Quality of Service

Wireless QoS Overview

Quality of Service (QoS), provides the ability to prioritize the traffic by giving preferential treatment to specific traffic over the other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

A target is the entity where the policy is applied. Wireless QoS policies for SSID and client are applied in the upstream and (or) downstream direction. The flow of traffic from a wired source to a wireless target is known as downstream traffic. The flow of traffic from a wireless source to a wired target is known as upstream traffic.

The following are some of the specific features provided by wireless QoS:

- SSID and client policies on wireless QoS targets
- Marking and Policing (also known as Rate Limiting) of wireless traffic
- Mobility support for QoS

Wireless QoS Targets

This section describes the various wireless QoS targets available on a device.

SSID Policies

You can create QoS policies on SSID in both the ingress and egress directions. If not configured, there is no SSID policy applied.

The policy is applicable per AP per SSID.

You can configure policing and marking policies on SSID.

Client Policies

Client policies are applicable in the ingress and egress direction. You can configure policing and marking policies on clients. AAA override is also supported.

Supported QoS Features on Wireless Targets

This table describes the various features available on wireless targets.

Table 1: QoS Features Available on Wireless Targets

Target	Features	Direction Where Policies Are Applicable
SSID	• Set • Police • Drop	Upstream and downstream
Client	• Set • Police • Drop	Upstream and downstream

This table describes the various features available on wireless targets.

Table 2: QoS Policy Actions

Policy Action Types	Wireless Target Support	
	Local Mode	Flex Mode
Police	Supported	Supported
Set	Supported	Supported

This table describes the various features available on wireless targets.

Table 3: QoS Policy Set Actions

Set Action Types	Supported	
	Local Mode	Flex Mode
set dscp	Supported	Supported
set qos-group	Supported	Not Supported
set wlan user-priority (downstream only)	Supported (BSSID only)	Supported (BSSID only)

Wireless QoS Mobility

Wireless QoS mobility enables you to configure QoS policies so that the network provides the same service anywhere in the network. A wireless client can roam from one location to another and as a result the client can get associated to different access points associated with a different device. Wireless client roaming can be classified into two types:

- Intra-device roaming
- Inter-device roaming

Note In a foreign WLC, client statistics are not displayed.

Note The client policies must be available on all of the devices in the mobility group. The same SSID policy must be applied to all devices in the mobility group so that the clients get consistent treatment.

Precious Metal Policies for Wireless QoS

The precious metal policies are system-defined policies that are available on the controller . They cannot be removed or changed.

The following policies are available:

- Platinum—Used for VoIP clients.
- Gold—Used for video clients.
- Silver— Used for traffic that can be considered best-effort.
- Bronze—Used for NRT traffic.

These policies are pre-configured. They cannot be modified.

For client metal policies, they can be pushed using AAA.

Based on the policies applied, the 802.11e (WMM), and DSCP fields in the packets are affected.

For more information about metal policies format see the Metal Policy Format, on page 5 section.

For more information about DSCP to UP mapping, see the #unique_1044 table.

Prerequisites for Wireless QoS

Before configuring wireless QoS, you must have a thorough understanding of these items:

- Wireless concepts and network topologies.
- Understanding of QoS implementation.
- Modular QoS CLI (MQC). For more information on Modular QoS, see the MQC guide
- The types of applications used and the traffic patterns on your network.
- Bandwidth requirements and speed of the network.

Restrictions for QoS on Wireless Targets

General Restrictions

A target is an entity where a policy is applied. A policy can be applied to a wireless target, which can be an SSID or client target, in the downstream and/or upstream direction. Downstream indicates that traffic is flowing from the controller to the wireless client. Upstream indicates that traffic is flowing from wireless client to the controller.

- Hierarchical (Parent policy and child policy) QoS is not supported.
- SSID and client targets can be configured only with marking and policing policies.
- One policy per target per direction is supported.
- Class maps in a policy map can have different types of filters. However, only one marking action (set dscp) is supported.
- Only one set action per class is supported.
- Access group matching is not supported.
- Access group (ACL) matching is not supported by access points in flex mode for local switching traffic.
- SIP Call Admission Control (CAC) is not supported on the central switching mode.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, SIP Call Admission Control (CAC) is not supported.
- Applying QoS on the WMI interface is not supported, as it may reboot the controller.

AP Side Restrictions

- In Cisco Embedded Wireless Controller, FlexConnect local switching, and SDA deployments, the QoS policies are enforced on the AP. Due to this AP-side restriction, police actions (e.g., rate limiting) are only enforced at a per flow (5-tuple) level and not per client.
- For FlexConnect local switching (local authentication) with AAA override enabled and external AAA server, only air space VLAN and ACL are supported as part of the AAA override and not the QoS override or other overrides.

Control Plane Rate Limiting and Policing

You need not explicitly configure control plane rate limiting or policing on the controller. The controller has embedded mechanisms (like policers) to protect the CPU by policing control plane traffic directed towards it. If you're migrating from AireOS to IOS-XE, this change is taken care of at the code level.

Metal Policy Format

Metal Policy Format

Metal Policies are system defined, and you cannot change it or delete it. There are four levels of metal policy - Platinum, Gold, Silver, and Bronze.

Note Each metal policy defines a DSCP ceiling so that the DSCP or the UP marking does not exceed a certain value.

For Platinum the value is 46, Gold is AF41, Silver is 22, and Bronze is CS1.

Policy Name	Policy-map Format	Class-map Format
platinum	policy-map platinum class cm-dscp-34 set dscp af41 class cm-dscp-45 set dscp 45 class cm-dscp-46 set dscp ef class cm-dscp-47 set dscp 47	class-map match-any cm-dscp-34 match dscp af41 class-map match-any cm-dscp-45 match dscp 45 class-map match-any cm-dscp-46 match dscp ef class-map match-any cm-dscp-47 match dscp 47 class-map match-any cm-dscp-0 match dscp default
gold	policy-map gold class cm-dscp-45 set dscp af41 class cm-dscp-46 set dscp af41 class cm-dscp-47 set dscp af41	
silver	policy-map silver class cm-dscp-34 set dscp default class cm-dscp-45 set dscp default class cm-dscp-46 set dscp default class cm-dscp-47 set dscp default	
bronze	policy-map bronze class cm-dscp-0 set dscp cs1 class cm-dscp-34 set dscp cs1 class cm-dscp-45 set dscp cs1 class cm-dscp-46 set dscp cs1 class cm-dscp-47 set dscp cs1	

Policy Name	Policy-map Format	Class-map Format

platinum-up	policy-map platinum-up
	 class cm-dscp-set1-for-up-4
	  set dscp af41
	 class cm-dscp-set2-for-up-4
	  set dscp af41
	 class cm-dscp-for-up-5
	  set dscp af41
	 class cm-dscp-for-up-6
	  set dscp ef
	 class cm-dscp-for-up-7
	  set dscp ef
		class-map match-any
		cm-dscp-for-up-0
		  match dscp default
		  match dscp cs2
		
		class-map match-any
		cm-dscp-for-up-1
		  match dscp cs1
		
		class-map match-any
		cm-dscp-set1-for-up-4
		  match dscp cs3
		  match dscp af31
		  match dscp af32
		  match dscp af33
		
		class-map match-any
		cm-dscp-set2-for-up-4
		  match dscp af41
		  match dscp af42
		  match dscp af43
		
		class-map match-any
		cm-dscp-for-up-5
		  match dscp cs4
		  match dscp cs5
		
		class-map match-any
		cm-dscp-for-up-6
		  match dscp 44
		  match dscp ef
		
		class-map match-any
		cm-dscp-for-up-7
		  match dscp cs6
		  match dscp cs7

gold-up	policy-map gold-up
	 class cm-dscp-for-up-6
	  set dscp af41
	 class cm-dscp-for-up-7
	  set dscp af41	

silver-up	policy-map silver-up
	 class cm-dscp-set1-for-up-4
	  set dscp default
	 class cm-dscp-set2-for-up-4
	  set dscp default
	 class cm-dscp-for-up-5
	  set dscp default
	 class cm-dscp-for-up-6
	  set dscp default
	 class cm-dscp-for-up-7
	  set dscp default	

bronze-up	policy-map bronze-up
	 class cm-dscp-for-up-0
	  set dscp cs1
	 class cm-dscp-for-up-1
	  set dscp cs1
	 class cm-dscp-set1-for-up-4
	  set dscp cs1
	 class cm-dscp-set2-for-up-4
	  set dscp cs1
	 class cm-dscp-for-up-5
	  set dscp cs1
	 class cm-dscp-for-up-6
	  set dscp cs1
	 class cm-dscp-for-up-7
	  set dscp cs1	

Policy Name	Policy-map Format	Class-map Format
clwmm-platinum	policy-map clwmm-platinum class voice-plat set dscp ef class video-plat set dscp af41 class class-default set dscp default	class-map match-any voice-plat match dscp ef class-map match-any video-plat match dscp af41 class-map match-any voice-gold match dscp ef class-map match-any video-gold match dscp af41
clwmm-gold	policy-map clwmm-gold class voice-gold set dscp af41 class video-gold set dscp af41 class class-default set dscp default	
clnon-wmm-platinum	policy-map clnon-wmm-platinum class class-default set dscp ef	
clnon-wmm-gold	policy-map clnon-wmm-gold class class-default set dscp af41	
clsilver	policy-map clsilver class class-default set dscp default	
clbronze	policy-map clbronze class class-default set dscp cs1	

Auto QoS Policy Format

Policy Name	Policy-map Format	Class-map Format
enterprise-avc	policy-map AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy class AutoQos-4.0-wlan-Voip-Data-Class set dscp ef class AutoQos-4.0-wlan-Voip-Signal-Class set dscp cs3 class AutoQos-4.0-wlan-Multimedia-Conf-Class set dscp af41 class AutoQos-4.0-wlan-Transaction-Class set dscp af21 class AutoQos-4.0-wlan-Bulk-Data-Class set dscp af11 class AutoQos-4.0-wlan-Scavanger-Class set dscp cs1 class class-default set dscp default policy-map AutoQos-4.0-wlan-ET-SSID-Output-Policy class AutoQos-4.0-RT1-Class set dscp ef class AutoQos-4.0-RT2-Class set dscp af31 class class-default	

Policy Name	Policy-map Format	Class-map Format
		class-map match-any AutoQos-4.0-wlan-Voip-Data-Class match dscp ef class-map match-any AutoQos-4.0-wlan-Voip-Signal-Class match protocol skinny match protocol cisco-jabber-control match protocol sip match protocol sip-tls class-map match-any AutoQos-4.0-wlan-Multimedia-Conf-Class match protocol cisco-phone-video match protocol cisco-jabber-video match protocol ms-lync-video match protocol webex-media class-map match-any AutoQos-4.0-wlan-Transaction-Class match protocol cisco-jabber-im match protocol ms-office-web-apps match protocol salesforce match protocol sap class-map match-any AutoQos-4.0-wlan-Bulk-Data-Class match protocol ftp match protocol ftp-data match protocol ftps-data match protocol cifs class-map match-any AutoQos-4.0-wlan-Scavanger-Class match protocol netflix match protocol youtube match protocol skype match protocol bittorrent class-map match-any AutoQos-4.0-RT1-Class match dscp ef

Policy Name	Policy-map Format	Class-map Format
		match dscp cs6 class-map match-any AutoQos-4.0-RT2-Class match dscp cs4 match dscp cs3 match dscp af41
voice	policy-map platinum-up class dscp-for-up-4 set dscp 34 class dscp-for-up-5 set dscp 34 class dscp-for-up-6 set dscp 46 class dscp-for-up-7 set dscp 46 policy-map platinum class cm-dscp-34 set dscp 34 class cm-dscp-46 set dscp 46	
guest	Policy Map AutoQos-4.0-wlan-GT-SSID-Output-Policy Class class-default set dscp default Policy Map AutoQos-4.0-wlan-GT-SSID-Input-Policy Class class-default set dscp default	
port (only applies to Local Mode)	policy-map AutoQos-4.0-wlan-Port-Output-Policy class AutoQos-4.0-Output-CAPWAP-C-Class priority level 1 class AutoQos-4.0-Output-Voice-Class priority level 2 class class-default ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C permit udp any eq 5246 16666 any	class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C class-map match-any AutoQos-4.0-Output-Voice-Class match dscp ef

Architecture for Voice, Video and Integrated Data (AVVID)

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Network Control	(CS7) CS6	0	AC_BE
Telephony	EF	6	AC_VO
VOICE-ADMIT	44	6	AC_VO
Signaling	CS5	5	AC_VI

IETF DiffServ Service Class	DSCP	IEEE 802.11e	
		User Priority	Access Category
Multimedia Conferencing	AF41 AF42 AF43	4	AC_VI
Real-Time Interactive	CS4	5	AC_VI
Multimedia Streaming	AF31 AF32 AF33	4	AC_VI
Broadcast Video	CS3	4	AC_VI
Low-Latency Data	AF21 AF22 AF23	3	AC_BE
OAM	CS2	0	AC_BE
High-Throughput Data	AF11 AF12 AF13	2	AC_BK
Standard	DF	0	AC_BE
Low-Priority Data	CS1	1	AC_BK
Remaining	Remaining	0	

How to apply Bi-Directional Rate Limiting

Information about Bi-Directional Rate Limiting

Bi-Directional Rate Limiting (BDRL) feature defines rate limits on both upstream and downstream traffic. These rate limits are individually configured. The rate limits can be configured on WLAN directly instead of QoS profiles, which will override QoS profile values. The WLAN rate limiting will always supersede Global QoS setting for controller and clients.

BDRL feature defines throughput limits for clients on their wireless networks and allows setting a priority service to a particular set of clients.

The following four QoS profiles are available to configure the rate limits:

- Gold

- Platinum
- Silver
- Bronze

The QoS profile is applied to all clients on the associated SSID. Therefore all clients connected to the same SSID will have the same rate limits.

To configure BDRL, select the QoS profile and configure the various rate limiting parameters. When rate limiting parameters are set to *0*, the rate limiting feature is not functional. Each WLAN has a QoS profile associated with it in addition to the configuration in the QoS profile.

Note BDRL in a mobility Anchor-Foreign setup must be configured both on Anchor and Foreign controller. As a best practice, it is recommended to perform identical configuration on both the controllers to avoid breakage of any feature.

BDRL is supported on Guest anchor scenarios. The feature is supported on IRCM guest scenarios with AireOS as Guest anchor or Guest Foreign. Cisco Catalyst 9800 Series Wireless Controller uses **Policing** option to rate limit the traffic.

To apply metal policy with BDRL, perform the following tasks:

- Configure Metal Policy on SSID
- Configure Metal Policy on Client
- #unique_1052
- #unique_1053
- #unique_1054
- #unique_1055

Prerequisites for Bi-Directional Rate Limiting

- Client metal policy is applied through AAA-override.
- You must specify the metal policy on ISE server.
- AAA-override must be enabled on policy profile.

Configure Metal Policy on SSID

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile1`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets platinum policy for input.
Step 5	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets platinum policy for output.

Configure Metal Policy on Client

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile1`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description profile with aaa override`	Adds a user defined description to the new wireless policy.
Step 4	**aaa-override** **Example:**	Enables AAA override on the WLAN.

	Command or Action	Purpose
	`Device(config-wireless-policy)# aaa-override`	**Note** After AAA-override is enabled and ISE server starts sending policy, client policy defined in service-policy client will not take effect.

Configure Bi-Directional Rate Limiting for All Traffic

Use the police action in the policy-map to configure BDRL.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map* **Example:** `Device(config)# policy-map policy-sample 1`	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-default`	Associates a class map with the policy map, and enters policy-map class configuration mode.
Step 4	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

Configure Bi-Directional Rate Limiting Based on Traffic Classification

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**policy-map** *policy-map* **Example:**	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy-map names can contain

	Command or Action	Purpose
	`Device(config)# policy-map policy-sample2`	alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-sample-youtube`	Associates a class map with the policy map, and enters policy-map class configuration mode.
Step 4	**police** *rate* **Example:** `Device(config-pmap-c)# police 1000000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
Step 5	**conform-action drop** **Example:** `Device(config-pmap-c-police)# conform-action drop`	Specifies the drop action to take on packets that conform to the rate limit.
Step 6	**exceed-action drop** **Example:** `Device(config-pmap-c-police)# exceed-action drop`	Specifies the drop action to take on packets that exceeds the rate limit.
Step 7	**exit** **Example:** `Device(config-pmap-c-police)# exit`	Exits the policy-map class configuration mode.
Step 8	**set dscp default** **Example:** `Device(config-pmap-c)# set dscp default`	Sets the DSCP value to default.
Step 9	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.
Step 10	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits the policy-map class configuration mode.
Step 11	**exit** **Example:** `Device(config-pmap)# exit`	Exits the policy-map configuration mode.
Step 12	**class-map match-any** *class-map-name* **Example:**	Selects a class map.

	Command or Action	Purpose
	`Device(config)# class-map match-any class-sample-youtube`	
Step 13	**match protocol** *protocol* **Example:** `Device(config-cmap)# match protocol youtube`	Configures the match criteria for a class map on the basis of the specified protocol.

Apply Bi-Directional Rate Limiting Policy Map to Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile3`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile3`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy client input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy client input platinum-up`	Sets the input client service policy as platinum.
Step 5	**service-policy client output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy client output platinum`	Sets the output client service policy as platinum.
Step 6	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets the input service policy as platinum.
Step 7	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets the output service policy as platinum.

Apply Metal Policy with Bi-Directional Rate Limiting

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy policy-profile3`	Configures WLAN policy profile and enters wireless policy configuration mode.
Step 3	**description** *description* **Example:** `Device(config-wireless-policy)# description policy-profile3`	Adds a user defined description to the new wireless policy.
Step 4	**service-policy client input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy client input platinum-up`	Sets the input client service policy as platinum.
Step 5	**service-policy client output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy client output platinum`	Sets the output client service policy as platinum.
Step 6	**service-policy input** *input-policy* **Example:** `Device(config-wireless-policy)# service-policy input platinum-up`	Sets the input service policy as platinum.
Step 7	**service-policy output** *output-policy* **Example:** `Device(config-wireless-policy)# service-policy output platinum`	Sets the output service policy as platinum.
Step 8	**exit** **Example:** `Device(config-wireless-policy)# exit`	Exits the policy configuration mode.
Step 9	**policy-map** *policy-map* **Example:** `Device(config)# policy-map policy-sample 1`	Creates a named object representing a set of policies that are to be applied to a set of traffic classes. Policy map names can contain alphabetic, hyphen, or underscore characters,

	Command or Action	Purpose
		are case sensitive, and can be up to 40 characters.
Step 10	**class** *class-map-name* **Example:** `Device(config-pmap)# class class-default`	Associates a class map with the policy map, and enters configuration mode for the specified system class.
Step 11	**police** *rate* **Example:** `Device(config-pmap-c)# police 500000`	Configures traffic policing (average rate, in bits per second). Valid values are 8000 to 200000000.

How to apply Per Client Bi-Directional Rate Limiting

Information About Per Client Bi-Directional Rate Limiting

The Per Client Bi-Directional Rate Limiting feature adds bi-directional rate limiting for each wireless clients on 802.11ac Wave 2 APs in a Flex local switching configuration. Earlier, the Wave 2 APs supported only per-flow rate limiting for a wireless client. When wireless client starts multiple streams of traffic, the client-based rate limiting does not work as expected. This limitation is addressed by this feature.

For instance, if the controller is configured with QoS policy and you expect each client to have a rate limiting cap of 1000 kbps. Due to per-flow rate limiting on the AP, if the wireless client starts a Youtube stream and FTP stream, each of them will be rate limited at 1000 Kbps, therefore the client will be 2000 Kbps rates. This is not desirable.

Use Cases

The following are the use cases supported by the Per Client Bi-Directional Rate Limiting feature:

Use Case -1

Configuring only default class map

If policy map is configured only with default class map and mapped only to QoS client policy, AP does a per client rate limit to the client connected to AP.

Use Case-2

Changing from per client rate limit to per flow rate limit

If policy map is configured with another different class map along with a default class map and mapped to QoS client policy, AP performs per flow rate limit to client. As policy map has different class map along with the default class map. The per client rate limit values are cleared, if the AP has previously configured per client rate limit.

If the policy map has more than one class map, then additional class map is configured along with the default class map. So, the rate limit is applied from per client to per flow. The per client rate limit value is deleted from the rate info token bucket.

Use Case-3

Changing from per flow rate limit to per client limit

If different class map is removed from policy map and policy map has only one default class map, AP performs a per client rate limit to client.

The following covers the high-level steps for Per Client Bi-Directional Rate Limiting feature:

1. Configure a policy map to WLAN through policy profile.
2. Map the QoS related policy map to WLAN.
3. Configure policy map with the default class map.
4. Configure different police rate value for class Default map.

Note If policy map has class Default with valid police rate value, AP applies that rate limit to the overall client data traffic flow.

5. Apply the policy map with class Default to QoS client policy in WLAN policy profile.

Prerequisites for Per Client Bi-Directional Rate Limiting

- This feature is exclusive to QoS client policy, that is, the policy profile must have only QoS Policy or policy target as client.
- If policy map has class default with valid police rate value, AP applies that rate limit value to the overall client data traffic flow.

Restrictions on Per Client Bi-Directional Rate Limiting

- If policy map has class map other than the class Default map, the per client rate limit does not work in AP.

Configuring Per Client Bi-Directional Rate Limiting (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name.

The **Edit Policy Profile** window is displayed.

Note The **Edit Policy Profile** window is displayed and configured in default class map only.

Step 3 Choose the **QOS And AVC** tab.

Step 4 In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress** drop-down lists.

Note You need to apply the default policy map to the QoS Client Policy.

Step 5 Click **Update & Apply to Device**.

Verifying Per Client Bi-Directional Rate Limiting

To verify whether per client is applied in AP, use the following command:

```
Device# show rate-limit client
Config:
            mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in
 nrt_burst_out nrt_burst_in
A0:D3:7A:12:6C:5E   0           0          0             0            0             0
   0             0            0
Statistics:
            name     up down
        Unshaped      0    0
  Client RT pass 697610 8200
 Client NRT pass      0    0
 Client RT drops      0    0
Client NRT drops      0   16
               9    180    0
Per client rate limit:
             mac vap rate_out rate_in            policy
A0:D3:7A:12:6C:5E   0       88      23 per_client_rate_2
```

Configuring BDRL Using AAA Override

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device (config)# wireless profile policy default-policy-profile`	Configures the WLAN policy profile and enters wireless policy configuration mode.
Step 3	**aaa-override** **Example:** `Device(config-wireless-policy)# aaa`	Configures AAA override to apply policies coming from the AAA server or ISE the Cisco Identify Services Engine (ISE) server. The following attributes are available in the RADIUS server: • Airespace-Data-Bandwidth-Average-Contract: 8001 • Airespace-Real-Time-Bandwidth-Average-Contract: 8002

	Command or Action	Purpose
		• Airespace-Data-Bandwidth-Burst-Contract: 8003 • Airespace-Real-Time-Bandwidth-Burst-Contract: 8004 • Airespace-Data-Bandwidth-Average-Contract-Upstream: 8005 • Airespace-Real-Time-Bandwidth-Average-Contract-Upstream: 8006 • Airespace-Data-Bandwidth-Burst-Contract-Upstream: 8007 • Airespace-Real-Time-Bandwidth-Burst-Contract-Upstream: 8008 **Note** 8001, 8002, 8003, 8004, 8005, 8006, 8007, and 8008 are the desired rate-limit values configured as an example.

Verifying Bi-Directional Rate-Limit

To verify the bi-directional rate limit, use the following command:

```
Device# show wireless client mac-address E8-8E-00-00-00-71 detailClient MAC Address :
e88e.0000.0071
Client MAC Type     : Universally Administered Address
Client IPv4 Address : 100.0.7.94
Client Username     : e88e00000071
AP MAC Address      : 0a0b.0c00.0200
AP Name             : AP6B8B4567-0002
AP slot             : 0
Client State        : Associated
Policy Profile      : dnas_qos_profile_policy
Flex Profile        : N/A
Wireless LAN Id     : 10
WLAN Profile Name   : QoS_wlan
Wireless LAN Network Name (SSID): QoS_wlan
BSSID : 0a0b.0c00.0200
Connected For       : 28 seconds
Protocol            : 802.11n - 2.4 GHz
Channel             : 1
Client IIF-ID       : 0xa0000034
Association Id      : 10
Authentication Algorithm : Open System
Idle state timeout  : N/A
Session Timeout     : 1800 sec (Remaining time: 1777 sec)
Session Warning Time : Timer not running
Input Policy Name    : None
Input Policy State   : None
Input Policy Source  : None
Output Policy Name   : None
Output Policy State  : None
```

```
Output Policy Source : None
WMM Support          : Enabled
U-APSD Support       : Disabled
Fastlane Support     : Disabled
Client Active State  : In-Active
Power Save           : OFF
Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
AAA QoS Rate Limit Parameters:
  QoS Average Data Rate Upstream             : 8005 (kbps)
  QoS Realtime Average Data Rate Upstream    : 8006 (kbps)
  QoS Burst Data Rate Upstream               : 8007 (kbps)
  QoS Realtime Burst Data Rate Upstream      : 8008 (kbps)
  QoS Average Data Rate Downstream           : 8001 (kbps)
  QoS Realtime Average Data Rate Downstream  : 8002 (kbps)
  QoS Burst Data Rate Downstream             : 80300 (kbps)
  QoS Realtime Burst Data Rate Downstream    : 8004 (kbps)
```

To verify the rate-limit details from the AP terminal, use the following command

```
Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst_out
 nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy
```

How to Configure Wireless QoS

Configuring a Policy Map with Class Map (GUI)

Procedure

Step 1 Choose **Configuration** > **Services** > **QoS**.

Step 2 Click **Add** to view the **Add QoS** window.

Step 3 In the text box next to the **Policy Name**, enter the name of the new policy map that is being added.

Step 4 Click **Add Class-Maps**.

Step 5 Configure **AVC** based policies or **User Defined** policies. To enable **AVC** based policies, and configure the following:

a) Choose either **Match Any** or **Match All**.

b) Choose the required **Mark Type**. If you choose **DSCP** or **User Priority**, you must specify the appropriate **Mark Value**.

c) Check the **Drop** check box to drop traffic from specific sources.

Note When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.

d) Based on the chosen **Match Type**, select the required protocols from the **Available Protocol(s)** list and move them to the **Selected Protocol(s)** list. These selected protocols are the ones from which traffic is dropped.
e) Click **Save**.

Note To add more Class Maps, repeat steps 4 and 5.

Step 6 To enable **User-Defined** QoS policy, and the configure the following:

a) Choose either **Match Any** or **Match All**.
b) Choose either **ACL** or **DSCP** as the **Match Type** from the drop-down list, and then specify the appropriate **Match Value**.
c) Choose the required **Mark Type** to associate with the mark label. If you choose *DSCP*, you must specify an appropriate **Mark Value**.
d) Check the **Drop** check box to drop traffic from specific sources.

Note When **Drop** is enabled, the **Mark Type** and **Police(kbps)** options are disabled.

e) Click **Save**.

Note To define actions for all the remaining traffic, in the Class Default, choose **Mark** and/or **Police(kbps)** accordingly.

Step 7 Click **Save & Apply to Device**.

Configuring a Class Map (CLI)

Follow the procedure given below to configure class maps for voice and video traffic:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**class-map** *class-map-name* **Example:** `Device(config)# class-map test`	Creates a class map.
Step 3	**match dscp** *dscp-value* **Example:** `Device(config-cmap)# match dscp 46`	Matches the DSCP value in the IPv4 and IPv6 packets. **Note** By default for the class map the value is match-all.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-cmap)# end`	Exits the class map configuration and returns to the privileged EXEC mode.
Step 5	**show class-map** *class-map-name* **Example:** `Device# show class-map class_map_name`	Verifies the class map details.

Configuring Policy Profile to Apply QoS Policy (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click the name of the policy profile.

Step 3 In the **Edit Policy Profile** window, click the **QoS and AVC** tab.

Step 4 Under **QoS SSID Policy**, choose the appropriate **Ingress** and **Egress** policies for WLANs.

Note The ingress policies can be differentiated from the egress policies by the suffix *-up*. For example, the Platinum ingress policy is named *platinum-up*.

Step 5 Under **QoS Client Policy**, choose the appropriate **Ingress** and **Egress** policies for clients.

Step 6 Click **Update & Apply to Device**.

Note Only custom policies are displayed under **QoS Client Policy**. AutoQoS policies are auto generated and not displayed for user selection.

Configuring Policy Profile to Apply QoS Policy (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy qostest`	Configures WLAN policy profile and enters the wireless policy configuration mode.

	Command or Action	Purpose
Step 3	**service-policy client** {**input** | **output**} *policy-name* **Example:** `Device(config-wireless-policy)# service-policy client input policy-map-client`	Applies the policy. The following options are available. • **input**—Assigns the client policy for ingress direction on the policy profile. • **output**—Assigns the client policy for egress direction on the policy profile.
Step 4	**service-policy** {**input** | **output**} *policy-name* **Example:** `Device(config-wireless-policy)# service-policy input policy-map-ssid`	Applies the policy to the BSSID. The following options are available. • **input**—Assigns the policy-map to all clients in WLAN. • **output**—Assigns the policy-map to all clients in WLAN.
Step 5	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.

Applying Policy Profile to Policy Tag (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 On the **Manage Tags** page in the **Policy** tab, click **Add**.

Step 3 In the **Add Policy Tag** window that is displayed, enter a name and description for the policy tag.

Step 4 Map the required WLAN IDs and WLAN profiles with appropriate policy profiles.

Step 5 Click **Update & Apply to Device**.

Applying Policy Profile to Policy Tag (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy qostag`	Configures policy tag and enters the policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan test policy qostest`	Maps a policy profile to a WLAN profile.
Step 4	**end** **Example:** `Device(config-policy-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 5	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	Displays the configured policy tags. **Note** To view the detailed information of a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Attaching Policy Tag to an AP

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters the ap profile configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag qostag`	Maps a Policy tag to the AP.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-ap-tag)# end`	Saves the configuration and exits the configuration mode and returns to privileged EXEC mode.
Step 5	**show ap tag summary** **Example:** `Device# show ap tag summary`	Displays the ap details and tags associated to it.

SIP Call Admission Control (CAC)

Call Admission Control (CAC) is a concept that applies to voice traffic only—not data traffic. The CAC implementation requires the traffic specification (TSPEC) to be sent by the client to reserve the bandwidth. The SIP CAC feature enables CAC in order to support SIP calls. Most of the available SIP phones do not have TSPEC implemented. TSPEC is needed to invoke CAC and reserve bandwidth.

CAC regulates voice quality by limiting the number of calls that can be active at the same time on a particular link. It allows you to regulate the bandwidth consumed by active calls on the link, but does not guarantee a particular level of audio quality on the link. This configuration is used to track the bandwidth used for voice calls on a per radio basis and to protect current active calls. After the maximum bandwidth is reached (configurable value), new calls are not accepted on this radio. Also, this feature does not guarantee bandwidth reservation for future calls.

Note In cases where the client supports both SIP and TSPEC, then the bandwidth reservation with the help of TSPEC takes priority.

Restrictions and Limitations

- SIP CAC can be enabled only if SIP Call Snoop is enabled globally and in the Policy Profile of the controller .

Configuring SIP CAC (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name. The **Edit Policy Profile** window is displayed.

Step 3 Choose the **QOS And AVC** tab.

Step 4 In the **QoS SSID Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 5 In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 6 In the **SIP-CAC** settings, check the **Call Snooping** check box. You can check or uncheck the **Send Disassociate** and **Send 486 Busy** check boxes.

Step 7 Click **Update & Apply to Device**.

Configuring SIP CAC

SIP CAC controls the total number of SIP calls that can be made.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** **<policy-name>** **Example:** `Device(config)# wireless profile policy policy1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config)# shutdown`	Disables the wireless policy profile.
Step 4	**service-policy input** *policy-name* **Example:** `Device(config-wireless-policy)# service-policy input platinum`	Configures the policy profile with the Platinum metal QoS Policy. The upstream policy is specified with the keyword platinum-up as shown in the example. **Note** Upstream policies differ from downstream policies. The upstream policies have a suffix of -up. **Note** SSID policies should be configured with Platinum when Call Snoop is enabled
Step 5	**service-policy output** *policy-name* **Example:** `Device(config-wireless-policy)# service-policy output platinum-up`	Configures the policy profile with the Platinum metal QoS Policy. The upstream policy is specified with the keyword platinum-up as shown in the example.
Step 6	**service-policy client input** *client-policy-name* **Example:** `Device(config-wireless-policy)#`	Assigns the ingress policy map to all the clients.

	Command or Action	Purpose
	`service-policy client input client-policy-name`	
Step 7	**service-policy client output** *client-policy-name* **Example:** `Device(config-wireless-policy)# service-policy client output client-policy-name`	Assigns the egress policy map to all the clients.
Step 8	**call-snoop** **Example:** `Device(config-wireless-policy)# call-snoop`	Enables call snooping for WLAN.
Step 9	**[no] shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 10	**ap dot11** {**5ghz** | **24ghz**} **cac** {**voice** | **video**} **acm** **Example:** `Device(config-wireless-policy)# ap dot11 5ghz cac voice acm`	Enables the ACM static on the radio. When enabling SIP snooping, use the static CAC, not the load-based CAC.
Step 11	**ap dot11** {**5ghz** | **24ghz**} **cac voice sip** **Example:** `Device(config)# ap dot11 5ghz cac voice sip`	Configures SIP-based CAC.
Step 12	**Example:** `Device(config)# ap dot11 24ghz cac voice sip bandwidth <8-64> sample-interval <10-80>`	(Optional) Configures the bandwidth and the interval value. For example, enter bandwidth as <8-64>. 8 kbps for G729 and 64 kbps for G711. Enter the interval value as <10-80>, which means the packetization interval 10-80 ms (10, 20, 30, 40, 80 ms for G711 or G729 codec; default is 20). **Note** This configuration step can be done only through the CLI, and not from the WebUI.

	Command or Action	Purpose
Step 13	**end** **Example:** `Device(config)#end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.

Verifying SIP CAC

To verify the SIP CAC feature, use the following command:

show ap cac voice

The following is a sample output.

```
Device # show ap cac voice
AP Name: AP5897.bdd0.61d4
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-----------------------------------------------------------
0       802.11b/g   1       23437         765         3


AP Name: AP70DF.2FA2.39E0
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-----------------------------------------------------------


AP Name: APA023.9F11.C6DC
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-----------------------------------------------------------
0       802.11b/g   1       23437   765         3
```

SIP Voice Call Snooping

This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) calls and then report them to the controller. You can enable or disable SIP 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.

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 of any major call events, such as call establishment, termination, and failure.

Note This feature is supported in the central switching mode, supported on Wave 1 and Wave 2 APs, supported in the mesh AP bridge mode; but not supported on Fabric.

Note When you run SIP call with L3 roaming, the controllers should be in sync with the NTP server, or, its time should be the same.

Configuring SIP Voice Call Snooping (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name. The **Edit Policy Profile** window is displayed.

Step 3 Choose **QOS And AVC** tab.

Step 4 In the **QoS SSID Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 5 In the **QoS Client Policy** settings, choose the policies from the **Egress** and **Ingress**drop-down lists.

Step 6 In the **SIP-CAC** settings, check the **Call Snooping** check box. You can check or uncheck the **Send Disassociate** and **Send 486 Busy** check boxes.

Step 7 Click **Update & Apply to Device**.

Configuring SIP Voice Call Snooping

Before you begin

- To enable call-snoop, the BSSID platinum policy should be configured first.

Procedure

	Command or Action	Purpose
Step 1	**Configure Terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** <*policy-name*> **Example:** `Device(config)# wireless profile policy policy-name`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**shutdown** **Example:** `Device(config)# Shutdown`	Disables the wireless policy profile.
Step 4	**service-policy** {**input** | **output**} *policy-name*	Configure the policy profile with the Platinum metal QoS Policy. The upstream policy is

	Command or Action	Purpose

	Example:
	`Device(config-wireless-policy)# service-policy input platinum-up`
	`Device(Config-wireless-policy)# service-policy output platinum`
		specified with the keyword **platinum-up** as shown in the example.
		Note Upstream policies differ from downstream policies. The upstream policies have a suffix of -up.
		Note SSID policies should be configured with Platinum when Call Snoop is enabled.

Step 5	**service-policy client** {**input** | **output**} *client-policy-name*
	Example:
	`Device(config-wireless-policy)# service-policy client input voice-client`
	`Device(Config-wireless-policy)# service-policy client output voice-client`
		Configure the client policy profile.

Step 6	**call-snoop** **Example:** `Device(config-wireless-policy)# call-snoop`	Enables call snooping for WLAN.
Step 7	**[no] shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the wireless policy profile.
Step 8	**end** **Example:** `Device(config)#end`	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-z to exit global configuration mode.

Verifying SIP Voice Call Snooping

Use the following command to verify if the call-snoop command is enabled:

```
Device# sh wireless profile policy detailed <policy-name>
Classmap name for Reanchoring
  Reanchoring Classmap Name   : Not Configured
QOS per SSID
  Ingress Service Name        : platinum-up
  Egress Service Name         : platinum
QOS per Client
  Ingress Service Name        : voice-client
  Egress Service Name         : voice-client
```

```
Umbrella information
  Ciso Umbrella Parameter Map : Not Configured
Autoqos Mode                  : None
Call Snooping                 : Enabled
Fabric Profile
  Profile Name                : Not Configured
Accounting list
```

To view the number of active calls, use the following command:

show wireless client calls active

The following is a sample output.

```
Device# show wireless client calls active
Number of Active TSPEC calls on 802.11a and 802.11b/g : 0
Number of Active SIP calls on 802.11a and 802.11b/g : 3
```