

Réglementation QoS (Qualité de service) sur les commutateurs de la gamme Catalyst 6500/6000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Paramètres de réglementation QoS](#)

[Calculer les paramètres](#)

[Actions de réglementation](#)

[Fonctionnalités de réglementation prises en charge par Catalyst 6500/6000](#)

[Fonctionnalités de réglementation mises à jour pour Supervisor Engine 720](#)

[Configurer et contrôler la réglementation dans le logiciel CatOS](#)

[Configurer et contrôler la réglementation dans le logiciel Cisco IOS](#)

[Informations connexes](#)

[Introduction](#)

La réglementation QoS sur un réseau détermine si le trafic sur le réseau est dans un profil spécifié (contrat). Ceci peut conduire le trafic hors profil à être rejeté ou démarqué vers une autre valeur de point de code de services différenciés (DSCP) pour mettre en place un niveau de service contracté. (DSCP est une mesure du niveau de QoS de la trame.)

Ne confondez pas la réglementation du trafic avec le formatage du trafic. Chacun s'assure que le trafic reste dans le profil (contrat). Vous ne mettez pas en mémoire tampon des paquets hors profil quand vous réglemez le trafic. Par conséquent, vous n'affectez pas le retard de transmission. Vous supprimez le trafic ou l'identifiez avec un niveau QoS plus bas (démarcation de DSCP). En revanche, avec le formatage du trafic, vous mettez en mémoire tampon le trafic hors profil et facilitez les salves du trafic. Ceci affecte le retard et la variation du retard. Vous pouvez appliquer le formatage du trafic uniquement sur une interface de sortie. Vous pouvez appliquer la réglementation sur des interfaces d'entrée et de sortie.

Catalyst 6500/6000 Policy Feature Card (PFC) et PFC2 prennent en charge uniquement la réglementation d'entrée. Le PFC3 prend en charge la réglementation d'entrée et de sortie. Le formatage du trafic est seulement pris en charge sur certains modules WAN pour la gamme Catalyst 6500/7600, tels que les modules de services optiques (OSM) et les modules FlexWAN. Consultez les [Notes de configuration de module du routeur de la gamme Cisco 7600 pour plus d'informations](#)

[Conditions préalables](#)

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Paramètres de réglementation QoS

Pour configurer la réglementation, vous définissez les régulateurs et vous les appliquez aux ports (QoS basé sur port) ou aux VLAN (QoS basé sur VLAN). Chaque régulateur définit un nom, un type, un débit, une salve et des actions pour le trafic dans le profil et hors profil. Les régulateurs sur Supervisor Engine II prennent en charge également des paramètres de débit de dépassement. Il y a deux types de régulateurs : par microflux et par agrégation.

- **Microflux - réglemente le trafic pour chaque port/VLAN appliqué séparément par-flux.**
- **Agrégation - réglemente le trafic de routage à travers tous les ports/VLAN appliqués.**

Chaque régulateur peut être appliqué à plusieurs ports ou VLAN. Le flux est défini à l'aide de ces paramètres :

- adresse IP source
- adresse IP de destination
- Protocole de la couche 4 (tel que protocole de datagramme utilisateur [UDP])
- numéro du port source
- numéro du port de destination

Vous pouvez dire que les paquets qui correspondent à un ensemble particulier de paramètres défini appartiennent au même flux. (C'est essentiellement le même concept de flux que celui que la commutation Netflow utilise.)

Par exemple, si vous configurez un régulateur de microflux pour limiter le trafic TFTP à 1 Mbits/s sur VLAN 1 et VLAN 3, alors 1 Mbits/s est autorisé pour chaque flux dans VLAN 1 et 1 Mbits/s pour chaque flux dans VLAN 3. En d'autres termes, s'il y a trois flux dans VLAN 1 et quatre flux dans VLAN 3, le régulateur de microflux autorise chacun de ces flux à 1 Mbits/s. Si vous configurez un régulateur d'agrégation, il limite le trafic TFTP pour tous les flux combinés sur le VLAN 1 et le VLAN 3 à 1 Mbit/s.

Si vous appliquez à la fois le régulateur d'agrégation et de microflux, QoS prend toujours la mesure la plus stricte spécifiée par les régulateurs. Par exemple, si un régulateur indique de jeter le paquet, mais que d'autres indiquent de marquer le paquet vers le bas, le paquet est jeté.

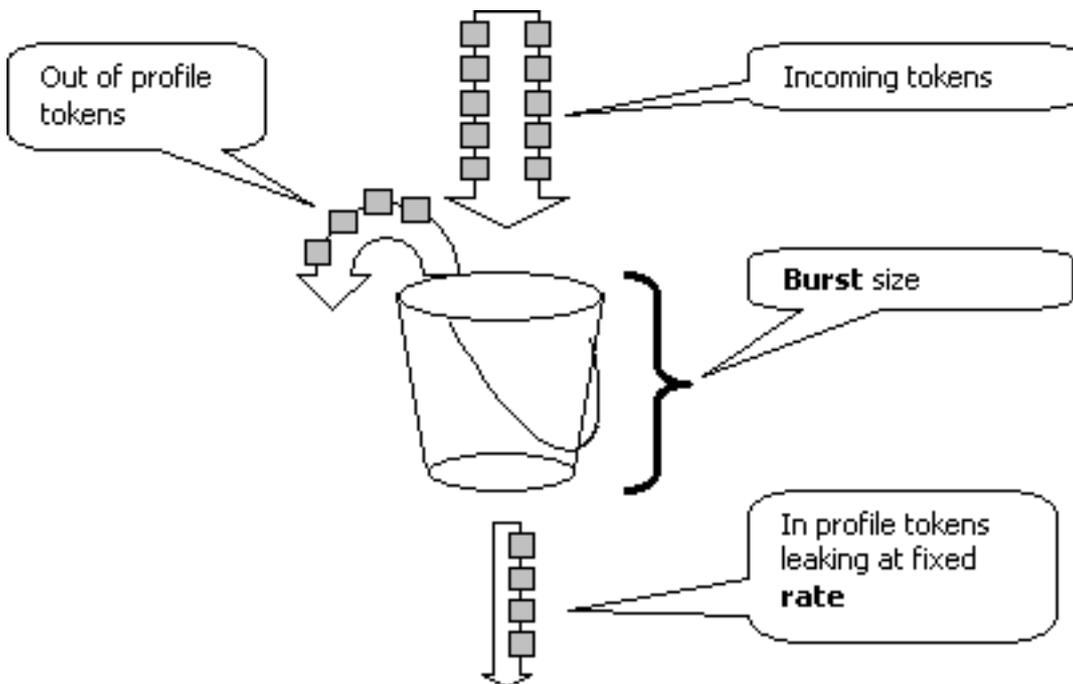
Par défaut, les régulateurs de microflux fonctionnent seulement avec un trafic routé (couche 3 [L3]). Pour réglementer également le trafic ponté (couche 2 [L2]), vous devez activer la réglementation de microflux ponté. Sur Supervisor Engine II, vous devez activer la réglementation

de microflux ponté, même pour la réglementation du microflux L3.

La réglementation est consciente du protocole. Tout le trafic est divisé en trois types :

- IP
- Internetwork Packet Exchange (IPX)
- Other (autre)

La réglementation est mise en place sur Catalyst 6500/6000 selon un concept de « leaky bucket ». Des tokens correspondant aux paquets du trafic entrant sont placés dans un compartiment. (Chaque token représente un bit, ainsi un grand paquet est représenté par plus de tokens qu'un petit paquet.) À intervalles réguliers, un nombre défini de tokens est supprimé du compartiment et envoyé. S'il n'y a aucune place dans le compartiment pour héberger des paquets entrant, les paquets sont considérés hors de profil. Ils sont jetés ou marqués vers le bas selon l'action de réglementation configurée.



Remarque : Le trafic n'est pas mis en mémoire tampon dans le compartiment, comme il peut apparaître dans l'image ci-dessus. Le trafic réel ne passe pas du tout par le compartiment ; le compartiment est seulement utilisé pour décider si le paquet est dans le profil ou hors profil.

Calculer les paramètres

Plusieurs paramètres contrôlent le fonctionnement du compartiment de token, comme montré ici :

- **Débit** - définit combien de tokens sont supprimés à chaque intervalle. Ceci définit effectivement le débit de réglementation. Tout le trafic au-dessous du débit est considéré comme dans le profil.
- **Intervalle** - définit à quelle fréquence les tokens sont supprimés du compartiment. L'intervalle est fixé à 0,00025 seconde, ainsi des tokens sont supprimés du compartiment 4 000 fois par seconde. L'intervalle ne peut pas être modifié.
- **Salve** - définit le nombre maximal de tokens que le compartiment peut contenir en même temps. Pour maintenir le débit du trafic indiqué, la salve ne doit pas être inférieure à la fréquence de l'intervalle. Une autre considération est que le paquet de la taille maximale doit

s'insérer dans le compartiment.

Pour déterminer le paramètre de rafale, utilisez cette équation :

- $\text{Salve} = (\text{débit [bps]} * 0,00025 [\text{sec/intervalle}]) \text{ ou } (\text{taille de paquet maximale [bits]}), \text{ selon ce qui est le plus grand.}$

Par exemple, si vous voulez calculer la valeur minimale de rafale requise pour maintenir un débit de 1 Mbit/s sur un réseau Ethernet, le débit est défini sur 1 Mbit/s et la taille de paquet Ethernet maximale est de 1 518 octets. L'équation est :

- $\text{Salve} = (1\ 000\ 000 \text{ bits/s} * 0,00025) \text{ ou } (1\ 518 \text{ octets} * 8 \text{ bits/octet}) = 250 \text{ ou } 12\ 144.$

Le résultat le plus grand est 12 144, qui vous arrondissez à 13 Kbits/s.

Remarque : dans le logiciel Cisco IOS®, le taux de réglementation est défini en bits par seconde (bits/s), par opposition aux kbits/s dans Catalyst OS (CatOS). Également dans le logiciel Cisco IOS, le débit en rafale est défini en octets, par opposition aux kilobits dans CatOS.

Remarque : en raison de la granularité de la réglementation matérielle, le taux exact et la rafale sont arrondis à la valeur prise en charge la plus proche. Assurez-vous que la valeur de rafale est inférieure à la taille de paquet maximale. Autrement, tous les paquets dont la taille est supérieure à la taille de rafale sont jetés.

Par exemple, si vous essayez de définir la rafale à 1 518 dans le logiciel Cisco IOS, elle est arrondie à 1 000. En conséquence, toutes les trames de plus de 1 000 octets sont jetés. La solution de routage est de configurer la salve à 2000.

Quand vous configurez le débit de rafale, prenez en considération que quelques protocoles (comme TCP) implémentent un mécanisme de contrôle de flux qui réagit à la perte de paquets. Par exemple, TCP réduit le fenêtrage par deux pour chaque paquet perdu. En conséquence, une fois réglementée à un certain débit, l'utilisation effective de la liaison est inférieure au débit configuré. Vous pouvez augmenter la rafale pour une meilleure utilisation. Un bon début pour un tel trafic est de doubler la taille de rafale. (Dans cet exemple, la taille des rafales est augmentée de 13 kbits/s à 26 kbits/s). Puis, surveillez les performances et effectuez d'autres réglages si nécessaire.

Pour la même raison, il n'est pas recommandé de tester le fonctionnement du régulateur en utilisant le trafic orienté connexion. Les performances illustrées sont généralement inférieures à celles que le régulateur permet.

[Actions de réglementation](#)

Comme mentionné dans l'[Introduction](#), le régulateur peut faire une de deux choses dans un paquet hors profil :

- abandonner le paquet (le paramètre `drop` dans la configuration)
- marquer le paquet avec un DSCP inférieur (le paramètre `policed-dscp` dans la configuration)

Pour marquer le paquet vers le bas, vous devez modifier le mappage DSCP réglementé. Le DSCP réglementé est défini par défaut pour re-marquer le paquet avec le même DSCP. (Aucun marquage vers le bas n'a lieu.)

Remarque : si les paquets « hors profil » sont marqués vers un DSCP mappé dans une file d'attente de sortie différente de celle du DSCP d'origine, certains paquets peuvent être envoyés

dans le désordre. Pour cette raison, si la commande des paquets est importante, il est recommandé de marquer vers le bas des paquets hors profil avec un DSCP qui est mappé à la même file d'attente de sortie que des paquets dans le profil.

Sur Supervisor Engine II, qui prend en charge le débit de dépassement, deux déclencheurs sont possibles :

- Quand le trafic dépasse le débit normal
- Quand le trafic de routage dépasse le débit de dépassement

Un exemple de l'application du débit de dépassement est de marquer vers le bas des paquets qui dépassent le débit normal et de jeter les paquets qui dépassent le débit de dépassement.

[Fonctionnalités de réglementation prises en charge par Catalyst 6500/6000](#)

Comme stipulé dans l'[Introduction](#), le PFC1 sur Supervisor Engine 1a et le PFC2 sur Supervisor Engine 2 prennent en charge seulement la réglementation d'entrée (interface d'entrée). Le PFC3 sur Supervisor Engine 720 prend en charge la réglementation d'entrée et de sortie (interface de sortie).

Catalyst 6500/6000 prend en charge jusqu'à 63 régulateurs de microflux et jusqu'à 1 023 régulateurs d'agrégation.

Supervisor Engine 1a prend en charge la réglementation d'entrée, en commençant par la version 5.3(1) de CatOS et le logiciel Cisco IOS version 12.0(7)XE.

Remarque : Une carte fille PFC ou PFC2 est requise pour la réglementation avec le Supervisor Engine 1a.

Supervisor Engine 2 prend en charge la réglementation d'entrée, en commençant par la version 6.1(1) de CatOS et le logiciel Cisco IOS version 12.1(5c)EX. Supervisor Engine II prend en charge le paramètre de réglementation de débit de dépassement.

Les configurations avec des cartes de transfert distribué (cartes DFC) prennent en charge seulement la réglementation basée sur port. En outre, le régulateur d'agrégation compte seulement le trafic en se basant sur le moteur de transfert, non sur le système. DFC et PFC sont tous deux des moteurs de transfert ; si un module (carte de ligne) n'a pas de DFC, il utilise un PFC comme moteur de transfert.

[Fonctionnalités de réglementation mises à jour pour Supervisor Engine 720](#)

Remarque : Si vous n'êtes pas familier avec la réglementation QoS de Catalyst 6500/6000, veuillez à lire les sections [Paramètres de réglementation](#) et [fonctionnalités de réglementation QoS prises en charge par Catalyst 6500/6000](#) de ce document.

Supervisor Engine 720 a introduit ces nouvelles fonctionnalités de réglementation QoS :

- **Réglementation de sortie.** Supervisor 720 prend en charge la réglementation d'entrée sur un

port ou une interface VLAN. Il prend en charge la réglementation de sortie sur un port ou une interface routée L3 (dans le cas du logiciel système Cisco IOS). Tous les ports dans le VLAN sont réglementés sur la sortie indépendamment du mode de QoS du port (que le QoS soit basé sur le port ou sur le VLAN). La réglementation microflux n'est pas prise en charge sur la sortie. Des exemples de configuration sont fournis dans les sections [Configurer et contrôler la réglementation dans le logiciel CatOS](#) et [Configurer et contrôler la réglementation dans le logiciel Cisco IOS de ce document](#).

- **Réglementation microflux par utilisateur.** Supervisor 720 prend en charge une amélioration de la réglementation microflux connue sous le nom de réglementation microflux par utilisateur. Cette fonctionnalité est seulement prise en charge avec le logiciel système Cisco IOS. Elle vous permet de fournir une certaine bande passante pour chaque utilisateur (par adresse IP) derrière des interfaces données. Ceci est réalisé en spécifiant un masque de flux à l'intérieur de la politique de service. Le masque de flux définit quelles informations sont utilisées pour différencier entre les flux. Par exemple, si vous spécifiez un masque de flux de source uniquement, tout le trafic d'une adresse IP est considéré comme un flux. Avec cette technique, vous pouvez réglementer le trafic par utilisateur sur certaines interfaces (où vous avez configuré la politique de service correspondante) ; sur d'autres interfaces, vous continuez à utiliser le masque de flux par défaut. Il est possible d'avoir jusqu'à deux masques de flux QoS différents actifs dans le système à un moment donné. Vous pouvez associer une seule classe à un masque de flux. Une réglementation peut avoir jusqu'à deux masques de flux différents.

Un autre changement important de la réglementation sur le Supervisor Engine 720 est qu'il peut compter le trafic par la longueur L2 de la trame. Ceci diffère du Supervisor Engine 2 et du Supervisor Engine 1, qui comptent des trames d'IP et d'IPX par leur longueur L3. Avec certaines applications, la longueur L2 et L3 peut ne pas être cohérente. Prenons pour exemple un petit paquet L3 à l'intérieur d'une grande trame L2. Dans ce cas, le Supervisor Engine 720 peut afficher un taux de trafic réglementé légèrement différemment par rapport au Supervisor Engine 1 et au Supervisor Engine 2.

[Configurer et contrôler la réglementation dans le logiciel CatOS](#)

La configuration de réglementation pour CatOS se compose de trois étapes importantes :

1. Définir un régulateur - le taux de trafic, le débit de dépassement (le cas échéant), la salve et l'action de réglementation normaux.
2. Créer un ACL de QoS pour sélectionner le trafic à réglementer et joindre un régulateur à cet ACL.
3. Appliquer l'ACL de QoS aux ports ou aux VLAN nécessaires.

Cet exemple montre comment réglementer tout le trafic vers le port UDP 111 sur le port 2/8.

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
```

```
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

L'exemple suivant est identique ; cependant, dans cet exemple, vous attachez le régulateur à un VLAN. Le port 2/8 appartient à VLAN 20.

Remarque : Vous devez changer la QoS du port en mode `vlan`. Pour cela, utilisez la commande `set port qos`.

Ce régulateur évalue le trafic de tous les ports dans ce VLAN configuré pour QoS basé sur VLAN :

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

Ensuite, au lieu de déposer des paquets hors profil avec le DSCP 32, marquez-les vers le bas avec un DSCP de 0 (le meilleur effort).

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

Cet exemple montre la configuration pour la réglementation de sortie pour le Supervisor Engine 720 seulement. Il montre comment réglementer tout le trafic IP sortant sur le VLAN 3 à l'agrégation de 10 Mbits/s.

Catalyst 6500/6000

```
set qos enable
```

```

!--- This enables QoS. set qos policer aggregate
egress_10mbps rate 10000 burst 20 drop !--- This defines
a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
trust-ipprec aggregate egress_10mbps ip any any !---
This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
This compiles the QoS ACL. set qos acl map egress_pol 3
output !--- This maps the QoS ACL to VLAN 3 in the
output direction.

```

Utilisez **show qos maps runtime policed-dscp-map** pour consulter le mappage DSCP réglementé actuel.

Utilisez **show qos policer runtime {policer_name | all}** pour vérifier les paramètres du régulateur. Vous pouvez également consulter l'ACL de QoS auquel le régulateur est attaché.

Remarque : avec Supervisor Engine 1 et 1a, il n'est pas possible d'avoir des statistiques de réglementation pour des contrôleurs agrégés individuels. Pour afficher les statistiques par système de réglementation, utilisez cette commande :

```

Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0

```

Pour vérifier les statistiques de réglementation microflux, utilisez cette commande :

```

Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
-----
IP bridged entries:
239.77.77.77 192.168.10.200UDP  63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628

```

Only out of the profile MLS entries are displayed
Cat6k> (enable)

Avec Supervisor Engine II, vous pouvez afficher des statistiques globales de réglementation sur une base par régulateur avec la commande **show qos statistics aggregate-policer**.

Pour cet exemple, un générateur du trafic est attaché au port 2/8. Il envoie 17 Mbits/s du trafic UDP avec le port de destination 111. Vous vous attendez à ce que le régulateur jette 16/17 du trafic, de sorte que 1 Mbit/s devrait passer :

```

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed

```

```

count          normal rate      excess rate
-----
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
count          normal rate      excess rate
-----
udp_1mbps58250497331989733198

```

Remarque : Notez que les paquets autorisés ont augmenté de 65 et que les paquets excédentaires ont augmenté de 1090. Ceci signifie que le régulateur a déposé 1 090 paquets et permis le passage de 65 paquets. Vous pouvez calculer que $65/(1\ 090 + 65) = 0,056$, ou approximativement 1/17. Par conséquent, le régulateur fonctionne correctement.

[Configurer et contrôler la réglementation dans le logiciel Cisco IOS](#)

La configuration de la réglementation dans le logiciel Cisco IOS implique ces étapes :

1. Définissez un régulateur.
2. Créez un ACL pour sélectionner le trafic à régler.
3. Définissez une class map pour sélectionner le trafic avec la priorité ACL et/ou DSCP/IP.
4. Définissez une politique de service qui utilise la classe, et appliquez le régulateur à une classe spécifiée.
5. Appliquez la politique de service à un port ou à un VLAN.

Considérez le même exemple que celui fourni dans la section [Configurer et contrôler la réglementation dans le logiciel CatOS](#), mais maintenant avec le logiciel Cisco IOS. Pour cet exemple, un générateur du trafic est attaché au port 2/8. Il envoie 17 Mbits/s du trafic UDP avec le port de destination 111 :

Catalyst 6500/6000

```

mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.

```

Il y a deux types de régulateurs d'agrégation dans le logiciel Cisco IOS : **nommé et par interface**. Le régulateur d'agrégation nommé régleme le trafic combiné de toutes les interfaces auxquelles il est appliqué. C'est le type de régulateur utilisé dans l'exemple ci-dessus. Le

régulateur par interface régleme le trafic de routage séparément sur chaque interface d'entrée à laquelle il est appliqué. Un régulateur par interface est défini dans la configuration de mappage de réglementation. Considérez cet exemple, qui présente un régulateur d'agrégation par interface :

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit udp any
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
interface.
```

Des régulateurs de microflux sont définis dans la configuration de mappage de réglementation, de même que les régulateurs d'agrégation par interface. Dans l'exemple ci-dessous, chaque flux de l'hôte 192.168.2.2 qui entre dans le VLAN 2 est réglementé à 100 Kbits/s. Tout le trafic de 192.168.2.2 est réglementé à 500 Kbits/s d'agrégation. Le VLAN 2 inclut les interfaces fa4/11 et fa4/12 :

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 1 permit 192.168.2.2
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
This applies the QoS policy to VLAN 2.
```

L'exemple ci-dessous montre une configuration pour la réglementation de sortie pour le Supervisor Engine 720. Il établit la réglementation de tout le trafic sortant sur des interfaces Gigabit Ethernet 8/6 à 100 Kbits/s :

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
```

```

cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
pol_out !--- This attaches the policy to an interface.

```

L'exemple ci-dessous montre une configuration pour la réglementation par utilisateur pour le Supervisor Engine 720. Le trafic qui provient d'utilisateurs derrière le port 1/1 et se dirige vers Internet est réglementé à 1 Mbit/s par utilisateur. Le trafic qui provient d'Internet et se dirige vers les utilisateurs est réglementé à 5 Mbits/s par utilisateur :

Catalyst 6500/6000

```

mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in

```

Pour contrôler la réglementation, vous pouvez utiliser ces commandes :

```

bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

```

```

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

```

```

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
-----

```

```

Gi2/8 1   In  udp_qos   0     1*   No0 127451 2129602

```

```

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.

```

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

```
Int Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
```

```
-----  
Gi2/8 1 In udp_qos 0 1* No0 127755 2134670
```

Remarque : les paquets autorisés ont augmenté de 304 et les paquets excédentaires de 5068. Ceci signifie que le régulateur a déposé 5 068 paquets et permis le passage de 304 paquets. Étant donné que le taux d'entrée est de 17 Mbits/s, le régulateur devrait passer 1/17 du trafic. Si vous comparez les paquets jetés et transférés, vous observez la situation suivante : $304 / (304 + 5068) = 0,057$, ou approximativement 1/17. Quelques différences mineures sont possibles en raison de la granularité de la réglementation de matériel.

Pour des statistiques de réglementation microflux, utilisez la commande **show mls ip detail** :

```
Orion# show mls ip detail
```

```
IP Destination IP Source Protocol L4 Ports Vlan Xtag L3-protocol  
-----+-----+-----+-----+-----+  
192.168.3.33192.168.2.2udp555 / 5550 lip  
192.168.3.3192.168.2.2udp63 / 630 lip
```

```
[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
```

```
-----+-----+-----+-----+-----+  
Fa4/11 - ----ARPA3 0030.7137.1000 0000.3333.3333314548  
Fa4/11 - ----ARPA3 0030.7137.1000 0000.2222.2222314824
```

```
Packets Age Last SeenQoS Police Count ThresholdLeak
```

```
-----+-----+-----+-----+-----+  
6838 36 18:50:090x80 34619762*2^5 3*2^0  
6844 36 18:50:090x80 34669562*2^5 3*2^0
```

```
Drop Bucket Use-Tbl Use-Enable
```

```
-----+-----+-----+  
YES 1968 NONO  
YES 1937 NONO
```

Remarque : Le champ `Police Count` indique le nombre de paquets contrôlés par flux.

[Informations connexes](#)

- [Configuration QoS](#)
- [Présentation de Qos \(Qualité de service\) sur les commutateurs de la gamme Catalyst 6000](#)
- [Support pour les produits LAN](#)
- [Prise en charge de la technologie de commutation LAN](#)
- [Support et documentation techniques - Cisco Systems](#)