Quality of Service

- Wireless Quality of Service, on page 1
- Wireless QoS targets, on page 2
- Wireless QoS mobility, on page 3
- Precious metal policies for wireless QoS, on page 4
- Prerequisites for wireless QoS, on page 5
- Restrictions for QoS on wireless targets, on page 5
- Metal Policy Format, on page 7
- How to apply Bi-Directional Rate Limiting, on page 17
- How to apply Per Client Bi-Directional Rate Limiting, on page 24
- How to Configure Wireless QoS, on page 27
- SIP Call Admission Control (CAC), on page 33
- SIP Voice Call Snooping, on page 36

Wireless Quality of Service

A wireless Quality of Service policy is a network management policy that

- prioritizes specific types of wireless traffic by giving preferential treatment
- applies different rules to SSID and client targets in both upstream and downstream directions, and
- supports traffic marking, rate limiting (policing), mobility features, and compatibility with advanced controller functions.

- Upstream traffic: The flow of data from a wireless source to a wired target.
- Downstream traffic: The flow of data from a wired source to a wireless target.
- Target: The entity (SSID or client) where the QoS policy is enforced.

Additional reference information

- Without QoS, network devices transmit packets with best-effort service, offering no guarantees for reliability, delay bounds, or throughput. Wireless QoS policies enhance the network by ensuring that traffic with higher priority receives preferential treatment. This policy improves overall performance for critical applications.

- Applying a wireless QoS policy to prioritize voice traffic on an SSID ensures that calls suffer less latency or jitter compared to general web browsing traffic.
- Rate limiting is used to prevent a single client from consuming excessive bandwidth and to maintain fair usage for all wireless clients.
- A network with no configured QoS policies treats all wireless traffic equally, which can lead to poor performance for delay-sensitive applications.
- QoS policies designed for wired networks do not automatically apply to wireless environments, as wireless traffic has unique constraints.

Wireless QoS targets

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

Service set identifiers policies

An Service Set Identifiers (SSID) policy is a wireless network configuration policy that

- controls the application of QoS settings to a wireless SSID in both ingress and egress directions
- applies per AP and per SSID, and
- allows configuration of policing and marking actions on SSID traffic.

If an SSID policy is not configured, no QoS policy is applied to the 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

Wireless controllers support various QoS features to manage traffic and ensure optimal performance for both SSIDs and client devices. These tables show the supported features, applicable directions, and configuration modes for 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

Target	Features	Direction where policies Are applicable
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	FlexConnect 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	FlexConnect 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

A wireless QoS mobility feature is a network mobility mechanism that

- enables configuration of QoS policies to provide consistent service for wireless clients
- supports seamless roaming between different access points and network devices and
- maintains the same service levels no matter where the client connects in the network.

Wireless client roaming can occur in two forms:

- Intra-device roaming: Roaming across access points managed by the same device.
- Inter-device roaming: Roaming across access points managed by different devices.

Additional reference information

Note

- In a foreign wireless LAN controller (WLC), client statistics are not displayed.
- Make sure that all client policies are available on every device in the mobility group.
- Apply the same Service Set Identifier (SSID) policy to every device in the mobility group to ensure clients receive consistent treatment.

Precious metal policies for wireless QoS

Precious metal policies for wireless QoS are system-defined QoS policies

- assign different service levels to wireless network traffic based on pre-set categories,
- remain unmodifiable, cannot be removed by administrators, and
- affect packet attributes, such as 802.11e (WMM) and DSCP fields, when policies are applied.

- Platinum: Used for VoIP clients, assigns the highest priority.
- Gold: Used for video clients, assigns high priority, lower than platinum.
- Silver: Used for best-effort traffic, assigns standard priority.
- Bronze: Used for Non-Real-Time (NRT) traffic, assigns the lowest priority.

Additional reference information

Preconfigured precious metal policies are available on wireless controllers. Administrators cannot modify or delete these policies. AAA mechanisms may push client metal policies. These policies determine packet scheduling and marking on the network.

In FlexConnect local switching mode, APs do not enforce QoS metal policy ceiling limits for upstream traffic. Limit enforcement occurs at the controller exit point. The AP does not change DSCP values.

See the Metal policy format, on page 7 section for more information about metal policy formats.

See the Metal policy map section for more information about metal policies.

Precious metal policies for wireless QoS

- Assigning the platinum policy to VoIP devices ensures minimal latency for voice communication.
- Assigning the gold policy to video streaming clients optimizes traffic for media applications.
- The silver policy applied to laptops browsing the internet handles general best-effort data.
- The bronze policy used for devices performing background updates minimizes their network priority.

- Custom user-defined QoS policies that administrators can modify or remove are not considered precious metal policies.
- Policies that do not map traffic types to platinum, gold, silver, or bronze levels are not included.

Prerequisites for wireless QoS

Before you configure wireless QoS, make sure you understand key concepts and network factors to ensure effective deployment.

The required prerequisites include:

- Understand wireless concepts and network topologies.
- Understand QoS implementation.
- Modular QoS CLI (MQC). To learn more about Modular QoS CLI, see the MQC guide.
- Understand the types of applications used and the traffic patterns on your network.
- Understand your network's bandwidth requirements and speed.

Restrictions for QoS on wireless targets

QoS policy application on wireless targets (such as SSIDs, BSSIDs, and wireless clients) has these key restrictions and considerations.

General Restrictions

- QoS policy application on wireless targets (such as Service Set Identifier (SSID), BSSID, and wireless clients) includes these key restrictions and considerations:

Hierarchical (parent policy and child policy) QoS is not supported.

- Configure SSID and client targets only with marking and policing policies.
- You can assign only one policy per target for each direction.
- Although class maps in a policy map can have different types of filters, only one marking action (set dscp) is supported.
- Only one set action per class is supported.
- You cannot use access group matching.
- Access points in flex mode do not support Access Control List (ACL) matching for local switching traffic.
- SIP Call Admission Control (CAC) is not supported on central switching mode.
- From Cisco IOS XE Amsterdam 17.3.1 and later, SIP Call Admission Control (CAC) is not supported.
- Do not apply QoS on the WMI interface because it may reboot the controller.

- AP QoS statistics for each radio stop updating after 32,768 minutes (546 hours). At that point, the offered rate shows zero and the minute counter stops increasing.

  The system calculates rates within a 32,768-minute window (546 hours). After 32,768 minutes, the data rate calculation is zero.

  To reset the statistics, run this command to clear the QoS statistics for the target policy map and SSID:

  ```
  show policy-map interface wireless ssid profile-name <wlan_profile_name> radio type
  <radio_type> ap name <AP_name> input clear
  ```

AP Side Restrictions

- In Cisco Embedded Wireless Controller, FlexConnect local switching, and Software-Defined Access (SDA) deployments, the AP enforces QoS policies and rate-limiting actions at the per-flow (5-tuple) level, not per client.
- For FlexConnect local switching with local authentication and AAA override enabled (using an external AAA server), you can use only air space VLAN and ACL as AAA overrides. QoS and other overrides are not available.
- Rate limiting per SSID is not supported in FlexConnect local switching mode. For rate limiting to work as expected, FlexConnect central switching mode should be used.

Control Plane Rate Limiting and Policing

You do not need to configure control plane rate limiting or policing. Built-in mechanisms, such as policers, protect the CPU from control plane traffic. Migrations from AireOS to IOS-XE handle this automatically.

Restriction: Client connectivity and TCP packet drops on SSIDs with AAA rate limiting

Do not configure rate limits or AAA overrides on Cisco ISE for any SSID where AAA rate limiting is applied. These settings can cause the APs in local mode to drop TCP packets. In such a scenario, use Modular QoS CLI (MCQ)-based method only for configuring Quality of Service (QoS) and rate limiting.

Behavior explanation

When a client connects to an SSID with AAA rate limiting configured on APs in local mode, the AP forwards ICMP, DHCP, and DNS packets to the controller but drops TCP packets. This issue is caused when rate limits are configured on Cisco ISE and AAA overrides are in place. You can verify that TCP packets are dropped using the **show datapath drop trace** comand.

Workaround

Review the configuration of rate limits and consider removing them or adjusting the settings to avoid dropping TCP packets. Use Modular QoS CLI (MCQ)-based method only for configuring Quality of Service (QoS) and rate limiting. For more information about the MCQ-based method, see Configure QoS Rate Limit on Catalyst 9800 Wireless Controllers.

Verify client connectivity

- To observe the AP configuration, use this command.

  ```
  show ap dot11 5ghz network
  ```

- To verify the AP configuration, use this command.

  ```
  show ap dot11 5ghz network
  ```

- To check the client summary, use this command.

  ```
  show wireless client summary
  ```

- To verify client details and troubleshoot connectivity issues, use this command:

  ```
  show wireless client mac-address MAC-address detail
  ```

Metal Policy Format

Metal policy format

Metal Policies are system defined, and you cannot change it or delete it.

Metal policies are system defined. You cannot change or delete them. 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.

Table 4: Metal Policy Map Formats

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	

Table 5: Metal Policy Map Formats (UP)

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	

Table 6: Metal Policy Map Formats (CLWMM/CLNON)

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

This section provides the Auto QoS policy format, including policy-map and class-map configurations.

Policy name	Policy-map format	Class-map format
enterprise-avc		

Policy name	Policy-map format	Class-map format
	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-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

Policy name	Policy-map format	Class-map format
	class AutoQos-4.0-RT2-Class set dscp af31 class class-default	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 match dscp cs6

Policy name	Policy-map format	Class-map format
		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	-

Policy name	Policy-map format	Class-map format
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)

The table lists how AVVID service classes map to the IETF DiffServ DSCP values and IEEE 802.11e categories. Use this information to classify traffic and assign appropriate QoS markings for voice, video, and integrated data services.

Table 7: Mapping of IETF diffServ, DSCP, and IEEE 802.11e

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
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

Bidirectional rate limiting

A bidirectional rate limit is a wireless network traffic management feature that

- establishes configurable rate limits for both upstream and downstream traffic directions
- enables administrators to set individual limits per direction directly on the WLAN, overriding QoS profile values, and global controller configurations, and
- supports prioritization of client groups by assigning them to specific QoS profiles.

QoS profiles

There are four distinct QoS profiles to configure rate limits:

- Gold
- Platinum
- Silver
- Bronze

Additional reference information

- Apply rate limiting directly to a WLAN. This action overrides both global QoS settings and QoS profiles for the controller and clients.
- Bidirectional rate limits apply to all clients associated with a given SSID. Every client connected to the same SSID has identical rate restrictions.
- Set throughput limits to control wireless client performance for both traffic directions. Assign service priority to specific client sets for prioritization.

Configuration guidance

- Select a QoS profile and configure the rate limiting parameters for upstream and downstream directions. Setting a parameter to `0` disables rate limiting for that direction.
- Assign a QoS profile to each WLAN to determine the rate limits for all connected clients.

Scenario considerations

- Configure bidirectional rate limits on both the Anchor and Foreign controllers in mobility Anchor–Foreign controller setups. Use identical configuration across both controllers to prevent feature failure.
- The feature is supported in guest anchor scenarios, including IRCM guest deployments where AireOS devices function as guest anchor or guest foreign.
- Cisco Catalyst 9800 Series Wireless Controller uses a policing option to enforce bidirectional rate limits.

Bidirectional rate limiting

If a guest SSID uses the Bronze QoS profile and sets both upstream and downstream limits to specific values, all guests on that SSID have consistent rate restrictions, regardless of any global QoS or profile settings.

Requirements for bidirectional rate limiting configuration

Ensure you meet the essential requirements before configuring bidirectional rate limiting.

To configure bidirectional rate limiting, ensure these prerequisites are met:

- Apply the client metal policy through AAA override.
- Specify the metal policy on the Identity Services Engine (ISE) server.
- Enable AAA override on the policy profile.

Configure the metal policy on the SSID

Apply a metal service policy to a wireless SSID using a WLAN policy profile.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy policy-profile-name
```

Step 3 Add a user-defined description to the new wireless policy.

Example:

```
Device(config-wireless-policy)# description description
```

Step 4 Set the platinum policy for input.

Example:

```
Device(config-wireless-policy)# service-policy input input-policy
```

Step 5 Set the platinum policy for output.

Example:

```
Device(config-wireless-policy)# service-policy output output-policy
```

The system applies the configured policy profile to the SSID. It enforces platinum-level input and output service policies.

Configure a metal policy on your client device

Set up a wireless metal policy profile that uses AAA override on your client device.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy policy-profile-name
```

Step 3 Add a user-defined description to the new wireless policy.

Example:

```
Device(config-wireless-policy)# description description
```

Step 4 Enable AAA override on your WLAN.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Note
After you enable AAA override and the ISE server starts sending policy, the client policy defined in the service-policy client does not take effect.

With AAA override enabled, your wireless policy profile allows external RADIUS authentication and policy control.

Configure bidirectional rate limiting for all traffic

Enforce bidirectional rate limiting on all traffic by using policy maps.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a named object to apply policies to traffic classes.

Example:

```
Device(config)# policy-map policy-map
```

Policy-map names can contain alphabetic, hyphen, or underscore characters. The names are case sensitive. Names can be up to 40 characters long.

Step 3 Associate a class map with the policy map and enter policy-map class configuration mode.

Example:

```
Device(config-pmap)# class class-map-name
```

Step 4 Configure traffic policing for your traffic class.

Example:

```
Device(config-pmap-c)# police rate
```

Valid values are 8,000 to 200,000,000 bps.

The bidirectional rate limiting policy limits all traffic that matches the class map.

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:** `Device(config)# policy-map policy-sample2`	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-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:**	Specifies the drop action to take on packets that conform to the rate limit.

	Command or Action	Purpose
	`Device(config-pmap-c-police)# conform-action drop`	
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:** `Device(config)# class-map match-any class-sample-youtube`	Selects a class map.
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 bidirectional rate limiting policy map to policy profile

Apply bidirectional rate limiting to your wireless network by attaching a policy map to a policy profile.

Procedure

Step 1 Enter global configuration mode to begin setup.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN policy profile to enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy policy-profile-name
```

Step 3 Add a user-defined description to your new wireless policy.

Example:

```
Device(config-wireless-policy)# description description
```

Step 4 Set the input client service policy to platinum.

Example:

```
Device(config-wireless-policy)# service-policy client input platinum-up
```

Step 5 Set the output client service policy to platinum.

Example:

```
Device(config-wireless-policy)# service-policy client output output-policy
```

Step 6 Set the input service policy to platinum.

Example:

```
Device(config-wireless-policy)# service-policy input input-policy
```

Step 7 Set the output service policy to platinum.

Example:

```
Device(config-wireless-policy)# service-policy output platinum
```

Your wireless policy profile applies bidirectional rate limiting based on the service policies you set.

Apply metal policy with bidirectional rate limiting

Use a metal policy to enforce bidirectional bandwidth limits on wireless traffic.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy policy-profile-name
```

Step 3 Add a description for the new wireless policy.

Example:

```
Device(config-wireless-policy)# description description
```

Step 4 Assign 'platinum' as the input client service policy.

Example:

```
Device(config-wireless-policy)# service-policy client input input-policy
```

Step 5 Assign 'platinum' as the output client service policy.

Example:

```
Device(config-wireless-policy)# service-policy client output output-policy
```

Step 6 Assign 'platinum' as the input service policy.

Example:

```
Device(config-wireless-policy)# service-policy input input-policy
```

Step 7 Assign 'platinum' as the output service policy.

Example:

```
Device(config-wireless-policy)# service-policy output platinum
```

Step 8 Exit the policy configuration mode.

Example:

```
Device(config-wireless-policy)# exit
```

Step 9 Create a named object to apply policies to traffic classes.

Example:

```
Device(config)# policy-map policy-sample 1
```

Policy map names can contain alphabetic characters, hyphens, or underscores. They are case sensitive and can be up to 40 characters long.

Step 10 Associate a class map with the policy map, and enter configuration mode for the specified system class.

Example:

```
Device(config-pmap)# class class-map-name
```

Step 11 Configure traffic policing.

Example:

```
Device(config-pmap-c)# police 500,000
```

Valid values range from 8,000 to 200,000,000 bytes.

The metal policy enforces bidirectional rate limiting so wireless traffic meets the input and output bandwidth limits you specified.

How to apply Per Client Bi-Directional Rate Limiting

Per-client bidirectional rate limiting

A per-client bidirectional rate limit is a wireless traffic control feature that

- enforces, for each wireless client, bandwidth caps separately on both upstream and downstream traffic,
- ensures that each client receives a single aggregate limit, no matter how many concurrent flows or streams are active,
- addresses limitations of legacy per-flow rate limiting on 802.11ac Wave 2 APs in Flex local switching mode.

Additional reference information

Previously, per-flow rate limiting capped each client stream, such as a YouTube stream or an FTP transfer, independently. As a result, clients could exceed the intended per-client bandwidth limit.

With per-client bidirectional rate limits, the total bandwidth used by all of a client's streams cannot exceed the configured limit. This restriction applies no matter how many streams are active.

Per-client bidirectional rate limiting

If a controller limits each client to 1000 Kbps (1 megabit per second), and a client initiates both a YouTube and an FTP stream, both streams together will share the 1000 Kbps (1 megabit per second) limit, ensuring the client cannot exceed the cap.

Prerequisites for per-client bidirectional rate limiting

- You can use this feature only with a QoS client policy. Ensure the policy profile contains only a QoS Policy or a policy target as client.
- If the policy map includes class default with a valid police rate value, the access point applies this rate limit to the the data traffic flow for the client.

Restrictions on per-client bidirectional rate limiting

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

Configure per-client bidirectional rate limiting (GUI)

Set limits on upload and download data rates for each client. This ensures fair bandwidth distribution.

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**.

The selected policies in the policy profile enforce bidirectional rate limiting for each client.

Verify per client bi-directional rate limiting

To verify whether per client is applied in AP, use this 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
```

Configure bi-directional rate limiting using AAA override (CLI)

Enable WLAN policy profiles to enforce upstream and downstream bandwidth limits based on RADIUS server (e.g., Cisco ISE) attributes through AAA override.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN policy profile and enter wireless policy configuration mode.

Example:

```
Device (config)# wireless profile policy profile-name
```

Step 3 Configure AAA override to apply policies coming from the AAA server or Cisco Identity Services Engine (ISE) server.

Example:

```
Device(config-wireless-policy)# aaa-override
```

These attributes are available in the RADIUS server:

- Airespace-Data-Bandwidth-Average-Contract: 8001
- Airespace-Real-Time-Bandwidth-Average-Contract: 8002
- 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 example rate-limit values.

The WLAN policy profile is configured to honor bi-directional rate limiting instructions received via AAA override from the RADIUS server.

Verify bi-directional rate-limit

To verify the bi-directional rate limit, use this 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 : 192.0.2.1
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 this 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

Configure a policy map with class map (GUI)

Define and apply a QoS policy map with associated class maps to control network traffic behavior.

Use this task when you need to create or update a QoS policy map containing class maps, specifying how different types of network traffic are marked, policed, or dropped.

Before you begin

Use these steps to configure a policy map with class map using the 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 **Policy Name**, enter the name of the new policy map.

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) Select the required protocols from the **Available Protocol(s)** list based on the chosen **Match Type**. Move them to the **Selected Protocol(s)** list. The system drops traffic from these selected protocols.

e) Click **Save**.

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

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

Step 6 To enable the **User-Defined** QoS policy, configure these options:

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

b) From the drop-down list, choose either **ACL** or **DSCP** as the **Match Type**. 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 either **Mark**, **Police(kbps)**, or both as appropriate.

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

The system deploys the defined policy map with its class maps and associated actions. QoS settings are enforced on network traffic as specified.

Configure a class map (CLI)

Define and customize a class map to identify and match specific network traffic, such as voice and video, using CLI commands.

Use this procedure to configure class maps for voice and video traffic:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a class map.

Example:

```
Device(config)# class-map class-map-name
```

Step 3 Match the DSCP value in IPv4 and IPv6 packets.

Example:

```
Device(config-cmap)# match dscp dscp-value
```

Note
By default, the class map uses match-all.

Step 4 Exit class map configuration mode and return to privileged EXEC mode.

Example:

```
Device(config-cmap)# end
```

Step 5 Verify class map details.

Example:

```
Device# show class-map class_map_name
```

You have configured the class map with the specified matching criteria. It is ready for use in traffic policies.

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.

Configure policy profile to apply QoS policy (CLI)

Apply a QoS policy to a WLAN policy profile using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN policy profile. Enter the wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy profile-policy
```

Step 3 Apply the policy.

Example:

```
Device(config-wireless-policy)# service-policy client input policy-map-client
```

These 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 Apply the policy to the Basic Service Set Identifier (BSSID).

Example:

```
Device(config-wireless-policy)# service-policy input output policy-name
```

These 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 Enable the wireless policy profile.

Example:

```
Device(config-wireless-policy)# no shutdown
```

The specified QoS policy is applied to the WLAN policy profile, and all clients associated with the WLAN receive the defined QoS treatment.

Apply policy profile to policy tag (GUI)

Associate a policy profile with a policy tag to manage network behavior for specific WLANs.

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, 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**.

The device applies the specified policy profile to the policy tag and controls WLAN behavior based on the configuration.

Apply policy profile to policy tag (CLI)

Associate a policy profile with a policy tag through command-line configuration to enforce desired wireless policy settings.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure policy tag and enter the policy tag configuration mode.

Example:

```
Device(config-policy-tag)# wireless tag policy policy-tag-name
```

Step 3 Map a policy profile to a WLAN profile.

Example:

```
Device(config-policy-tag)# wlan test policy profile-policy-name
```

Step 4 Save the configuration, exit configuration mode, and return to privileged EXEC mode.

Example:

```
Device(config-policy-tag)# end
```

Step 5 Display the configured policy tags.

Example:

```
Device# show wireless tag policy summary
```

Note
To view the detailed information of a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

The policy profile is applied to the policy tag. You can verify the configuration through summary and detailed display commands.

Attach policy tag to an AP

Assign a policy tag to a wireless AP to determine its network and functional behavior.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the AP, then enter the AP profile configuration mode.

Example:

```
Device(config)# ap F866.F267.7DFB
```

Step 3 Map a policy tag to the AP.

Example:

```
Device(config-ap-tag)# policy-tag policy-tag-name
```

Step 4 Save the configuration. Exit configuration mode. Return to privileged EXEC mode.

Example:

```
Device(config-ap-tag)# end
```

Step 5 Display the AP details and the tags associated with it.

Example:

```
Device# show ap tag summary
```

The specified AP is associated with the chosen policy tag. You can verify the mapping by displaying the AP details.

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:**	Assigns the ingress policy map to all the clients.

	Command or Action	Purpose
	`Device(config-wireless-policy)# 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.

	Command or Action	Purpose

Step 4	**service-policy** {**input** | **output**} *policy-name*
	Example:
	`Device(config-wireless-policy)# service-policy input platinum-up`
	`Device(Config-wireless-policy)# service-policy output platinum`
		Configure 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 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
```