



## QoS

- [ワイヤレス QoS の概要 \(1 ページ\)](#)
- [ワイヤレス QoS ターゲット \(2 ページ\)](#)
- [ワイヤレス QoS の貴金属ポリシー \(3 ページ\)](#)
- [ワイヤレス QoS の前提条件 \(3 ページ\)](#)
- [ワイヤレス ターゲットの QoS に関する制約事項 \(3 ページ\)](#)
- [メタルポリシー形式 \(4 ページ\)](#)
- [双方向のレート制限の適用方法 \(12 ページ\)](#)
- [クライアントごとの双方向のレート制限の適用方法 \(19 ページ\)](#)
- [ワイヤレス QoS の設定方法 \(24 ページ\)](#)

## ワイヤレス QoS の概要

Quality of Service (QoS) では、特定のトラフィックを他のトラフィック タイプよりも優先的に処理することで、トラフィックに優先順位を付けることができます。QoS を設定しない場合、デバイスはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。デバイスは信頼性、遅延限界、スループットを保証せずにパケットを送信します。

ターゲットは、ポリシーが適用されるエンティティです。SSID およびクライアントに対するワイヤレス QoS ポリシーは、アップストリーム方向やダウンストリーム方向で適用されます。有線ソースからワイヤレス ターゲットへのトラフィック フローは、ダウンストリーム トラフィックと呼ばれます。ワイヤレスソースから有線ターゲットへのトラフィックフローは、アップストリーム トラフィックと呼ばれます。

次は、ワイヤレス QoS によって提供される特定の機能の一部です。

- [ワイヤレス QoS ターゲットに対する SSID ポリシーおよびクライアント ポリシー](#)
- [ワイヤレストラフィックのマーキングおよびポリシング \(レート制限とも呼ばれる\)](#)

## ワイヤレス QoS ターゲット

ここでは、デバイスで使用可能なさまざまなワイヤレス QoS ターゲットについて説明します。

### SSID ポリシー

入力と出力の両方向で SSID の QoS ポリシーを作成できます。設定されていない場合は、SSID ポリシーは適用されません。

このポリシーは、SSID ごと、AP ごとに適用されます。

SSID のポリシング ポリシーとマーキング ポリシーを設定できます。

### クライアント ポリシー

クライアントポリシーは、入力方向と出力方向に適用できます。クライアントではポリシング ポリシーおよびマーキング ポリシーを設定できます。AAA オーバーライドもサポートされません。

## ワイヤレス ターゲットでサポートされる QoS 機能

次の表に、ワイヤレス ターゲットで使用可能なさまざまな機能について説明します。

表 1: ワイヤレス ターゲットで使用可能な QoS 機能

ターゲット	機能	ポリシーが適用される方向
SSID	<ul style="list-style-type: none"> <li>• Set</li> <li>• ポリシング</li> <li>• ドロップ</li> </ul>	アップストリームおよびダウンストリーム
クライアント	<ul style="list-style-type: none"> <li>• Set</li> <li>• ポリシング</li> <li>• ドロップ</li> </ul>	アップストリームおよびダウンストリーム



(注) ドロップサポートの場合、ドロップアクションは次の設定によって実現します。

```
police <rate>
  conform-action drop
  exceed-action drop
```

直接 **action drop** はサポートされていません。

## ワイヤレス QoS の貴金属ポリシー

貴金属ポリシーは、組み込みワイヤレスコントローラで使用可能なシステム定義のポリシーです。これらのポリシーは削除または変更できません。

次のポリシーを使用できます。

- プラチナ：VoIP クライアントに使用されます。
- ゴールド：ビデオ クライアントに使用されます。
- シルバー：ベスト エフォートであると考えられるトラフィックに使用されます。
- ブロンズ：NRT トラフィックに使用されます。

これらのポリシーは事前に設定されています。変更はできません。

クライアントのメタルポリシーは、AAA を使用してプッシュできます。

適用されたポリシーに基づいて、パケット内の 802.11e (WMM) および DSCP フィールドが影響を受けます。

メタルポリシー形式の詳細については、[メタルポリシー形式 \(4 ページ\)](#) セクションを参照してください。

DSCP から UP へのマッピングの詳細については、[Architecture for Voice, Video and Integrated Data \(AVVID\) \(11 ページ\)](#) の表を参照してください。

## ワイヤレス QoS の前提条件

ワイヤレス QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- ワイヤレスの概念とネットワーク トポロジ。
- QoS 実装について。
- モジュラ QoS CLI (MQC)
- 使用するアプリケーションのタイプおよびネットワークのトラフィックパターン
- ネットワークの帯域幅要件および速度

## ワイヤレス ターゲットの QoS に関する制約事項

### 一般的な制約事項

ターゲットとは、ポリシーが適用されるエンティティです。ポリシーはワイヤレスターゲットに適用できます。ワイヤレスターゲットになるのはダウンストリーム方向またはアップスト

リーム方向の SSID またはクライアントターゲットです。ダウンストリームは、トラフィックがコントローラからワイヤレスクライアントに流れていることを示します。アップストリームは、トラフィックがワイヤレスクライアントからコントローラに流れていることを示します。

- 階層型（親ポリシーと子ポリシー） QoS はサポートされていません。
- 方向単位ターゲットあたり 1 つのポリシーがサポートされています。
- 両方向で、BSSID とクライアントターゲットのみがサポートされています。
- 次のポリシー形式がサポートされています。

- QoS ポリシーアクション

- Police :

```
police [cir | rate] bps [conform-action action] [exceed-action action]
```

ポリサーアクションタイプは **transmit** または **drop** です。

- Set:

```
set dscp
set wlan user-priority
```




---

**注** **set wlan user-priority**（ダウンストリームのみ、BSSID のみ）

---

- QoS ポリシー分類

```
match [not] access-group
match [not] dscp
match [not] protocol
```

### AP 側の制限事項

- Cisco 組み込みワイヤレスコントローラ、FlexConnect ローカルスイッチング、および SDA 展開では、QoS ポリシーが AP に適用されます。この AP 側の制限により、ポリシングアクション（レート制限など）は、クライアント単位ではなく、フロー単位（5 タプル）レベルでのみ適用されます。

## メタルポリシー形式

### メタルポリシー形式

メタルポリシーはシステム定義であり、変更も削除もできません。メタルポリシーには、Platinum、Gold、Silver、Bronze の 4 つのレベルがあります。



(注) 各メタルポリシーでは、DSCP または UP マーキングが特定の値を超えないように DSCP 上限を定義します。

Platinum の値は 46、Gold は AF41、Silver は 0、Bronze は CS1 です。

ポリシー名	ポリシーマップ形式	クラスマップ形式
platinum	<pre>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</pre>	<pre>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</pre>
Gold	<pre>policy-map gold class cm-dscp-45   set dscp af41 class cm-dscp-46   set dscp af41 class cm-dscp-47   set dscp af41</pre>	<pre>class-map match-any cm-dscp-47   match dscp 47  class-map match-any cm-dscp-0   match dscp default</pre>
silver	<pre>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</pre>	
bronze	<pre>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</pre>	

[Policy Name]	ポリシーマップ形式	クラスマップ形式
platinum-up	<pre> 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 </pre>	<pre> 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-for-up-4   match dscp cs3   match dscp af31   match dscp af32   match dscp af33   match dscp af41 </pre>
gold-up	<pre> policy-map gold-up   class cm-dscp-for-up-6     set dscp af41   class cm-dscp-for-up-7     set dscp af41 </pre>	<pre>   match dscp af42 </pre>
silver-up	<pre> 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 </pre>	<pre>   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 </pre>
bronze-up	<pre> 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 </pre>	<pre> class-map match-any cm-dscp-for-up-7   match dscp cs6   match dscp cs7 </pre>

[Policy Name]	ポリシーマップ形式	クラスマップ形式
clwmm-platinum	<pre> policy-map clwmm-platinum class voice-plat set dscp ef class video-plat set dscp af41 class class-default set dscp default </pre>	<pre> 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 </pre>
clwmm-gold	<pre> policy-map clwmm-gold class voice-gold set dscp af41 class video-gold set dscp af41 class class-default set dscp default </pre>	
clnon-wmm-platinum	<pre> policy-map clnon-wmm-platinum class class-default set dscp ef </pre>	
clnon-wmm-gold	<pre> policy-map clnon-wmm-gold class class-default set dscp af41 </pre>	
clsilver	<pre> policy-map clsilver class class-default set dscp default </pre>	
clbronze	<pre> policy-map clbronze class class-default set dscp cs1 </pre>	

## 自動 QoS ポリシー形式

[Policy Name]	ポリシーマップ形式	クラスマップ形式
enterprise-avc	<pre> 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 </pre>	

[Policy Name]	ポリシーマップ形式	クラスマップ形式
		<pre> 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-Cnf-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-Streaming-Class     match protocol netflix     match protocol youtube </pre>

[Policy Name]	ポリシーマップ形式	クラスマップ形式
		<pre> match protocol skype match protocol bittorrent  class-map match-any  AutoQos-4.0-RT1-Class match dscp ef match dscp cs6  class-map match-any  AutoQos-4.0-RT2-Class match dscp cs4 match dscp cs3 match dscp af41 </pre>
voice	<pre> 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 </pre>	
guest	<pre> 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 </pre>	
port (ローカル モードにのみ 適用)	<pre> 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 </pre>	<pre> 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 </pre>

## Architecture for Voice, Video and Integrated Data (AVVID)

IETF DiffServ サービス クラス	DSCP	IEEE 802.11e	
		ユーザー優先度	アクセス カテゴリ
ネットワーク制御	(CS7) CS6	0	AC_BE
テレフォニー	EF	6	AC_VO
VOICE-ADMIT	44	6	AC_VO
シグナリング	CS5	5	AC_VI
マルチメディア会議	AF41 AF42 AF43	4	AC_VI
リアルタイムインタラ クティブ	CS4	5	AC_VI
マルチメディアスト リーミング	AF31 AF32 AF33	4	AC_VI
ブロードキャストビデ オ	CS3	4	AC_VI
低遅延データ	AF21 AF22 AF23	3	AC_BE
OAM	CS2	0	AC_BE
高スループットデータ	AF11 AF12 AF13	2	AC_BK
標準	DF	0	AC_BE
優先順位の低いデータ	CS1	1	AC_BK
Remaining	Remaining	0	

# 双方向のレート制限の適用方法

## 双方向のレート制限に関する情報

双方向のレート制限（BDRL）機能により、アップストリームとダウンストリームの両方のトラフィックのレート制限が定義されます。これらのレート制限は個別に設定されています。レート制限は、QoS プロファイルの代わりに WLAN 上で直接設定でき、その値で QoS プロファイル値がオーバーライドされます。WLAN レート制限は、コントローラおよびクライアントのグローバル QoS 設定より常に優先されます。

BDRL 機能により、ワイヤレスネットワーク上のクライアントのスループット制限が定義されるため、特定のクライアントセットに優先サービスを設定できます。

次の 4 つの QoS プロファイルを使用して、レート制限を設定できます。

- Gold
- Platinum
- Silver
- ブロンズ

QoS プロファイルは、関連付けられた SSID 上のすべてのクライアントに適用されるため、同じ SSID に接続されているすべてのクライアントのレート制限は同じになります。

BDRL を設定するには、QoS プロファイルを選択し、さまざまなレート制限パラメータを設定します。レート制限パラメータが 0 に設定されている場合、レート制限機能は機能しません。各 WLAN には、QoS プロファイル内の設定に加えて、QoS プロファイルが関連付けられています。



(注) モビリティアンカーの BDRL：外部セットアップは、アンカーコントローラとフォーリンコントローラの両方で設定する必要があります。ベストプラクティスとして、機能の破損を避けるために、両方のコントローラで同じ設定を実行することをお勧めします。

BDRL は、ゲストアンカーシナリオでサポートされています。この機能は、AireOS をゲストアンカーまたはゲストフォーリンとして使用する IRCM ゲストシナリオでサポートされています。Cisco Catalyst 9800 シリーズワイヤレスコントローラは、[Policing] オプションを使用してトラフィックをレート制限します。

BDRL でメタルポリシーを適用するには、次のタスクを実行します。

- [SSID でのメタルポリシーの設定](#)
- [クライアントでのメタルポリシーの設定](#)
- [全トラフィックに対する双方向のレート制限の設定](#)（14 ページ）

- [トラフィック分類に基づいた双方向のレート制限の設定 \(15 ページ\)](#)
- [ポリシープロファイルへの双方向のレート制限ポリシーマップの適用 \(17 ページ\)](#)
- [双方向のレート制限によるメタルポリシーの適用 \(18 ページ\)](#)

## 双方向のレート制限の前提条件

- クライアントメタルポリシーは、AAA オーバーライドによって適用されます。
- ISE サーバーでメタルポリシーを指定する必要があります。
- ポリシープロファイルで AAA オーバーライドを有効にする必要があります。

## SSID でのメタルポリシーの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	<b>wireless profile policy <i>policy-profile-name</i></b> 例： Device(config)# wireless profile policy <i>policy-profile1</i>	WLAN ポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーションモードを開始します。
ステップ 3	<b>description</b> 説明 例： Device(config-wireless-policy)# description <i>policy-profile1</i>	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	<b>service-policy input <i>input-policy</i></b> 例： Device(config-wireless-policy)# service-policy input <i>platinum-up</i>	入力の Platinum ポリシーを設定します。
ステップ 5	<b>service-policy output <i>output-policy</i></b> 例： Device(config-wireless-policy)# service-policy output <i>platinum</i>	出力の Platinum ポリシーを設定します。

## クライアントでのメタルポリシーの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>wireless profile policy policy-profile-name</b> 例： Device(config)# wireless profile policy policy-profile1	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	<b>description</b> 説明 例： Device(config-wireless-policy)# description profile with aaa override	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	<b>aaa-override</b> 例： Device(config-wireless-policy)# aaa-override	WLANのAAAオーバーライドをイネーブルにします。  (注) AAAオーバーライドが有効になり、ISEサーバーがポリシーの送信を開始すると、サービスポリシー クライアントに定義されているクライアントポリシーは有効になりません。

## 全トラフィックに対する双方向のレート制限の設定

ポリシーマップでポリシングアクションを使用して、BDRL を設定します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>policy-map</b> ポリシーマップ 例： Device(config)# policy-map policy-sample 1	トラフィック クラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。ポリシーマップ名は、最大 40 文字の英字、ハイフ

	コマンドまたはアクション	目的
		ン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	<b>class class-map-name</b> 例： Device(config-pmap)# class class-default	クラスマップをポリシーマップに関連付け、ポリシーマップクラス コンフィギュレーション モードを開始します。
ステップ 4	<b>police rate</b> 例： Device(config-pmap-c)# police 500000	トラフィックポリシングを設定します (平均レート、1秒あたりのビット数)。有効値は 8000 ~ 200000000 です。

## トラフィック分類に基づいた双方向のレート制限の設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>policy-map</b> ポリシーマップ 例： Device(config)# policy-map policy-sample2	トラフィッククラスのセットに適用されるポリシーのセットを表す名前付きオブジェクトを作成します。ポリシーマップ名は、最大 40 文字の英字、ハイフン、または下線文字を使用でき、大文字と小文字が区別されます。
ステップ 3	<b>class class-map-name</b> 例： Device(config-pmap)# class class-sample-youtube	クラスマップをポリシーマップに関連付け、ポリシーマップクラス コンフィギュレーション モードを開始します。
ステップ 4	<b>police rate</b> 例： Device(config-pmap-c)# police 1000000	トラフィックポリシングを設定します (平均レート、1秒あたりのビット数)。有効値は 8000 ~ 200000000 です。
ステップ 5	<b>conform-action drop</b> 例： Device(config-pmap-c-police)# conform-action drop	レート制限に適合したパケットに対して実行するドロップアクションを指定します。

	コマンドまたはアクション	目的
ステップ 6	<b>exceed-action drop</b> 例： Device(config-pmap-c-police)# exceed-action drop	レート制限を超過したパケットに対して実行するドロップアクションを指定します。
ステップ 7	<b>exit</b> 例： Device(config-pmap-c-police)# exit	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 8	<b>set dscp default</b> 例： Device(config-pmap-c)# set dscp default	DSCP 値をデフォルトに設定します。
ステップ 9	<b>police rate</b> 例： Device(config-pmap-c)# police 500000	トラフィックポリシングを設定します（平均レート、1秒あたりのビット数）。有効値は 8000 ~ 200000000 です。
ステップ 10	<b>exit</b> 例： Device(config-pmap-c)# exit	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 11	<b>exit</b> 例： Device(config-pmap)# exit	ポリシーマップコンフィギュレーション モードを終了します。
ステップ 12	<b>class-map match-any class-map-name</b> 例： Device(config)# class-map match-any class-sample-youtube	クラスマップを選択します。
ステップ 13	<b>match protocol protocol</b> 例： Device(config-cmap)# match protocol youtube	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。

## ポリシープロファイルへの双方向のレート制限ポリシーマップの適用

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>wireless profile policy <i>policy-profile-name</i></b> 例： Device (config)# wireless profile policy policy-profile3	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	<b>description</b> 説明 例： Device (config-wireless-policy)# description policy-profile3	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	<b>service-policy client input <i>input-policy</i></b> 例： Device (config-wireless-policy)# service-policy client input platinum-up	入力クライアント サービス ポリシーを Platinum として設定します。
ステップ 5	<b>service-policy client output <i>output-policy</i></b> 例： Device (config-wireless-policy)# service-policy client output platinum	出力クライアント サービス ポリシーを Platinum として設定します。
ステップ 6	<b>service-policy input <i>input-policy</i></b> 例： Device (config-wireless-policy)# service-policy input platinum-up	入力サービスポリシーを Platinum として設定します。
ステップ 7	<b>service-policy output <i>output-policy</i></b> 例： Device (config-wireless-policy)# service-policy output platinum	出力サービスポリシーを Platinum として設定します。

## 双方向のレート制限によるメタルポリシーの適用

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	<b>wireless profile policy policy-profile-name</b> 例： Device(config)# wireless profile policy policy-profile3	WLAN ポリシー プロファイルを設定し、ワイヤレスポリシーコンフィギュレーションモードを開始します。
ステップ 3	<b>description</b> 説明 例： Device(config-wireless-policy)# description policy-profile3	新しいワイヤレスポリシーにユーザー定義の説明を追加します。
ステップ 4	<b>service-policy client input input-policy</b> 例： Device(config-wireless-policy)# service-policy client input platinum-up	入力クライアントサービスポリシーを Platinum として設定します。
ステップ 5	<b>service-policy client output output-policy</b> 例： Device(config-wireless-policy)# service-policy client output platinum	出力クライアントサービスポリシーを Platinum として設定します。
ステップ 6	<b>service-policy input input-policy</b> 例： Device(config-wireless-policy)# service-policy input platinum-up	入力サービスポリシーを Platinum として設定します。
ステップ 7	<b>service-policy output output-policy</b> 例： Device(config-wireless-policy)# service-policy output platinum	出力サービスポリシーを Platinum として設定します。
ステップ 8	<b>exit</b> 例： Device(config-wireless-policy)# exit	ポリシーコンフィギュレーションモードを終了します。
ステップ 9	<b>policy-map</b> ポリシーマップ 例：	トラフィッククラスのセットに適用されるポリシーのセットを表す名前付き

	コマンドまたはアクション	目的
	Device(config)# policy-map policy-sample 1	オブジェクトを作成します。ポリシーマップ名は、最大40文字の英字、ハイフン、またはアンダースコアを使用でき、大文字と小文字が区別されます。
ステップ10	<b>class class-map-name</b>  例： Device(config-pmap)# class class-default	クラスマップをポリシーマップに関連付け、指定されたシステムクラスのコンフィギュレーションモードを開始します。
ステップ11	<b>police rate</b>  例： Device(config-pmap-c)# police 500000	トラフィックポリシングを設定します（平均レート、1秒あたりのビット数）。有効値は8000～200000000です。

## クライアントごとの双方向のレート制限の適用方法

### クライアントごとの双方向のレート制限に関する情報

クライアントごとの双方向のレート制限機能は、Flex ローカルスイッチング構成の 802.11ac Wave 2 AP の各ワイヤレスクライアントに双方向のレート制限を追加します。以前は、Wave 2 AP は、ワイヤレスクライアントのフローごとのレート制限のみをサポートしていました。ワイヤレスクライアントが複数のトラフィックのストリームを開始すると、クライアントベースのレート制限が期待どおりに機能しませんが、この制限は、この機能によって対処されます。

たとえば、コントローラに QoS ポリシーが設定されており、各クライアントのレート上限が 1000 kbps であることが予想される場合、AP のフローごとのレート制限により、ワイヤレスクライアントが Youtube ストリームと FTP ストリームを開始すると、各ストリームが 1000 Kbps にレート制限されるため、クライアントは 2000 Kbps レートになります。これは望ましくありません。

#### ユースケース

クライアントごとの双方向のレート制限機能でサポートされるユースケースは次のとおりです。

ユースケース：1

デフォルトクラスマップのみの設定

ポリシーマップがデフォルトクラスマップだけで設定され、QoS クライアントポリシーだけにマッピングされている場合、AP は、その AP に接続されているクライアントに対してクライアントごとのレート制限を実行します。

ユースケース：2

### クライアントごとのレート制限からフローごとのレート制限への変更

ポリシーマップがデフォルトクラスマップとともに別のクラスマップで設定され、QoS クライアントポリシーにマッピングされている場合、AP はクライアントへのフローごとのレート制限を実行します。ポリシーマップには、デフォルトクラスマップとともに別のクラスマップがあるため、AP が以前にクライアントごとのレート制限を設定している場合、クライアントごとのレート制限値はクリアされます。

ポリシーマップに複数のクラスマップがある場合は、デフォルトクラスマップとともに追加のクラスマップが設定されるため、レート制限はクライアントごとからフローごとに適用されません。クライアントごとのレート制限値は、レート情報トークンバケットから削除されます。

ユースケース : 3

### フローごとのレート制限からクライアントごとのレート制限への変更

ポリシーマップから別のクラスマップが削除され、そのポリシーマップにデフォルトクラスマップが 1 つしかない場合、AP はクライアントに対してクライアントごとのレート制限を実行します。

以下では、クライアントごとの双方向のレート制限機能の高レベルの手順について説明します。

1. ポリシープロファイルを使用して、WLAN へのポリシーマップを設定します。
2. QoS 関連のポリシーマップを WLAN にマッピングします。
3. デフォルトクラスマップを使用してポリシーマップを設定します。
4. クラスのデフォルトマップに異なるポリシングレート値を設定します。



**注** ポリシーマップに有効なポリシングレート値を持つクラスのデフォルトがある場合、AP はそのレート制限をクライアントデータトラフィックフロー全体に適用します。

5. WLAN ポリシープロファイルの QoS クライアントポリシーに、クラスのデフォルトのポリシーマップを適用します。

## クライアントごとの双方向のレート制限の前提条件

- この機能は、QoS クライアントポリシー専用です。つまり、ポリシープロファイルには、クライアントとして QoS ポリシーまたはポリシーターゲットのみが含まれている必要があります。
- ポリシーマップに有効なポリシングレート値を持つクラスデフォルトがある場合、AP はそのレート制限値をクライアントデータトラフィックフロー全体に適用します。

## クライアントごとの双方向のレート制限に関する制約事項

- ポリシーマップにクラスのデフォルトマップ以外のクラスマップがある場合、クライアントごとのレート制限は AP では機能しません。

## クライアントごとの双方向のレート制限の設定 (GUI)

### 手順

**ステップ 1** [Configuration] > [Tags & Profiles] > [Policy] を選択します。

**ステップ 2** [Policy Profile Name] をクリックします。

[Edit Policy Profile] ウィンドウが表示されます。

(注) [Edit Policy Profile] ウィンドウは、デフォルトクラスマップでのみ表示および設定されます。

**ステップ 3** [QoS and AVC] タブを選択します。

**ステップ 4** [QoS Client Policy] 設定で、[Egress] および [Ingress] ドロップダウンリストからポリシーを選択します。

(注) デフォルトのポリシーマップを QoS クライアントポリシーに適用する必要があります。

**ステップ 5** [Update & Apply to Device] をクリックします。

## クライアントごとの双方向のレート制限の確認

クライアントごとに AP で適用されているかどうかを確認するには、次のコマンドを使用します。

```
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
```

## AAA オーバーライドを使用した BDRL の設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>wireless profile policy profile-name</b> 例： Device (config)# <b>wireless profile policy default-policy-profile</b>	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	<b>aaa-override</b> 例： Device(config-wireless-policy)# <b>aaa</b>	<p>AAA サーバーまたは Cisco Identify Services Engine (ISE) サーバーから受信したポリシーを適用するように AAA オーバーライドを設定します。</p> <p>RADIUS サーバーでは、次の属性を使用できます。</p> <ul style="list-style-type: none"> <li>• Airespace-Data-Bandwidth-Average-Contract: 8001</li> <li>• Airespace-Real-Time-Bandwidth-Average-Contract: 8002</li> <li>• Airespace-Data-Bandwidth-Burst-Contract: 8003</li> <li>• Airespace-Real-Time-Bandwidth-Burst-Contract: 8004</li> <li>• Airespace-Data-Bandwidth-Average-Contract-Upstream: 8005</li> <li>• Airespace-Real-Time-Bandwidth-Average-Contract-Upstream: 8006</li> <li>• Airespace-Data-Bandwidth-Burst-Contract-Upstream: 8007</li> <li>• Airespace-Real-Time-Bandwidth-Burst-Contract-Upstream: 8008</li> </ul> <p>(注) 8001、8002、8003、8004、8005、8006、8007、および 8008 は、例として設定された望ましいレート制限値です。</p>

## 双方向のレート制限の確認

双方向のレート制限を確認するには、次のコマンドを使用します。

```
Device# show wireless client mac-address E8-8E-00-00-00-71 detail
Client 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)
```

AP 端末からレート制限の詳細を確認するには、次のコマンドを使用します。

```
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
```

## ワイヤレス QoS の設定方法

### クラスマップを使用したポリシーマップの設定（GUI）

#### 手順

- ステップ 1 [Configuration] > [Services] > [QoS] を選択します。
- ステップ 2 [Add] をクリックして、[Add QoS] ウィンドウを表示します。
- ステップ 3 [PolicyName] の横にあるテキストボックスに、追加する新しいポリシーマップの名前を入力します。
- ステップ 4 [Add Class-Maps] をクリックします。
- ステップ 5 [AVC] ベースのポリシーまたは [User Defined] のポリシーを設定します。AVC ベースのポリシーを有効にするには、次のように設定します。
  - a) [Match Any] または [Match All] のいずれかを選択します。
  - b) 必要な [Mark Type] を選択します。[DSCP] または [User Priority] を選択した場合は、適切な [Mark Value] を指定する必要があります。
  - c) 特定の送信元からのトラフィックをドロップするには、[Drop] チェックボックスをオンにします。

(注) [Drop] が有効になっている場合、[Mark Type] および [Police(kbps)] オプションは無効になります。
  - d) 選択した [Match Type] に基づいて、[Available Protocol(s)] リストから必要なプロトコルを選択し、[Selected Protocol(s)] リストに移動します。選択したこれらのプロトコルによってトラフィックがドロップされます。
  - e) [Save] をクリックします。

(注) さらにクラスマップを追加するには、ステップ 4 と 5 を繰り返します。
- ステップ 6 [User-Defined] の QoS ポリシーを有効にするには、次のように設定します。
  - a) [Match Any] または [Match All] のいずれかを選択します。
  - b) ドロップダウンリストから [Match Type] として [ACL] または [DSCP] を選択し、適切な [Match Value] を指定します。
  - c) 必要な [Mark Type] を選択してマーク ラベルに関連付けます。[DSCP] を選択した場合は、適切な [Mark Value] を指定する必要があります。
  - d) 特定の送信元からのトラフィックをドロップするには、[Drop] チェックボックスをオンにします。

(注) [Drop] が有効になっている場合、[Mark Type] および [Police(kbps)] オプションは無効になります。

e) [Save] をクリックします。

(注) 残りのすべてのトラフィックに対するアクションを定義するには、[Class Default] で、対応する [Mark] や [Police(kbps)] を選択します。

ステップ7 [Save & Apply to Device] をクリックします。

## クラスマップの設定 (CLI)

音声およびビデオトラフィックのクラスマップを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b> 例：  デバイス# <b>configure terminal</b>	グローバル コンフィギュレーションモードを開始します。
ステップ2	<b>class-map class-map-name</b> 例：  デバイス(config)# <b>class-map test</b>	クラスマップを作成します。
ステップ3	<b>match dscp dscp-value</b> 例：  デバイス(config-cmap)# <b>match dscp 46</b>	IPv4 および IPv6 パケットの DSCP 値を照合します。  (注) クラスマップのデフォルトでは、値は match-all です。
ステップ4	<b>end</b> 例：  デバイス(config-cmap)# <b>end</b>	クラスマップ コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

## QoS ポリシーを適用するためのポリシープロファイルの設定 (GUI)

手順

ステップ1 [Configuration] > [Tags & Profiles] > [Policy] > > を選択します。

ステップ 2 [Policy Profile] ページでポリシー プロファイルの名前をクリックします。

ステップ 3 [Edit Policy Profile] ウィンドウで [QoS and AVC] タブをクリックします。

ステップ 4 [QoS SSID Policy] で、WLAN の適切な [Ingress] および [Egress] ポリシーを選択します。

(注) 入力ポリシーを出力ポリシーと区別するには、サフィックス **-up** を使用します。たとえば、Platinum 入力ポリシーは **platinum-up** という名前になります。

ステップ 5 [QoS Client Policy] で、クライアントの適切な [Ingress] および [Egress] ポリシーを選択します。

ステップ 6 [Update & Apply to Device] をクリックします。

(注) カスタムポリシーのみが [QoS Client Policy] の下に表示されます。自動 QoS ポリシーは自動生成され、ユーザーの選択肢には表示されません。

## QoS ポリシーを適用するためのポリシープロファイルの設定 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>wireless profile policy profile-policy</b> 例： Device (config)# wireless profile policy qostest	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	<b>service-policy client {input   output} policy-name</b> 例：  デバイス (config-wireless-policy)# <b>service-policy client input policy-map-client</b>	ポリシーを適用します。選択できるオプションは、次のとおりです。  <ul style="list-style-type: none"> <li>• <b>input</b> : クライアント ポリシーをポリシー プロファイルの入力方向に割り当てます。</li> <li>• <b>output</b> : クライアント ポリシーをポリシー プロファイルの出力方向に割り当てます。</li> </ul>
ステップ 4	<b>service-policy {input   output} policy-name</b> 例：	ポリシーを BSSID に適用します。選択できるオプションは、次のとおりです。

	コマンドまたはアクション	目的
	デバイス (config-wireless-policy) # <b>service-policy input policy-map-ssid</b>	<ul style="list-style-type: none"> <li>• <b>input</b> : WLAN のすべてのクライアントにポリシー マップを割り当てます。</li> <li>• <b>output</b> : WLAN のすべてのクライアントにポリシー マップを割り当てます。</li> </ul>
ステップ 5	<b>no shutdown</b>  例 : Device (config-wireless-policy) # no shutdown	ワイヤレス ポリシー プロファイルを有効にします。

## ポリシータグへのポリシープロファイルの適用 (GUI)

### 手順

- ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。
- ステップ 2 [Manage Tags] ページの [Policy] タブで [Add] をクリックします。
- ステップ 3 表示される [Add Policy Tag] ウィンドウに、ポリシー タグの名前と説明を入力します。
- ステップ 4 必要な WLAN ID および WLAN プロファイルを適切なポリシー プロファイルにマッピングします。
- ステップ 5 [Update & Apply to Device] をクリックします。

## ポリシータグへのポリシープロファイルの適用 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例 :  デバイス# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<b>wireless tag policy <i>policy-tag-name</i></b> 例： Device(config-policy-tag)# wireless tag policy qostag	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	<b>wlan <i>wlan-name</i> policy <i>profile-policy-name</i></b> 例： Device(config-policy-tag)# wlan test policy qostest	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 4	<b>end</b> 例： Device(config-policy-tag)# end	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 5	<b>show wireless tag policy summary</b> 例： Device# show wireless tag policy summary	設定されたポリシータグを表示します。  (注) ポリシー タグの詳細情報を表示するには、 <b>show wireless tag policy detailed <i>policy-tag-name</i></b> コマンドを使用します。

## AP へのポリシー タグの付加

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap <i>mac-address</i></b> 例： Device(config)# ap F866.F267.7DFB	Cisco AP を設定し、AP プロファイル コンフィギュレーション モードを開始します。
ステップ 3	<b>policy-tag <i>policy-tag-name</i></b> 例： Device(config-ap-tag)# policy-tag qostag	ポリシー タグを AP にマッピングします。

	コマンドまたはアクション	目的
ステップ 4	<b>end</b> 例 : Device(config-ap-tag)# end	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 5	<b>show ap tag summary</b> 例 : Device# show ap tag summary	AP の詳細と AP に関連付けられているタグを表示します。

