

# AAAオーバーライドを使用したCatalyst 9800ワイヤレスコントローラのQoS(BDRL)レート制限の設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

#### [例：ゲストおよび企業のQoSポリシー](#)

### [設定](#)

#### [AAAサーバと方式リスト](#)

#### [WLANポリシー、サイトタグ、およびAPタグ](#)

#### [QoS](#)

### [確認](#)

#### [WLC上](#)

#### [AP上](#)

#### [パケットキャプチャIOグラフ分析](#)

### [トラブルシューティング](#)

### [Flexconnectローカルスイッチング \(またはファブリック/SDA\) のシナリオ](#)

#### [コンフィギュレーション](#)

#### [Flexconnect/ファブリックのトラブルシューティング](#)

### [参考資料](#)

---

## はじめに

このドキュメントでは、Catalyst 9800シリーズワイヤレスコントローラでの双方向レート制限(BDRL)の設定例について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- [Catalyst Wireless 9800設定モデル](#)
- Cisco Identity Service Engine(ISE)によるAAA

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン16.12.1sのCisco Catalyst 9800-CLワイヤレスコントローラ
- バージョン2.2のIdentity Service Engine

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

9800 WLCプラットフォームのQoSは、Catalyst 9000プラットフォームと同じ概念とコンポーネントを使用します。

このセクションでは、これらのコンポーネントがどのように機能し、さまざまな結果を得るためにどのように設定できるかについて、グローバルな概要を説明します。

基本的に、QoS再帰は次のように動作します。

1. Class-Map：特定のタイプのトラフィックを識別します。クラスマップは、Application Visibility and Control(AVC)エンジンを利用できます。

また、ユーザはカスタムクラスマップを定義して、アクセスコントロールリスト(ACL)または差別化サービスコードポイント(DSCP)に一致するトラフィックを識別できます


2. ポリシーマップ：クラスマップに適用されるポリシーです。

これらのポリシーは、クラスマップに一致するトラフィックに対してDSCPのマーキング、廃棄、またはレート制限を行う可能性があります

4. サービスポリシー：ポリシーマップは、service-policyコマンドを使用して、SSIDのポリシープロファイルまたは特定の方向のクライアントごとに適用できます。

3. (任意) テーブルマップ：CoSからDSCPなど、あるタイプのマークを別のタイプのマークに変換するために使用されます。

---

 注: テーブルマップでは、変更する値(4 ~ 32)を指定します。ポリシーマップでは、テクノロジーが指定されます (COSからDSCP)。

---

## class-map = MATCH

- AVC (Application or Group)
- User defined
  - ACL
  - DSCP


## policy-map = TAKE ACTION

- Mark DSCP
- Drop
- Police (rate-limit)

## service-policy = WHERE and DIRECTION

- Client            Ingress / Egress
- SSID             Ingress / Egress

---

 注：ターゲットごとに2つ以上のポリシーを適用できる場合、ポリシーの解決は次の優先順位に基づいて選択されます。

---

- AAAオーバーライド (最高)
- ネイティブ・プロファイリング (ローカル・ポリシー)
- ポリシーの構成
- デフォルト・ポリシー (最下位)

詳細については、[9800の公式QoS設定ガイド](#)を参照してください。

QoS理論についての詳細は、『[9000シリーズQoSコンフィギュレーションガイド](#)』を参照してください。

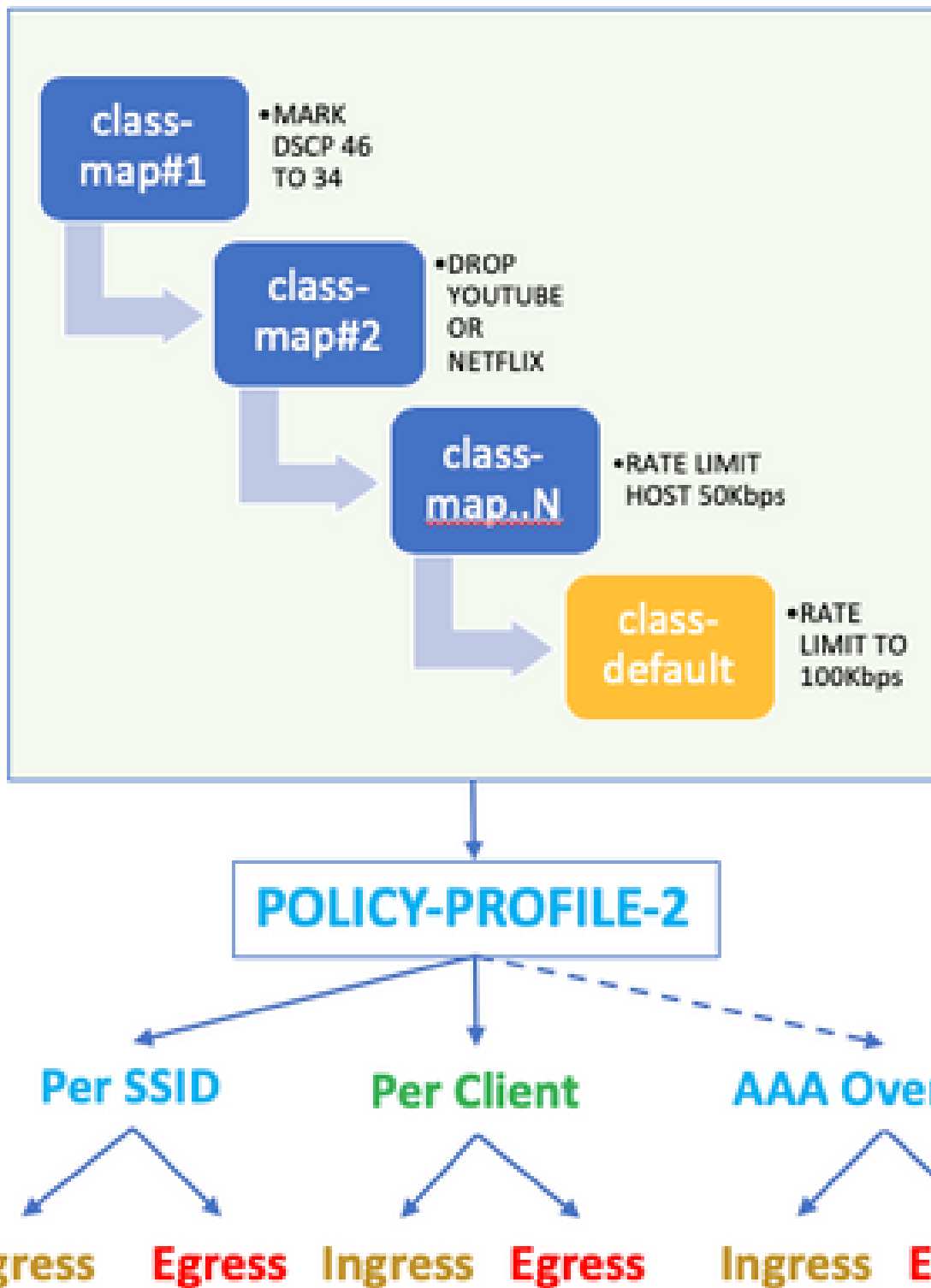
### 例：ゲストおよび企業のQoSポリシー

この例では、説明されているQoSコンポーネントが実際のシナリオでどのように適用されるかを示します。

目的は、次のようなゲスト用のQoSポリシーを設定することです。

- 備考DSCP
- YoutubeとNetflixのビデオをドロップ
- レート：ACLで指定されたホストを50Kbpsに制限します。
- レートは他のすべてのトラフィックを100 Kbpsに制限します。

## POLICY MAP - Guest



たとえば、QoSポリシーは、ゲストWLANにリンクするポリシープロファイルに、入力と出力の

両方向でSSIDごとに適用する必要があります。

## 設定

### AAAサーバと方式リスト

ステップ 1 : Configuration > Security > AAA > Authentication > Servers/Groupsの順に移動し、+Addを選択します。

AAAサーバ名、IPアドレス、およびキーを入力します。これらは、ISEのAdministration > Network Resources > Network Devicesで共有される秘密と一致している必要があります。

Name*	ISE22
IPv4 / IPv6 Server Address*	172.16.13.6
PAC Key	<input type="checkbox"/>
Key Type	0 ▾
Key*	.....
Confirm Key*	.....
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

ステップ 2 : Configuration > Security > AAA > Authentication > AAA Method List の順に移動し、+Addを選択します。「使用可能なサーバー・グループ」から「割り当てられたサーバー・グループ」を選択します。

Method List Name*	ISE-Auth
Type*	dot1x ▼
Group Type	group ▼
Fallback to local	<input type="checkbox"/>
Available Server Groups	Assigned Server Groups
radius ldap tacacs+	ISE22G

ステップ 3 : Configuration > Security > AAA > Authorization > AAA method List の順に移動し、Addを選択します。デフォルトの方式とタイプとして「ネットワーク」を選択します。

## Quick Setup: AAA Authorization

Method List Name\*

default

Type\*

network ▼

Group Type

group ▼

Fallback to local

Authenticated

Available Server Groups

ldap  
tacacs+

>

<

Assigned Server

radius

これは、コントローラがAAAサーバから返された認可属性（ここではQoSポリシーなど）を適用するために必要です。そうしないと、RADIUSから受信したポリシーは適用されません。

### WLANポリシー、サイトタグ、およびAPタグ

ステップ 1 : Configuration > Wireless Setup > Advanced > Start Now > WLAN Profileの順に選択し、+Addを選択して新しいWLANを作成します。SSID、プロファイル名、WLAN IDを設定し、ステータスを有効に設定します。

次に、Security > Layer 2の順に移動し、レイヤ2認証パラメータを設定します。



General **Security** Advanced

---

**Layer2** Layer3 AAA

---

Layer 2 Security Mode  Fast Transition

MAC Filtering  Over the DS

**Protected Management Frame**

PMF  Reassociation Timeout

**WPA Parameters**

WPA Policy

WPA2 Policy


WPA2 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>
CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>
GCMP256	<input type="checkbox"/>

MPSK

Auth Key Mgmt

802.1x	<input checked="" type="checkbox"/>
PSK	<input type="checkbox"/>
CCKM	<input type="checkbox"/>
FT + 802.1x	<input type="checkbox"/>
FT + PSK	<input type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>
PSK-SHA256	<input type="checkbox"/>

 SSIDセキュリティは、QoSの要件として802.1xである必要はありませんが、この設定例ではAAAオーバーライドに使用されます。

ステップ 2 : Security > AAAに移動し、Authentication ListドロップダウンボックスでAAAサーバを選択します。

General

Security

Advanced

Layer2

Layer3

AAA

Authentication List

ISE-Auth

Local EAP Authentication

ステップ 3 : Policy Profile を選択し、+Addを選択します。ポリシープロファイル名を設定します。

ステータスをEnabledに設定します。また、中央スイッチング、認証、DHCP、およびアソシエーションも有効にします。

General

Access Policies

QoS and AVC

Mobility

Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name\*

QoS-PP

Description

QoS-PP

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Central Association

ENABLED

Flex NAT/PAT

DISABLED

ステップ 4 : Access Policiesに移動し、クライアントがSSIDに接続する際にワイヤレスクライアントが割り当てられるVLANを設定します。

General

**Access Policies**

QOS and AVC

Mobility

Advanced

RADIUS Profiling

Local Subscriber Policy Name

Search or Select



### WLAN Local Profiling

Global State of Device  
Classification

Disabled ⓘ

HTTP TLV Caching

DHCP TLV Caching

### VLAN

VLAN/VLAN Group

VLAN2613



Multicast VLAN

Enter Multicast VLAN

ステップ 5 : Policy Tagを選択し、+Addを選択します。Policy Tag名を設定します。

WLAN-Policy Mapsの下の+Addで、ドロップダウンメニューからWLAN ProfileとPolicy Profileを選択し、設定するマップのチェックを選択します。

Name\* QoS-PT  
Description QoS-PT

WLAN-POLICY Maps: 0

+ Add × Delete

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile\* QoSWLAN Policy Profile\* QoS-PP  
× ✓

手順 6 : Site Tagを選択し、+Addを選択します。APをローカルモードで動作させるには、Enable Local Siteボックスにチェックマークを付けます (または、FlexConnectの場合はチェックマークをはずしたままにします)。

Name\* QoS-ST  
Description Enter Description  
AP Join Profile default-ap-profile  
Control Plane Name  
Enable Local Site ✓

手順 7 : Tag APsを選択し、APを選択して、ポリシー、サイト、およびRFタグを追加します。

## Tags

Policy	QoS-PT	▼
Site	QoS-ST	▼
RF	default-rt-tag	▼

*Changing AP Tag(s) will cause associated AP(s) to reconnect*

### QoS

ステップ 1 : Configuration > Services > QoSの順に移動し、+Addを選択してQoSポリシーを作成します。

名前を付けます ( 例 : BWLimitAAAClients ) 。

## Add QoS



Auto QoS

DISABLED

Policy Name\*

BWLimitAAAClients

Description

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<p>◀◀ 0 ▶▶ 10 items per page No items to display</p> <p><a href="#">+ Add Class-Maps</a> <a href="#">x Delete</a></p>							

Class Default

Mark	None	Police(kbps)	8 - 10000000
------	------	--------------	--------------

Drag and Drop, double click or click on the button to add/remove Profiles from Selected Profiles

🔍 Search

Available (2)

Selected (0)

Profiles

Profiles

Ingress

Egress

ステップ 2 : クラスマップを追加して、YoutubeとNetflixをドロップします。Add Class-Mapsをクリックします。AVC、match any、dropアクションを選択し、両方のプロトコルを選択します。

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<p>◀◀ 0 ▶▶ 10 items per page No items to display</p> <p><a href="#">+ Add Class-Maps</a> <a href="#">x Delete</a></p>							
AVC/User Defined	AVC						
Match	<input checked="" type="radio"/> Any <input type="radio"/> All						
Drop	<input checked="" type="checkbox"/>						
Match Type	protocol						
Available Protocol(s)				Selected Protocol(s)			
netbios-ssn netblt netflow				<input type="button" value="&gt;"/> <input type="button" value="&lt;"/> youtube netflix			
						<a href="#">Cancel</a>	<a href="#">Save</a>

[Save] をクリックします。

ステップ 3 : DSCP 46から34に注釈を付けるクラスマップを追加します。

Add Class-Mapsをクリックします。

- Match any,ユーザ定義
- 一致タイプDSCP
- 値46に一致
- マークタイプDSCP
- マーク値34

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol	youtube,netflix	None	8	Enabled	AVC	

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

+ Add Class-Maps    × Delete

AVC/User Defined: User Defined

Match:  Any     All

Match Type: DSCP

Match Value\*: 46

Mark Type: DSCP    Mark Value: 34

Drop:

Police(kbps): 8 - 10000000

[Save] をクリックします。

ステップ 4 : 特定のホストへのトラフィックをルールするクラスマップを定義するには、そのACLを作成します。

Add Class-Mapsをクリックします。

User Defined、match any、 match type ACLの順に選択し、ACL名を選択し(ここでは specifichostACL)、mark type noneを選択して、レート制限値を選択します。

[Save] をクリックします。

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol	youtube,netflix	None	8	Enabled	AVC	
<input type="checkbox"/>	DSCP	46	DSCP	34	Disabled	User Defined	

items per page 1 - 2 of 2 items

AVC/User Defined:

Match:  Any  All

Match Type:

Match Value\*:

Mark Type:

Drop:

Police(kbps):

次に、特定のホストトラフィックを識別するために使用するACLの例を示します（この例ではIPアドレスが使用されています）。

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 1	permit	any		192.168.1.59		ip			None	Disablec
<input type="checkbox"/> 2	permit	192.168.1.59		any		ip			None	Disablec

items per page 1 - 2 of 2 items

ステップ 5：クラスマップフレームで、デフォルトクラスを使用して、他のすべてのトラフィックのレート制限を設定します。

これにより、前述のルールの1つで対象とされていないすべてのクライアントトラフィックにレート制限が設定されます。



	Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol	youtube,netflix	None		8	Enabled	AVC	
<input type="checkbox"/>	DSCP	46	DSCP	34		Disabled	User Defined	
<input type="checkbox"/>	ACL	specifichostACL	None		50	Disabled	User Defined	

1 - 3 of 3 items

#### Class Default

Mark	<input type="text" value="None"/>	Police(kbps)	<input type="text" value="100"/>
------	-----------------------------------	--------------	----------------------------------

手順 6 : 下部にあるApply to Deviceをクリックします。

CLIに相当する設定 :

```

policy-map BWLimitAAAclients
class BWLimitAAAclients1_AVC_UI_CLASS
  police cir 8000
  conform-action drop
  exceed-action drop
class BWLimitAAAclients1_ADV_UI_CLASS
  set dscp af41
class BWLimitAAAclients2_ADV_UI_CLASS
  police cir 50000
  conform-action transmit
  exceed-action drop
class class-default
  police cir 100000
  conform-action transmit
  exceed-action drop


```

```

class-map match-all BWLimitAAAclients1_AVC_UI_CLASS
  description BWLimitAAAclients1_AVC_UI_CLASS UI_policy_DO_NOT_CHANGE
  match protocol youtube
  match protocol netflix
class-map match-any BWLimitAAAclients1_ADV_UI_CLASS
  description BWLimitAAAclients1_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match dscp ef
class-map match-all BWLimitAAAclients2_ADV_UI_CLASS
  description BWLimitAAAclients2_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match access-group name specifichostACL

```

注 : この例では、AAA Overrideによって適用されるため、QoSポリシーの下でプロファイルが選択されていません。ただし、QoSポリシーをポリシープロファイルに手動で適用する

 には、目的のプロファイルを選択します。

ステップ 2 : ISEで、Policy > Policy Elements > Results > Authorization Profilesの順に移動し、+Addを選択して認可プロファイルを作成します。

QoSポリシーを適用するには、Cisco AVペアを使用してそれらをAdvanced Attributes Settingsとして追加します。

ISE認証および認可ポリシーは、正しいルールに一致し、この認可結果を取得するように設定されていることを前提としています。


属性はip:sub-qos-policy-in=<policy name>およびip:sub-qos-policy-out=<policyname>です

### ▼ Advanced Attributes Settings

<input type="text" value="Cisco:cisco-av-pair"/>	▼	=	<input type="text" value="ip:sub-qos-policy-in=BWLimitA..."/>	▼	—
<input type="text" value="Cisco:cisco-av-pair"/>	▼	=	<input type="text" value="ip:sub-qos-policy-out=BWLimit..."/>	▼	— +

### ▼ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:sub-qos-policy-in=BWLimitAAAClients
cisco-av-pair = ip:sub-qos-policy-out=BWLimitAAAClients
```

 注 : ポリシー名では大文字と小文字が区別されます。ケースが正しいことを確認してください。

## 確認

ここでは、設定が正常に動作していることを確認します。

## WLC上

```
# show run wlan
# show run aaa
# show aaa servers
# show ap tag summary
# show ap name <AP-name> tag detail
```

```
# show wireless tag policy summary
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
# show policy-map <policy-map name>
# sh policy-map interface wireless ssid/client profile-name <WLAN> radio type <2.4/5GHz> ap name <name>

# show wireless client mac <client-MAC-address> detail
# show wireless client <client-MAC-address> service-policy input
# show wireless client <client-MAC-address> service-policy output

To verify EDCA parameters :
sh controllers dot11Radio 1 | begin EDCA
```

<#root>

```
9800#show wireless client mac e836.171f.a162 det

Client MAC Address : e836.171f.a162
Client IPv4 Address : 192.168.1.11
Client IPv6 Addresses : fe80::c6e:2ca4:56ea:ffbf
                        2a02:a03f:42c2:8400:187c:4faf:c9f8:ac3c
                        2a02:a03f:42c2:8400:824:e15:6924:ed18
                        fd54:9008:227c:0:1853:9a4:77a2:32ae
                        fd54:9008:227c:0:1507:c911:50cd:2062

Client Username : Nico
AP MAC Address : 502f.a836.a3e0
AP Name: AP780C-F085-49E6
AP slot : 1
Client State : Associated
```

(...)

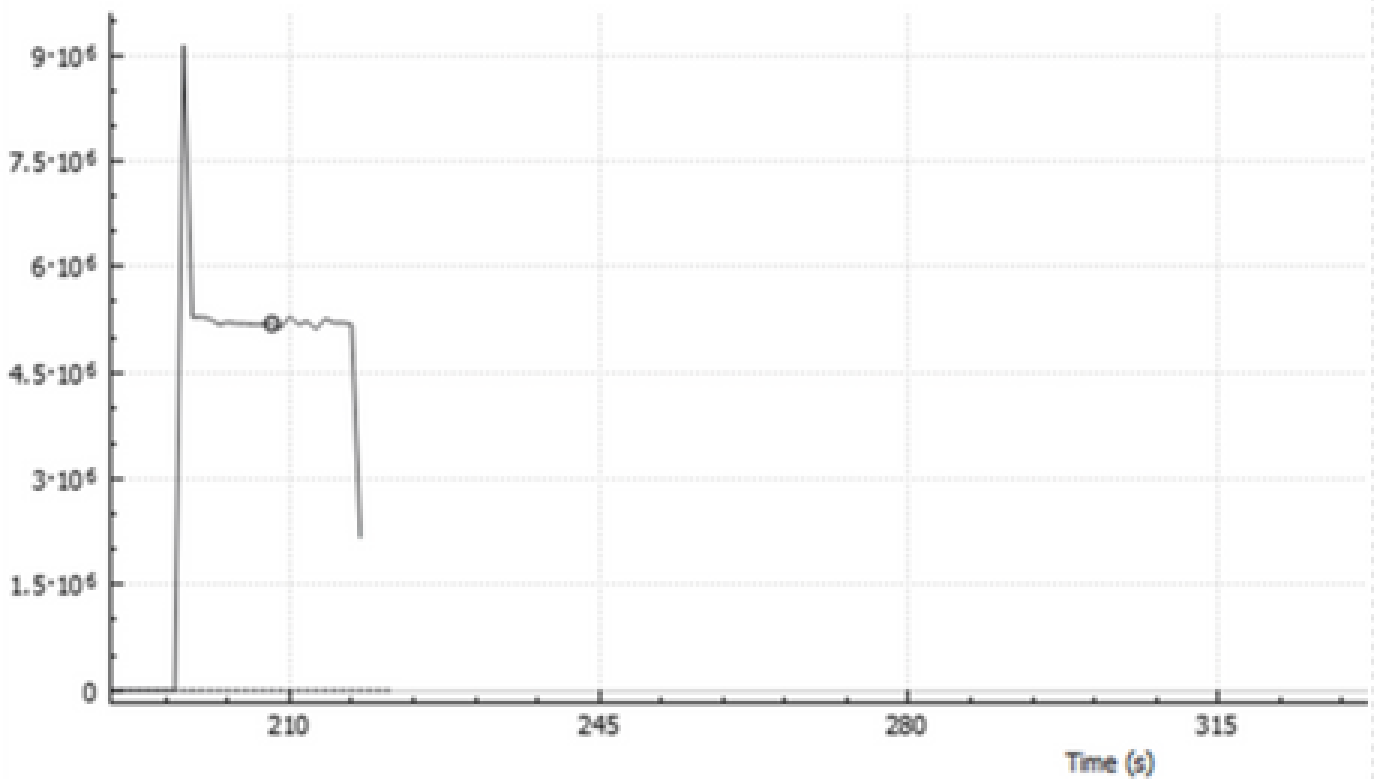
```
Local Policies:
  Service Template : wlan_svc_QoS-PP (priority 254)
    VLAN           : 1
    Absolute-Timer : 1800
Server Policies:
  Input QOS       : BWLimitAAAClients
  Output QOS      : BWLimitAAAClients
Resultant Policies:
  VLAN Name       : default
  Input QOS       : BWLimitAAAClients
  Output QOS      : BWLimitAAAClients
  VLAN           : 1
  Absolute-Timer : 1800
```

## AP上

APがローカルモードの場合、またはFlexconnect中央スイッチングモードのSSIDの場合は、WLCによってQoSおよびサービスポリシーが実行されるため、APでトラブルシューティングを行う必要はありません。

## パケットキャプチャIOグラフ分析

## Wireshark IO Graphs: wireshark\_59472C4E-A14B-4A09-9E28-CCECC120



Click to select packet 17372 (209s = 5.129e+6).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis
<input checked="" type="checkbox"/>	All packets	tcp.port eq 8022	■	Line	Bits

## トラブルシューティング

このセクションでは、設定のトラブルシューティングを行うための情報について説明します。

ステップ 1：既存のデバッグ条件をすべてクリアします。

```
# clear platform condition all
```

ステップ 2：対象のワイヤレスクライアントのデバッグを有効にします。

```
# debug wireless mac <client-MAC-address> {monitor-time <seconds>}
```

ステップ 3：問題を再現するには、ワイヤレスクライアントをSSIDに接続します。

ステップ 4：問題が再現したら、デバッグを停止します。

```
# no debug wireless mac <client-MAC-address>
```

テスト中にキャプチャされたログは、WLCのローカルファイルに次の名前で保存されます。

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

このトレースの生成にGUIワークフローを使用している場合、保存されるファイル名は debugTrace\_aaaa.bbbb.cccc.txt です。

ステップ 5 : 以前に生成されたファイルを収集するには、 ra trace .log を外部サーバにコピーするか、出力を画面に直接表示します。

次のコマンドを使用して、RAトレースファイルの名前を確認します。

```
# dir bootflash: | inc ra_trace
```

ファイルを外部サーバーにコピーします。

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

または、次のコンテンツを表示します。

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

手順 6 : デバッグ条件を削除します。

```
# clear platform condition all
```

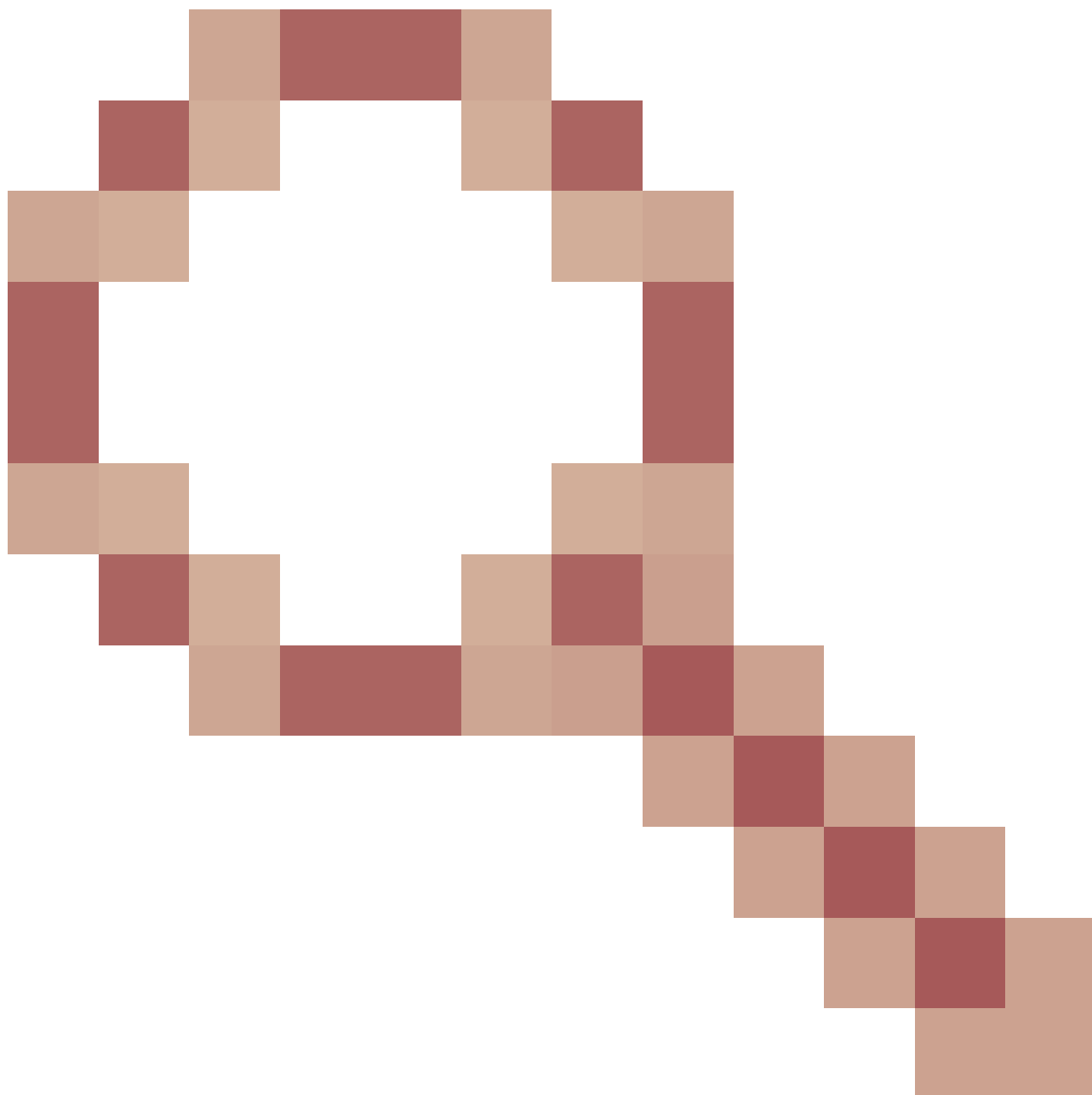
## Flexconnectローカルスイッチング ( またはファブリック /SDA ) のシナリオ

Flexconnectローカルスイッチング ( またはファブリック/SDA ) の場合、WLCで定義したQoSポリシーを適用するのはAPです。



警告: Cisco Bug ID [CSCwh74415](#)

---




が原因で、RADIUSサーバから返される最新のQoSポリシーが同じアクセスポイントに接続しているすべてのクライアントに適用され、他のすべてのQoSポリシーよりも優先されます。17.6.2リリースからは、AAAオーバーライドによるクライアントごとのレート制限が適切に機能しなくなりました。修正済みリリースを確認するには、バグの説明を参照してください。

Wave2および11axアクセスポイントでは、レート制限はフロー（5タプル）単位で発生し、17.6より前はクライアント単位やSSID単位で発生しません。これは、Flexconnect/ファブリックのEmbedded Wireless Controller on Access Point(EWc-AP)環境のAPに適用されます。

17.5の時点では、クライアントごとのレート制限を実現するために属性をプッシュするためにAAA Overrideを利用できます。

17.6の時点では、Flexローカルスイッチング設定の802.11ac Wave 2および11ax APでクライアントごとの双方向レート制限がサポートされています。

 注:Flex APでは、QoSポリシーでのACLの使用はサポートされていません。また、これらのスイッチでは、BRR (帯域幅の残存) とポリシー優先度もサポートされていません。これらはCLIを通じて設定できますが、9800 Web UIでは使用できず、9800ではサポートされていません。Cisco Bug ID [CSCvx81067](#)では、Flex APのQoSポリシーにおけるACLのサポートが追跡されています。

## コンフィギュレーション

設定は、次の2つの例外を除いて、この記事の最初の部分とまったく同じです。

1. ポリシープロファイルがローカルスイッチングに設定されている。Flex導入では、ベンガロール17.4リリースまで中央結合を無効にする必要があります。

17.5の時点では、このフィールドはハードコードされているため、ユーザ設定では使用できません。

### WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

2. サイトタグがローカルサイトでないように設定されている



# Enable Local Site



## Flexconnect/ファブリックのトラブルシューティング

APはQoSポリシーを適用するデバイスであるため、これらのコマンドは適用する対象を絞り込むのに役立ちます。

show dot11 qos ( 隠しコマンド )

show policy-map

show rate-limitクライアント

show rate-limit bssid ( デフォルト )

show rate-limit wlan ( デフォルト )

FlexConnectクライアントの表示

```
<#root>
```

```
AP780C-F085-49E6#
```

```
show dot11 qos
```

```
Qos Policy Maps (UPSTREAM)
```

```
ratelimit targets:
```

```
Client: A8:DB:03:6F:7A:46
```

```
platinum-up targets:
```

```
VAP: 0 SSID:LAB-DNAS
```

```
VAP: 1 SSID:VlanAssign
```

```
VAP: 2 SSID:LAB-Qos
```

```
Qos Stats (UPSTREAM)
```

```
total packets: 29279
```

```
dropped packets: 0
```

```
marked packets: 0
```

```
shaped packets: 0
```

```
policed packets: 182
```

```
copied packets: 0
```

```
DSCP TO DOT1P (UPSTREAM)
```

Default dscp2dot1p Table Value:

[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48

Active dscp2dot1p Table Value:

[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48

Trust DSCP Upstream : Disabled

Qos Policy Maps (DOWNSTREAM)

ratelimit targets:

Client: A8:DB:03:6F:7A:46

Qos Stats (DOWNSTREAM)

total packets: 25673

dropped packets: 0

marked packets: 0

shaped packets: 0

policed packets: 150

copied packets: 0

DSCP TO DOT1P (DOWNSTREAM)

Default dscp2dot1p Table Value:

[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1

[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1

[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1

[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1

[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1

[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1

[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1

[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1

Active dscp2dot1p Table Value:

[0]->0 [1]->0 [2]->1 [3]->0 [4]->1 [5]->0 [6]->1 [7]->0

[8]->1 [9]->1 [10]->2 [11]->1 [12]->2 [13]->1 [14]->2 [15]->1

[16]->2 [17]->2 [18]->3 [19]->2 [20]->3 [21]->2 [22]->3 [23]->2

[24]->3 [25]->3 [26]->4 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3

[32]->4 [33]->4 [34]->5 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4

[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->6 [47]->5

[48]->7 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6

[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7

Profinet packet recieved from

wired port:

0

wireless port:

?

AP780C-F085-49E6#

show policy-map

2 policymaps

Policy Map BWLimitAAAClients type:qos client:default

Class BWLimitAAAClients\_AVC\_UI\_CLASS

drop

Class BWLimitAAAClients\_ADV\_UI\_CLASS

set dscp af41 (34)

```
Class class-default
  police rate 5000000 bps (625000Bytes/s)
  conform-action
  exceed-action
```

```
Policy Map platinum-up          type:qos client:default
  Class cm-dscp-set1-for-up-4
    set dscp af41 (34)
```

```
Class cm-dscp-set2-for-up-4
  set dscp af41 (34)
```

```
Class cm-dscp-for-up-5
  set dscp af41 (34)
```

```
Class cm-dscp-for-up-6
  set dscp ef (46)
```

```
Class cm-dscp-for-up-7
  set dscp ef (46)
```

```
Class class-default
  no actions
```

AP780C-F085-49E6#

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
A8:DB:03:6F:7A:46		2	0	0	0	0	0	0	0	0

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	38621
		9 54922	0

AP780C-F085-49E6#

AP780C-F085-49E6#

show flexconnect client

Flexconnect Clients:

	mac	radio	vap	aid	state	encr	aaa-vlan	aaa-ac1	aaa-ipv6-ac1	assoc	auth	switching
A8:DB:03:6F:7A:46		1	2	1	FWD	AES_CCM128	none	none	none	Local	Central	Local

AP780C-F085-49E6#

## 参考資料

[Catalyst 9000 16.12 QoSガイド](#)

[9800 QoSコンフィギュレーションガイド](#)

[Catalyst 9800設定モデル](#)

[Cisco IOS® XE 17.6リリースノート](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。