

Dépannage de QoS sur les commutateurs Catalyst 6500

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Dépannage de la QoS](#)

[Procédure de dépannage étape par étape](#)

[Directives et limites de qualité de service sur les commutateurs Catalyst 6500](#)

[Limitation QoS TCAM](#)

[Limitation NBAR](#)

[Commandes cos-map manquantes dans Supervisor 2](#)

[Limitations de la stratégie de service](#)

[Les instructions de sortie de la stratégie de service ne s'affichent pas dans la sortie de la commande running-config](#)

[Limitation de la réglementation](#)

[Problèmes de limite de débit ou de réglementation avec MSFC dans le système d'exploitation hybride](#)

[Moyenne de forme de commande non prise en charge dans les interfaces VLAN de Cisco 7600](#)

[ERREUR QoS : L'ajout/la modification apporté à la picymap \[chars\] et à la classe \[chars\] n'est pas valide, la commande est rejetée](#)

[Informations connexes](#)

Introduction

Ce document présente les étapes de dépannage de base, les limites de la qualité de service (QoS), et facilite le dépannage de problèmes courants de QoS sur les commutateurs Catalyst 6500. Ce document discute également des problèmes de QoS qui se produisent lors de la classification, du marquage et de la surveillance.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur les commutateurs de la gamme Catalyst 6500.

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

La QoS est une fonctionnalité réseau permettant de classer le trafic et de fournir des services de livraison déterministes. Ces éléments expliquent les différentes étapes du processus QoS :

- **Input Scheduling** - Il est géré par des ASIC de port matériel et il s'agit d'une opération QoS de couche 2. Il ne nécessite pas de carte PFC (Policy Feature Card).
- **Classification** : il est géré par le superviseur et/ou PFC via le moteur de liste de contrôle d'accès (ACL). Le superviseur gère le fonctionnement de la QoS de couche 2. PFC gère le fonctionnement de la QoS des couches 2 et 3.
- **Réglementation** : elle est gérée par PFC via le moteur de transfert de couche 3. La carte PFC est requise et elle gère le fonctionnement de la QoS de couche 2 et de couche 3.
- **Réécriture de paquets** : elle est gérée par les circuits ASIC des ports matériels. Il s'agit d'une opération de qualité de service de couche 2 et de couche 3 basée sur la classification effectuée précédemment.
- **Output Scheduling** - Il est géré par les ASIC des ports matériels. Il s'agit d'une opération de qualité de service de couche 2 et de couche 3 basée sur la classification effectuée précédemment.

Dépannage de la QoS

La qualité de service fonctionne différemment dans les commutateurs Catalyst 6500 et dans les routeurs. L'architecture QoS est assez complexe dans les commutateurs Catalyst 6500. Il est recommandé de comprendre l'architecture MSFC (Multilayer Switch Feature Card), PFC et Supervisor Engine du Catalyst 6500. La configuration de la qualité de service dans le système d'exploitation hybride nécessite une meilleure compréhension de la fonctionnalité CatOS de couche 2 et de la carte MSFC de couche 3 avec la fonctionnalité Cisco IOS®. Il est recommandé de lire ces documents en détail avant de configurer QoS :

- [Configuration de la QoS PFC - IOS natif](#)
- [Configuration de QoS - CatOS](#)

Procédure de dépannage étape par étape

Cette section contient la procédure de dépannage de base étape par étape pour QoS afin d'isoler

le problème pour un dépannage ultérieur.

1. **Enable QoS** —La commande `show mls qos` affiche les statistiques de contrôle et l'état de QoS, qu'elle soit activée ou désactivée.

```
Switch#show mls qos
QoS is enabled globally
QoS ip packet dscp rewrite enabled globally
Input mode for GRE Tunnel is Pipe mode
Input mode for MPLS is Pipe mode
Vlan or Portchannel(Multi-Earl)policies supported: Yes
Egress policies supported: Yes

----- Module [5] -----
QoS global counters:
  Total packets: 244
  IP shortcut packets: 0
  Packets dropped by policing: 0
  IP packets with TOS changed by policing: 5
  IP packets with COS changed by policing: 4
  Non-IP packets with COS changed by policing: 0
  MPLS packets with EXP changed by policing: 0
```

2. **Classification du trafic entrant à l'aide du port d'approbation** - Cette classification classe le trafic entrant dans l'une des sept valeurs de classe de service (CoS). La valeur CoS du trafic entrant peut déjà être attribuée par la source. Dans ce cas, vous devez configurer le port pour qu'il fasse confiance à la valeur CoS du trafic entrant. La confiance permet au commutateur de conserver les valeurs CoS ou ToS de la trame reçue. Cette commande montre comment vérifier l'état d'approbation du port :

```
Switch#show queueing int fa 3/40
Port QoS is enabled
Trust state: trust CoS
  Extend trust state: not trusted [CoS = 0]
  Default CoS is 0
```

!--- Output suppressed.

La valeur CoS est transportée uniquement par les trames ISL (Inter-Switch Link) et dot1q. Les trames non étiquetées ne portent pas de valeurs CoS. Les trames non étiquetées transportent des valeurs ToS dérivées de la priorité IP ou du point de code de services différenciés (DSCP) de l'en-tête de paquet IP. Afin de faire confiance à la valeur ToS, vous devez configurer le port pour qu'il fasse confiance à la priorité IP ou au DSCP. DSCP est rétrocompatible avec la priorité IP. Par exemple, si vous avez configuré un port de commutateur comme port de couche 3, il ne transporte pas de trames dot1q ou ISL. Dans ce cas, vous devez configurer ce port pour qu'il fasse confiance à DSCP ou à la priorité IP.

```
Switch#show queueing interface gigabitEthernet 1/1
Interface GigabitEthernet1/1 queueing strategy: Weighted Round-Robin
Port QoS is enabled
Trust state: trust DSCP
  Extend trust state: not trusted [COS = 0]
  Default CoS is 0
```

!--- Output suppressed.

3. **Classification du trafic entrant à l'aide des listes de contrôle d'accès et des ACE** : vous pouvez également configurer le commutateur pour classer et marquer le trafic. Les étapes de configuration de la classification et du marquage sont les suivantes : créez des listes d'accès, une carte-classe et une carte-politique et émettez la commande `service-policy input` afin d'appliquer la carte-politique à l'interface. Vous pouvez vérifier les statistiques de la carte

de stratégie comme indiqué ici :

```
Switch#show policy-map interface fa 3/13
FastEthernet3/13
```

```
Service-policy input: pqos2
```

```
class-map: qos1 (match-all)
  Match: access-group 101
  set precedence 5:
  Earl in slot 5 :
    590 bytes
  5 minute offered rate 32 bps
  aggregate-forwarded 590 bytes
```

```
Class-map: class-default (match-any)
  36 packets, 2394 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

```
Switch#show mls qos ip ingress
```

```
QoS Summary [IPv4]: (* - shared aggregates, Mod - switch module)
```

Int	Mod	Dir	Class-map	DSCP	Agg Id	Trust	Fl Id	AgForward-By	AgPoliced-By
Fa3/13	5	In	qos1	40	1	No	10	590	0
All	5	-	Default	0	0*	No	0	365487	0

Notez que les compteurs **AgForward-By** qui correspondent au class-map qos1 augmentent. Si vous ne voyez pas les statistiques de la carte-classe correspondante, vérifiez la liste d'accès jointe à la carte-classe.

4. **Planification des entrées** : PFC n'est pas nécessaire pour configurer la planification des entrées. Vous ne pouvez pas configurer les commandes **rcv-queue threshold** ou **set qos drop-threshold** sur un seul port 10/100. En effet, la planification des entrées est gérée par les ports ASIC Coil qui contiennent douze ports 10/100. Par conséquent, vous devez configurer la planification des entrées dans des jeux de 12 ports, tels que 1-12, 13-24, 25-36, 37-48. L'architecture de mise en file d'attente est intégrée à l'ASIC et ne peut pas être reconfigurée. Émettez la commande **show queueing interface fastethernet slot/port | include type** pour afficher la structure de file d'attente d'un port LAN.

```
Switch#show queueing interface fastEthernet 3/40
```

```
Queueing Mode In Rx direction: mode-cos
```

```
Receive queues [type = 1q4t]: <----- 1 Queue 4 Threshold
Queue Id      Scheduling  Num of thresholds
-----
1             Standard    4
```

```
queue tail-drop-thresholds
```

```
1 50[1] 60[2] 80[3] 100[4] <----- Threshold levels 50%, 60%, 80% and 100%
```

```
Packets dropped on Receive:
```

```
BPDU packets: 0
```

```
queue thresh  dropped  [cos-map]
-----
1 1           0 [0 1 ]
1 2           0 [2 3 ]
1 3           0 [4 5 ]
```

!--- Output suppressed.

Par défaut, tous les 4 seuils sont de 100 %. Vous pouvez émettre la commande **rcv-queue threshold <Queue Id> <Threshold 1> <Threshold 2> <Threshold 3> <Threshold 14>** afin de configurer les niveaux de seuil. De cette manière, les données de valeurs CoS supérieures ne sont pas supprimées avant les données de valeurs CoS inférieures pendant l'encombrement.

```
Switch(config)#interface range fa 3/37 - 48
Switch(config-if-range)#rcv-queue threshold 1 50 60 80 100
```

5. Mapping : si le port est configuré pour faire confiance à la CoS, utilisez la table de mappage CoS-DSCP afin de mapper la valeur CoS reçue en une valeur DSCP interne.

```
Switch#show mls qos maps cos-dscp
Cos-dscp map:
  cos:   0  1  2  3  4  5  6  7
-----
  dscp:  0  8 16 24 32 40 48 56
```

Si le port est configuré pour approuver la priorité IP d'approbation, utilisez la table de mappage ip-cipdscp afin de mapper la valeur de priorité IP reçue en une valeur DSCP interne.

```
Switch#show mls qos maps ip-prec-dscp
IpPrecedence-dscp map:
  ipprec: 0  1  2  3  4  5  6  7
-----
  dscp:   0  8 16 24 32 40 48 56
```

Si le port est configuré pour faire confiance au DSCP, la valeur DSCP reçue est utilisée comme valeur DSCP interne. Ces tables doivent être identiques sur tous les commutateurs de votre réseau. Si l'un des commutateurs possède une table avec des mappages différents, vous ne recevez pas le résultat souhaité. Vous pouvez modifier ces valeurs de table comme indiqué ici :

```
Switch(config)#mls qos map cos-dscp 0 8 16 24 40 48 48 56
Switch(config)#mls qos map ip-prec-dscp 0 8 16 24 40 48 48 56
```

6. Réglementation - Deux types de réglementation sont disponibles dans les commutateurs Catalyst 6500 : **Aggregate Policy** - Aggregate Policy contrôle la bande passante d'un flux dans le commutateur. La commande **show mls qos aggregate-policer** affiche tous les agrégateurs configurés sur le commutateur. Voici les statistiques de la police :

```
Switch#show mls qos ip fastEthernet 3/13
[In] Policy map is pqos2   [Out] Default.
QoS Summary [IPv4]:      (* - shared aggregates, Mod - switch module)

  Int Mod Dir  Class-map DSCP  Agg  Trust Fl  AgForward-By  AgPoliced-By
                Id      Id      Id      Id
-----
  Fa3/13  5  In      qos1     0    1*  dscp  0           10626         118860
  Fa3/13  5  In  class-defa  40    2    No   0           3338          0
```

```
Switch#show mls qos
QoS is enabled globally
QoS ip packet dscp rewrite enabled globally
Input mode for GRE Tunnel is Pipe mode
Input mode for MPLS is Pipe mode
Vlan or Portchannel(Multi-Earl) policies supported: Yes
Egress policies supported: Yes
```

----- Module [5] -----

QoS global counters:

Total packets: 163

IP shortcut packets: 0

Packets dropped by policing: 120

IP packets with TOS changed by policing: 24

IP packets with COS changed by policing: 20

Non-IP packets with COS changed by policing: 3

MPLS packets with EXP changed by policing: 0

Contrôle de microflux - Contrôle de microflux contrôlant la bande passante d'un flux par interface dans le commutateur. Par défaut, les régulateurs de microflux affectent uniquement le trafic routé. Émettez la commande `mls qos bridged` dans l'interface VLAN afin d'activer le contrôle de microflux pour le trafic ponté. Il s'agit de la vérification des statistiques de contrôle des microflux :

Switch#**show mls ip detail**

Displaying Netflow entries in Supervisor Earl

DstIP SrcIP Prot:SrcPort:DstPort Src i/f :AdjPtr

Pkts Bytes Age LastSeen Attributes

Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST

Ig/acli Ig/acli Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags

QoS	Police	Count	Threshold	Leak	Drop	Bucket	Use-Tbl	Use-Enable
10.175.50.2	10.175.51.2	icmp:8	:0	--		:0x0		
43	64500	84	21:37:16	L3 - Dynamic				
1	1 0 0	1 0 0	1 1 0	0 0 0	0 0 0	0		
0	0	0	0	0	0	0		
0x0	0	0	0	0	NO	1518	NO	NO
10.175.50.2	10.175.51.2	icmp:0	:0	--		:0x0		
43	64500	84	21:37:16	L3 - Dynamic				
1	1 0 0	1 0 0	1 1 0	0 0 0	0 0 0	0		
0	0	0	0	0	0	0		
0x0	664832	0	0	0	NO	1491	NO	NO
0.0.0.0	0.0.0.0	0	:0	:0	--	:0x0		
1980	155689	1092	21:37:16	L3 - Dynamic				
0	1 0 0	1 0 0	1 1 0	0 0 0	0 0 0	0		
0	0	0	0	0	0	0		
0x0	0	0	0	0	NO	0	NO	NO

Switch#**show mls qos**

QoS is enabled globally

QoS ip packet dscp rewrite enabled globally

Input mode for GRE Tunnel is Pipe mode

Input mode for MPLS is Pipe mode

Vlan or Portchannel(Multi-Earl) policies supported: Yes

Egress policies supported: Yes

----- Module [5] -----

QoS global counters:

Total packets: 551

IP shortcut packets: 0

Packets dropped by policing: 473

IP packets with TOS changed by policing: 70

IP packets with COS changed by policing: 44

Non-IP packets with COS changed by policing: 11

MPLS packets with EXP changed by policing: 0

Remarque : La commande `show mls qos ip type mod/number` n'affiche pas les statistiques de régulation de microflux. Il ne montre que les statistiques agrégées de la police. Si vous ne voyez pas les statistiques de réglementation souhaitées, vérifiez la configuration de la réglementation. Reportez-vous à [Contrôle QoS sur les commutateurs de la gamme Catalyst 6500/6000](#) pour voir l'exemple de configuration. Consultez également la section [Directives et limitations de QoS sur les commutateurs Catalyst 6500](#) de ce document.

7. Vérifiez les [notes de version](#) de votre système d'exploitation et assurez-vous qu'il n'y a aucun bogue lié à votre configuration QoS.
8. Notez le modèle de superviseur de commutateur, le modèle PFC, le modèle MSFC et la version Cisco IOS/CatOS. Reportez-vous aux [directives et limitations de QoS sur les commutateurs Catalyst 6500](#) en fonction de vos spécifications. Assurez-vous que votre configuration est applicable.

[Directives et limites de qualité de service sur les commutateurs Catalyst 6500](#)

Il existe des limitations de QoS dont vous devez tenir compte avant de configurer la QoS sur les commutateurs Catalyst 6500 :

- [Lignes directrices générales](#)
- [Directives PFC3](#)
- [Directives PFC2](#)
- [Restrictions de commande de carte de classe](#)
- [Restrictions de commande de carte de stratégie](#)
- [Restrictions des commandes de la classe de carte de stratégie](#)
- [Directives et restrictions relatives au mappage des seuils de file d'attente et de perte](#)
- [confiance cos dans les limites d'entrée de liste de contrôle d'accès](#)
- [Limitations des cartes de ligne WS-X6248-xx, WS-X6224-xx et WS-X6348-xx](#)
- PFC ou PFC2 ne fournissent pas de QoS pour le trafic WAN. Avec PFC ou PFC2, la QoS PFC ne modifie pas l'octet ToS dans le trafic WAN.
- Le trafic LAN entrant commuté de couche 3 ne passe pas par la MSFC ou la MSFC2 et conserve la valeur CoS attribuée par le moteur de commutation de couche 3.
- La QoS n'implémente pas la prévention de congestion des ports d'entrée sur les ports configurés avec les mots clés **non approuvés**, **trust-ipprec** ou **trust-dscp**. Le trafic va directement au moteur de commutation.
- Le commutateur utilise le seuil de perte arrière pour le trafic qui transporte les valeurs CoS qui sont mappées uniquement à la file d'attente. Le commutateur utilise les seuils WRED-drop pour le trafic qui porte les valeurs CoS mappées à la file d'attente et un seuil.
- La classification avec un moteur de commutation de couche 3 utilise les valeurs des couches 2, 3 et 4. Le marquage avec un moteur de commutation de couche 3 utilise les valeurs CoS de couche 2 et les valeurs DSCP ou de priorité IP de couche 3.
- Une liste de contrôle d'accès trust-cos ne peut pas restaurer la CoS reçue dans le trafic provenant des ports non approuvés. Le trafic en provenance des ports non approuvés a toujours la valeur CoS du port.

Remarque : la QoS PFC ne détecte pas l'utilisation de commandes non prises en charge tant que vous n'avez pas joint une carte de stratégie à une interface.

[Limitation QoS TCAM](#)

Le TCAM (Ternary CAM) est une mémoire spécialisée conçue pour les recherches rapides dans les tables, basée sur les paquets passant par le commutateur, exécutés par le moteur ACL sur PFC, PFC2 et PFC3. Les listes de contrôle d'accès sont traitées dans le matériel des commutateurs de la gamme Cisco Catalyst 6500 appelés TCAM. Lorsque vous configurez une liste de contrôle d'accès, associez-la à la QoS et lorsque vous appliquez la stratégie QoS sur l'interface, le commutateur programme la TCAM. Si vous avez déjà utilisé tout l'espace TCAM disponible sur le commutateur pour la QoS, vous rencontrez ce message d'erreur :

```
Switch(config)#interface vlan 52
Switch(config-if)#service-policy input test
Switch(config-if)#
3w0d: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

Cette sortie de commande **show tcam count** indique que les masques d'entrée TCAM sont utilisés à 95 %. C'est pourquoi, lorsque vous appliquez la stratégie QoS sur l'interface, vous rencontrez la %QM-4-TCAM_ENTRY :

```
Switch#show tcam count
          Used          Free          Percent Used          Reserved
          ----          -
Labels:(in) 43          4053          1
Labels:(eg) 2           4094          0

ACL_TCAM
-----
Masks:      19          4077          0          72
Entries:     95          32673         0          576

QOS_TCAM
-----
Masks:      3902          194          95          18
Entries:     23101         9667          70          144

LOU:        0           128           0
ANDOR:      0           16            0
ORAND:      0           16            0
ADJ:        3           2045          0
```

Les entrées TCAM et les étiquettes ACL sont des ressources limitées. Par conséquent, en fonction de votre configuration de liste de contrôle d'accès, vous devrez peut-être prendre soin de ne pas épuiser les ressources disponibles. En outre, avec des configurations de listes de contrôle d'accès QoS et de listes de contrôle d'accès VLAN (VACL) de grande taille, vous devrez peut-être également tenir compte de l'espace NVRAM (Non-Volatile Random Access Memory). Les ressources matérielles disponibles diffèrent sur Supervisor 1a avec PFC, Supervisor 2 avec PFC2 et Supervisor 720 avec PFC3.

Module de supervision	TCAM QoS	Étiquettes ACL
Supervisor 1a et PFC	2000 masques et modèles 1600 partagés entre les listes de contrôle d'accès (RACL), les VACL et les ACL QoS des routeurs	Étiquettes de liste de contrôle d'accès 512 partagées entre les listes de contrôle d'accès RACL,

		VACL et QoS
Super visor 2 et PFC2	Masques 4000 et modèles 32000 pour ACL QoS	Étiquettes de liste de contrôle d'accès 512 partagées entre les listes de contrôle d'accès RACL, VACL et QoS
Super visor 720 et PFC3	Masques 4000 et modèles 32000 pour ACL QoS	Étiquettes de liste de contrôle d'accès 512 partagées entre les listes de contrôle d'accès RACL, VACL et QoS

Remarque : Indépendamment de la limite d'étiquette de la liste de contrôle d'accès 512, Cisco CatOS comporte une limite logicielle supplémentaire de 250 listes de contrôle d'accès QoS à l'échelle du système lorsque vous utilisez le mode de configuration (binaire) par défaut. Cette restriction est supprimée en mode de configuration de texte. Tapez la **commande set config mode text afin de faire passer le mode de configuration au mode texte**. Le mode texte utilise généralement moins de mémoire NVRAM ou Flash que le mode de configuration binaire. Vous devez émettre la commande **write memory** pendant que vous opérez en mode texte afin d'enregistrer la configuration dans la mémoire NVRAM. Émettez la commande **set config mode text auto-save** afin d'enregistrer automatiquement la configuration de texte dans la mémoire NVRAM.

Voici la solution de contournement pour le problème TCAM :

- Si vous avez mis en oeuvre la commande **service-policy** sur de nombreuses interfaces de couche 2 qui appartiennent à un VLAN, vous pouvez mettre en oeuvre une réglementation basée sur VLAN au lieu d'une réglementation basée sur le port de commutateur. Voici un exemple :

```
Switch(config)#interface range fastethernet x/y - z
Switch(config-if)#mls qos vlan-based
Switch(config-if)#exit
Switch(config)#interface vlan 100
Switch(config-if)#service-policy input Test_Policy
```
- Désactivez les statistiques de marquage QoS. La commande **no mls qos marking statistics** ne permet pas d'implémenter le maximum de 1020 AgID. Ceci est dû au fait qu'il alloue le régulateur par défaut pour les régulateurs dscp set. L'inconvénient est qu'il n'y a pas de statistiques pour le régulateur spécifique parce qu'ils partagent tous le régulateur par défaut.

```
Switch(config)#no mls qos marking statistics
```
- Si possible, utilisez les mêmes listes de contrôle d'accès sur plusieurs interfaces afin de réduire les conflits de ressources TCAM.

Limitation NBAR

NBAR (Network-Based Application Recognition) est un moteur de classification qui reconnaît une grande variété d'applications, qui inclut des protocoles basés sur le Web et d'autres protocoles difficiles à classer qui utilisent des affectations de ports TCP/UDP dynamiques. Lorsqu'une

application est reconnue et classée par NBAR, un réseau peut appeler des services pour cette application spécifique. NBAR classe les paquets, puis applique la QoS au trafic classifié afin de garantir une utilisation efficace de la bande passante du réseau. Il existe certaines restrictions dans la mise en oeuvre de la QoS lorsque vous utilisez NBAR :

- PFC3 ne prend pas en charge NBAR.
- Avec Supervisor Engine 2, PFC2 et MSFC2 :Vous pouvez configurer NBAR sur les interfaces de couche 3 au lieu de la QoS PFC.PFC2 fournit la prise en charge matérielle des listes de contrôle d'accès d'entrée sur les ports où vous configurez NBAR.Lorsque la QoS PFC est activée, le trafic via les ports où vous configurez NBAR passe par les files d'attente d'entrée et de sortie et les seuils de perte.Lorsque la QoS PFC est activée, le MSFC2 définit la CoS de sortie comme priorité IP de sortie dans le trafic NBAR.Une fois que tout le trafic passe par une file d'attente d'entrée, il est traité dans le logiciel sur la MSFC2 sur les interfaces où vous configurez NBAR.

Commandes cos-map manquantes dans Supervisor 2

Sous Native IOS Software Versions 12.1(8a)EX-12.1(8b)EX5 et 12.1(11b)E et ultérieures, les mappages CoS QoS par défaut pour les liaisons ascendantes Gigabit situées sur Supervisor2 ont changé. Toutes les valeurs CoS ont été affectées à la file d'attente 1 et au seuil 1 et ne peuvent pas être modifiées.

Ces commandes ne peuvent pas être configurées sur un port de liaison ascendante Gigabit Sup2 sur ces versions :

```
rcv-queue cos-map
priority-queue
wrr-queue cos-map
```

Les configurations QoS sont limitées et la file d'attente de priorité stricte ne peut pas être utilisée. Cela affecte uniquement les ports Gigabit physiquement situés sur le Supervisor 2 Engine. Les ports Gigabit des autres modules de cartes de ligne ne sont pas affectés.

Une mise à niveau du micrologiciel permet de résoudre ce problème. Cette mise à niveau peut être effectuée via un logiciel. Contactez le support technique si une mise à niveau du micrologiciel est nécessaire. Notez qu'une mise à niveau du micrologiciel n'est nécessaire que si la version matérielle de Supervisor2 est inférieure à 4.0. Si la version matérielle de Supervisor2 est 4.0 ou ultérieure, la QoS doit être autorisée sur les ports de liaison ascendante Gigabit sans mise à niveau du micrologiciel. Vous pouvez émettre la commande **show module** afin de trouver le niveau du micrologiciel. Ce problème est identifié dans l'ID de bogue Cisco [CSCdw89764](#) (clients [enregistrés](#) uniquement).

Limitations de la stratégie de service

Afin d'appliquer policy-map à l'interface, émettez la commande **service-policy**. Si vous avez une commande non prise en charge dans policy-map, après l'avoir appliquée à la commande **service-policy**, le commutateur invite les messages d'erreur sur la console. Ces points doivent être pris en compte lors du dépannage des problèmes liés aux **politiques de services**.

- N'associez pas une stratégie de service à un port membre d'un EtherChannel.
- Avec les cartes DFC (Distributed Forwarding Card) installées, PFC2 ne prend pas en charge la QoS basée sur VLAN. Vous ne pouvez pas émettre la commande **mls qos vlan-based** ou attacher des stratégies de service aux interfaces VLAN.
- La QoS PFC prend en charge le mot clé de sortie uniquement avec PFC3 et uniquement sur les interfaces de couche 3 (soit les ports LAN configurés en tant qu'interfaces de couche 3, soit les interfaces VLAN). Avec PFC3, vous pouvez associer une carte de stratégie d'entrée et de sortie à une interface de couche 3.
- La QoS PFC basée sur VLAN ou sur port sur les ports de couche 2 n'est pas pertinente pour les politiques associées aux interfaces de couche 3 avec le mot clé de sortie.
- Les stratégies associées au mot clé de sortie ne prennent pas en charge le contrôle de microflux.
- Vous ne pouvez pas joindre une carte de stratégie qui configure un état d'approbation avec la sortie de commande **service-policy**.
- La QoS PFC ne prend pas en charge le balisage d'entrée avec la perte de sortie ou la perte d'entrée avec le balisage de sortie.

Les instructions de sortie de la stratégie de service ne s'affichent pas dans la sortie de la commande **running-config**

Lorsque vous configurez la QoS sur la liaison multiple sur le module FlexWan, vous ne pouvez pas voir la sortie de la commande **service-policy** dans la sortie de la commande **show running-config**. Cela se produit lorsque le commutateur exécute des versions de Cisco IOS antérieures à 12.2SX. Le FlexWAN pour la gamme Cisco 7600 prend en charge la dLLQ sur les interfaces non groupées. Il ne prend pas en charge dLLQ sur les interfaces de bundle MLPPP. Cette assistance est disponible avec le logiciel Cisco IOS Version 12.2S.

La solution de contournement de cette limitation consiste à associer la stratégie de service aux interfaces dégroupées ou à mettre à niveau la version de Cisco IOS vers 12.2SX ou une version ultérieure, où la fonctionnalité est prise en charge.

Limitation de la réglementation

La réglementation est effectuée dans le matériel sur PFC sans impact sur les performances du commutateur. La réglementation ne peut pas avoir lieu sur la plate-forme 6500 sans PFC. Dans le système d'exploitation hybride, la réglementation doit être configurée sur le CatOS. Ces points doivent être pris en compte lors du dépannage des problèmes de réglementation :

- Lorsque vous appliquez à la fois le contrôle d'entrée et le contrôle de sortie au même trafic, la stratégie d'entrée et la stratégie de sortie doivent marquer le trafic descendant ou abandonner le trafic. La QoS PFC ne prend pas en charge le balisage d'entrée avec la perte de sortie ou la perte d'entrée avec le balisage de sortie.
- Lorsque vous créez un régulateur qui n'utilise pas le mot clé **pir** et que le paramètre **maximum_burst_bytes** est égal au paramètre **normal_burst_bytes** (ce qui est le cas si vous n'entrez pas le paramètre **maximum_burst_bytes**), les mots clés de **transmission-dscp-policed-action** font que la QoS PFC marque le trafic comme défini par le mappage de marquage **max-burst**.
- Lorsque l'action de dépassement est abandonnée, la QoS PFC ignore toute action de violation configurée.

- Lorsque vous configurez Drop comme action de conformité, la QoS PFC configure Drop comme action de dépassement et action de violation.
- Les exigences de masque de flux de la réglementation de microflux, de NetFlow et de NetFlow Data Export (NDE) peuvent être en conflit.

[Problèmes de limite de débit ou de réglementation avec MSFC dans le système d'exploitation hybride](#)

Sur les commutateurs Catalyst 6500 qui exécutent un système d'exploitation hybride, la configuration de la limite de débit ne donne pas le résultat souhaité. Par exemple, si vous configurez la commande **rate-limit** sous la commande **interface vlan** sur le MSFC, elle ne limite pas réellement le trafic.

```
interface Vlan10
  rate-limit input 256000 2000 2000 conform-action transmit exceed-action drop
  rate-limit output 256000 2000 2000 conform-action transmit exceed-action drop
```

OU:

```
interface Vlan10
  service-policy input Test_Policy
```

La raison derrière cela est que la MSFC s'occupe uniquement des fonctions de contrôle, mais le transfert de trafic réel se produit sur les ASIC PFC sur le superviseur. La carte MSFC compile les tables FIB et de contiguïté, ainsi que d'autres informations de contrôle, et la télécharge vers la carte PFC pour l'implémenter dans le matériel. Avec la configuration que vous avez créée, vous limitez uniquement le trafic commuté du logiciel, qui doit être minimal (ou nul).

La solution de contournement consiste à utiliser l'interface de ligne de commande (CLI) de CatOS afin de configurer la limite de débit sur le superviseur. Référez-vous à [QoS CatOS](#) pour une explication détaillée de la façon de configurer la réglementation QoS dans CatOS. Vous pouvez également vous reporter à [QoS Policing on Catalyst 6500/6000 Series Switches](#) pour voir l'exemple de configuration.

[Moyenne de forme de commande non prise en charge dans les interfaces VLAN de Cisco 7600](#)

Lorsque vous appliquez une entrée de stratégie de service à une interface sur Cisco 7600, ce message d'erreur apparaît :

```
7600_1(config)#int Gi 1/40
7600_1(config-if)#service-policy input POLICY_1
shape average command is not supported for this interface
```

La commande **shape Average** n'est pas prise en charge pour les interfaces VLAN dans Cisco 7600. Au lieu de cela, vous devez utiliser la police.

```
7600_1(config)#policy-map POLICY_1
7600_1(config-pmap)#class TRAFFIC_1
7600_1(config-pmap-c)#police conform-action transmit exceed-action drop
```

Référez-vous à [Configuration de la police de classe de carte de stratégie](#) pour plus d'informations

sur la façon de mettre en oeuvre la police pour le trafic de limite de débit.

Lorsque vous associez cette stratégie de service à une interface VLAN (SVI), vous devez activer la QoS basée sur VLAN sur tous les ports de couche 2 qui appartiennent à ce VLAN dans lequel vous voulez appliquer cette carte de stratégie.

```
7600_1(config)#interface Gi 1/40
7600_1(config-if)#mls qos vlan-based
```

Référez-vous à [Activation de la QoS PFC basée sur VLAN sur les ports LAN de couche 2](#) pour plus d'informations.

[ERREUR QoS : L'ajout/la modification apporté à la policymap \[chars\] et à la classe \[chars\] n'est pas valide, la commande est rejetée](#)

```
QoS-ERROR: Addition/Modification made to policymap vtc-map and class voice-video is
not valid, command is rejected
```

Ce message d'erreur indique que les actions définies dans la classe mentionnée ne sont pas autorisées dans les commutateurs de la gamme Cisco Catalyst 6500. Il existe certaines restrictions lors de la configuration des actions de classe de mappage de stratégie.

- Vous ne pouvez pas effectuer ces trois opérations dans une classe de mappage de stratégie : Marquer le trafic avec les commandes **set** Configurer l'état d'approbation Configurer la réglementation Vous ne pouvez marquer le trafic qu'avec les commandes **set**. OU Configurez l'état d'approbation et/ou configurez la réglementation.
- Pour le trafic à commutation matérielle, la QoS PFC ne prend pas en charge les commandes de classe de mappage de stratégie **bande passante**, **priorité**, **file-limit** ou **détection aléatoire**. Vous pouvez configurer ces commandes car elles peuvent être utilisées pour le trafic commuté par logiciel.
- PFC QoS ne prend pas en charge les commandes **set qos-group policy map class**.

Référez-vous à [Configuration des actions de classe de carte de stratégie](#) pour plus d'informations sur ces restrictions.

Informations connexes

- [Classification et signalisation QoS sur les commutateurs des gammes Catalyst 6500/6000 qui exécutent le logiciel Cisco IOS](#)
- [Planification de la sortie QoS sur les commutateurs des gammes Catalyst 6500/6000 exécutant le logiciel système Cisco IOS](#)
- [Réglementation QoS \(Qualité de service\) sur les commutateurs de la gamme Catalyst 6500/6000](#)
- [Classification et signalisation QoS sur les commutateurs des gammes Catalyst 6500/6000 exécutant le logiciel CatOS](#)
- [Planification de la sortie QoS sur les commutateurs des gammes Catalyst 6500/6000 exécutant le logiciel système CatOS](#)
- [Pages de support pour les produits LAN](#)
- [Page de support sur la commutation LAN](#)
- [Support et documentation techniques - Cisco Systems](#)