



Quality of Service

- [Configuring Quality of Service, page 1](#)
- [Quality of Service Roles, page 8](#)
- [Configuring QoS Mapping, page 10](#)
- [Fastlane QoS, page 13](#)
- [Media and EDCA, page 24](#)

Configuring Quality of Service

Information About 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.

Configuring Quality of Service Profiles

You can configure the Platinum, Gold, Silver, and Bronze QoS profiles.

Configuring QoS Profiles (GUI)

-
- Step 1** Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles. To disable the radio networks, choose **Wireless > 802.11a/n/ac** or **802.11b/g/n > Network**, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.
- Step 2** Choose **Wireless > QoS > Profiles** to open the QoS Profiles page.
- Step 3** Click the name of the profile that you want to configure to open the Edit QoS Profile page.
- Step 4** Change the description of the profile by modifying the contents of the Description text box.
- Step 5** Define the data rates on a per-user basis as follows:
- a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.
 - b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

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

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

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.
 - d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
- Step 6** Define the data rates on a per-SSID basis as follows:
- a) Define the average data rate TCP traffic per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.
 - b) Define the peak data rate for TCP traffic per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

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

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

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

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

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

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

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

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

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Step 11 Reenable the 802.11 networks.

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

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

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

Step 14 Click **Apply**.

Step 15 Click **Save Configuration**.

Configuring QoS Profiles (CLI)

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

config 802.11 {a | b} disable network

- Step 2** Change the profile description by entering this command:
config qos description {bronze | silver | gold | platinum} *description*
- Step 3** Define the average data rate for TCP traffic per user or per SSID by entering this command:
config qos average-data-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} *rate*
- Note** For the *rate* parameter, you can enter a value between 0 and 512,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.
- Step 4** Define the peak data rate for TCP traffic per user or per SSID by entering this command:
config qos burst-data-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} *rate*
- Step 5** Define the average real-time data rate for UDP traffic per user or per SSID by entering this command:
config qos average-realtime-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} *rate*
- Step 6** Define the peak real-time data rate for UDP traffic per user or per SSID by entering this command:
config qos burst-realtime-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} *rate*
- Step 7** Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN by entering this command:
config qos priority {bronze | gold | platinum | silver} {*maximum priority*} {*default unicast priority*} {*default multicast priority*}
- You choose from the following options for the *maximum priority*, *default unicast priority*, and *default multicast priority* parameters:
- besteffort
 - background
 - video
 - voice
- Step 8** Define the maximum value (0–7) for the priority tag associated with packets that fall within the profile, by entering these commands:
config qos protocol-type {bronze | silver | gold | platinum} dot1p
config qos dot1p-tag {bronze | silver | gold | platinum} *tag*
- The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.
- Note** The 802.1p tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for a QoS profile.
- Note** If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.
- Step 9** Reenable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:
config 802.11 {a | b} enable network
- Step 10** Apply the new QoS profile to a WLAN, by entering these commands:

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

QoS Profile per WLAN

Information About QoS Profiles

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

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

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

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

Table 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 MSB bits of DSCP.

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

Assigning a QoS Profile to a WLAN (GUI)

Before You Begin

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

-
- Step 1** Choose **WLANs** to open the WLANs page.
- Step 2** Click the ID number of the WLAN to which you want to assign a QoS profile.
- Step 3** When the **WLANs > Edit** page appears, choose the **QoS** tab.
- Step 4** From the **Quality of Service (QoS)** drop-down list, choose one of the following:
- **Platinum (voice)**
 - **Gold (video)**
 - **Silver (best effort)**
 - **Bronze (background)**
- Note** Silver (best effort) is the default value.
- Step 5** To define the data rates on a per-user basis, do the following:
- a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.
 - b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

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

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

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.
 - d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

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

- Step 6** To define the data rates on a per-SSID basis, do the following:
- 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.
 - 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.
 - 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.
 - Define the peak real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic in the WLANs.
- Step 7** Click **Apply**.
- Step 8** Click **Save Configuration**.
-

Assigning a QoS Profile to a WLAN (CLI)

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

-
- Step 1** Assign a QoS profile to a WLAN by entering this command:
config wlan qos wlan_id {bronze | silver | gold | platinum}
 Silver is the default value.
- Step 2** To override QoS profile rate limit parameters, enter this command:
config wlan override-rate-limit wlan-id {average-data-rate | average-realtime-rate | burst-data-rate | burst-realtime-rate} {per-ssid | per-client} {downstream | upstream} rate
- Step 3** Enter the **save config** command.
- Step 4** Verify that you have properly assigned the QoS profile to the WLAN by entering this command:
show wlan wlan_id
 Information similar to the following appears:

```

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

```

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

```

Quality of Service Roles

Information About 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 needs to be added on the RADIUS server with a datatype of “string” and a return value of “11.” 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 to that role is enforced for the guest user after authentication completes successfully.

Configuring QoS Roles (GUI)

-
- 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)

- 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

```

Configuring QoS Mapping

Information About 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 Cisco WLC.

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 Cisco WLC.

This feature is supported on all Cisco AP models.

Restrictions in QoS Map

- QoS Map feature is not configurable on the Cisco WLC GUI
- 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
- Network needs to be disabled before enabling the QoS maps

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.

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:
- 1 From the **QoS Map** drop-down list, choose **Disable**.
 - 2 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:
- 1 From the **User Priority** drop-down list, select the value.
 - 2 Enter the **DSCP Default**, **DSCP Start**, **DSCP End** values.
 - 3 Click **Modify**.
- Step 5** To create a DSCP exception, perform the following steps:
- 1 Enter the **DSCP Exception** value.
 - 2 From the **User Priority** drop-down list, select the value.
 - 3 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**, select the **802.11a** (or **802.11b/g**) **Network Status** check box.
- Step 12** Save your configuration.
-

Configuring QoS Map (CLI)

- 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

Fastlane QoS

Configuring Fastlane QoS (CLI)

The Fastlane QoS feature provides increased quality of service (QoS) treatment for iOS 10 or higher clients. This feature is disabled by default.



Note

You should enable or disable this feature only during a maintenance window when not many clients are connected, as there will be a disruption in service when all the WLANs and the network are disabled and enabled again.



Note

When Flex Local switching is enabled on the WLAN, default Flex AVC profile is not created and mapped to the WLAN, unlike AUTOQOS-AVC-PROFILE, which is created for central switching and mapped to a WLAN.

Enabling Fastlane QoS per WLAN

To enable the Fastlane QoS feature per WLAN, use **config qos fastlane enable wlan_id** command.

When you run the **config qos fastlane enable wlan_id** command, fastlane is activated on the target WLAN, which enables supporting iOS 10 devices to activate a QoS whitelist in their profile, if present. The command also runs the commands listed in the following table.



Note

If the commands are executed, then Fastlane QoS feature is enabled and applied to the target WLAN. If a command that is associated with the Fastlane QoS feature fails while is being enabled on a WLAN, all the changes will be reverted to their original values, except for QoS map. The QoS map value will revert to the default value instead of the previously configured value. Also, the new AVC Profile will not be deleted; it will only be removed from the WLAN.

Table 2: Commands Executed for Enabling Fastlane QoS

Description	Commands
Temporarily disables 802.11a and 802.11b networks and WLANs.	<ul style="list-style-type: none"> • config 802.11a disable network • config 802.11b disable network • config wlan disable all
Configures the Platinum QoS profile to set unmarked (best effort) unicast packets, and multicast packets, to best effort over wifi link.	<ul style="list-style-type: none"> • config qos priority platinum voice besteffort besteffort
Disables 802.1p marking (all wired marking is DSCP-based).	<ul style="list-style-type: none"> • config qos protocol-type platinum none
Disables bandwidth limitation for UDP traffic.	<ul style="list-style-type: none"> • config qos average-realtime-rate platinum per-ssid downstream 0
Disables bandwidth limitation for UDP bursts.	<ul style="list-style-type: none"> • config qos burst-realtime-rate platinum per-ssid downstream 0
Enables ACM for 5 GHz and 2.4 GHz.	<ul style="list-style-type: none"> • config 802.11a cac voice acm enable • config 802.11b cac voice acm enable
Limits allocation for voice traffic to 50 percent of available bandwidth on any 5 GHz or 2.4 GHz radio.	<ul style="list-style-type: none"> • config 802.11a cac voice max-bandwidth 50 • config 802.11b cac voice max-bandwidth 50

Description	Commands
Allocates 6 percent of the bandwidth to voice users for roaming.	<ul style="list-style-type: none"> • config 802.11a cac voice roam-bandwidth 6 • config 802.11b cac voice roam-bandwidth 6
Sets the EDCA parameters to their values recommended by 802.11-2017.	<ul style="list-style-type: none"> • config advanced 802.11b edca-parameter fastlane • config advanced 802.11a edca-parameter fastlane
Enables expedited bandwidth for 5 GHz and 2.4 GHz.	<ul style="list-style-type: none"> • config 802.11a exp-bwreq enable • config 802.11b exp-bwreq enable
Configures the user priority (UP) to differentiated services code point (DSCP) maps.	<ul style="list-style-type: none"> • config qos qosmap disable • config qos qosmap default • config qos qosmap up-to-dscp-map 0 0 0 7 • config qos qosmap up-to-dscp-map 1 8 8 15 • config qos qosmap up-to-dscp-map 2 16 16 23 • config qos qosmap up-to-dscp-map 3 24 24 31 • config qos qosmap up-to-dscp-map 4 32 32 39 • config qos qosmap up-to-dscp-map 5 34 40 47 • config qos qosmap up-to-dscp-map 6 46 48 62 • config qos qosmap up-to-dscp-map 7 56 63 63 • config qos qosmap clear all

Description	Commands
Configures DSCP-to-UP mapping exceptions.	

Description	Commands
	<ul style="list-style-type: none"> • <code>config qos qosmap dscp-to-up-exception 56 0</code> • <code>config qos qosmap dscp-to-up-exception 48 0</code> • <code>config qos qosmap dscp-to-up-exception 46 6</code> • <code>config qos qosmap dscp-to-up-exception 44 6</code> • <code>config qos qosmap dscp-to-up-exception 40 5</code> • <code>config qos qosmap dscp-to-up-exception 38 4</code> • <code>config qos qosmap dscp-to-up-exception 36 4</code> • <code>config qos qosmap dscp-to-up-exception 34 4</code> • <code>config qos qosmap dscp-to-up-exception 32 5</code> • <code>config qos qosmap dscp-to-up-exception 30 4</code> • <code>config qos qosmap dscp-to-up-exception 28 4</code> • <code>config qos qosmap dscp-to-up-exception 26 4</code> • <code>config qos qosmap dscp-to-up-exception 24 4</code> • <code>config qos qosmap dscp-to-up-exception 22 3</code> • <code>config qos qosmap dscp-to-up-exception 20 3</code> • <code>config qos qosmap dscp-to-up-exception 18 3</code> • <code>config qos qosmap dscp-to-up-exception 16 0</code> • <code>config qos qosmap dscp-to-up-exception 14 2</code> • <code>config qos qosmap dscp-to-up-exception 12 2</code>

Description	Commands
	<ul style="list-style-type: none"> • config qos qosmap dscp-to-up-exception 10 2 • config qos qosmap dscp-to-up-exception 8 1
Enables DSCP-Trust (new QoS maps).	<ul style="list-style-type: none"> • config qos qosmap trust-dscp-upstream enable • config qos qosmap enable
Creates the Application Visibility and Control (AVC) profile.	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE create
Configures AVC to mark voice applications and subcomponents to expedited forwarding (EF) (DSCP 46).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-audio mark 46 • config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-audio mark 46 • config avc profile AUTOQOS-AVC-PROFILE rule add application ms-lync-audio mark 46 • config avc profile AUTOQOS-AVC-PROFILE rule add application citrix-audio mark 46
Configures AVC to mark multimedia conferencing applications to assured forwarding (AF) 41 (DSCP 34).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-video mark 34 • config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-video mark 34 • config avc profile AUTOQOS-AVC-PROFILE rule add application ms-lync-video mark 34 • config avc profile AUTOQOS-AVC-PROFILE rule add application webex-media mark 34

Description	Commands
Configures AVC to mark multimedia streaming applications to AF31 (DSCP 26).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application citrix mark 26 • config avc profile AUTOQOS-AVC-PROFILE rule add application pcoip mark 26 • config avc profile AUTOQOS-AVC-PROFILE rule add application vnc mark 26 • config avc profile AUTOQOS-AVC-PROFILE rule add application vnc-http mark 26
Configures AVC to mark signaling protocols to CS3 (DSCP 24).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application skinny mark 24 • config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-control mark 24 • config avc profile AUTOQOS-AVC-PROFILE rule add application sip mark 24 • config avc profile AUTOQOS-AVC-PROFILE rule add application sip-tls mark 24
Configures AVC to mark transactional data applications to AF21 (DSCP 18).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-im mark 18 • config avc profile AUTOQOS-AVC-PROFILE rule add application ms-office-web-apps mark 18 • config avc profile AUTOQOS-AVC-PROFILE rule add application salesforce mark 18 • config avc profile AUTOQOS-AVC-PROFILE rule add application sap mark 18

Description	Commands
Configures AVC to mark OAM applications to CS2 (DSCP 16).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application dhcp mark 16 • config avc profile AUTOQOS-AVC-PROFILE rule add application dns mark 16 • config avc profile AUTOQOS-AVC-PROFILE rule add application ntp mark 16 • config avc profile AUTOQOS-AVC-PROFILE rule add application snmp mark 16
Configures AVC to mark bulk data applications marking to AF11 (DSCP 10).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application ftp mark 10 • config avc profile AUTOQOS-AVC-PROFILE rule add application ftp-data mark 10 • config avc profile AUTOQOS-AVC-PROFILE rule add application ftps-data mark 10 • config avc profile AUTOQOS-AVC-PROFILE rule add application cifs mark 10
Configures AVC to mark scavenger applications to CS1 (DSCP 8).	<ul style="list-style-type: none"> • config avc profile AUTOQOS-AVC-PROFILE rule add application netflix mark 8 • config avc profile AUTOQOS-AVC-PROFILE rule add application youtube mark 8 • config avc profile AUTOQOS-AVC-PROFILE rule add application skype mark 8 • config avc profile AUTOQOS-AVC-PROFILE rule add application bittorrent mark 8
Applies the platinum QoS profile to the WLAN.	<ul style="list-style-type: none"> • config wlan qos <i>wlan_id</i> platinum

Description	Commands
Applies the AVC profile AUTOQOS-AVC-PROFILE to the WLAN ID <i>wlan-id</i> if AVC visibility is enabled on the WLAN.	<ul style="list-style-type: none"> • config wlan avc <i>wlan_id</i> profile AUTOQOS-AVC-PROFILE enable
Re-enables 802.11a and 802.11b networks and WLANs.	<ul style="list-style-type: none"> • config 802.11a enable network • config 802.11b enable network • config wlan enable all

Disabling Fastlane QoS in WLANs

To disable Fastlane QoS in WLANs, use the **config qos fastlane disable *wlan_id*** command.

When you disable fastlane for a target WLAN, supporting iOS 10 devices stop using a QoS whitelist for that WLAN. Disabling fastlane for a target WLAN also returns the WLAN configuration to QoS defaults as per the following table.



Note

When the Fastlane QoS feature is disabled per WLAN, all the values will revert to the default state, except the WLAN status, which moves to the previous state.

While disabling Fastlane QoS in WLANs, if media stream is enabled, it will be disabled before enabling a Silver profile to QoS.

Table 3: Commands Executed for Disabling Fastlane QoS in WLAN

Description	Commands
Disables the WLANs to make changes to WLAN configuration. Note If Call Snooping and KTS are enabled, then they will be disabled.	<ul style="list-style-type: none"> • config wlan disable <i>wlan_id</i>
Applies the Silver (default) QoS profile to the WLAN.	<ul style="list-style-type: none"> • config wlan qos <i>wlan_id</i> silver
Removes the AVC profile AUTOQOS-AVC-PROFILE from the WLAN ID <i>wlan-id</i> , if attached.	<ul style="list-style-type: none"> • config wlan avc <i>wlan_id</i> profile AUTOQOS-AVC-PROFILE disable
Reverts the WLAN to the earlier state (if WLAN was in Enabled state before, it will revert to Enabled state and if WLAN was in Disabled state, it will revert to Disabled state).	<ul style="list-style-type: none"> • config wlan enable <i>wlan_id</i>

Disabling Fastlane QoS Globally

To disable Fastlane QoS globally, use the **config qos fastlane disable global** command.

When the Fastlane QoS feature is disabled globally, the WLC QoS configuration will be reverted back to the default values shown in the following table.



Note

Fastlane QoS must be disabled on all the WLANs before **config qos fastlane disable global** command is executed.

If a command associated with the Fastlane QoS feature fails while the command is being enabled globally, all the changes will be reverted to their original values, except QoS map, whose value is reverted to the default, instead of the previously configured value.

Table 4: Commands Executed for Disabling Fastlane QoS Globally

Description	Commands
Temporarily disable 802.11a and 802.11b networks to make changes to QoS Profiles.	<ul style="list-style-type: none"> • config 802.11a disable network • config 802.11b disable network
Disable all the WLANs to make changes to QoS profile.	<ul style="list-style-type: none"> • config wlan disable all
Reverts the Platinum QoS profile to the default QoS configuration.	<ul style="list-style-type: none"> • config qos priority platinum voice voice voice • config qos protocol-type platinum none • config qos average-realtime-rate platinum per-ssid downstream 0 • config qos burst-realtime-rate platinum per-ssid downstream 0
Disables ACM for 2.4 GHz and 5 GHz. Also, reverts Video CAC to its defaults.	<ul style="list-style-type: none"> • config 802.11a cac voice acm disable • config 802.11b cac voice acm disable • config 802.11a cac video max-bandwidth 5 • config 802.11b cac video max-bandwidth 5
Limits voice traffic to the default of the total bandwidth for 2.4 GHz and 5 GHz.	<ul style="list-style-type: none"> • config 802.11a cac voice max-bandwidth 75 • config 802.11b cac voice max-bandwidth 75

Description	Commands
Reverts roaming bandwidth for voice users to its default values.	<ul style="list-style-type: none"> • config 802.11a cac voice roam-bandwidth 6 • config 802.11b cac voice roam-bandwidth 6
Reverts the EDCA parameters to their defaults.	<ul style="list-style-type: none"> • config advanced 802.11b edca-parameter wmm-default • config advanced 802.11a edca-parameter wmm-default
Disables the expedited bandwidth for 2.4 GHz and 5 GHz.	<ul style="list-style-type: none"> • config 802.11a exp-bwreq disable • config 802.11b exp-bwreq disable
Disables the UP-to-DSCP maps.	<ul style="list-style-type: none"> • config qos qosmap disable • config qos qosmap default
Re-enable the 802.11a and 802.11b networks.	<ul style="list-style-type: none"> • config 802.11a enable network • config 802.11b enable network
Reverts the WLAN to the earlier state (if WLAN was in Enabled state before, it will revert to Enabled state and if WLAN was in Disabled state, it will revert to Disabled state.)	config wlan enable <i>wlan-id</i>

Configuring Fastlane QoS (GUI)

-
- Step 1** Select **WLANs** to open the **WLANs** window.
- Step 2** Select **QoS** to open the **WLANs > Edit** window.
- Step 3** From the **Fastlane** drop-down, enable or disable Fastlane QoS.
- Step 4** Click **Apply** to save your settings.
-

Disabling Fastlane QoS Globally (GUI)

-
- Step 1** Choose **Wireless > Advanced > QoS > Fastlane** to open the **Fastlane Configuration** window.
- Step 2** Click **Apply** at the Revert Fastlane AutoQoS global parameters to defaults to disable Fastlane globally.
-

Media and EDCA

Aggressive Load Balancing

Information About Configuring Aggressive Load Balancing

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

**Note**

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

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

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

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

**Note**

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

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

**Note**

Cisco 600 Series OfficeExtend Access Points do not support client load balancing.
With the 7.4 release, FlexConnect access points do support client load balancing.

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

**Note**

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

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

Configuring Aggressive Load Balancing (GUI)

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

Step 2 In the Client Window Size text box, enter a value between 1 and 20.

The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

$$\text{load-balancing window} + \text{client associations on AP with the lightest load} = \text{load-balancing threshold}$$

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

Step 3 In the Maximum Denial Count text box, enter a value between 0 and 10.

The denial count sets the maximum number of association denials during load balancing.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

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

- Choose **WLANs > WLAN ID**. The WLANs > Edit page appears.
- In the **Advanced** tab, select or unselect the **Client Load Balancing** check box.
- Click **Apply**.
- Click **Save Configuration**.

Configuring Aggressive Load Balancing (CLI)

-
- Step 1** Set the client window for aggressive load balancing by entering this command:
config load-balancing window *client_count*
 You can enter a value between 0 and 20 for the *client_count* parameter.
- Step 2** Set the denial count for load balancing by entering this command:
config load-balancing denial *denial_count*
 You can enter a value between 1 and 10 for the *denial_count* parameter.
- Step 3** Save your changes by entering this command:
save config
- Step 4** Enable or disable aggressive load balancing on specific WLANs by entering this command:
config wlan load-balance allow {**enable** | **disable**} *wlan_ID*
 You can enter a value between 1 and 512 for *wlan_ID* parameter.
- Step 5** Verify your settings by entering this command:
show load-balancing
- Step 6** Save your changes by entering this command:
save config
- Step 7** Configure the load balance mode on a WLAN by entering this command:
config wlan load-balance mode {*client-count* | *uplink-usage*} *wlan-id*
 This feature requires the AP to upload its uplink usage statistics to the controller periodically. Check these statistics by entering this command:
show ap stats system *cisco-AP*
-

Media Session and Snooping

Information About Media Session Snooping and Reporting

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

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

WMM clients and at the access point for non-WMM clients. The access points notify the controller and Cisco Prime Infrastructure of any major call events, such as call establishment, termination, and failure.

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

Restrictions for Media Session Snooping and Reporting

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

Configuring Media Session Snooping (GUI)

-
- Step 1** Choose **WLANs** to open the WLANs page.
- Step 2** Click the ID number of the WLAN for which you want to configure media session snooping.
- Step 3** On the **WLANs > Edit** page, click the **Advanced** tab.
- Step 4** Under Voice, select the **Media Session Snooping** check box to enable media session snooping or unselect it to disable this feature. The default value is unselected.
- Step 5** Click **Apply**.
- Step 6** Click **Save Configuration**.
- Step 7** See the VoIP statistics for your access point radios as follows:
- a) Choose **Monitor > Access Points > Radios > 802.11a/n/ac** or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.
 - b) Scroll to the right and click the **Detail** link for the access point for which you want to view VoIP statistics. The **Radio > Statistics** page appears.
The VoIP Stats section shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the controller.
- Step 8** Choose **Management > SNMP > Trap Logs** to see the traps generated for failed calls. The Trap Logs page appears. For example, log 0 in the figure shows that a call failed. The log provides the date and time of the call, a description of the failure, and the reason why the failure occurred.
-

Configuring Media Session Snooping (CLI)

-
- Step 1** Enable or disable VoIP snooping for a particular WLAN by entering this command:
config wlan call-snoop {enable | disable} wlan_id
- Step 2** Save your changes by entering this command:

save config

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

show wlan *wlan_id*

Information similar to the following appears:

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

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

show call-control client callInfo *client_MAC_address*

Information similar to the following appears:

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

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

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

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

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

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

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

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

Table 5: Error Codes for Failed VoIP Calls

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

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

Error Code	Integer	Description
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

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

QoS Enhanced BSS

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

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

- Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11b dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The 7921 or 7920 phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- Both the 7921 and 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7921 or 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7921 or 7920.
- For standalone 7921 phones, load-based CAC must be enabled, and the WMM Policy must be set to Required on the WLAN.
- The controller supports traffic classification (TCLAS) coming from 7921 phones using firmware version 1.1.1. This feature ensures proper classification of voice streams to the 7921 phones.
- When using a 7921 phone with the 802.11a radio of a 1242 series access point, set the 24-Mbps data rate to Supported and choose a lower Mandatory data rate (such as 12 Mbps). Otherwise, the phone might experience poor voice quality.

Information About QoS Enhanced BSS

The QoS Enhanced Basis Service Set (QBSS) information element (IE) enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might

not be able to handle real-time traffic effectively, the 7921 or 7920 phone uses the QBSS value to determine if they should associate to another access point. You can enable QBSS in these two modes:

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

The 7920 support mode has two options:

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

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

Restrictions for QoS Enhanced BSS

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

Because 7921 phones support WMM and 7920 phones do not, capacity and voice quality problems can arise if you do not properly configure both phones when they are used in a mixed environment. To enable both 7921 and 7920 phones to co-exist on the same network, make sure that load-based CAC and 7920 AP CAC are both enabled on the controller and the WMM Policy is set to Allowed. These settings become particularly important if you have many more 7920 users than 7921 users.

- We recommend that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, if the handset is refused at its first reassociation attempt.

Configuring QBSS (GUI)

-
- Step 1** Choose **WLANs** to open the WLANs page.
 - Step 2** Click the ID number of the WLAN for which you want to configure WMM mode.
 - Step 3** When the **WLANs > Edit** page appears, choose the **QoS** tab to open the **WLANs > Edit (Qos)** page.
 - Step 4** From the WMM Policy drop-down list, choose one of the following options, depending on whether you want to enable WMM mode for 7921 phones and other devices that meet the WMM standard:

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

- Step 5** Select the **7920 AP CAC** check box if you want to enable 7920 support mode for phones that require access point-controlled CAC. The default value is unselected.
- Step 6** Select the **7920 Client CAC** check box if you want to enable 7920 support mode for phones that require client-controlled CAC. The default value is unselected.
- Note** You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.
- Step 7** Click **Apply** to commit your changes.
- Step 8** Click **Save Configuration** to save your changes.
-

Configuring QBSS (CLI)

-
- Step 1** Determine the ID number of the WLAN to which you want to add QBSS support by entering this command:
show wlan summary
- Step 2** Disable the WLAN by entering this command:
config wlan disable *wlan_id*
- Step 3** Configure WMM mode for 7921 phones and other devices that meet the WMM standard by entering this command:
config wlan wmm {disabled | allowed | required} *wlan_id*
where
- **disabled** disables WMM mode on the WLAN.
 - **allowed** allows client devices to use WMM on the WLAN.
 - **required** requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.
- Step 4** Enable or disable 7920 support mode for phones that require client-controlled CAC by entering this command:
config wlan 7920-support client-cac-limit {enable | disable} *wlan_id*
- Note** You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.
- Step 5** Enable or disable 7920 support mode for phones that require access point-controlled CAC by entering this command:
config wlan 7920-support ap-cac-limit {enable | disable} *wlan_id*
- Step 6** Reenable the WLAN by entering this command:
config wlan enable *wlan_id*
- Step 7** Save your changes by entering this command:
save config

Step 8

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

show wlan *wlan_id*
