

# Configuration de la limite de débit QoS (BDRL) sur les contrôleurs sans fil Catalyst 9800 avec remplacement AAA

## Table des matières

- [Introduction](#)
- [Conditions préalables](#)
- [Exigences](#)
- [Composants utilisés](#)
- [Informations générales](#)
- [Exemple : Politiques QoS invité et entreprise](#)
- [Configurer](#)
- [Serveur AAA et liste de méthodes](#)
- [Politique WLAN, balise de site et balise AP](#)
- [QoS](#)
- [Vérifier](#)
- [Sur le WLC](#)
- [Sur le point d'accès](#)
- [Capture des paquets Analyse du graphique E/S](#)
- [Dépannage](#)
- [Scénario de commutation locale Flexconnect \(ou fabric/SDA\)](#)
- [Configuration](#)
- [Dépannage de Flexconnect/Fabric](#)
- [Références](#)

## Introduction

Ce document décrit un exemple de configuration pour Limite BDRL (Bi Directional Rate Limit) sur les contrôleurs sans fil Catalyst 9800.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- [Modèle de configuration Catalyst Wireless 9800](#)
- AAA avec Cisco Identity Service Engine (ISE)

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur sans fil Cisco Catalyst 9800-CL sur la version 16.12.1s
- Identity Service Engine sur la version 2.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

La QoS de la plate-forme WLC 9800 utilise les mêmes concepts et composants que les plates-formes Catalyst 9000.

Cette section fournit une vue d'ensemble globale du fonctionnement de ces composants et de la manière dont ils peuvent être configurés pour obtenir différents résultats.

En substance, la récursivité QoS fonctionne de la manière suivante :

1. Class-Map : identifie un certain type de trafic. Les cartes-classes peuvent tirer parti du moteur AVC (Application Visibility and Control).

En outre, l'utilisateur peut définir des mappages de classes personnalisés pour identifier le trafic correspondant à une liste de contrôle d'accès (ACL) ou à un point de code de services différenciés (DSCP)

2. Policy-Map : politiques qui s'appliquent aux cartes-classes.

Ces politiques pourraient marquer DSCP, abandonner ou limiter le débit du trafic qui correspond à la carte de classe

4. Service-Policy : Policy-maps peut être appliqué sur le profil de stratégie d'un SSID ou par client dans une certaine direction avec la commande service-policy.

3. (Facultatif) Table-Map : Ils sont utilisés pour convertir un type de marque à un autre, par exemple, CoS à DSCP.

---

**Remarque** : dans la table-map, spécifiez les valeurs à modifier (4 à 32) ; dans la carte-politique, la technologie est spécifiée (COS à 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

---

**Remarque** : si deux stratégies ou plus sont applicables par cible, la résolution des stratégies est

---

choisie en fonction de ce classement par priorité :

- AAA Override (le plus élevé)
- Profil natif (politiques locales)
- Stratégie configurée
- Stratégie par défaut (la plus basse)

Vous trouverez plus de détails dans le [guide de configuration QoS](#) officiel [du 9800](#)

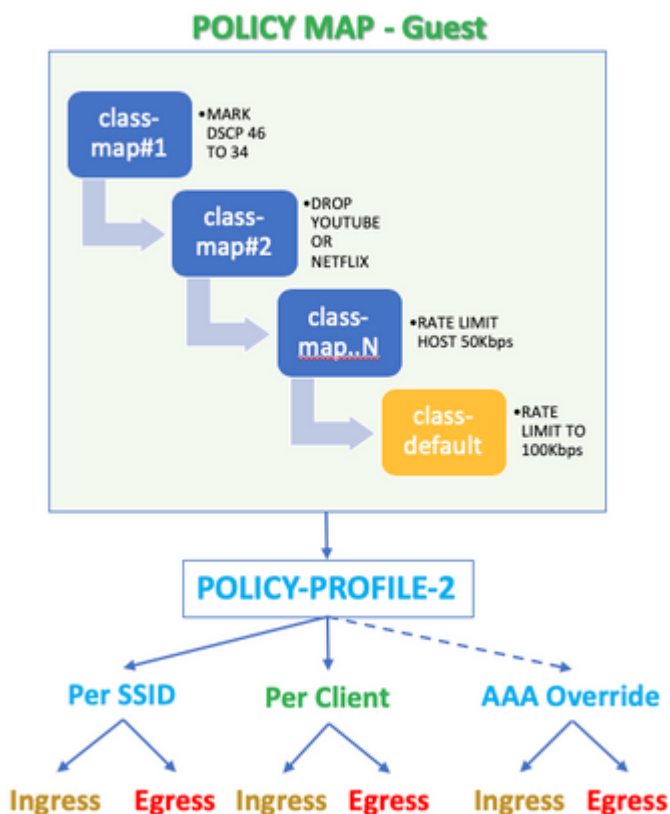
Pour plus d'informations sur la théorie de la QoS, consultez le [guide de configuration de la QoS de la gamme 9000](#)

## Exemple : Politiques QoS invité et entreprise

Cet exemple montre comment les composants QoS expliqués s'appliquent dans un scénario réel.

L'objectif est de configurer une stratégie QoS pour les invités qui :

- Remarque DSCP
- Abandonne les vidéos Youtube et Netflix
- Débit Limite un hôte spécifié dans une liste de contrôle d'accès à 50 Kbits/s
- Rate Limite tout autre trafic à 100 Kbits/s



Dans cet exemple, la stratégie QoS doit être appliquée par SSID dans les deux sens, en entrée et en sortie, vers le profil de stratégie qui est lié au WLAN invité.

## Configurer

## Serveur AAA et liste de méthodes

Étape 1. Accédez à **Configuration > Security > AAA > Authentication > Servers/Groups** et sélectionnez **+Add**.

Entrez le nom du serveur AAA, l'adresse IP et la clé, qui doivent correspondre au secret partagé sous **Administration > Network Resources > Network Devices** sur ISE.

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"/>

Étape 2. Accédez à **Configuration > Security > AAA > Authentication > AAA Method List** et sélectionnez **+Add**. Sélectionnez Groupes de serveurs affectés dans Groupes de serveurs disponibles.

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

Étape 3. Accédez à **Configuration > Security > AAA > Authorization > AAA method List** et sélectionnez **Add**. Choisissez la méthode par défaut et « network » comme type.

## Quick Setup: AAA Authorization

Method List Name\*

default

Type\*

network ▼

Group Type

group ▼

Fallback to local

Authenticated

Available Server Groups

Assigned Server

ldap  
tacacs+



radius

Ceci est nécessaire pour que le contrôleur applique les attributs d'autorisation (par exemple la stratégie QoS ici) retournés par le serveur AAA. Sinon, la stratégie reçue de RADIUS n'est pas appliquée.

### Politique WLAN, balise de site et balise AP

Étape 1. Accédez à **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile** et sélectionnez **+Add** pour créer un nouveau WLAN. Configurez le SSID, le nom de profil, l'ID WLAN et définissez l'état sur **Activé**.

Accédez ensuite à **Security > Layer 2** et configurez les paramètres d'authentification de la couche 2 :

General **Security** Advanced

---

**Layer2** Layer3 AAA

---

Layer 2 Security Mode  Fast Transition

MAC Filtering  Over the DS

**Protected Management Frame** Reassociation Timeout

PMF

**WPA Parameters**

WPA Policy

WPA2 Policy

WPA2 Encryption

- AES(CCMP128)
- CCMP256
- GCMP128
- GCMP256

MPSK

Auth Key Mgmt

- 802.1x
- PSK
- CCKM
- FT + 802.1x
- FT + PSK
- 802.1x-SHA256
- PSK-SHA256

La sécurité SSID n'a pas besoin d'être 802.1x comme condition requise pour la QoS, mais elle est utilisée dans cet exemple de configuration pour le remplacement AAA.

Étape 2. Accédez à **Security > AAA** et sélectionnez le serveur AAA dans la zone déroulante **Authentication List**.

General **Security** Advanced

---

Layer2 Layer3 **AAA**

---

Authentication List

Local EAP Authentication

Étape 3. Sélectionnez **Profil de stratégie** et sélectionnez **+Ajouter**. Configurez le nom du profil de stratégie.

Définissez l'état sur **Activé** ; activez également la commutation centrale, l'authentification, DHCP et l'association :

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

Étape 4. Accédez à **Access Policies** et configurez le VLAN auquel le client sans fil est affecté lorsque le client se connecte au SSID :

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

Étape 5. Sélectionnez **Balise de stratégie** et sélectionnez **+Ajouter**. Configurez le nom de la balise de stratégie.

Sous **WLAN-Policy Maps**, sur **+Add**, sélectionnez les options **WLAN Profile** et **Policy Profile** dans les menus déroulants, puis activez la case à cocher correspondant à la carte à configurer.

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\*

Étape 6. Sélectionnez **Balise de site** et sélectionnez **+Ajouter**. Cochez la case **Enable Local Site** pour que les points d'accès fonctionnent en mode local (ou laissez-la décochée pour FlexConnect) :

Name\*

Description

AP Join Profile

Control Plane Name

Enable Local Site

Étape 7. Sélectionnez **Tag APs**, choisissez les AP et ajoutez la politique, le site et la balise RF :

**Tags**

Policy

Site

RF

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

## QoS

Étape 1. Accédez à **Configuration > Services > QoS** et sélectionnez **+Add** pour créer une stratégie QoS.

Nommez-le (pour cet exemple : 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
◀ ◁ 0 ▷ ▶ 10 items per page No items to display							
<a href="#">+ Add Class-Maps</a>		<a href="#">× 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

Profiles	Ingress	Egress

Étape 2. Ajoutez une carte de classe pour supprimer Youtube et Netflix. Cliquez sur **Add Class-Maps**. Sélectionnez **AVC**, match **any**, **drop** action et choisissez les deux protocoles.

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined
<p>◀◀ 0 ▶▶ 10 items per page No items</p> <p>+ Add Class-Maps    × Delete</p> <p>AVC/User Defined: AVC</p> <p>Match: <input checked="" type="radio"/> Any    <input type="radio"/> All</p> <p>Drop: <input checked="" type="checkbox"/></p> <p>Match Type: protocol</p> <p>Available Protocol(s): netbios-ssn, netblt, netflow</p> <p>Selected Protocol(s): youtube, netflix</p> <p>Cancel</p>						

Appuyez sur **Enregistrer**.

Étape 3. Ajoutez une carte de classe qui remarque les DSCP 46 à 34.

Cliquez sur **Add Class-Maps**.

- Correspondance **quelconque, Défini par l'utilisateur**
- Correspondance du type **DSCP**
- Valeur de correspondance **46**
- Marquer le type **DSCP**
- Valeur de marquage **34**

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

1  items per page 1 - 1

AVC/User Defined:

Match:  Any  All

Match Type:

Match Value\*:

Mark Type:  Mark Value:

Drop:

Police(kbps):

Appuyez sur **Enregistrer**.

Étape 4. Pour définir un mappage de classe qui gère le trafic vers un hôte spécifique, créez une liste de contrôle d'accès pour celui-ci.

Cliquez sur **Add Class-Maps**,

Choisissez Défini par l'utilisateur, correspondez à **tout**, correspondez au type de **liste de contrôle d'accès**, choisissez votre nom de liste de contrôle d'accès (ici **spécifique hostACL**), marquez le type **aucun** et choisissez la valeur de limite de débit.

Cliquez sur Save.

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

items per page

AVC/User Defined:

Match:  Any  All

Match Type:

Match Value\*:

Mark Type:

Drop:

Police(kbps):

Voici un exemple de liste de contrôle d'accès que nous utilisons pour identifier un trafic hôte spécifique :

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port
<input type="checkbox"/>	1	permit	any		192.168.1.59		ip	
<input type="checkbox"/>	2	permit	192.168.1.59		any		ip	

items per page

Étape 5. Sous la trame class maps, utilisez la classe par défaut pour définir la limite de débit pour tout le reste du trafic.

Ceci définit une limite de débit sur tout le trafic client qui n'est pas ciblé par l'une des règles ci-dessus.

	Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined
<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

#### Class Default

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

Étape 6. Cliquez sur **Apply to Device** en bas.

Configuration CLI équivalente :

```

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

```

---

**Remarque** : dans cet exemple, aucun **profil n**'a été sélectionné sous la stratégie QoS car elle est appliquée par le remplacement AAA. Toutefois, pour appliquer manuellement la stratégie QoS à un profil de stratégie, sélectionnez les profils souhaités.

---

Étape 2. Dans ISE, accédez à **Policy > Policy Elements > Results > Authorization Profiles** et sélectionnez on **+Add** pour créer un profil d'autorisation.

Pour appliquer la stratégie QoS, ajoutez-les en tant que **Paramètres d'attributs avancés** via les paires Cisco AV.

On suppose que les stratégies d'authentification et d'autorisation ISE sont configurées pour correspondre à la règle appropriée et obtenir ce résultat d'autorisation.

Les attributs sont **ip:sub-qos-policy-in=<nom de la stratégie>** et **ip:sub-qos-policy-out=<nom de la stratégie>**

The screenshot shows the configuration interface for an Authorization Profile. Under the 'Advanced Attributes Settings' section, two attribute pairs are defined: 'Cisco:cisco-av-pair' is mapped to 'ip:sub-qos-policy-in=BWLimitAA...' and 'Cisco:cisco-av-pair' is mapped to 'ip:sub-qos-policy-out=BWLimit...'. Below this, the 'Attributes Details' section shows the resulting configuration: 'Access Type = ACCESS\_ACCEPT', 'cisco-av-pair = ip:sub-qos-policy-in=BWLimitAAClients', and 'cisco-av-pair = ip:sub-qos-policy-out=BWLimitAAClients'.

---

**Remarque** : les noms de stratégie sont sensibles à la casse. Assurez-vous que la casse est correcte !

---

## Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration:

### Sur le WLC

```
# 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
```

```
detail
# show wireless client
```

```
service-policy input
# show wireless client
```

```
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
```

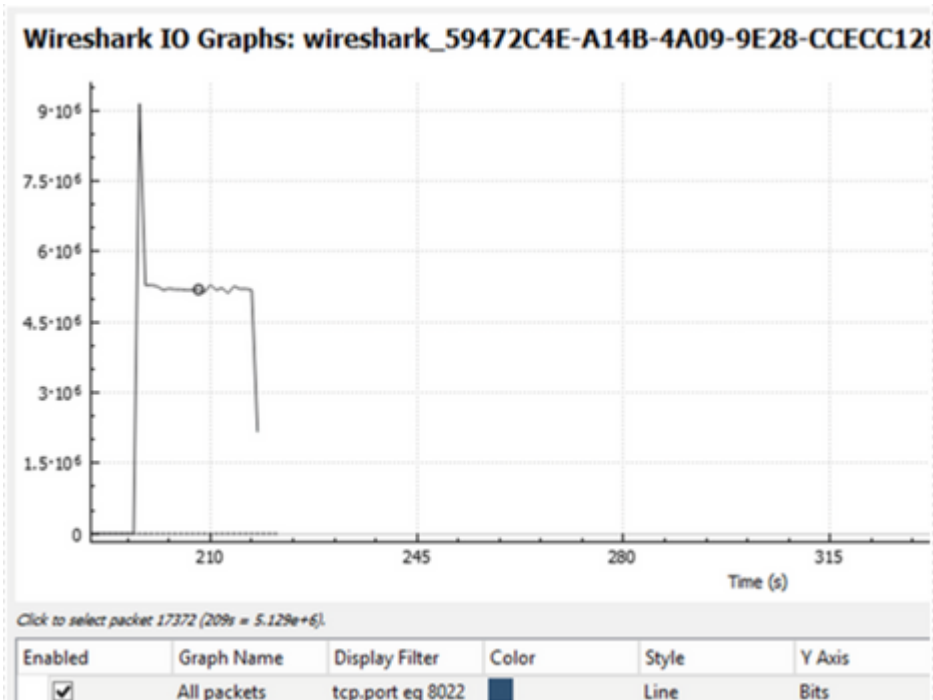
```
(...)
```

```
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
```

## Sur le point d'accès

Aucun dépannage n'est requis sur l'AP lorsque l'AP est en mode local ou le SSID en mode de commutation Flexconnect Central, car les politiques de QoS et de service sont effectuées par le WLC.

## Capture des paquets Analyse du graphique E/S



## Dépannage

Cette section fournit des informations pour dépanner votre configuration.

Étape 1. Effacez toutes les conditions de débogage préexistantes.

```
# clear platform condition all
```

Étape 2. Activez le débogage pour le client sans fil en question.

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

Étape 3. Connectez le client sans fil au SSID afin de reproduire le problème.

Étape 4. Arrêtez les débogages une fois le problème reproduit.

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

Les journaux capturés pendant le test sont stockés sur le WLC dans un fichier local portant le nom :

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```



Si le workflow de l'interface graphique utilisateur est utilisé pour générer cette trace, le nom de fichier enregistré est debugTrace\_aaaa.bbb.cccc.txt.

Étape 5. Pour collecter le fichier généré précédemment, copiez le fichier ra trace .log sur un serveur externe ou affichez le résultat directement à l'écran.

Vérifiez le nom du fichier de suivi RA avec cette commande :

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

Copiez le fichier sur un serveur externe :

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

Vous pouvez également afficher le contenu :

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

Étape 6. Supprimez les conditions de débogage.

```
# clear platform condition all
```

## Scénario de commutation locale Flexconnect (ou fabric/SDA)

En cas de commutation locale flexconnect (ou fabric / SDA), c'est le point d'accès qui applique n'importe quelle politique de QoS que vous avez définie sur le WLC.

Sur les points d'accès wave2 et 11ax, la limite de débit se produit à un niveau par flux (5 tuples) et non par client ou par SSID avant 17.6.

Ceci s'applique aux points d'accès dans les déploiements Flexconnect/Fabric, Contrôleur sans fil intégré sur point d'accès (EWc-AP).

À partir de la version 17.5, le remplacement AAA peut être utilisé pour pousser les attributs afin d'atteindre la limite de débit par client.

À partir de la version 17.6, la limite de débit bidirectionnel par client est prise en charge sur les points d'accès 802.11ac de phase 2 et 11ax dans la configuration de commutation locale Flex.

---

**Remarque** : les points d'accès flexibles ne prennent pas en charge la présence de listes de contrôle d'accès dans les stratégies QoS. Ils ne prennent pas non plus en charge le BRR (bande passante)

---

---

restante) et la priorité de stratégie, qui sont configurables via l'interface de ligne de commande, mais ne sont pas disponibles dans l'interface utilisateur Web du 9800 et ne sont pas pris en charge sur le 9800. L'ID de bogue Cisco [CSCvx81067](#) effectue le suivi de la prise en charge des ACL dans les politiques de QoS pour les AP flexibles.

---

## Configuration

La configuration est exactement la même que dans la première partie de cet article, à deux exceptions près :

1. Le profil de stratégie est défini sur la commutation locale. Le déploiement flexible nécessite que l'association centrale soit désactivée jusqu'à la version 17.4 de Bengaluru.

À partir de la version 17.5, ce champ n'est plus disponible pour la configuration utilisateur car il est codé en dur.

WLAN Switching Policy	
Central Switching	<input type="checkbox"/> DISABLED
Central Authentication	<input checked="" type="checkbox"/> ENABLED
Central DHCP	<input type="checkbox"/> DISABLED
Central Association	<input type="checkbox"/> DISABLED
Flex NAT/PAT	<input type="checkbox"/> DISABLED

2. La balise de site est définie pour ne pas être un site local

Enable Local Site

## Dépannage de Flexconnect/Fabric

Étant donné que le point d'accès est le périphérique qui applique les stratégies QoS, ces commandes peuvent aider à restreindre ce qui est appliqué.

**show dot11 qos**

**show policy-map**

**show rate-limit client**

**show rate-limit bssid**

**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-acl	aaa-ipv6-acl	assoc	auth	switching
A8:DB:03:6F:7A:46	1	2	1	FWD	AES_CCM128	none	none	none	Local	Central	Local

AP780C-F085-49E6#

## Références

[Guide QoS du Catalyst 9000 16.12](#)

[Guide de configuration QoS du 9800](#)

[Modèle de configuration Catalyst 9800](#)

[Notes de version de Cisco IOS® XE 17.6](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.