Wireless Quality of Service

Call Admission Control

This section contains the following subsections:

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.

This section contains the following subsections:

Configuring Voice Parameters

Configuring Voice Parameters (GUI)

Procedure

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

Step 2 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, uncheck the 802.11a (or 802.11b/g) **Network Status** check box, and click **Apply** to disable the radio network.

Step 3 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 4 (Optional) Check the **Admission Control (ACM)** check box to enable static CAC for this radio band. The default value is disabled.

Step 5 (Optional) 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 6 In the **Max RF Bandwidth** field, 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 7 In the **Reserved Roaming Bandwidth** field, 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 8 To enable expedited bandwidth requests, check the **Expedited Bandwidth** check box. By default, this field is disabled.

Step 9 To enable SIP CAC support, check the **SIP CAC Support** check box. By default, SIP CAC support is disabled.

Step 10 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 11 In the **SIP Bandwidth (kbps)** field, enter the bandwidth in kilobits per second.

The possible range is 8 to 64.

The default value is 64.

Note
The **SIP Bandwidth (kbps)** field 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)** field is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (kbps) field is set to 8.

Step 12 In the **SIP Voice Sample Interval (msecs)** field, enter the value for the sample interval.

Step 13 In the **Maximum Calls** field, 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 14 Check 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 15 Click **Apply**.

Step 16 Choose **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** to reenable the radio network.

Step 17 Click **Save Configuration**.

Step 18 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.

Procedure

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 the radio network by entering this command:

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

Step 4 Save your settings by entering this command:

save config

Step 5 Enable or disable static 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 6 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 7 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 8 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 9 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 10 Reenable the radio network by entering this command:

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

Step 11 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 12 Enter the **save config** command to save your settings.

Step 13 Configure voice automatically for a WLAN by entering this command:

config auto-configure voice cisco *wlan-id* **radio** {**802.11a** | **802.11b** | **all**}

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

Configuring Video Parameters

Configuring Video Parameters (GUI)

Procedure

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

Step 2 Choose **Wireless** and then **Network** under 802.11a/n/ac or 802.11b/g/n, uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 3 Choose **Wireless** > **802.11a/n/ac** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media page appears.

Step 4 In the **Video** tab, check the **Admission Control (ACM)** check box to enable video CAC for this radio band. The default value is disabled.

Step 5 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 6 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 7 In the Reserved Roaming Bandwidth text box, enter the percentage of the maximum RF bandwidth that is reserved for roaming clients for video.

Step 8 Configure the SIP CAC Support by checking or unchecking 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 9 Click **Apply**.

Step 10 Choose **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** to reenable the radio network.

Step 11 Click **Save Configuration**.

Step 12 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.

Procedure

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 the radio network by entering this command:

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

Step 4 Save your settings by entering this command:

save config

Step 5 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 6 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 7 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 8 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 9 To configure the CAC parameters for SIP-based video calls, enter this command:

config {**802.11a** | **802.11b**} **cac video sip** {**enable** | **disable**}

Step 10 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 11 Reenable the radio network by entering this command:

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

Step 12 Enter the **save config** command to save your settings.

Viewing Voice and Video Settings

Viewing Voice and Video Settings (GUI)

Procedure

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)

Procedure

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_ma*c | **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.

Procedure

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)

Procedure

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**}

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.

This section contains the following subsections:

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)

Procedure

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)

Procedure

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

Enhanced Distributed Channel Access 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.

This section contains the following subsections:

Configuring EDCA Parameters (GUI)

Procedure

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. The WMM option is default and we recommend this setting if you have SpectraLink phones deployed in your network.
- **Spectralink Voice Priority**—This setting is not recommended.
- **Voice Optimized**—Enables Enhanced Distributed Channel Access (EDCA) voice-optimized profile parameters. Choose this option when 8821 phones are deployed in your network, and video services are not in use.
- **Voice & Video Optimized**—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. This setting is not recommended because it is deprecated.

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

- **Fastlane**—Enables fastlane EDCA parameters. This setting is recommended for use with Apple client devices.

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 that you do not enable 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)

Procedure

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 |fastlane**}

- **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.

- **Fastlane**—Enables Fast Lane EDCA parameters.

Step 4 View the current status of MAC (low latency 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
The low latency MAC option is not supported.

This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight APs. This, in turn 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

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.

This section contains the following subsections:

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
- All RLAN clients are disconnected when Call Admission Control (CAC) is enabled or disabled to apply policies.

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).

Procedure

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**

Procedure

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

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.

AVC is configured by defining a class map in a QoS client policy to match a protocol.

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 controller to AP through CAPWAP. It does not change the DSCP of the original packet.

Traffic flows are analyzed and recognized using the NBAR2 engine for CAPWAP data at the controller and for FlexConnect locally switched data, analysis is done at the AP. For more information about the NBAR2 Protocol Library, see http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/

nbar-prot-pack-library.html. The specific flow is marked with the recognized protocol or application, such as WebEx. This per-flow information can be used for application visibility using Flexible NetFlow (FNF).

AVC QoS actions are applied with AVC filters in both upstream and downstream directions. The QoS actions supported for upstream flow are drop, mark, and police, and for downstream flow are mark and police. AVC QoS is applicable only when the application is classified correctly and matched with the class map filter in the policy map. For example, if the policy has a filter based on an application name, and the traffic has also been classified to the same application name, then the action specified for this match in the policy will be applied.

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.

The number of concurrent flows supported for AVC classification on different controller platforms are noted in the following table.

Controller Platform	Flow
Cisco 3504 Wireless Controller	183750
Cisco 5520 Wireless Controller	336,000
Cisco 8540 Wireless Controller	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 pair. The string option is defined as **avc-profile-name** and this value has to be configured for any AVC profile available in the controller.

Default DSCP Value for AVC Profile

Prior to Release 8.8 with AVC enabled, you could override DSCP values for only those application flows that were configured on an AVC profile. For the application flows that were not configured, no action was performed and DSCP was left intact. The maximum number of application rules that the AVC profile can contain is 32. For managed service, to control and rewrite DSCP values (example with DSCP 0) for all flows that are not presented on the AVC profile is not possible.

In Release 8.8, the new enhancement includes a new *default-class* rule that you can use to override the DSCP values for all application flows in which AVC rule is not configured. The goal of this enhancement is to protect the network for all flows with unwanted or controlled DSCP values.

This enhancement comes with the following restrictions:

- Only the start of an application flow is captured.
- Supported only for marking. Rate limit and drop are not supported.
- Default DSCP works only if AVC is in enabled state.
- An AVC profile can support up to 32 rules, including the *default-class* rule. If the *default-rule* is configured, you can configure up to 31 rules.
- Multicast and broadcast traffic is not supported.
- IPv6 is not supported in AVC.
- Cascading of rules is not supported, which means that for the same flow, it is not possible to have rate limiting and marking. Therefore, if rate limiting is performed for a flow, *default* marking is not performed on the flow.

This section contains the following subsections:

Restrictions for Application Visibility and Control

- IPv6 packet classification is not supported.
- Layer 2 roaming across controllers is not supported.
- Multicast traffic is not supported.
- Controller GUI support is not present for the AVC Protocol Pack feature.
- You can apply rate limiting to up to 3 applications.
- Each application can be configured with one rule only. An application cannot have both a rate limit and a Mark rule.
- If the standby controller has a different protocol pack version that is 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 the 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 that is installed, then after pairing one controller contains Protocol Pack version 9.0 and the other controller contains Protocol Pack 11.0 installed.

Configuring Application Visibility and Control (GUI)

Procedure

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

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles**.
b) Click **New** and enter the AVC profile name.
c) Click **Apply**.
d) On the AVC Profile Name page, click the AVC profile name to open the AVC Profile > Edit page.
e) Click **Add New Rule**.
f) Choose the application group and the application name from the respective drop-down lists.

See the list of default AVC applications available by choosing **Wireless** > **Application Visibility and Control** > **AVC Applications**.

g) 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 permit all applications.

h) 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 quality of service 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 the high-quality video applications.
- **Silver (Best Effort)**—Supports the 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.

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

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

a) Choose **WLANs** and click the WLAN ID to open the WLANs > Edit page.
b) In the QoS tab, choose the AVC profile from the AVC Profile drop-down list.
c) Click **Apply**.
d) 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**}

AVC-based Reanchoring

This feature is designed to reanchor clients when they roam from one controller to another controller. Reanchoring of Apple clients prevents depletion of IP addresses available for new clients in controller. The AVC profile-based statistics is used to decide whether the client must be reanchored or deferred. This is useful when the client is actively running voice or video application defined in the AVC rules.

The clients get deauthenticated when they are not transmitting any traffic for applications listed in the AVC rules when they are roaming between controllers.

Guidelines and Restrictions for AVC-based Reanchoring

- This feature is supported only in Central Switch mode.
- Some Apple clients roaming to another controller fails to reassociate with the new controller with the new IP address. These clients do not release the old IP address and therefore do not re-associate with the current controller.
- If the Wi-Fi calling signature in any application is changed and AVC fails to recognize this signature, this rule stops working.
- For the client to roam between controllers:
  - The controllers must be in the same mobility group.
  - Roaming is limited to within the same SSID.
- For the updated configuration to be available via CLI or GUI, we recommend that you refresh the interface. However, this is not required for the updated information to be visible on the Monitoring page in the GUI.

This section contains the following subsections:

Configuring AVC-based Selective Reanchoring (GUI)

Procedure

Step 1 Choose **WLANs** and click the WLAN ID.

Step 2 Click the **QoS** tab.

Step 3 Check the **Application Visibility** check box.

Step 4 Click **Advanced** tab.

Step 5 In the **Mobility** section, check the **AVC Based Reanchor** check box.

Step 6 Click **Apply** to save the configuration.

Step 7 (Optional) To add rules in the AVC profile:

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles** page.
b) Select the AVC profile **AVC_BASED_REANCHOR**.

   This profile by default contains Jabber-Audio, Jabber-Video, WebEx, and Wifi calling applications.

c) Click **Add New Rule**.
d) From the **Application Group** drop-down list, choose the application from the various options available.
e) From the **Application Name** drop-down list, choose the application name from the various options available.
f) Click **Apply**.

   Note
   When enabling AVC-based re-anchoring, the action function is disabled for the application profiles.

Step 8 (Optional) To delete rules from the AVC profile

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles** page.
b) Hover your cursor over the blue drop-down arrow for the rule.
c) Click **Remove**.

   Note
   The **AVC_BASED_REANCHOR** AVC profile can contain up to 32 applications as rules.

Configuring AVC-based Selective Reanchoring (CLI)

Procedure

Step 1 Enable Application Visibility on a WLAN by entering this command:

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

Step 2 Enable Selective Reanchoring feature on a WLAN by entering this command:

config wlan mobility selective re-anchoring enable *wlan-id*

Step 3 Disable Selective Reanchoring feature on a WLAN by entering this command:

config wlan mobility selective re-anchoring disable *wlan-id*

Step 4 View the status of Selective Reanchor by entering this command:

show wlan *wlan-id*

Step 5 View the Reanchor statistics by entering this command:

show mobility statistics

Application Visibility Control for FlexConnect

AVC provides application-aware control on a wireless network and enhances manageability and productivity. AVC is already supported on ASR and ISR G2 and controller platforms. The support of AVC embedded within the FlexConnect AP extends as this is an end-to-end solution. This gives a complete visibility of applications in the network and allows the administrator to take some action on the application.

AVC has the following components:

- Next-generation Deep Packet Inspection (DPI) technology, called Network Based Application Recognition (NBAR2), allows for identification and classification of applications. NBAR is a deep-packet inspection technology available on Cisco IOS-based platforms, which supports stateful L4 to L7 classification. NBAR2 is based on NBAR and has extra requirements such as having a common flow table for all IOS features that use NBAR. NBAR2 recognizes application and passes this information to other features such as Quality of Service (QoS), and Access Control List (ACL), which can take action based on this classification.
- Ability to Apply Mark using QoS, Drop and Rate-limit applications.

The important use cases for NBAR AVC are capacity planning, network usage base lining, and better understanding of the applications that are consuming bandwidth. Trending of application usage helps the network administrator to plan for network infrastructure upgrade, improve quality of experience by protecting important applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop some application traffic.

Supported Hardware

- Supported Access Points—All Wave 2 and 802.11ax APs
- Supported Controllers—3504, 5520, 8540, and vWLC
- Supported Modes—FlexConnect and Flex+Bridge mode

Restrictions for AVC for FlexConnect

- IPv6 packet classification is not supported.
- Multicast traffic is not supported.
- Downloading the AVC Protocol Pack is not supported on FlexConnect APs.
- You can apply rate limiting to up to 3 applications.
- 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.
- 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 controller.
- Netflow Export from controller is not supported.

- In the stats, DHCP information is not supported on the controller.
- Foreign anchor scenario: AVC for FlexConnect statistics can be seen only on the foreign controller.
- 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.

This section contains the following subsections:

Configuring Application Visibility and Control for FlexConnect (GUI)

Procedure

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

Procedure

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 controller or directly specify the Ethernet MAC address of the AP that is associated with the controller.
e) Click **Add**.

Note
Applications that can be identified, classified, and controlled are listed under **Wireless** > **Application Visibility 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)

Procedure

- 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.

Procedure

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

NetFlow is an embedded instrumentation within the controller 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 controller acts as an exporter.

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

NetFlow has added an enhanced template in Release 8.2 using the Version 9 export format, which provides additional 17-field information about the flow. This report is compatible with third-party NetFlow collectors, including Lancope. The minimum supported protocol pack version is 14 with NBAR engine version 23.

The following are the template enhancements in NetFlow Version 9 :

- New features can be added to NetFlow quickly, without breaking existing implementations.
- NetFlow is future-proofed against new or developing protocols, because NetFlow Version 9 can be adapted to provide support for those protocols.
- NetFlow Version 9 is the IETF standard mechanism for information export.
- Third-party business partners who produce applications that provide collector or display services for NetFlow are not required to recompile their applications each time a new NetFlow feature is added.

Table 1: List of data points in a NetFlow template

Existing Template [1]: ipv4_client_app_flow_record	Enhanced template [2]: ipv4_client_src_dst_flow_record
applicationTag	applicationTag
ipDiffServCodePoint	staMacAddress
octetDeltaCount	wtpMacAddress
packetDeltaCount	WlanID
postIpDiffServCodePoint	Source IP
staIPv4Address	Dest IP
staMacAddress	Source Port
wlanSSID	Dest Port
wtpMacAddress	Protocol
—	Start Time
—	End Time
—	Direction
—	Packet count
—	Byte count
—	VLAN id

Existing Template [1]: ipv4_client_app_flow_record	Enhanced template [2]: ipv4_client_src_dst_flow_record
—	TOS
—	Client username

[1] Supported on Cisco 5520, 8540 Wireless Controllers

[2] Supported on Cisco 5520 and 8540 Wireless Controllers

Restrictions for Using Netflow

- The enhanced template is supported only on Cisco 3504, 5520, and 8540 controllers.
- NetFlow is not supported on Cisco Virtual Wireless Controller (vWLC).
- FlexConnect mode is not supported.
- IPv6 traffic is not supported.
- Only one collector and exporter each can be configured.

Configuring NetFlow (GUI)

Before you begin

You have to enable AVC before enabling netflow on a WLAN.

Procedure

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
- Client Source and Destination Record—Higher Visibility

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 the new template record by entering this command:

  config flow {**add** | **delete**} **monitor** *monitor-name* **record ipv4_client_src_dst_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

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 2: 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 most significant 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.

This section contains the following subsections:

Configuring QoS Profiles (GUI)

Procedure

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)

Procedure

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**}

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.

Procedure

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 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 6 To define the data rates on a per-SSID 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 7 Save the 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.

Procedure

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
...
```

Cisco Air Time Fairness

Cisco Air Time Fairness (ATF) for High Density Experience (HDX) allows network administrators to group devices of a defined category and enables some groups to receive traffic from the WLAN more frequently than other groups. Therefore, some groups are entitled to more *air time* than other groups.

Cisco ATF has the following capabilities:

- Allocates Wi-Fi *air time* for user groups or device categories
- Air time fairness is defined by the network administrator and not by the network
- Provides a simplified mechanism for allocating air time
- Dynamically adapts to changing conditions in a WLAN
- Enables a more efficient fulfillment of service-level agreements
- Augments standards-based Wi-Fi QoS mechanisms

By enabling network administrators to define what *fairness* means within their environments with regard to the amount of *on air* time per client group, the amount of traffic is also controlled.

To control air time on a percentage basis, the air time, which includes both uplink and downlink transmissions of a client/SSID, is continuously measured.

Only air time in the downlink direction, that is AP to client, can be controlled accurately by the AP. Although air time in the uplink direction, that is client to AP, can be measured, it cannot be strictly controlled. Although the AP can constrain air time for packets that it sends to clients, the AP can only measure air time for packets that it *hears* from clients because it cannot strictly limit their air time.

Cisco ATF establishes air time limits (defined as a percentage of total air time) and to apply those limits on a per SSID basis, where the SSID is used as a parameter to define a client group. Other parameters can be used as well to define groups of clients. Furthermore, a single air time limit (defined as a percentage of total air time) can be applied to individual clients.

If the air time limit for an SSID (or client) is exceeded, the packets that are in the downlink direction are dropped. Dropping downlink packets (AP to client) frees up air time whereas dropping uplink packets (client to AP) does not do anything to free up air time because the packet has already been transmitted over the air by the client.

Client Fair Sharing

With Cisco Wireless Release 8.2, Cisco Air Time Fairness can be enforced on clients that are associated with an SSID/WLAN. This ensures that all clients within an SSID/WLAN are treated equally based on their utilization of the radio bandwidth. This feature is useful in scenarios where one or a few clients could use the complete air time allocated for an SSID/WLAN, thereby depriving Wi-Fi experience for other clients associated with the same SSID/WLAN.

- The percentage of air time to be given to each client is recomputed every time a client connects or disconnects.
- Client fair sharing is applicable to only downstream traffic.
- Clients can be categorized into the following usage groups at the policy level: low, medium, and high.
- Client-based ATF metrics accumulation is performed in the transmit complete routine. This allows the air time that is unused by clients in low-usage or medium-usage groups to be accumulated to a common share pool bucket where the high-usage clients can be replenished.

Supported Access Point Platforms

Cisco ATF is supported on the following access points:

- Cisco Aironet 1570 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points

Note Cisco ATF is supported only on Local and FlexConnect mode APs.

Cisco ATF Modes

Cisco ATF operates in the following modes:

- Monitor mode in which users can do the following:
  - View the air time
  - Report air time usage for all AP transmissions
  - View reports

        - per SSID/WLAN
        - per AP Group
        - per AP
        - per client
    - Report air time usage at periodic intervals
    - Block ACKs are not reported
    - No enforcement as part of Monitor mode
- Enforce Policy mode in which users can do the following:
    - Enforce air time based on configured policy
    - Enforce air time on
        - a WLAN
        - All APs connected within a controller's network
        - an AP group
        - an AP
        - a client
    - An AP can have multiple WLANs with multiple policies (1:16)
    - Strict Enforcement per WLAN—Air time used by the WLANs on a radio is strictly enforced up to the configured limits in the policies
    - Optimal Enforcement per WLAN—Share unused air time from other SSIDs
    - The sum of all policies should amount to 100 percent; there can be no oversubscription.

Restrictions on Cisco Air Time Fairness

- ATF can be implemented only on data frames that are in the downstream direction.
- When ATF is configured in per-SSID mode, all of the WLANs must be disabled before you can enter any ATF configuration commands. The WLANs can be enabled after all of the ATF commands have been entered.

Cisco Air Time Fairness (ATF) Use Cases

Public Hotspots (Stadium/Airport/Convention Center/Other)

In this instance a public network is sharing a WLAN between two (or more) service providers and the venue. Subscribers to each service provider can be grouped and each group can be allocated a certain percentage of air time.

Education

In this instance, a university is sharing a WLAN between students, faculty, and guests. The guest network can be further partitioned by service provider. Each group can be assigned a certain percentage of air time.

Enterprise/Hospitality/Retail

In this instance, the venue is sharing a WLAN between employees and guests. The guest network can be further partitioned by service provider. The guests could be sub-grouped by tier of service type with each subgroup being assigned a certain percentage of air time, for example a paid group is entitled to more air time than the free group.

Time Shared Managed Hotspot

In this instance, the business entity managing the hotspot, such as a service provider or an enterprise, can allocate and subsequently lease air time to other business entities.

The following are the high-level steps to configure Cisco ATF:

1. Enable Monitor mode to determine network usage (optional)
2. Create Cisco ATF policies
3. Add WLAN ATF policies per network, AP group, or AP. Policies set in AP or AP group override per network polices.
4. Determine if optimization should be enabled.
5. Periodically check Cisco ATF statistics.

Related Documentation

- Air Time Fairness(ATF) Phase1 and Phase 2 Deployment Guide
- Feature Matrix for Cisco Wave 2 Access Points and Wi-Fi 6 (802.11ax) Access Points

This section contains the following subsections:

Configuring Cisco Air Time Fairness (GUI)

Configuring Cisco ATF Monitor Mode (GUI)

Procedure

Step 1 Choose **Wireless** > **ATF** > **Monitor Configuration**.

Step 2 On the **ATF Monitor Mode Configuration** page, choose an AP, AP group, or an entire network. If you choose the entire network, specify the radio type(s).

Step 3 Click **Enable**.

Step 4 Save the configuration.

Configuring Cisco ATF Policy (GUI)

Procedure

Step 1 Choose **Wireless** > **ATF** > **Policy Configuration**.

Step 2 On the **ATF Policy Configuration** page, specify an ID, name, and a weight to the ATF policy, and click **Create**.

Weighted ratio is used instead of percentages so that the total can exceed 100. The minimum weight that you can set is 10.

Step 3 Check the **Client Fair Sharing** check box to apply Client Fair Sharing on the policy.

Step 4 Save the configuration.

Configuring Cisco ATF Enforcement SSID (GUI)

Procedure

Step 1 Choose **Wireless** > **ATF** > **Enforcement SSID Configuration**.

Step 2 On the **ATF Enforcement SSID Configuration** page, apply the ATF policy created to an AP, an AP group, or the entire network with the radio type specified.

Step 3 Choose the enforcement type as either **Optimized** or **Strict**.

Step 4 Click **Enable**.

Step 5 Enforce an ATF policy on a WLAN by selecting the WLAN and the ATF policy and clicking **Add**.

Step 6 Save the configuration.

Monitoring ATF Statistics (GUI)

Procedure

To monitor per WLAN per AP ATF statistics with percentage of used time, choose **Wireless** > **ATF** > **ATF Statistics**. Select the AP name in the drop-down list to view the statistics.

- abs—Number of air time units being used per SSID
- Relative Time—Percentage of time used per SSID
- Total Air time—Total air time used per SSID

Configuring Cisco Air Tme Fairness (CLI)

Procedure

- Configure Cisco ATF at the network level (global) by entering these commands:
  - **config atf 802.11**{**a** | **b**} **mode disable**
  - **config atf 802.11**{**a** | **b**} **mode monitor**
  - **config atf 802.11**{**a** | **b**} **mode enforce-policy**
  - **config atf 802.11**{**a** | **b**} **optimization** {**enable** | **disable**}
- Configure Cisco ATF on a per AP group basis by entering these commands:
  - **config wlan apgroup atf 802.11**{**a** | **b**} **mode disable** *ap-group-name*
  - **config wlan apgroup atf 802.11**{**a** | **b**} **mode monitor** *ap-group-name*
  - **config wlan apgroup atf 802.11**{**a** | **b**} **mode enforce-policy** *ap-group-name*
  - **config wlan apgroup atf 802.11**{**a** | **b**} **optimization** {**enable** | **disable**} *ap-group-name*
- Configure Cisco ATF on a per AP radio basis by entering these commands:
  - **config ap atf 802.11**{**a** | **b**} **mode disable** *ap-name*
  - **config ap atf 802.11**{**a** | **b**} **mode monitor** *ap-name*
  - **config ap atf 802.11**{**a** | **b**} **mode enforce-policy** *ap-name*
  - **config ap atf 802.11**{**a** | **b**} **optimization** {**enable** | **disable**} *ap-name*
- Configure ATF policies by entering these commands:
  - **config atf policy create** *policy-id policy-name policy-weight*
  - **config atf policy modify** {**weight** *policy-weight policy-name*} | {**client-sharing** {**enable** | **disable**} *policy-name*}
  - **config atf policy delete** *policy-name*
- Configure WLAN with a policy ID by entering this command:
  - **config wlan atf** *wlan-id* **policy** *policy-id*
- Configure AP group-level override for Cisco ATF policy on a WLAN by entering these commands:
  - **config wlan apgroup atf 802.11**{**a** | **b**} **policy** *ap-group-name wlan-id policy-name* **override** {**enable** | **disable**}
- Configure AP-level override for Cisco ATF policy on a WLAN by entering these commands:
  - **config ap atf 802.11**{**a** | **b**} **policy** *wlan-id policy-name ap-name* **override** {**enable** | **disable**}
- Monitor Cisco ATF configurations by entering these commands:
  - **show atf config all**
  - **show atf config ap-name** *ap-name*
  - **show atf config apgroup** *ap-group-name*
  - **show atf config 802.11**{**a** | **b**}
  - **show atf config policy**
  - **show atf config wlan**
  - **show atf statistics ap** *ap-name* **802.11**{**a** | **b**} **summary**
  - **show atf statistics ap** *ap-name* **802.11**{**a** | **b**} **wlan** *wlan-id*

- **show atf statistics ap** *ap-name* **802.11**{**a** | **b**} **policy** *policy-name*