation occurs only after the call ends, and then the client then gets reassociated to a new controller.

Note You can reanchor roaming of voice clients for each WLAN.

Restrictions for Configuring Reanchoring of Roaming Voice Clients

- The ongoing data session might be affected due to disassociation and then reassociation.
- This feature is supported for TSPEC-based calls and non-TSPEC SIP-based calls only when you enable the admission control.
- This feature is not recommended for use on Cisco 792x phones.

Configuring Reanchoring of Roaming Voice Clients (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure reanchoring of roaming voice clients.

Step 3 When the WLANs > Edit page appears, choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

Step 4 In the Voice area select the **Re-anchor Roamed Clients** check box.

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

Step 6 Click **Save Configuration** to save your changes.

Configuring Reanchoring of Roaming Voice Clients (CLI)

Step 1 Enable or disable reanchoring of roaming voice clients for a particular WLAN by entering this command:
config wlan roamed-voice-client re-anchor {enable | disable} *wlan id*

Step 2 Save your changes by entering this command:
save config

Step 3 See the status of reanchoring roaming voice client on a particular WLAN by entering this command:
show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
...
Call Snooping.................................... Enabled
Roamed Call Re-Anchor Policy..................... Enabled
Band Select...................................... Disabled
Load Balancing................................... Disabled
```

Step 4 Save your changes by entering this command:
save config

Call Admission Control

Information About Configuring Voice and Video Parameters

Three parameters on the controller affect voice and/or video quality:

- Call admission control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

Each of these parameters is supported in Cisco Compatible Extensions (CCX) v4 and v5.

Note Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi Multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, in order to maintain QoS under differing network loads, CAC in CCXv4 is required. Two types of CAC are available: bandwidth-based CAC and load-based CAC.

Note CAC is not supported in Flexconnect local auth, resulting in voice traffic not getting properly tagged.

Expedited Bandwidth Requests

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both bandwidth-based and load-based CAC. Expedited bandwidth requests are disabled by default. When this feature is disabled, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

This table lists examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 2: TSPEC Request Handling Examples

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Bandwidth-based CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

1 For bandwidth-based CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.
2 Bandwidth-based CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Note Admission control for TSPEC g711-40ms codec type is supported.

Note When video ACM is enabled, the controller rejects a video TSPEC if the non-MSDU size in the TSPEC is greater than 149 or the mean data rate is greater than 1 Kbps.

U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Traffic Stream Metrics

In a voice-over-wireless LAN (VoWLAN) deployment, traffic stream metrics (TSM) can be used to monitor voice-related metrics on the client-access point air interface. It reports both packet latency and packet loss. You can isolate poor voice quality issues by studying these reports.

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour's worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

TSM can be configured through either the GUI or the CLI on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

Note Access points support TSM entries in both local and FlexConnect modes.

Table 3: TSM Entries in Cisco 5508 and Flex 7510 WLCs

TSM Entries	5508	Flex 7510
MAX AP TSM entries	100	100
MAX Client TSM entries	250	250
MAX TSM entries	100*250=25000	100*250=25000

Note Once the upper limit is reached, additional TSM entries cannot be stored and sent to Cisco Prime Infrastructure. If client TSM entries are full and AP TSM entries are available, then only the AP entries are stored, and vice versa. This leads to partial output. TSM cleanup occurs every one hour. Entries are removed only for those APs and clients that are not in the system.

Configuring Voice Parameters

Configuring Voice Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Platinum QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, unselect the 802.11a (or 802.11b/g) Network Status check box, and click **Apply** to disable the radio network.

Step 4 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media page appears. The Voice tab is displayed by default.

Step 5 Select the **Admission Control (ACM)** check box to enable bandwidth-based CAC for this radio band. The default value is disabled.

Step 6 Select the **Admission Control (ACM)** you want to use by choosing from the following choices:

- **Load-based—**To enable channel-based CAC. This is the default option.
- **Static—**To enable radio-based CAC.

Step 7 In the **Max RF Bandwidth** text box, enter the percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band.
The range is 5% to 85%. The sum of maximum bandwidth percentage of voice and video should not exceed 85%.

The default is 75%.

Step 8 In the **Reserved Roaming Bandwidth** text box, enter the percentage of maximum allocated bandwidth that is reserved for roaming voice clients. The controller reserves this bandwidth from the maximum allocated bandwidth for roaming voice clients.
The range is 0% to 25%.

The default is 6%.

Step 9 To enable expedited bandwidth requests, select the **Expedited Bandwidth** check box. By default, this text box is disabled.

Step 10 To enable SIP CAC support, select the **SIP CAC Support** check box. By default, SIP CAC support is disabled.

Step 11 From the **SIP Codec** drop-down list, choose one of the following options to set the codec name. The default value is G.711. The options are as follows:

- User Defined
- G.711
- G.729

Step 12 In the **SIP Bandwidth (kbps)** text box, enter the bandwidth in kilobits per second.
The possible range is 8 to 64.

The default value is 64.

Note The **SIP Bandwidth (kbps)** text box is highlighted only when you select the SIP codec as User-Defined. If you choose the SIP codec as G.711, the **SIP Bandwidth (kbps)** text box is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (kbps) text box is set to 8.

Step 13 In the **SIP Voice Sample Interval (msecs)** text box, enter the value for the sample interval.

Step 14 In the **Maximum Calls** text box, enter the maximum number of calls that can be made to this radio. The maximum call limit includes both direct and roaming-in calls. If the maximum call limit is reached, the new or roaming-in calls result in failure.
The possible range is 0 to 25.

The default value is 0, which indicates that there is no check for maximum call limit.

Note If SIP CAC is supported and the CAC method is static, the Maximum Possible Voice Calls and Maximum Possible Roaming Reserved Calls fields appear.

Step 15 Select the **Metrics Collection** check box to collect traffic stream metrics. By default, this box is unselected. That is, the traffic stream metrics is not collected by default.

Step 16 Click **Apply**.

Step 17 Reenable all WMM WLANs and click **Apply**.

Step 18 Choose **Network** under 802.11a/n/ac or 802.11b/g/n, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to reenable the radio network.

Step 19 Click **Save Configuration**.

Step 20 Repeat this procedure if you want to configure voice parameters for another radio band.

Configuring Voice Parameters (CLI)

Before You Begin

Ensure that you have configured SIP-based CAC.

Step 1 See all of the WLANs configured on the controller by entering this command:
show wlan summary

Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Platinum by entering this command:
show wlan *wlan_id*

Step 3 Disable all WLANs with WMM enabled prior to changing the voice parameters by entering the command:
config wlan disable *wlan_id*

Step 4 Disable the radio network by entering this command:
config {**802.11a** | **802.11b**} **disable network**

Step 5 Save your settings by entering this command:
save config

Step 6 Enable or disable bandwidth-based voice CAC for the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac voice acm** {**enable** | **disable**}

Step 7 Set the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac voice max-bandwidth** *bandwidth*

The *bandwidth* range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new calls on this network.

Step 8 Set the percentage of maximum allocated bandwidth reserved for roaming voice clients by entering this command:
config {**802.11a** | **802.11b**} **cac voice roam-bandwidth** *bandwidth*

The *bandwidth* range is 0 to 25%, and the default value is 6%. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.

Step 9 Configure the codec name and sample interval as parameters and to calculate the required bandwidth per call by entering this command:
config {**802.11a** | **802.11b**} **cac voice sip codec** {**g711** | **g729**} **sample-interval** *number_msecs*

Step 10 Configure the bandwidth that is required per call by entering this command:
config {**802.11a** | **802.11b**} **cac voice sip bandwidth** *bandwidth_kbps* **sample-interval** *number_msecs*

Step 11 Reenable all WLANs with WMM enabled by entering this command:
config wlan enable *wlan_id*

Step 12 Reenable the radio network by entering this command:
config {**802.11a** | **802.11b**} **enable network**

Step 13 View the TSM voice metrics by entering this command:
show [802.11a | 802.11b] cu-metrics *AP_Name*

The command also displays the channel utilization metrics.

Step 14 Enter the **save config** command to save your settings.

Configuring Video Parameters

Configuring Video Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Gold QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 4 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media page appears.

Step 5 In the **Video** tab, select the **Admission Control (ACM)** check box to enable video CAC for this radio band. The default value is disabled.

Step 6 From the **CAC Method** drop-down list, choose between **Static** and **Load Based** methods.
The static CAC method is based on the radio and the load-based CAC method is based on the channel.

Note For TSpec and SIP based CAC for video calls, only Static method is supported.

Step 7 In the **Max RF Bandwidth** text box, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. When the client reaches the value specified, the access point rejects new requests on this radio band.
The range is 5% to 85%. The sum of maximum bandwidth percentage of voice and video should not exceed 85%. The default is 0%.

Step 8 In the Reserved Roaming Bandwidth text box, enter the percentage of the maximum RF bandwidth that is reserved for roaming clients for video.

Step 9 Configure the SIP CAC Support by selecting or unselecting the **SIP CAC Support** check box.
SIP CAC is supported only if SIP Snooping is enabled.

Note You cannot enable SIP CAC if you have selected the Load Based CAC method.

Step 10 Click **Apply**.

Step 11 Reenable all WMM WLANs and click **Apply**.

Step 12 Choose **Network** under 802.11a/n/ac or 802.11b/g/n, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to reenable the radio network.

Step 13 Click **Save Configuration**.

Step 14 Repeat this procedure if you want to configure video parameters for another radio band.

Configuring Video Parameters (CLI)

Before You Begin

Ensure that you have configured SIP-based CAC.

Step 1 See all of the WLANs configured on the controller by entering this command:
show wlan summary

Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Gold by entering this command:
show wlan *wlan_id*

Step 3 Disable all WLANs with WMM enabled prior to changing the video parameters by entering this command:
config wlan disable *wlan_id*

Step 4 Disable the radio network by entering this command:
config {**802.11a** | **802.11b**} **disable network**

Step 5 Save your settings by entering this command:
save config

Step 6 Enable or disable video CAC for the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac video acm** {**enable** | **disable**}

Step 7 To configure the CAC method as either static or load-based, enter this command:

config {**802.11a** | **802.11b**} **cac video cac-method** {**static** | **load-based**}

Step 8 Set the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac video max-bandwidth** *bandwidth*

The *bandwidth* range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.

Note If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

Step 9 To configure the percentage of the maximum RF bandwidth that is reserved for roaming clients for video, enter this command:
config {**802.11a** | **802.11b**} **cac video roam-bandwidth** *bandwidth*

Step 10 To configure the CAC parameters for SIP-based video calls, enter this command:
config {**802.11a** | **802.11b**} **cac video sip** {**enable** | **disable**}

Step 11 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command:
config {**802.11a** | **802.11b**} **cac video tspec-inactivity-timeout** {**enable** | **ignore**}

Step 12 Reenable all WLANs with WMM enabled by entering this command:
config wlan enable *wlan_id*

Step 13 Reenable the radio network by entering this command:
config {**802.11a** | **802.11b**} **enable network**

Step 14 Enter the **save config** command to save your settings.

Viewing Voice and Video Settings

Viewing Voice and Video Settings (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client to open the Clients > Detail page.
This page shows the U-APSD status (if enabled) for this client under Quality of Service Properties.

Step 3 Click **Back** to return to the Clients page.

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated as follows:

a) Hover your cursor over the blue drop-down arrow for the desired client and choose **802.11aTSM** or **802.11b/g TSM**. The Clients > AP page appears.

b) Click the **Detail** link for the desired access point to open the Clients > AP > Traffic Stream Metrics page.
This page shows the TSM statistics for this client and the access point to which it is associated. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point, as follows:

a) Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n/ac** or **802.11b/g/n**. The 802.11a/n/ac Radios or 802.11b/g/n Radios page appears.
b) Hover your cursor over the blue drop-down arrow for the desired access point and choose **802.11aTSM** or **802.11b/g TSM**. The AP > Clients page appears.
c) Click the **Detail** link for the desired client to open the AP > Clients > Traffic Stream Metrics page.
This page shows the TSM statistics for this access point and a client associated to it. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Viewing Voice and Video Settings (CLI)

Step 1 See the CAC configuration for the 802.11 network by entering this command:
show ap stats {**802.11a** | **802.11b**}

Step 2 See the CAC statistics for a particular access point by entering this command:
show ap stats {802.11a | 802.11b} *ap_name*

Information similar to the following appears:

```
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)..... 0
Total channel MT free..................... 0
Total voice MT free....................... 0
Na Direct................................. 0
Na Roam................................... 0
  Video Bandwidth in use(% of config bw)..... 0
  Total num of voice calls in progress...... 0
  Num of roaming voice calls in progress..... 0
  Total Num of voice calls since AP joined..... 0
  Total Num of roaming calls since AP joined..... 0
 Total Num of exp bw requests received..... 5
  Total Num of exp bw requests admitted..... 2

Num of voice calls rejected since AP joined..... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to insufficient bw....0
  Num of calls rejected due to invalid params.... 0
  Num of calls rejected due to PHY rate..... 0
  Num of calls rejected due to QoS policy..... 0
```

In the example above, “MT” is medium time, “Na” is the number of additional calls, and “exp bw” is expedited bandwidth.

Note Suppose an AP has to be rebooted when a voice client associated with the AP is on an active call. After the AP is rebooted, the client continues to maintain the call, and during the time the AP is down, the database is not refreshed by the controller. Therefore, we recommend that all active calls are ended before the AP is taken down.

Step 3 See the U-APSD status for a particular client by entering this command:

show client detail *client_mac*

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated by entering this command:
show client tsm {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**}

The optional **all** command shows all access points to which this client has associated. Information similar to the following appears:

```
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec).............................10
      Maximum Lost Packet count(5sec)............................5
      Average Lost Packet count(5secs)...........................2
    DownLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec).............................10
      Maximum Lost Packet count(5sec)............................5
      Average Lost Packet count(5secs)...........................2
```

Note The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Note Clear the TSM statistics for a particular access point or all the access points to which this client is associated by entering this **clear client tsm** {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**} command.

Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point by entering this command:
show ap stats {**802.11a** | **802.11b**} *ap_name* **tsm** {*client_mac* | **all**}

The optional **all** command shows all clients associated to this access point. Information similar to the following appears:

```
AP Interface Mac:                   00:0b:85:01:02:03
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
```

```
    Average Delay (5sec intervals).....................35
    Delay less than 10 ms..............................20
    Delay bet 10 - 20 ms...............................20
    Delay bet 20 - 40 ms...............................20
    Delay greater than 40 ms...........................20
   Total packet Count..................................80
   Total packet lost count (5sec).....................10
   Maximum Lost Packet count(5sec).....................5
   Average Lost Packet count(5secs)....................2
DownLink Stats
================
    Average Delay (5sec intervals).....................35
    Delay less than 10 ms..............................20
    Delay bet 10 - 20 ms...............................20
    Delay bet 20 - 40 ms...............................20
    Delay greater than 40 ms...........................20
   Total packet Count..................................80
   Total packet lost count (5sec).....................10
   Maximum Lost Packet count(5sec).....................5
   Average Lost Packet count(5secs)....................2
```

Note The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 6 Enable or disable debugging for call admission control (CAC) messages, events, or packets by entering this command: **debug cac** {**all** | **event** | **packet**} {**enable** | **disable**}

where **all** configures debugging for all CAC messages, **event** configures debugging for all CAC events, and **packet** configures debugging for all CAC packets.

Step 7 Use the following command to perform voice diagnostics and to view the debug messages between a maximum of two 802.11 clients:
debug voice-diag {**enable** | **disable**} *mac-id mac-id2* [**verbose**]

The verbose mode is an optional argument. When the verbose option is used, all debug messages are displayed in the console. You can use this command to monitor a maximum of two 802.11 clients. If one of the clients is a non-WiFi client, only the 802.11 client is monitored for debug messages.

Note It is implicitly assumed that the clients being monitored are on call.

Note The debug command automatically stops after 60 minutes.

Step 8 Use the following commands to view various voice-related parameters:

- **show client voice-diag status**

  Displays information about whether voice diagnostics is enabled or disabled. If enabled, will also displays information about the clients in the watch list and the time remaining for the diagnostics of the voice call.

  If voice diagnostics is disabled when the following commands are entered, a message indicating that voice diagnostics is disabled appears.

- **show client voice-diag tspec**

  Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.

- **show client voice-diag qos-map**

Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.

- **show client voice-diag avrg_rssi**

  Display the client's RSSI values in the last 5 seconds when voice diagnostics is enabled.

- **show client voice-diag roam-history**

  Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, the reason for the roaming-failure.

- **show client calls {active | rejected} {802.11a | 802.11bg | all}**

  This command lists the details of active TSPEC and SIP calls on the controller.

Step 9 Use the following commands to troubleshoot video debug messages and statistics:

- **debug ap show stats {802.11b | 802.11a}** *ap-name* **multicast—**Displays the access point's supported multicast rates.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **load—**Displays the access point's QBSS and other statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **tx-queue—**Displays the access point's transmit queue traffic statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **client** {**all** | **video** | *client-mac*}**—**Displays the access point's client metrics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name packet***—**Displays the access point's packet statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **video metrics—**Displays the access point's video metrics.
- **debug ap show stats video** *ap-name* **multicast mgid** *number* **—**Displays an access point's Layer 2 MGID database number.
- **debug ap show stats video** *ap-name* **admission—**Displays an access point's admission control statistics.
- **debug ap show stats video** *ap-name* **bandwidth—**Displays an access point's video bandwidth.

Configuring SIP-Based CAC

Restrictions for SIP-Based CAC

- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

Configuring SIP-Based CAC (GUI)

Before You Begin

- Ensure that you have set the voice to the platinum QoS level.
- Ensure that you have enabled call snooping for the WLAN.
- Ensure that you have enabled the Admission Control (ACM) for this radio.

Step 1 Choose **Wireless** > **Advanced** > **SIP Snooping** to open the SIP Snooping page.

Step 2 Specify the call-snooping ports by entering the starting port and the ending port.

Step 3 Click **Apply** and then click **Save Configuration**.

Configuring SIP-Based CAC (CLI)

Step 1 Set the voice to the platinum QoS level by entering this command:
config wlan qos *wlan-id* **Platinum**

Step 2 Enable the call-snooping feature for a particular WLAN by entering this command:
config wlan call-snoop enable *wlan-id*

Step 3 Enable the ACM to this radio by entering this command:
config {**802.11a** | **802.11b**} **cac** {**voice** | **video**} **acm enable**

Step 4 To configure the call snooping ports, enter this command:
config advanced sip-snooping-ports *starting-port ending-port*

Step 5 To troubleshoot SIP-based CAC events, enter this command:
debug sip event {**enable** | **disable**}

Configuring Media Parameters

Configuring Media Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Gold QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 4 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media > Parameters page appears.

Step 5 Choose the **Media** tab to open the Media page.

Step 6 Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.

Step 7 In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches the specified value, the access point rejects new calls on this radio band.
The default value is 85%; valid values are from 0 to 85%.

Step 8 In the **Client Phy Rate** text box, enter the value for the rate in kilobits per second at which the client operates.

Step 9 In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of the maximum retry. The default value is 80.

Step 10 Select the **Multicast Direct Enable** check box to enable the **Multicast Direct Enable** text box. The default value is enabled.

Step 11 From the **Max Streams per Radio** drop-down list, choose the maximum number of allowed multicast direct streams per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.

Step 12 From the **Max Streams per Client** drop-down list, choose the maximum number of allowed clients per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.

Step 13 If you want to enable the best radio queue for this radio, select the **Best Effort QoS Admission** check box. The default value is disabled.

Configuring Voice Prioritization Using Preferred Call Numbers

Information About Configuring Voice Prioritization Using Preferred Call Numbers

You can configure a controller to support calls from clients that do not support TSPEC-based calls. This feature is known as voice prioritization. These calls are given priority over other clients utilizing the voice pool. Voice prioritization is available only for SIP-based calls and not for TSPEC-based calls. If the bandwidth is available, it takes the normal flow and allocates the bandwidth to those calls.

You can configure up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the controller does not check on the maximum call limit. It invokes the CAC to allocate bandwidth for the preferred call. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

Prerequisites for Configuring Voice Prioritization Using Preferred Call Numbers

You must configure the following before configuring voice prioritization:

- Set WLAN QoS to platinum.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Configuring a Preferred Call Number (GUI)

Step 1 Set the WLAN QoS profile to Platinum.

Step 2 Enable ACM for the WLAN radio.

Step 3 Enable SIP call snooping for the WLAN.

Step 4 Choose **Wireless** > **Advanced** > **Preferred Call** to open the **Preferred Call** page.
All calls configured on the controller appear.

Note To remove a preferred call, hover your cursor over the blue drop-down arrow and choose **Remove**.

Step 5 Click **Add Number** to add a new preferred call.

Step 6 In the Call Index text box, enter the index that you want to assign to the call. Valid values are from 1 through 6.

Step 7 In the Call Number text box, enter the number.

Step 8 Click **Apply** to add the new number.

Configuring a Preferred Call Number (CLI)

Step 1 Set the voice to the platinum QoS level by entering this command:
config wlan qos wlan-id Platinum

Step 2 Enable the ACM to this radio by entering this command:
config {802.11a | 802.11b} cac {voice | video} acm enable

Step 3 Enable the call-snooping feature for a particular WLAN by entering this command:
config wlan call-snoop enable *wlan-id*

Step 4 Add a new preferred call by entering this command:
config advanced sip-preferred-call-no *call_index* {*call_number* | **none**}

Step 5 Remove a preferred call by entering this command:
config advanced sip-preferred-call-no *call_index* **none**

Step 6 View the preferred call statistics by entering the following command:
show ap stats {802.11{a | b} | wlan} *ap_name*

Step 7 Enter the following command to list the preferred call numbers:
show advanced sip-preferred-call-no

Configuring EDCA Parameters

Information About EDCA Parameters

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

Configuring EDCA Parameters (GUI)

Step 1 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 2 Click **EDCA Parameters**under 802.11a/n/ac or 802.11b/g/n.

Step 3 The **802.11a (or 802.11b/g) > EDCA Parameters** window is displayed.

Step 4 Choose one of the following options from the **EDCA Profile** drop-down list:

- **WMM—**Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- **Spectralink Voice Priority—**Enables SpectraLink voice-priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- **Voice Optimized—**Enables Enhanced Distributed Channel Access (EDCA) voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
- **Voice & Video Optimized—**Enables EDCA voice-optimized and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
- **Custom Voice—**Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

  Note If you deploy video services, admission control must be disabled.

Step 5 To enable MAC optimization for voice, check the **Enable Low Latency MAC** check box. By default, this check box is not checked. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.

Note We recommend against you enabling low latency MAC. You should enable low-latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low-latency MAC can be used with any of the EDCA profiles.

Step 6 Click **Apply** to commit your changes.

Step 7 To re-enable the radio network, click **Network** under 802.11a/n/ac or 802.11b/g/n, check the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 8 Click **Save Configuration**.

Configuring EDCA Parameters (CLI)

Step 1 Disable the radio network by entering this command:
config {**802.11a** | **802.11b**} **disable network**

Step 2 Save your settings by entering this command:
save config

Step 3 Enable a specific EDCA profile by entering this command:
config advanced {802.11a | 802.11b} edca-parameters {**wmm-default | svp-voice | optimized-voice | optimzed-voice-video | custom-voice** }

- **wmm-default—**Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option if voice or video services are not deployed on your network.
- **svp-voice—**Enables SpectraLink voice-priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- **optimized-voice—**Enables EDCA voice-optimized profile parameters. Choose this option if voice services other than SpectraLink are deployed on your network.
- **optimized-video-voice—**Enables EDCA voice-optimized and video-optimized profile parameters. Choose this option if both voice and video services are deployed on your network.
- **custom-voice—**Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

Note If you deploy video services, admission control (ACM) must be disabled.

Step 4 View the current status of MAC optimization for voice by entering this command:
show {**802.11a** | **802.11b**}

Information that is similar to the following example is displayed:

```
Voice-mac-optimization.................Disabled
```

Step 5 Enable or disable MAC optimization for voice by entering this command:
config advanced {**802.11a** | **802.11b**} **voice-mac-optimization** {**enable** | **disable**}

Note This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight APs. This, in tun improves the number of voice calls serviced per AP. The default value is disabled.

Step 6 Re-enable the radio network by entering this command:
config {**802.11a** | **802.11b**} **enable network**

Step 7 Save your settings by entering this command: **save config**.

Key Telephone System-based CAC

Restrictions for Key Telephone System-Based CAC

- The controller ignores the SSID Capability Check Request message from the clients.
- Preferred call is not supported for KTS CAC clients.
- Reason code 17 is not supported in intercontroller roaming scenarios.
- To make the KTS-based CAC feature functional, ensure that you do the following:
  - Enable WMM on the WLAN
  - Enable ACM at the radio level
  - Enable processing of TSPEC inactivity timeout at the radio level

Information About Key Telephone System-Based CAC

Key Telephone System-based CAC is a protocol that is used in NEC MH240 wireless IP telephones. You can configure the controller to support CAC on KTS-based SIP clients, to process bandwidth request message from such clients, to allocate the required bandwidth on the AP radio, and to handle other messages that are part of the protocol.

When a call is initiated, the KTS-based CAC client sends a Bandwidth Request message to which the controller responds with a Bandwidth Confirm message indicating whether the bandwidth is allocated or not. The call is allowed only if the bandwidth is available. If the client roams from one AP to another, the client sends another Bandwidth Request message to the controller.

Bandwidth allocation depends on the median time calculated using the data rate from the Bandwidth Request message and the packetization interval. For KTS-based CAC clients, the G.711 codec with 20 milliseconds as the packetization interval is used to compute the medium time.

The controller releases the bandwidth after it receives the bandwidth release message from the client. When the client roams to another AP, the controller releases the bandwidth on the previous AP and allocates bandwidth on the new AP, in both intracontroller and intercontroller roaming scenarios. The controller releases the bandwidth if the client is dissociated or if there is inactivity for 120 seconds. The controller does not inform the client when the bandwidth is released for the client due to inactivity or dissociation of the client.

Configuring KTS-based CAC (GUI)

Before You Begin

To enable KTS-based CAC for a WLAN, ensure that you do the following:

- Set the QoS profile for the WLAN to Platinum.
- Set the WLAN in disabled state.
- Set the FlexConnect Local Switching in disabled state for the WLAN (On the WLANs > Edit page, click the **Advanced** tab and uncheck the **FlexConnect Local Switching** check box).

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure the KTS-based CAC policy.

Step 3 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 4 Under Voice, check or uncheck the **KTS based CAC Policy** check box to enable or disable KTS-based CAC for the WLAN.

Step 5 Save the configuration.

Configuring KTS-based CAC (CLI)

Before You Begin

To enable KTS-based CAC for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:

  config wlan qos *wlan-id* **platinum**

- Disable the WLAN by entering the following command:

  config wlan disable *wlan-id*

- Disable FlexConnect Local Switching for the WLAN by entering the following command:

  config wlan flexconnect local-switching *wlan-id* **disable**

Step 1 To enable KTS-based CAC for a WLAN, enter the following command:
config wlan kts-cac enable *wlan-id*

Step 2 To enable the functioning of the KTS-based CAC feature, ensure you do the following:

a) Enable WMM on the WLAN by entering the following command:
config wlan wmm allow *wlan-id*

b) Enable ACM at the radio level by entering the following command:
config 802.11a cac voice acm enable

c) Enable the processing of the TSPEC inactivity timeout at the radio level by entering the following command: **config 802.11a cac voice tspec-inactivity-timeout enable**

Related Commands

- To see whether the client supports KTS-based CAC, enter the following command:

  show client detail *client-mac-address*

  Information similar to the following appears:

```
Client MAC Address..............................  00:60:b9:0d:ef:26
Client Username ................................  N/A
AP MAC Address..................................  58:bc:27:93:79:90

QoS Level.......................................  Platinum
802.1P Priority Tag.............................  disabled
KTS CAC Capability..............................  Yes
WMM Support.....................................  Enabled
Power Save......................................  ON
```

- To troubleshoot issues with KTS-based CAC, enter the following command:

  debug cac kts enable

- To troubleshoot other issues related to CAC, enter the following commands:
  - **debug cac event enable**
  - **debug call-control all enable**

Application Visibility and Control

Information About Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition (NBAR) engine, and provides application-level visibility and control (QoS) in wireless networks. After the applications are recognized, the AVC feature enables you to either drop, mark, or police the data traffic.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

Note You can view list of 30 applications in Top Applications in Monitor Summary section of the UI.

AVC DSCP marks only the DSCP of the original packet in the controller in both directions (upstream and downstream). It does not affect the outer CAPWAP DCSP. AVC DSCP is applicable only when the application is classified. For example, based on the AVC profile configuration, if an application is classified as ftp or http, the corresponding DSCP marking is applied irrespective of the WLAN QoS. For downstream, the DSCP

value of outer CAPWAP header and inner packet's DSCP are taken from AVC DSCP. WLAN QoS is only applicable for all traffic from WLC to AP through CAPWAP. It does not change the DSCP of the original packet.

Using AVC rule, you can limit the bandwidth of a particular application for all the clients joined on the WLAN. These bandwidth contracts coexist with per-client downstream rate limiting with per client downstream rate limits that takes precedence over the per-application rate limits.

Note When you downgrade the controller from 8.0 to any earlier version, the AVC rate limit rules display the action as drop. This action is expected since the AVC rate limit rule is introduced in the controller version 8.0.

AVC is supported in central switching mode on the following controller platforms: Cisco 2504 WLCs, Cisco 5508 WLCs, Cisco Flex 7510 WLCs, Cisco 8510 WLCs, and Cisco Wireless Services Module 2 (WiSM2).

The number of concurrent flows supported for AVC classification on different controller platforms for 8.0 release are noted in the following table. The absolute maximum number of flows supported on one platform cannot exceed more than 110% of the numbers shown in the following table and this 10% extra flows support will happen based on availability of the free memory in the system.

Cisco WLC Platform	Flow
Cisco 2504 WLC	26,250
Cisco 5508 WLC	183,750
Cisco WiSM2	393,750
Cisco 8510 WLC	336,000
Cisco 5520 WLC	336,000
Cisco 8540 WLC	336,000

Application Visibility and Control Protocol Packs

Protocol packs are a means to distribute protocol updates outside the controller software release trains, and can be loaded on the controller without replacing the controller software.

The Application Visibility and Control Protocol Pack (AVC Protocol Pack) is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. A set of required protocols can be loaded, which helps AVC to recognize additional protocols for classification on your network. The manifest file gives information about the protocol pack, such as the protocol pack name, version, and some information about the available PDLs in the protocol pack.

The AVC Protocol Packs are released to specific AVC engine versions. You can load a protocol pack if the engine version on the controller platform is the same or higher than the version required by the protocol pack.

AAA override for AVC profiles

The AAA attribute for client or user profile is configured on the AAA server using authentication from RADIUS server or Cisco ACS or ISE. The AAA attribute is processed during layer 2 or layer 3 authentication by the controller and the same is overridden by what is configured on the WLAN.

The AAA AVC profile is defined as a Cisco AV air. The string option is defined as **avc-profile-name** and this value has to be configured for any AVC profile available in the controller.

Restrictions for Application Visibility and Control

- IPv6 packet classification is not supported.
- Layer 2 roaming is not supported across controllers.
- Multicast traffic is not supported.
- Controller GUI support is not present for the AVC Protocol Pack feature.
- Downloading the AVC Protocol Pack is not supported on the Cisco 2504 WLCs.
- The number of applications that you can apply rate limit is 3.
- Only one rule can be configured per application. An application cannot have both a rate limit as well as a Mark rule.
- If the standby controller has a different protocol pack version installed before pairing, then the active and standby controllers will have different protocol packs versions after pairing, in a HA environment. In the standby controller, the transferred protocol pack takes the preference over default protocol pack.

  For example, the controller with the software release 8.0 contains Protocol Pack version 9.0 by default. Before pairing, if one of the controllers has a Protocol Pack version 11.0 installed, then after pairing one controller contains Protocol Pack version 9.0 and the other controller contains Protocol Pack 11.0 installed.
- AVC rate limiting is not supported on Cisco 2504 WLC.

Configuring Application Visibility and Control (GUI)

Step 1 Create and configure an AVC profile by following these steps:

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles**.
b) Click **New**.
c) Enter the AVC profile name.
d) Click **Apply**.
e) On the **AVC Profile Name** page, click the corresponding AVC profile name.
The **AVC Profile > Edit** page is displayed.
f) Click **Add New Rule**.
g) Choose the application group and the application name from the respective drop-down lists.
View the list of default AVC applications available by choosing **Wireless** > **Application Visibility and Control** > **AVC Applications**.
h) From the **Action** drop-down list, choose either of the following:

- **Drop—**Drops the upstream and downstream packets that correspond to the chosen application.

- **Mark—**Marks the upstream and downstream packets that correspond to the chosen application with the Differentiated Services Code Point (DSCP) value that you specify in the **DSCP (0 to 63)** drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.

  Note The default action is to give permission to all applications.

i) If you choose **Mark** from the **Action** drop-down list, choose a DSCP value from the **DSCP (0 to 63)** drop-down list. The DSCP value is a packet header code that is used to define QoS across the Internet. The DSCP values are mapped to the following QoS levels:

- **Platinum (Voice)—**Assures a high QoS for Voice over Wireless.
- **Gold (Video)—**Supports high-quality video applications.
- **Silver (Best Effort)—**Supports normal bandwidth for clients.
- **Bronze (Background)—**Provides the lowest bandwidth for guest services.

You can also choose **Custom** and specify the DSCP value. The valid range is from 0 to 63.

j) Click **Apply**.
k) Click **Save Configuration**.

Step 2 Associate an AVC profile to a WLAN by following these steps:

a) Choose **WLANs** and click the corresponding WLAN ID.
The **WLANs > Edit** page is displayed.
b) Click the **QoS** tab.
c) Choose the AVC profile from the **AVC Profile** drop-down list.
d) Click **Apply**.
e) Click **Save Configuration**.

Configuring Application Visibility and Control (CLI)

- Create or delete an AVC profile by entering this command:

  config avc profile *avc-profile-name* {**create** | **delete**}

- Add a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule add application** *application-name* {**drop** | **mark** *dscp-value* | **ratelimit** *Average Ratelimit value Burst Ratelimit value*}

- Remove a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule remove application** *application-name*

- Configure an AVC profile to a WLAN by entering this command:

  config wlan avc *wlan-id* **profile** *avc-profile-name* {**enable** | **disable**}

- Configure application visibility for a WLAN by entering this command:

config wlan avc *wlan-id* **visibility** {**enable** | **disable**}

Note Application visibility is the subset of an AVC profile. Therefore, visibility is automatically enabled when you configure an AVC profile on the WLAN.

- Download an AVC Protocol Pack to the controller by entering these commands:
  1. **transfer download datatype avc-protocol-pack**
  2. **transfer download start**
- View information about all AVC profile or a particular AVC profile by entering this command:

  show avc profile {**summary** | **detailed** *avc-profile-name*}
- View information about AVC applications by entering these commands:
  - **show avc applications** [*application-group*]**—**Displays all the supported AVC applications for the application group.
  - **show avc statistics application** *application_name* **top-users** [**downstream wlan** | **upstream wlan** | **wlan**] [*wlan_id*]} **—**Displays AVC statistics for the top users of an application.
  - **show avc statistics top-apps** [**upstream** | **downstream**]**—**Displays the AVC statistics for the most used application.
  - **show avc statistics wlan** *wlan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}**—**Displays the AVC statistics of a WLAN per application or top applications or top application groups.
  - **show avc statistics client** *client_MAC* {**application** *application_name* | **top-apps** [**upstream** | **downstream**]}**—**Displays the client AVC statistics per application or top applications.

Note You can view list of 30 applications using the **show avc applications** and **show avc statistics** commands.

- View the protocol pack that is used on the controller by entering this command:

  show avc protocol-pack version
- View the AVC engine version information by entering this command:

  show avc engine version
- Configure troubleshooting for AVC events by entering this command:

  debug avc events {**enable** | **disable**}
- Configure troubleshooting for AVC errors by entering this command:

  debug avc error {**enable** | **disable**}

Application Visibility Control for FlexConnect

Release 8.1 introduces support for Application Visibility and Control for locally switched WLANs on FlexConnect APs. Application Visibility Control (AVC) provides application-aware control on a wireless network and enhances manageability and productivity. The support of AVC embedded within the FlexConnect AP extends as this is an end-to-end solution, which gives a complete visibility of applications in the network and allows the administrator to perform necessary actions.

Supported Hardware

- Supported Access Points—1600, 1700, 2600, 2700, 3600, 3700, 1532, 1570
- Supported WLCs—5508, Flex 7510, 8510, WiSM2, 5520, 8540, and vWLC
- Supported Modes—FlexConnect and Flex+bridge mode

Restrictions on AVC for FlexConnect

- IPv6 packet classification is not supported.
- Cisco Aironet 1570 Access Points are not supported.
- Multicast traffic is not supported.
- Downloading the AVC Protocol Pack is not supported on FlexConnect APs.
- The number of applications that you can apply rate limit is 3.
- Only one rule can be configured per application. An application cannot have both a rate limit as well as a Mark rule.
- A maximum of 31 rules can be configured in a profile. You can configure a maximum of 16 profiles in the complete system.
- AAA override of AVC profiles is not supported.
- FlexConnect AVC feature is not supported on Cisco 2504 WLC.
- By design, WLAN-level FlexConnect AVC stats are not supported.
- When the AP is in a FLexGroup and the FlexGroup does not have FlexConnect AVC configured, then FlexConnect AVC configuration is not pushed to the AP from the WLC.
- Netflow Export from WLC is not supported.
- In the stats, DHCP information is not supported on the WLC.
- Foreign anchor scenario: AVC for FlexConnect statistics can be seen only on the foreign WLC.
- FlexConnect Group AVC configuration:
    - WLAN AVC configuration is not inherited when the AP is part of FlexConnect group.
    - It is mandatory to configure AVC for FlexConnect on a FlexConnect Group if the AP is part of the FlexConnect group, if you want to push the AVC for FlexConnect configuration to the AP.
    - If a FlexConnect AP is not part of a FlexConnect group, local switching WLAN AVC configuration is pushed to the FlexConnect AP.

- Upgrade to 8.1 or a later release from a previous release:
  - Enabling AVC on Local Switching WLAN might have performance issues on a FlexConnect AP.
  - After you upgrade to 8.1 or a later release, AVC configuration of WLAN is pushed to all FlexConnect APs that are not part of the FlexConnect Group. You can disable the AVC configuration at the WLAN level and can configure it at the FlexConnect group level based on your requirement.

Note We recommend that you do not change any configuration directly on the AP. Doing so might result in unexpected behavior.

Configuring Application Visibility and Control for FlexConnect (GUI)

Step 1 To create a FlexConnect AVC profile and add a rule:

a) Choose **Wireless** > **Application Visibility and Control** > **FlexConnect AVC Profiles** and click **New**.
b) Specify the FlexConnect profile name and click **Apply**.
c) Click the profile name and click **Add New Rule**.
d) Specify the **Application Group**, **Application Name**, and **Action** and click **Apply**.

Step 2 To check the visibility globally for all WLANs on a FlexConnect Group, choose **Monitor** > **Applications** > **FlexConnect Groups** and select the FlexConnect group that you created earlier.
This page provides more granular visibility per FlexConnect group and lists the top 10 applications in the last 90 seconds, as well as cumulative stats for the top 10 applications. You can view upstream and downstream statistics individually per FlexConnect group on the same page by clicking the **Upstream** and **Downstream** tabs.
You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Step 3 To specify more granular visibility of the top 10 applications per client on a locally switched WLAN where AVC visibility is enabled, choose **Monitor** > **Applications** > **FlexConnect Groups**, select the FlexConnect group name and click the **Client** tab. Then, click any individual client MAC address entry listed on the page.
This page provides further granular statistics per client associated on locally switched WLANs where AVC visibility is enabled on the WLAN itself or on the FlexConnect Group, and lists the top 10 applications in last the 180 seconds as well as cumulative stats for top 10 applications. You can view upstream and downstream stats individually per-client from same page by clicking the **Upstream** and **Downstream** tab. You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Configuration Example

Step 1 Create an open WLAN.
An open WLAN has Layer 2 security set to **None**.

Step 2 Enable FlexConnect Local Switching on the WLAN and click **Apply.**

a) On the **WLANs** page, click the WLAN ID.
b) On the **WLANs > Edit** page, click the **Advanced** tab.
c) In the FlexConnect area, select the **FlexConnect Local Switching** check box.

Step 3 Ensure that the APs connected to this WLAN are among the list of supported access points for this feature. Set the APs in FlexConnect mode.

a) Choose **Wireless** > **Access Points** > **All APs**.
b) Click the AP name.
c) From the **AP Mode** drop-down list, select **FlexConnect** and click **Apply**.

Step 4 Create a FlexConnect group and add the AP to the FlexConnect group.

a) Choose **Wireless** > **FlexConnect Groups**.
b) Click **New** and enter the name of the FlexConnect group, and then click **Apply**.
c) On the **FlexConnect Groups > Edit** page, in the FlexConnect APs area, click **Add AP**.
d) You can either select an AP from a list of APs associated with the WLC or directly specify the Ethernet MAC address of the AP that is associated with the WLC.
e) Click **Add**.

Note Applications that can be identified, classified, and controlled are listed under **Wireless** > **Application Visiblity and Control** > **FlexConnect AVC Applications**. The access points support Protocol Pack version 8.0 and NBAR engine version 16.

Step 5 Create an AVC profile and add a rule.

Note A FlexConnect AVC profile can have a maximum of 32 rules.

a) Choose **Wireless** > **Application Visibility and Control** > **FlexConnect AVC Profiles** and click **New**.
b) Specify the FlexConnect profile name and click **Apply**.
c) Click the profile name and click **Add New Rule**.
d) Specify the **Application Group**, **Application Name**, and **Action** and click **Apply**.

Step 6 Enable AVC on the FlexConnect group and apply the FlexConnect AVC profile to the FlexConnect group.

a) Choose **Wireless** > **FlexConnect Group** and click the FlexConnect group name.
b) Click the **WLAN AVC Mapping** tab.
c) Specify the WLAN ID and from the **Application Visibility** drop-down list, choose **Enable**.
d) From the **Flex AVC Profile** drop-down list, choose the FlexConnect AVC profile, and click **Add**.
e) Click **Apply**.

Step 7 After Application Visibility is enabled on the FlexConnect Group, you can start different types of traffic (from the associated wireless client) using the applications (already installed) such as Cisco Jabber, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, YouTube, Ping, Trace route.
After traffic is initiated from the wireless client, visibility of different traffic can be observed on a per-FlexConnect Group and per-client basis. This provides a good overview to the administrator of the network bandwidth utilization and type of traffic in the network per-client and per-branch site.

Step 8 To check the visibility globally for all WLANs on a FlexConnect Group, choose **Monitor** > **Applications** > **FlexConnect Groups** and select the FlexConnect group that you created earlier.
This page provides more granular visibility per FlexConnect group and lists the top 10 applications in the last 90 seconds, as well as cumulative stats for the top 10 applications. You can view upstream and downstream statistics individually per FlexConnect group on the same page by clicking the **Upstream** and **Downstream** tabs.

You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Step 9 To specify more granular visibility of the top 10 applications per client on a locally switched WLAN where AVC visibility is enabled, choose **Monitor** > **Applications** > **FlexConnect Groups**, select the FlexConnect group name and click the **Client** tab. Then, click any individual client MAC address entry listed on the page.
This page provides further granular statistics per client associated on locally switched WLANs where AVC visibility is enabled on the WLAN itself or on the FlexConnect Group, and lists the top 10 applications in last the 180 seconds as well as cumulative stats for top 10 applications. You can view upstream and downstream stats individually per-client from same page by clicking the **Upstream** and **Downstream** tab. You can set the number of applications that are displayed on this page through the **Max Number of Records** drop-down list. The default value is 10.

Step 10 Click **Clear AVC Stats** to clear all the AVC statistics for a particular client.

Configuring Application Visibility and Control for FlexConnect (CLI)

- Configure a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* {**create** | **delete**}
- Add a rule for a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* **rule add application** *app-name* {**drop** | {**mark** *dscp-value* {**upstream** | **downstream**}}}
- Delete a rule for a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* **rule remove application** *app-name*
- Apply rule changes to a FlexConnect AVC profile by entering this command:
  config flexconnect avc profile *profile-name* **apply**
- Apply FlexConnect group AVC profile to a WLAN by entering this command:
  config flexconnect group *group-name* **avc** *wlan-id* **visibility wlan-specific**
- See a summary of FlexConnect AVC profiles or detailed information about one FlexConnect AVC profile by entering this command:
  - **show flexconnect avc profile summary**
  - **show flexconnect avc profile detailed** *profile-name*

Note The FlexConnect AVC profile rules are pushed to the AP only when the rules are in 'Applied' state.

- Troubleshooting command:
  debug flexconnect avc {**event** | **error** | **detail**} {**enable** | **disable**}
- Monitoring commands to be entered on the AP console:
  a) Check whether the FlexConnect AVC profiles are present on the AP by entering this command:
  show policy-map
  b) See statistics for each application in the FlexConnect AVC profile by entering this command:
  show policy-map target
  c) Check the applications present in the FlexConnect AVC profiles by entering this command:

show class-map

d) See WLAN and FlexConnect AVC mapping on the AP by entering this command:
show dot11 qos

Configuration Example

Before You Begin

Ensure that you have created an open WLAN.

Step 1 Enable FlexConnect local switching on the WLAN:
config wlan flexconnect local-switching *wlan-id*

Step 2 Ensure that the APs connected to this WLAN are among the list of supported access points for this feature. Set the APs in FlexConnect mode.
config ap mode flexconnect submode none

Step 3 Create a FlexConnect group and add the AP to the FlexConnect group:

a) **config flexconnect group** *group-name* **add**

b) **config flexconnect group** *group-name* **ap add** *ap-mac-addr*

Step 4 Create a FlexConnect AVC profile and add a rule:

Note A FlexConnect AVC profile can have a maximum of 32 rules.

a) **config flexconnect avc profile** *profile-name* **create**

b) **config flexconnect avc profile** *profile-name* **rule add application** *app-name* {**drop** | **mark**}

Step 5 Enable AVC on the FlexConnect group and apply the FlexConnect AVC profile to the FlexConnect group.

a) **config flexconnect group** *group-name* **avc** *wlan-id* **visibility enable**

b) **config wlan avc** *wlan-id* **visibility enable**

c) **config wlan avc** *wlan-id* **flex-profile** *profile-name* **enable**

Step 6 Configure the FlexConnect group AVC to a WLAN in local switching mode.
config flexconnect group *group-name* **avc** *wlan-id* **visibility wlan-specific**

Step 7 After Application Visibility is enabled on the FlexConnect Group, you can start different types of traffic (from the associated wireless client) using the applications (already installed) such as Cisco Jabber, Skype, Yahoo Messenger, HTTP, HTTPS/SSL, YouTube, Ping, Trace route.
After traffic is initiated from the wireless client, visibility of different traffic can be observed on a per-FlexConnect Group and per-client basis. This provides a good overview to the administrator of the network bandwidth utilization and type of traffic in the network per-client and per-branch site.

Step 8 To check the visibility globally for all WLANs on a FlexConnect Group:
show flexconnect avc statistics

Step 9 To see a summary of AVC for FlexConnect profiles or detailed information about one AVC for FlexConnect profile:

- **show flexconnect avc profile summary**
- **show flexconnect avc profile detailed** *profile-name*

Note The AVC profile rules are pushed to the AP only when the rules are in 'Applied' state.

Step 10 To troubleshoot AVC for FlexConnect:

debug flexconnect avc {**event** | **error** | **detail**} {**enable** | **disable**}

Step 11 Monitoring commands to be entered on the AP console:

a) Check whether the FlexConnect AVC profiles are present on the AP by entering this command:
show policy-map

b) See statistics for each application in the FlexConnect AVC profile by entering this command:
show policy-map target

c) Check the applications present in the FlexConnect AVC profiles by entering this command:
show class-map

d) See WLAN and FlexConnect AVC mapping on the AP by entering this command:
show dot11 qos

NetFlow

Information About NetFlow

NetFlow is an embedded instrumentation within the Cisco WLC software to characterize wireless network flows. NetFlow monitors each IP flow and exports the aggregated flow data to the external NetFlow collectors.

The NetFlow architecture consists of the following components:

- Collector—Entity that collects all the IP traffic information from various NetFlow exporters.
- Exporter—Network entity that exports the template with the IP traffic information. The Cisco WLC acts as an exporter.

Note Cisco WLC does not support IPv6 address format when acting as an exporter for NetFlow.

Configuring NetFlow (GUI)

Step 1 Configure the Exporter by performing these steps:

a) Choose **Wireless** > **Netflow** > **Exporter.**

b) Click **New**.

c) Enter the Exporter name, IP address, and the port number.
The valid range for the port number is from 1 to 65535.

d) Click **Apply**.

e) Click **Save Configuration**.

Step 2 Configure the NetFlow Monitor by performing these steps:

a) Choose **Wireless** > **Netflow** > **Monitor.**

b) Click **New** and enter a Monitor name.
c) On the Monitor List window, click the Monitor name to open the **Netflow Monitor** > **Edit** window.
d) Choose the exporter name and the record name from the respective drop-down lists.

- Client App Record—Better Performance

e) Click **Apply**.
f) Click **Save Configuration**.

Step 3 Associate a NetFlow Monitor to a WLAN by performing these steps:

a) Choose **WLANs** and click a WLAN ID to open the **WLANs** > **Edit page.**
b) In the QoS tab, choose a NetFlow monitor from the **Netflow Monitor** drop-down list.
c) Click **Apply**.
d) Click **Save Configuration**.

Configuring NetFlow (CLI)

- Create an Exporter by entering this command:

  config flow create exporter *exporter-name ip-addr port-number*
- Create a NetFlow Monitor by entering this command:

  config flow create monitor *monitor-name*
- Associate or dissociate a NetFlow monitor with an exporter by entering this command:

  config flow {**add** | **delete**} **monitor** *monitor-name* **exporter** *exporter-name*
- Associate or dissociate a NetFlow monitor with a record by entering this command:

  config flow {**add** | **delete**} **monitor** *monitor-name* **record ipv4_client_app_flow_record**
- Associate or dissociate a NetFlow monitor with a WLAN by entering this command:

  config wlan flow *wlan-id* **monitor** *monitor-name* {**enable** | **disable**}
- View a summary of NetFlow monitors by entering this command:

  show flow monitor summary
- View information about the Exporter by entering this command:

  show flow exporter {**summary** | **statistics**}
- Configure NetFlow debug by entering this command:

  debug flow {**detail** | **error** | **info**} {**enable** | **disable**}

QoS Profiles

Information About QoS Profiles

Cisco UWN solution WLANs support four levels of QoS: Platinum/Voice, Gold/Video, Silver/Best Effort (default), and Bronze/Background. You can configure the voice traffic WLAN to use Platinum QoS, assign the low-bandwidth WLAN to use Bronze QoS, and assign all other traffic between the remaining QoS levels.

The WLAN QoS level defines a specific 802.11e user priority (UP) for over-the-air traffic. This UP is used to derive the over-the-wire priorities for non-WMM traffic, and it also acts as the ceiling when managing WMM traffic with various levels of priorities.

The wireless rate limits can be defined on both upstream and downstream traffic. Rate limits can be defined per SSID and/or specified as a maximum rate limit for all clients. These rate limits can be individually configured.

The access point uses this QoS-profile-specific UP in accordance with the values in the following table to derive the IP DSCP value that is visible on the wired LAN.

Table 4: Access Point QoS Translation Values

AVVID Traffic Type	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
Network control	56 (CS7)	Platinum	7	7
Inter-network control (CAPWAP control, 802.11 management)	48 (CS6)	Platinum	6	7
Voice	46 (EF)	Platinum	5	6
Interactive video	34 (AF41)	Gold	4	5
Mission critical	26 (AF31)	Gold	3	4
Transactional	18 (AF21)	Silver	2	3
Bulk data	10 (AF11)	Bronze	1	2
Best effort	0 (BE)	Silver	0	0
Scavenger	2	Bronze	0	1

Note The IEEE 802.11e UP value for DSCP values that are not mentioned in the table is calculated by considering 3 MSB bits of DSCP.

For example, the IEEE 802.11e UP value for DSCP 32 (100 000 in binary), would be the decimal equivalent of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.

Configuring Quality of Service Profiles

Configuring QoS Profiles (GUI)

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles.
To disable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 2 Choose **Wireless > QoS > Profiles** to open the QoS Profiles page.

Step 3 Click the name of the profile that you want to configure to open the Edit QoS Profile page.

Step 4 Change the description of the profile by modifying the contents of the Description text box.

Step 5 Define the data rates on a per-user basis as follows:

a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

c) Define the average real-time rate for UDP traffic per user by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 6 Define the data rates on a per-SSID basis as follows:

a) Define the average data rate TCP traffic per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic in the WLANs.

c) Define the average real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.
d) Define the peak real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic in the WLANs.

Step 7 Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN.

a) From the Maximum Priority drop-down list, choose the maximum QoS priority for any data frames transmitted by the AP to any station in the WLAN.
For example, a QoS profile named 'gold' targeted for video applications has the maximum priority set to video by default.
b) From the Unicast Default Priority drop-down list, choose the QoS priority for unicast data frames transmitted by the AP to non-WMM stations in the WLAN
c) From the Multicast Default Priority drop-down list, choose the QoS priority for multicast data frames transmitted by the AP to stations in the WLAN,

Note The default unicast priority cannot be used for non-WMM clients in a mixed WLAN.

Step 8 Choose **802.1p** from the Protocol Type drop-down list and enter the maximum priority value in the 802.1p Tag text box to define the maximum value (0–7) for the priority tag associated with packets that fall within the profile.
The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Step 11 Reenable the 802.11 networks.
To enable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 12 Choose **WLANs** and select a WLAN ID to apply the new QoS profile to it.

Step 13 In the **WLAN > Edit** page, go to the **QoS** tab and select the QoS Profile type from the Quality of Service drop-down list. The QoS profile will add the rate limit values configured on the controller on per WLAN, per radio and per AP basis. For example, if upstream rate limit of 5Mbps is configured for a QoS profile of type silver, then every WLAN that has silver profile will limit traffic to 5Mbps (5Mbps for each wlan) on each radio and on each AP where the WLAN is applicable.

Step 14 Click **Apply**.

Step 15 Click **Save Configuration**.

Configuring QoS Profiles (CLI)

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:

config 802.11{**a** | **b**} **disable network**

Step 2 Change the profile description by entering this command:
config qos description {**bronze** | **silver** | **gold** | **platinum** }*description*

Step 3 Define the average data rate for TCP traffic per user or per SSID by entering this command:
config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Note For the *rate* parameter, you can enter a value between 0 and 512,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Step 4 Define the peak data rate for TCP traffic per user or per SSID by entering this command:
config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 5 Define the average real-time data rate for UDP traffic per user or per SSID by entering this command:
config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 6 Define the peak real-time data rate for UDP traffic per user or per SSID by entering this command:
config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 7 Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN by entering this command:
config qos priority {**bronze** | **gold** | **platinum** | **silver**} {*maximum priority*} {*default unicast priority*} {*default multicast priority*}

You choose from the following options for the *maximum priority*, *default unicast priority*, and *default multicast priority* parameters:

- besteffort
- background
- video
- voice

Step 8 Define the maximum value (0–7) for the priority tag associated with packets that fall within the profile, by entering these commands:
config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} **dot1p**

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *tag*

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note The 802.1p tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for a QoS profile.

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9 Reenable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:
config 802.11{**a** | **b**} **enable network**

Step 10 Apply the new QoS profile to a WLAN, by entering these commands:

config wlan qos <WLAN ID> {**bronze** | **silver** | **gold** | **platinum**}

QoS Profile per WLAN

Assigning a QoS Profile to a WLAN (GUI)

Before You Begin

If you have not already done so, configure one or more QoS profiles using the instructions in the Configuring QoS Profiles (GUI) section.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to which you want to assign a QoS profile.

Step 3 When the **WLANs > Edit** page appears, choose the **QoS** tab.

Step 4 From the **Quality of Service (QoS)** drop-down list, choose one of the following:

- **Platinum** (**voice**)
- **Gold (video)**
- **Silver (best effort)**
- **Bronze** (**background**)

Note Silver (best effort) is the default value.

Step 5 To define the data rates on a per-user basis, do the following:

a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

c) Define the average real-time rate for UDP traffic per user by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 6 To define the data rates on a per-SSID basis, do the following:

a) Define the average data rate TCP traffic per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic in the WLANs.

c) Define the average real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

d) Define the peak real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic in the WLANs.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Assigning a QoS Profile to a WLAN (CLI)

If you have not already done so, configure one or more QoS profiles using the instructions in the Configuring QoS Profiles (CLI) section.

Step 1 Assign a QoS profile to a WLAN by entering this command:
config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}

Silver is the default value.

Step 2 To override QoS profile rate limit parameters, enter this command:
config wlan override-rate-limit *wlan-id* {**average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 3 Enter the **save config** command.

Step 4 Verify that you have properly assigned the QoS profile to the WLAN by entering this command:
show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist.................................... Disabled
Session Timeout.................................. 0
Interface........................................ management
```

```
WLAN ACL..................................... unconfigured
DHCP Server.................................. 1.100.163.24
DHCP Address Assignment Required............. Disabled
Quality of Service........................... Silver (best effort)
WMM.......................................... Disabled
...
```