Quality of Service

Quality of Service

Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

The controller supports four QoS levels:

- Platinum/Voice—Ensures a high quality of service for voice over wireless.
- Gold/Video—Supports high-quality video applications.
- Silver/Best Effort—Supports normal bandwidth for clients. This is the default setting.
- Bronze/Background—Provides the lowest bandwidth for guest services.

Note VoIP clients should be set to Platinum.

You can configure the bandwidth of each QoS level using QoS profiles and then apply the profiles to WLANs. The profile settings are pushed to the clients associated to that WLAN. In addition, you can create QoS roles to specify different bandwidth levels for regular and guest users. Follow the instructions in this section to configure QoS profiles and QoS roles. You can also define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN.

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.

This section contains the following subsections:

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 1: 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
...
```

Quality of Service Roles

After you configure a QoS profile and apply it to a WLAN, it limits the bandwidth level of clients associated to that WLAN. Multiple WLANs can be mapped to the same QoS profile, which can result in bandwidth contention between regular users (such as employees) and guest users. In order to prevent guest users from using the same level of bandwidth as regular users, you can create QoS roles with different (and presumably lower) bandwidth contracts and assign them to guest users.

You can configure up to ten QoS roles for guest users.

Note If you choose to create an entry on the RADIUS server for a guest user and enable RADIUS authentication for the WLAN on which web authentication is performed rather than adding a guest user to the local user database from the controller, you need to assign the QoS role on the RADIUS server itself. To do so, a "guest-role" Airespace attribute called the *Airespace-Guest-Role-Name* with the attribute identifier value of 11 and the datatype of string, which should match the name of the "guest-role" configured on the controller, needs to be added on the RADIUS server. This attribute is sent to the controller when authentication occurs. If a role with the name returned from the RADIUS server is found configured on the controller, the bandwidth associated with that role is enforced for the guest user after authentication completes successfully.

Ensure that the Layer 3 security of *Web Policy* is configured on the WLAN before the AAA parameter is processed by the controller. If the WLAN does not have a Layer 3 Security of *Web Policy*, the AAA parameter is ignored.

This section contains the following subsections:

Configuring QoS Roles (GUI)

Procedure

Step 1 Choose **Wireless** > **QoS** > **Roles** to open the QoS Roles for the Guest Users page.

This page shows any existing QoS roles for guest users.

Note If you want to delete a QoS role, hover your cursor over the blue drop-down arrow for that role and choose **Remove**.

Step 2 Click **New** to create a new QoS role. The **QoS Role Name > New** page appears.

Step 3 In the **Role Name** text box, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on).

Step 4 Click **Apply**.

Step 5 Click the name of the QoS role to edit the bandwidth of a QoS role. The **Edit QoS Role Data Rates** page appears.

Note The values that you configure for the per-user bandwidth contracts affect only the amount of bandwidth going downstream (from the access point to the wireless client). They do not affect the bandwidth for upstream traffic (from the client to the access point).

Note The Access Points that support per-user bandwidth contracts for upstream (from the client to the access point) are - AP1140, AP1040, AP3500, AP3600, AP1250, and AP1260.

Step 6 Define the average data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the **Average Data Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 7 Define the peak data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the Burst Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

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.

Step 8 Define the average real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the **Average Real-Time Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 9 Define the peak real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the **Burst Real-Time Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

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 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Step 12 Apply a QoS role to a guest user by following the instructions in the Configuring Local Network Users for the Controller (GUI) section.

Configuring QoS Roles (CLI)

Procedure

Step 1 Create a QoS role for a guest user by entering this command:

config netuser guest-role create *role_name*

Note If you want to delete a QoS role, enter the **config netuser guest-role delete** *role_name* command.

Step 2 Configure the bandwidth contracts for a QoS role by entering these commands:

- **config netuser guest-role qos data-rate average-data-rate** *role_name rate*—Configures the average data rate for TCP traffic on a per-user basis.
- **config netuser guest-role qos data-rate burst-data-rate** *role_name rate*—Configures the peak data rate for TCP traffic on a per-user basis.

  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.

- **config netuser guest-role qos data-rate average-realtime-rate** *role_name rate*—Configures the average real-time rate for UDP traffic on a per-user basis.
- **config netuser guest-role qos data-rate burst-realtime-rate** *role_name rate*—Configures the peak real-time rate for UDP traffic on a per-user basis.

  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.

  Note For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 3 Apply a QoS role to a guest user by entering this command:

config netuser guest-role apply *username role_name*

For example, the role of *Contractor* could be applied to guest user *jsmith*.

Note If you do not assign a QoS role to a guest user, the Role text box in the User Details shows the role as "default." The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

Note If you want to unassign a QoS role from a guest user, enter the **config netuser guest-role apply** *username* **default command**. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

Step 4 Save your changes by entering this command:

save config

Step 5 See a list of the current QoS roles and their bandwidth parameters by entering this command:

show netuser guest-roles

Information similar to the following appears:

```
Role Name..................................... Contractor
     Average Data Rate..... 10
     Burst Data Rate..... 10
     Average Realtime Rate..... 100
     Burst Realtime Rate..... 100

Role Name..................................... Vendor
     Average Data Rate..... unconfigured
     Burst Data Rate..... unconfigured
     Average Realtime Rate..... unconfigured
     Burst Realtime Rate..... unconfigured
```

QoS Map

The QoS Map feature maintains the QoS policies in situations where appropriate QoS markings that match the application type are not marked by clients or applications. The administrator gets to map the differentiated services code point (DSCP) to user priority (UP) values and also is able to mark from UP to DSCP in a controller.

With QoS in enabled state, the QoS feature is advertised by the AP in the frame. The map is propagated through a frame to a compatible device when it associates or re-associates with the network.

With QoS in disabled state, the default map is propagated to the AP and the clients from controller.

This feature is supported on all Cisco AP models.

This section contains the following subsections:

Guidelines and Restrictions for QoS Map

- You can configure QoS Map only when this feature is in disabled state.
- This feature does not function with non-801.11u supported hardware. The frames with QoS map is not sent to these clients, yet, the packets sent by these clients follow the DSCP-UP map that you have configured.
- Ensure that you configure all UP values from 0 to 7 before QoS Map is enabled.
- Ensure the DSCP range for each user priority is non-overlapping.
- Ensure the DSCP High Value is greater than or equal to the DSCP Low Value.
- You can configure up to 21 exceptions at a time.
- You must disable your network before you can enable QoS maps.

- The Trust DSCP Upstream feature does not have any dependency on the QoS Map feature. If you do not want to use any QoS Map features and want to leave it disabled, but do want to trust the upstream client DSCP markings, we recommend that you enable Trust DSCP Upstream using the CLI. Use of the CLI to enable or disable Trust DSCP Upstream circumvents the GUI restriction to disable the 802.11 networks.

Configuring QoS Map (GUI)

Before you begin

We recommend that you disable QoS Map to change the QoS map configuration. When the QoS map is disabled, the DSCP values reset to default values automatically.

Note

- To enable the QoS map after configuring the values, the following conditions must be met:
  - Configure all the UP values.
  - Do not overlap DSCP ranges for UP values. For example, if UP1 value range is 10 to 20, do not use any of the numbers within 10 and 20 for any other UP value range.

Procedure

Step 1 Disable the 802.11a/n/ac and 802.11b/g/n networks so that you can configure the QoS map.

To disable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, uncheck the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

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

Step 3 To disable the QoS Map feature, perform the following steps:

a. From the **QoS Map** drop-down list, choose **Disable**.

b. To reset the DSCP Exception values, select the **Default** option.

The **Default** option resets the UP to DSCP and DSCP to UP table values to 255. This also adds DSCP UP exceptions if not present previously.

Step 4 To modify the **UP to DSCP Map**, perform the following steps:

a. From the **User Priority** drop-down list, select the value.

b. Enter the **DSCP Default**, **DSCP Start**, **DSCP End** values.

c. Click **Modify**.

Step 5 To create a DSCP exception, perform the following steps:

a. Enter the **DSCP Exception** value.

b. From the **User Priority** drop-down list, select the value.

c. Click **Add**.

Step 6 To delete a DSCP Exception, hover your cursor over the blue drop-down arrow for the DSCP Exception and click **Remove**.

Click **OK** when you are prompted to confirm your action.

Step 7 To clear the DSCP Exception list, click **Clear ALL**.

Step 8 Check or uncheck the **Trust DSCP UpStream** check box to enable or disable the marking of the upstream packets.

Step 9 To enable the QoS Map feature, choose **Enable** from the **QoS Map** drop-down list.

Step 10 Click **Apply**.

Step 11 Reenable the 802.11 networks.

To enable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, check the **802.11a** (or **802.11b/g**) **Network Status** check box.

Step 12 Save your configuration.

Configuring QoS Map (CLI)

Procedure

- Enable, disable or revert to default map by entering this command:

  config qos qos-map {**enable** | **disable** | **default**}

  The default command resets the UP to DSCP and DSCP to UP table values to default values (255). This also adds DSCP UP exceptions if not present previously.

- Set DSCP range for UP by entering this command:

  config qos qosmap up-to-dscp-map *up dscp-default dscp-start dscp-end*

  You can run the above command in the following situations:

  - Clients are QoS map supportive and marks the DSCP or UP with unusual value and the clients
  - Clients are not QoS map supportive, then this allows the administrator to map particular UP to DSCP upstream and downstream of Client Packets

- Set an exception for DSCP by entering this command:

  config qos qosmap dscp-up-to-exception *dscp up*

  You can run the above command in situations when the client marks DSCP with an unusual value.

- Delete a specific DSCP exception by entering this command:

  config qos qosmap delete-dscp-exception *dscp*

  You can run the above command in situations when specific exceptions are to be deleted from the QoS map.

- Delete all exceptions by entering this command:

  config qos qosmap clear-all

  You can run the above command in a situation where all the values needs to be cleared from the map.

- Enable or disable marking of the upstream packets using the client DSCP by entering this command:

  config qos qosmap trust-dscp-upstream {**enable** | **disable** }

  You can run the above command in situations where the client marks DSCP and not UP, or marks UP to an unusual value. When in enabled state, it will use the DSCP to mark the upstream packets at AP instead of UP

- See the QoS mapping configuration by entering this command:

  show qos qosmap

SIP (Media Session) Snooping, CAC, and Reporting

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

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

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

This section contains the following subsections:

Restrictions for SIP (Media Session) Snooping, CAC, and Reporting

SIP snooping is not supported in FlexConnect in Release 8.5 and later releases.

Configuring Media Session Snooping (GUI)

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 media session snooping.

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

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

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

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

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

b) Scroll to the right and click the **Detail** link for the access point for which you want to view VoIP statistics. The **Radio > Statistics** page appears.

The VoIP Stats section shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the controller.

Step 8 Choose **Management** > **SNMP** > **Trap Logs** to see the traps generated for failed calls. The Trap Logs page appears.

For example, log 0 in the figure shows that a call failed. The log provides the date and time of the call, a description of the failure, and the reason why the failure occurred.

Configuring Media Session Snooping (CLI)

Procedure

Step 1 Enable or disable VoIP snooping for a particular WLAN by entering this command:

config wlan call-snoop {**enable** | **disable**} *wlan_id*

Step 2 Save your changes by entering this command:

save config

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

show wlan *wlan_id*

Information similar to the following appears:

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

Step 4 See the call information for an MSA client when media session snooping is enabled and the call is active by entering this command:

show call-control client callInfo *client_MAC_address*

Information similar to the following appears:

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

Step 5 See the metrics for successful calls or the traps generated for failed calls by entering this command:

show call-control ap {**802.11a** | **802.11b**} *Cisco_AP* {**metrics** | **traps**}

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

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

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

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

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

Table 2: Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotallowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.
406	notAcceptabl	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header text box sent in the request.

Error Code	Integer	Description
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time, if it could not determine the location of the user in time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header text box.
480	temporarilyNotAvailable	The callee’s end system was contacted successfully, but the callee is currently unavailable.
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header text box with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee’s end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.

Error Code	Integer	Description
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

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

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:

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. It works by rejecting requested calls (traffic streams) if the channel lacks the capacity to service the request. It requires that WMM be enabled on the WLAN. CAC is also known as ACM (Admission Control).

The following two types of CAC are available:

- Load-based CAC (recommended): All channel utilization (QBSS) is considered, including interference and noise, as well as AP traffic.
- Static CAC: Only the traffic to and from this AP is considered when evaluating the channel's capacity.

The following restrictions apply:

- CAC is not supported in FlexConnect local authentication, resulting in voice traffic not getting properly tagged.
- CAC supports the following PHY rates: 6,11,12,24 megabits per second. If CAC is enabled, then at least one of these rates should be enabled on the AP.

This section contains the following subsections:

Static CAC

Static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of static CAC support. To use static CAC with voice applications, the WLAN must be configured for Platinum QoS. To use static CAC with video applications, the WLAN must be configured for Gold QoS. Also, make sure that WMM is enabled for the WLAN. See the 802.3 Bridging section for QoS and WMM configuration instructions.

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, static CAC does not operate properly.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types (including that from clients), co-channel access point loads, and collocated channel interference, for voice applications. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point continuously measures and updates the utilization of the RF channel (that is, the percentage of bandwidth that has been exhausted), channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Expedited Bandwidth Requests

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

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

Table 3: TSPEC Request Handling Examples

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

[1] For static CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

[2] Static CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

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

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

U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual

packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Traffic Stream Metrics

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

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

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

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

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

Table 4: TSM Entries in Cisco 5508 and Flex 7510 WLCs

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

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

Configuring Voice Parameters

Configuring Voice Parameters (GUI)

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.

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_mac* | **all**}

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

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

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

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

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

Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point by entering this command:

show ap stats {**802.11a** | **802.11b**} *ap_name* **tsm** {*client_mac* | **all**}

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

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

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

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

Step 6 Enable or disable debugging for call admission control (CAC) messages, events, or packets by entering this command:

debug cac {**all** | **event** | **packet**} {**enable** | **disable**}

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

Step 7 Use the following command to perform voice diagnostics and to view the debug messages between a maximum of two 802.11 clients:

debug voice-diag {**enable** | **disable**} *mac-id mac-id2* [**verbose**]

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

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

Note The debug command automatically stops after 60 minutes.

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

- **show client voice-diag status**

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

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

- **show client voice-diag tspec**

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

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

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

- **show client voice-diag avrg_rssi**

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

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

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

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

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

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

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

SIP-based CAC

This section contains the following subsections:

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**}

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.

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** }

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

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

Step 4 View the current status of MAC (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**.