

# 在具有AAA覆寫功能的Catalyst 9800無線控制器上設定QoS (BDRL)速率限制

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

#### [示例：訪客和公司QoS策略](#)

### [設定](#)

#### [AAA伺服器和方法清單](#)

#### [WLAN策略、站點標籤和AP標籤](#)

#### [Qos](#)

### [驗證](#)

#### [在WLC上](#)

#### [在AP上](#)

#### [資料包捕獲IO圖分析](#)

### [疑難排解](#)

### [Flexconnect本地交換 \(或交換矩陣/SDA\) 方案](#)

#### [組態](#)

#### [Flexconnect/交換矩陣故障排除](#)

### [參考資料](#)

---

## 簡介

本檔案介紹Catalyst 9800系列無線控制器上雙向速率限制(BDRL)的組態範例。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- [Catalyst無線9800組態型號](#)
- [AAA與思科身份服務引擎\(ISE\)](#)

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 9800-CL無線控制器(版本16.12.1s)
- 2.2版上的身份服務引擎

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

9800 WLC平台中的QoS使用與Catalyst 9000平台相同的概念和元件。

本節提供這些元件如何運作的整體概觀，以及如何設定這些元件以取得不同的結果。

實質上，QoS遞迴的工作方式如下：

1. 類對映：標識特定型別的流量。類對映可以利用應用可視性與可控性(AVC)引擎。

此外，使用者可以定義自定義類對映以標識與訪問控制清單(ACL)或區分服務代碼點(DSCP)匹配的流量

2. 策略對映：是應用於類對映的策略。

這些策略可以標籤DSCP、丟棄或速率限制與類對映匹配的流量

4. Service-Policy：使用service-policy命令，策略對映可以應用於SSID的策略配置檔案或特定方向的每個客戶端。

3. ( 可選 ) 表對映：用於將一種標籤轉換為另一種標籤，例如，CoS轉換為DCSP。



注意：在表對映中，指定要更改的值 ( 4到32 )；在策略對映中，指定技術 ( COS到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

---

 註：如果每個目標適用兩個或更多策略，則根據以下優先順序級別選擇策略解決方案：

---

- AAA覆寫 (最高)
- 本機分析 (本地策略)
- 配置的策略
- 預設策略 (最低)

有關詳細資訊，請參閱[9800的QoS配置指南](#)

有關QoS理論的其他資訊，請參閱[9000系列QoS配置指南](#)

### 示例：訪客和公司QoS策略

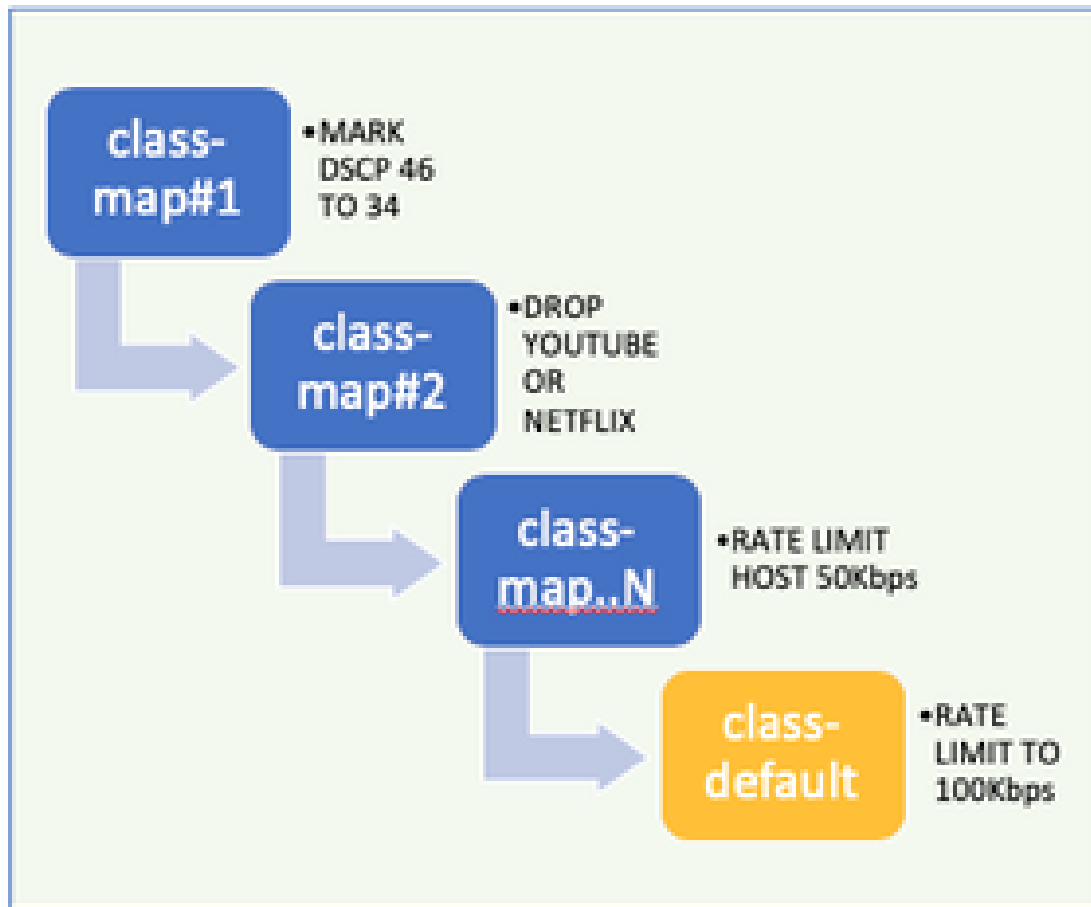
此示例演示說明的QoS元件如何應用於實際場景。

目的是為訪客配置QoS策略，該策略應：

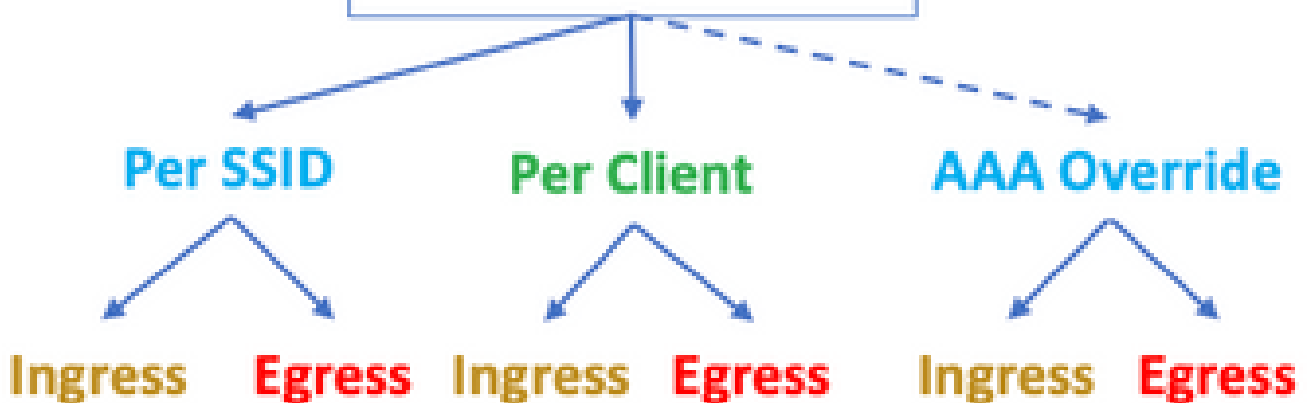
- 備註DSCP
- 刪除Youtube和Netflix影片

- ACL中指定的主機速率限制為50Kbps
- 速率限制所有其他流量為100Kbps

## POLICY MAP - Guest



## POLICY-PROFILE-2



例如，QoS策略必須在入口和出口兩個方向對每個SSID應用於連結到訪客WLAN的策略配置檔案。

設定

## AAA伺服器和方法清單

步驟 1. 導航到 Configuration > Security > AAA > Authentication > Servers/Groups，然後選擇 +Add。

輸入AAA伺服器名稱、IP地址和金鑰，這必須與ISE上的Administration > Network Resources > Network Devices下的共用金鑰匹配。

Name\*

ISE22

IPv4 / IPv6 Server Address\*

172.16.13.6

PAC Key

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



步驟 2. 導航到 Configuration > Security > AAA > Authentication > AAA Method List，然後選擇 +Add。從「可用的伺服器群組」中選取「指定的伺服器群組」。

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

步驟 3. 導航到 Configuration > Security > AAA > Authorization > AAA method List , 然後選擇 Add。選擇預設方法並將「network」作為型別。

## 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

控制器需要應用由AAA伺服器返回的授權屬性（例如，此處的QoS策略）。否則，將不會應用從RADIUS接收的策略。

### WLAN策略、站點標籤和AP標籤

步驟 1. 導航到配置>無線設定>高級>立即開始> WLAN配置檔案，選擇+增加以建立一個新的WLAN。配置SSID、配置檔名稱、WLAN ID，並將狀態設定為啟用。

然後，導航到Security > Layer 2並配置第2層身份驗證引數：

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安全並不一定是802.1x作為QoS的必要條件，但在此配置示例中仍用於AAA覆蓋。

步驟 2. 導航到Security > AAA，然後在Authentication List下拉框中選擇AAA伺服器。



General

Security

Advanced

Layer2

Layer3

AAA

Authentication List

ISE-Auth

Local EAP Authentication

步驟 3.選擇Policy Profile，然後選擇+Add。配置策略配置檔名稱。

將「Status ( 狀態 )」設定為「Enabled ( 啟用 )」；同時啟用「Central Switching ( 集中交換 )」、「Authentication ( 身份驗證 )」、「DHCP(DHCP)」和「Association ( 關聯 )」：

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

步驟 4.導航到訪問策略，並配置當客戶端連線到SSID時無線客戶端所分配的VLAN：

General **Access Policies** QOS and AVC Mobility Advanced

---

RADIUS Profiling

Local Subscriber Policy Name

**WLAN Local Profiling**

Global State of Device Classification **Disabled** ⓘ

HTTP TLV Caching

DHCP TLV Caching

**VLAN**

VLAN/VLAN Group

Multicast VLAN

步驟 5.選擇Policy Tag 並選擇+Add。配置策略標籤名稱。

在WLAN-Policy Maps下，在+Add上，從下拉選單中選擇WLAN Profile和Policy Profile，然後選擇針對要配置的對映的檢查。

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

步驟 6.選擇Site Tag，然後選擇+Add。選中Enable Local Site框，使AP以本地模式運行（或者使FlexConnect保持未選中狀態）：

Name\*

Description

AP Join Profile

Control Plane Name

步驟 7.選擇Tag APs，選擇AP並增加策略、站點和RF標籤：

## Tags

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

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

### Qos

步驟 1. 導航到配置>服務> QoS，然後選擇+Add建立QoS策略。

命名它（在本示例中：BWLimitAAClients）。

## 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
◀ 0 ▶ 10 items per page No items to display							
<a href="#">+ Add Class-Maps</a> <a href="#">x Delete</a>							

Class Default


Mark	<input type="text" value="None"/>	Police(kbps)	<input type="text" value="8 - 10000000"/>
------	-----------------------------------	--------------	---

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

Available (2)

Selected (0)

Profiles

 vlan3000
--

Profiles

Ingress

Egress

步驟 2. 增加一個類對映以刪除Youtube和Netflix。按一下Add Class-Maps。選擇AVC、match any、drop操作並選擇兩個協定。

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

點選儲存。

步驟 3.增加註釋DSCP 46到34的類對映。

按一下Add Class-Maps。

- 匹配任意，使用者定義
- 匹配型別DSCP
- 匹配值46
- 標籤型別DSCP
- 標籤值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

點選儲存。

步驟 4.要定義一個類對映，該對映用於為發往特定主機的流量制定規則，請為該主機建立一個ACL。

按一下Add Class-Maps，

依次選擇User Defined、match any、match type ACL、choose your ACL name(此處specific hostACL)、mark type none並選擇速率限制值。

點選儲存。

	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	

10 items per page 1 - 2 of 2 items

AVC/User Defined:

Match:  Any  All

Match Type:

Match Value\*:

Mark Type:

Drop:

Police(kbps):

以下是用於辨識特定主機流量的ACL示例：

	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

10 items per page 1 - 2 of 2 items

步驟 5.在類對映幀下，使用預設類設定所有其他流量的速率限制。

這會設定不受上述規則之一影響的所有客戶端流量的速率限制。

	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	

items per page 1 - 3 of 3 items

Class Default

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

步驟 6. 按一下底部的Apply to Device。

等效的CLI配置：

```

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

```

注意：在本示例中，由於QoS策略由AAA覆蓋應用，因此未選擇該策略下的配置檔案。但是，為了將QoS策略手動應用到策略配置檔案，請務必選擇所需的配置檔案。



步驟 2. 在ISE上，導航到策略>策略元素>結果>授權配置檔案，選擇+增加以建立授權配置檔案。

要應用QoS策略，請透過Cisco AV對將其增加為高級屬性設定。

假設ISE身份驗證和授權策略配置為匹配正確的規則並獲得此授權結果。


屬性包括ip : sub-qos-policy-in=<policy name>和ip : sub-qos-policy-out=<policyname>

### Advanced Attributes Settings

The screenshot shows two rows of attribute settings. Each row consists of a dropdown menu containing 'Cisco:cisco-av-pair', followed by an equals sign, another dropdown menu, and a minus sign. The first dropdown menu is set to 'ip:sub-qos-policy-in=BWLimitA...'. The second dropdown menu is set to 'ip:sub-qos-policy-out=BWLimit...'. A green plus sign is visible to the right of the second row.

### Attributes Details

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

 注意：策略名稱區分大小寫。確保案例正確！

## 驗證

使用本節內容，確認您的組態是否正常運作：

在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
```

```
(...)
```

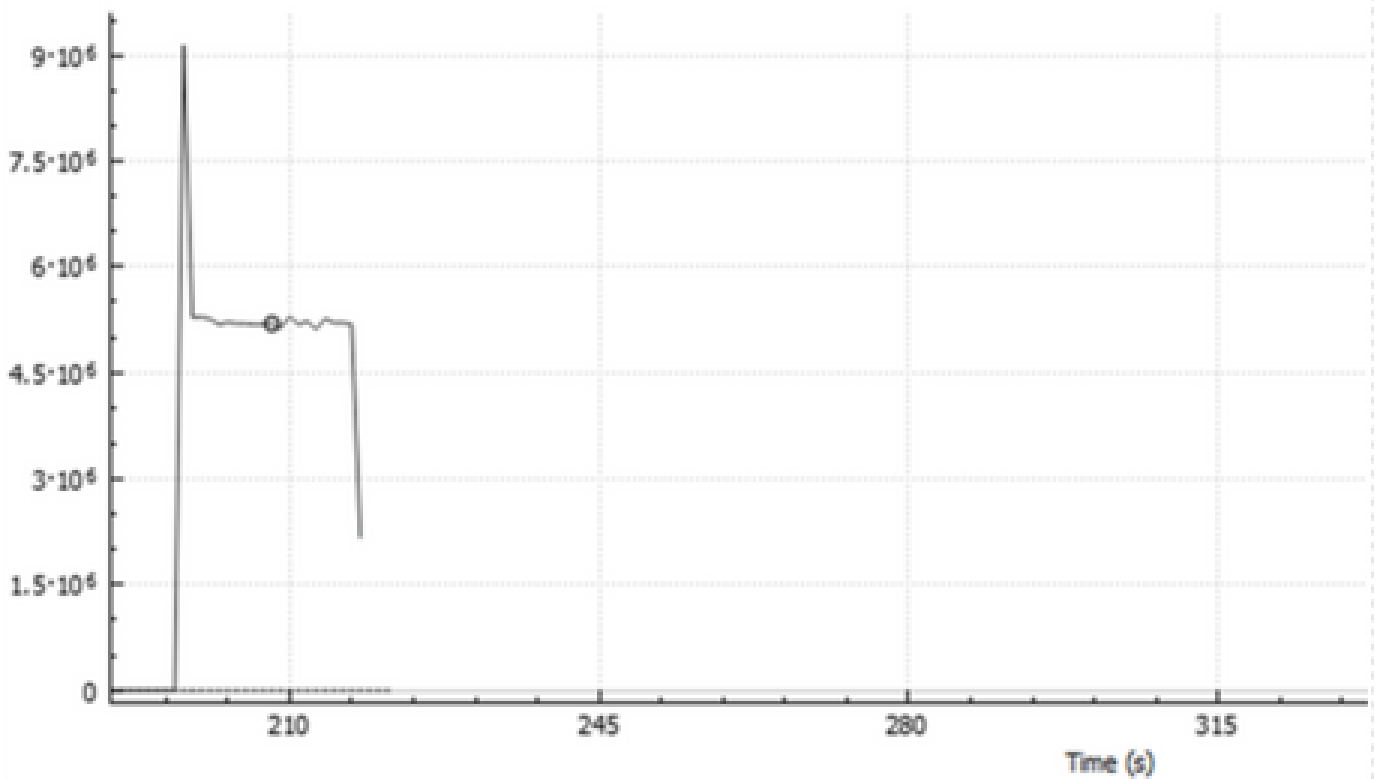
```
Local Policies:  
  Service Template : wlan_svc_QoS-PP (priority 254)  
    VLAN           : 1  
    Absolute-Timer : 1800  
Server Policies:  
  Input QoS       : BWLimitAAAClients  
  Output QoS      : BWLimitAAAClients  
Resultant Policies:  
  VLAN Name       : default  
  
  Input QoS      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

## 在AP上

當AP處於本地模式或SSID處於Flexconnect中央交換模式時，無需對AP進行故障排除，因為QoS和服務策略由WLC完成。

## 資料包捕獲IO圖分析

## 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

## 疑難排解

本節提供的資訊用於對組態進行疑難排解。

步驟 1.清除所有預先存在的調試條件。

```
# clear platform condition all
```

步驟 2.啟用有問題的無線客戶端的調試。

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

步驟 3.將無線客戶端連線到SSID以重現問題。

步驟 4.在重現問題後停止調試。

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

測試期間捕獲的日誌儲存在WLC上的本地檔案中，其名稱為：

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

如果使用GUI工作流程產生此追蹤，則儲存的檔案名稱為debugTrace\_aaaa.bbbb.cccc.txt。

步驟 5.若要收集先前產生的檔案，請將ra trace .log複製到外部伺服器，或直接在熒幕上顯示輸出。

使用以下命令檢查RA跟蹤檔案的名稱：

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

將檔案複製到外部伺服器：

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

或者，顯示內容：

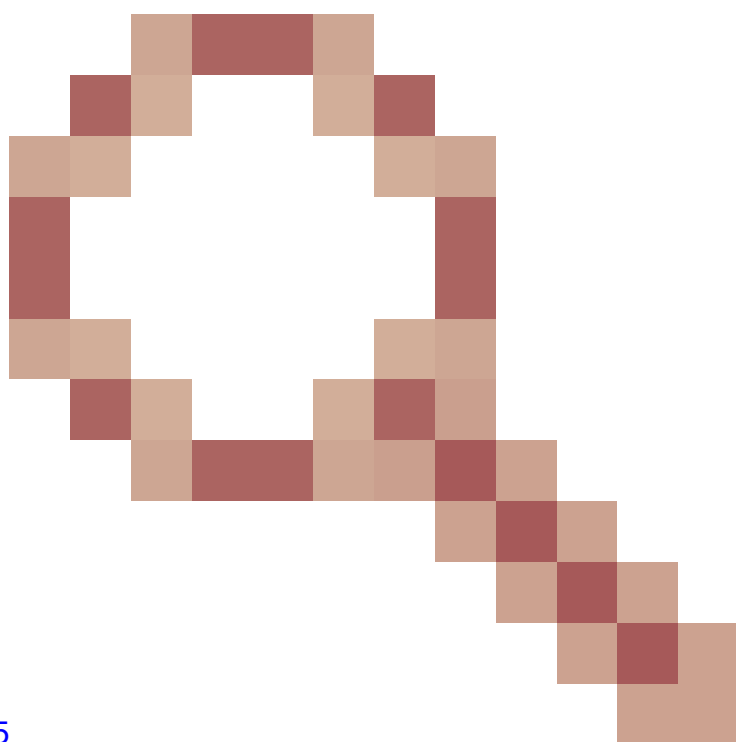
```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

步驟 6.移除偵錯條件。

```
# clear platform condition all
```

## Flexconnect本地交換 ( 或交換矩陣/SDA ) 方案

對於flexconnect本地交換 ( 或交換矩陣/SDA ) ， AP將應用您在WLC上定義的所有QoS策略。



警告：由於Cisco bug ID [CSCwh74415](#)

---

---

，RADIUS伺服器返回的最新QoS策略將應用於連線到同一存取點的所有客戶端，因此將覆蓋所有其他QoS策略。從17.6.2版本開始，使用AAA覆蓋的每客戶端速率限制不再正常工作。請參閱錯誤說明，以檢查修正版本。


---

在wave2和11ax存取點上，速率限制發生在每個流（5元組）級別，而不是在17.6之前的每個客戶端或每個SSID。這適用於Flexconnect/Fabric中的存取點、存取點上的嵌入式無線控制器(EWc-AP)部署。

從17.5開始，可以利用AAA覆蓋來推送屬性以達到每個客戶端的速率限制。

從17.6開始，在Flex本地交換配置中的802.11ac Wave 2和11ax AP上支援每客戶端雙向速率限制。

---

 注意：Flex AP不支援QoS策略中存在ACL。它們也不支援BRR（剩餘頻寬）和策略優先順序，後者可以透過CLI進行配置但在9800 Web UI中不可用，在9800上也不支援。思科漏洞ID [CSCvx81067](#)跟蹤Flex AP的QoS策略中的ACL支援。

---

## 組態

配置與本文第一部分完全相同，但有兩個例外：

1. 策略配置檔案已設定為本地交換。Flex部署要求在本埠17.4發佈之前停用中央關聯。

自17.5起，此欄位已硬編碼，因此不可用於使用者配置。

## WLAN Switching Policy

Central Switching



Central Authentication



Central DHCP



Central Association



Flex NAT/PAT



2. 站點標籤設定為不是本地站點

# Enable Local Site



Flexconnect/交換矩陣故障排除

因為AP是應用QoS策略的裝置，所以這些命令有助於縮小應用的範圍。

```
show dot11 qos
```

show policy-map

show rate-limit client

show rate-limit ssid

show rate-limit wlan

show flexconnect client

<#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
A8:DB:03:6F:7A:46 2 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#
```

## 參考資料

[Catalyst 9000 16.12 QoS指南](#)

[9800 QoS配置指南](#)

[Catalyst 9800組態型號](#)

[Cisco IOS® XE 17.6發行版本註釋](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。