

Comparaison entre la réglementation du trafic et le formatage du trafic pour limiter la bande passante

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Réglementation et formatage](#)

[Critères de sélection](#)

[Fréquence d'actualisation des jetons](#)

[Formation du trafic](#)

[Réglementation du trafic](#)

[Contrôles de bande passante minimum et maximum](#)

[Informations connexes](#)

[Introduction](#)

Ce document clarifie les différences fonctionnelles entre le formatage et la réglementation, qui limitent tous deux le débit en sortie. Bien que les deux mécanismes utilisent un saut à jetons comme mesure du trafic pour mesurer le débit de paquets, ils ont des différences fonctionnelles importantes. (Un saut à jetons est décrit dans [Qu'est-ce qu'un saut à jetons ?](#)).

[Avant de commencer](#)

[Conventions](#)

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

[Conditions préalables](#)

Aucune condition préalable spécifique n'est requise pour ce document.

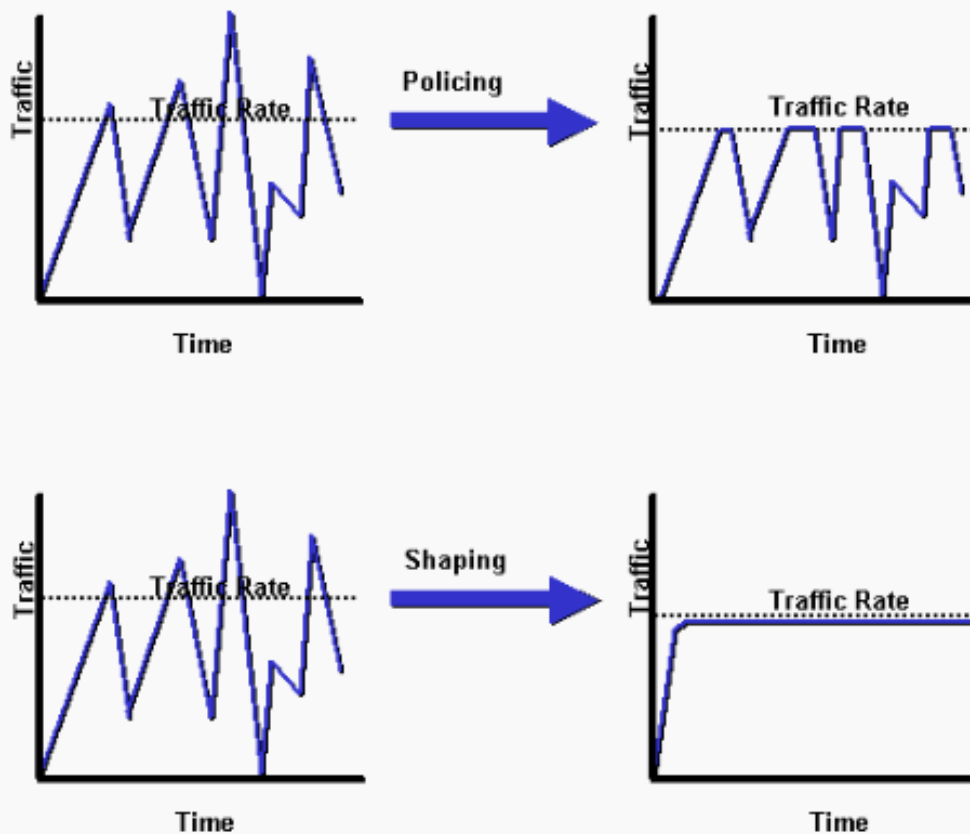
[Composants utilisés](#)

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Réglementation et formatage

Le diagramme suivant illustre la différence principale. La réglementation de trafic propage des rafales. Quand le débit de trafic atteint le débit maximal configuré, le trafic excessif est extrait (ou marqué une nouvelle fois). Le résultat est un débit en sortie qui apparaît en dents de scie avec des hauts et des bas. Contrairement à la réglementation, le formatage de trafic retient les paquets en excès dans une file d'attente, puis les programme pour une transmission postérieure sur des incréments de temps. Le résultat du formatage de trafic est un débit en sortie en douceur de paquets.



Le formatage implique l'existence d'une file d'attente et de la mémoire suffisante pour mettre en mémoire tampon des paquets différés, contrairement à la réglementation. La mise en file d'attente est un concept sortant ; les paquets sortant d'une interface sont mis en file d'attente, puis formatés. Seule la réglementation peut être appliquée au trafic entrant sur une interface. Assurez-vous que vous avez la mémoire suffisante en activant le formatage. En outre, le formatage exige une fonction de planification pour la transmission postérieure de tous les paquets différés. Cette fonction de planification vous permet d'organiser la file d'attente de formatage en différentes files d'attente. Des exemples des fonctions de planification sont la mise en file d'attente pondérée

basée sur les classes (CBWFQ) et Low Latency Queuing (LLQ).

Critères de sélection

Le tableau suivant présente les différences entre le formatage et la réglementation pour vous aider à choisir la meilleure solution.

	Formation	Maintien de l'ordre
Objectif	Mise en mémoire tampon et en file d'attente des paquets qui dépassent les débits validés.	Extraction (ou nouveau marquage) des paquets qui dépassent les débits validés. Pas de mise en mémoire tampon.*
Fréquence d'actualisation des jetons	Incrémentée au début d'un intervalle de temps. (Un nombre minimal d'intervalles est requis.)	Continue selon la formule : $1 / \text{committed information rate}$
Valeurs des jetons	Configurées en bits par seconde.	Configurées en octets.
Options de configuration	<ul style="list-style-type: none"> • Commande shape dans l'interface de ligne de commande QoS modulaire (MQC) pour mettre en application le formatage basé sur les classes. • Commande frame-relay traffic-shape pour mettre en application le formatage de trafic de relais de trame (FRTS). • Commande traffic-shape pour mettre en application Generic Traffic 	<ul style="list-style-type: none"> • Commande police dans MQC pour mettre en application la réglementation basée sur les classes. • Commande rate-limit pour mettre en application Committed Access Rate (CAR).

	Shaping (GTS).	
Applicable en entrée	Non	Oui
Applicable en sortie	Oui	Oui
Rafales	Contrôle les rafales en lissant le débit en sortie sur au moins huit intervalles de temps. Utilise un saut percé pour retarder le trafic, ce qui aboutit à un effet de lissage.	Propage les rafales. Pas de lissage.
Avantages	Moins de risques d'extraction des paquets excédentaires puisque ceux-ci sont mis en mémoire tampon. (Met les paquets en mémoire tampon sur toute la longueur de la file d'attente. Des extractions peuvent se produire si le trafic excédentaire est maintenu à des débits élevés.) Évite typiquement les retransmissions en raison des paquets extraits.	Contrôle le débit en sortie par des extractions de paquets. Évite des retards dus à la mise en file d'attente.
Inconvénients	Peut introduire des retards dus à la mise en file d'attente, en particulier les files d'attente profondes.	Extrait les paquets excédentaires (lorsque configurés), en limitant les tailles de fenêtres TCP et réduisant le débit en sortie global des flux de trafic affectés. Les tailles de rafales excessivement agressives peuvent aboutir à des extractions de paquets excédentaires et à limiter le débit en sortie

		global, en particulier avec des flux basés sur TCP.
Nouve au marqu age faculta tif des paquet s	Non	Oui (avec fonctionnalité CAR existante).

* Bien que la réglementation n'applique pas la mise en mémoire tampon, un mécanisme de mise en file d'attente configuré s'applique aux paquets « en conformité » qui peuvent devoir être placés en file d'attente tout en attendant d'être sérialisés au niveau de l'interface physique.

Fréquence d'actualisation des jetons

Une différence principale entre le formatage et la réglementation est le débit auquel les jetons sont réapprovisionnés. Cette section examine la différence.

En termes simples, le formatage et la réglementation utilisent tous deux la métaphore du saut à jetons. Un saut à jetons lui-même n'a aucune stratégie de rejet ni de priorité. Regardons comment la métaphore du saut à jetons fonctionne :

- Les jetons sont placés dans le saut à un certain débit.
- Chaque jeton est une autorisation pour la source d'envoyer un certain nombre de bits dans le réseau.
- Pour envoyer un paquet, le régulateur de trafic doit pouvoir retirer du saut un certain nombre de jetons égal dans la représentation à la taille de paquet.
- Si le nombre de jetons dans le saut est insuffisant pour envoyer un paquet, le paquet attend que le saut ait assez de jetons (dans le cas d'un modélisateur), ou le paquet est ignoré ou démarqué (dans le cas d'un régulateur).
- Le saut lui-même a une capacité spécifique. Si le saut est totalement rempli, les jetons nouvellement arrivés sont ignorés et ne sont pas disponibles pour de futurs paquets. Ainsi, à tout moment, la plus grande rafale qu'une source peut envoyer dans le réseau est approximativement proportionnelle à la taille du saut. Un saut à jetons permet les rafales, mais les lie.

Avec la métaphore du saut à jetons à l'esprit, regardons comment le formatage et la réglementation ajoutent des jetons au saut.

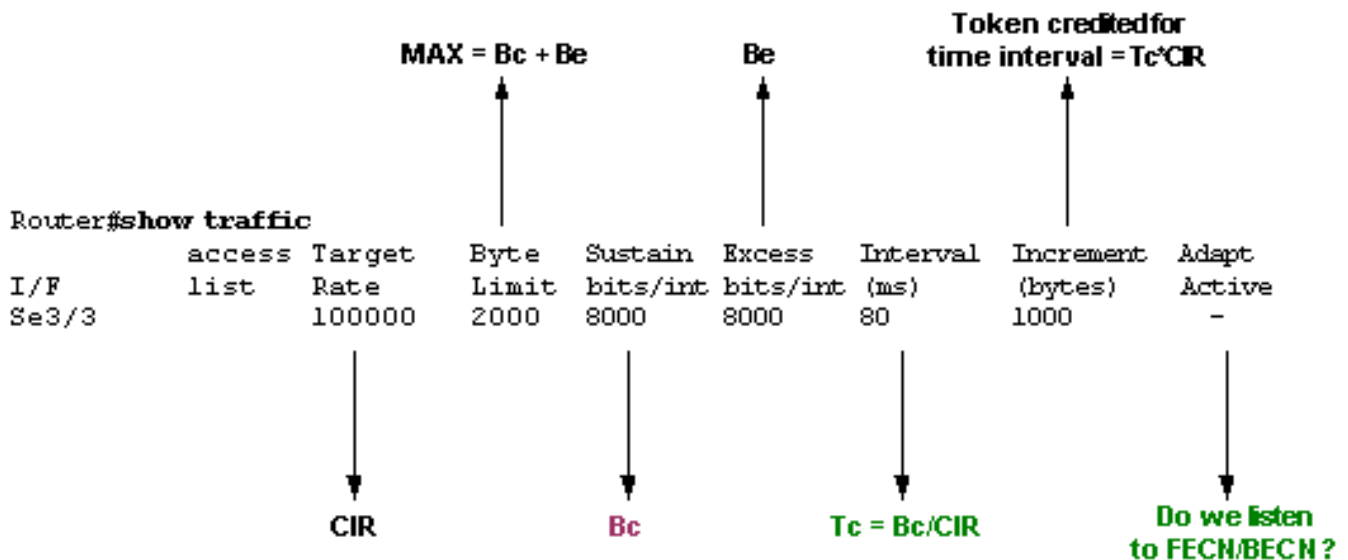
Le formatage incrémente le saut à jetons à intervalles chronométrés à l'aide d'une valeur bits par seconde (bits/s). Un modélisateur utilise la formule suivante :

$$T_c = B_c / CIR \text{ (in seconds)}$$

Dans cette équation, B_c représente la rafale validée et CIR représente le taux d'informations obligatoires. (Référez-vous à [Configuration du formatage de trafic de relais de trame](#) pour plus d'informations.) La valeur de T_c définit le délai pendant lequel vous envoyez les bits B_c afin de maintenir le débit moyen de CIR en secondes.

La plage de T_c se situe entre 10 ms et 125 ms. Avec le formatage de trafic distribué (DTS) sur la

gamme Cisco 7500, le Tc minimum est de 4 ms. Le routeur calcule en interne cette valeur selon les valeurs CIR et Bc. Si Bc/CIR est inférieur à 125 ms, il utilise le Tc calculé à partir de cette équation. Si Bc/CIR est plus qu'ou égal à 125 ms, il utilise une valeur interne comité technique si le Cisco IOS® détermine que la circulation sera plus stable avec un plus petit intervalle. Employez la commande **show traffic-shape** pour déterminer si votre routeur utilise une valeur interne pour Tc ou la valeur que vous avez configurée sur la ligne de commande. L'exemple de sortie suivant de la commande **show traffic-shape** est expliqué dans [Commandes show pour le formatage de trafic de relais de trame](#).



Quand la rafale en excès (Be) est configurée à une valeur différente de 0, le modélisateur permet de stocker des jetons dans le saut, jusqu'à Bc + Be. La plus grande valeur que le saut à jetons peut jamais atteindre est Bc + Be, et les jetons de dépassement sont extraits. La seule façon d'avoir plus de Bc jetons dans le saut est de ne pas utiliser tous les Bc jetons pendant un ou plusieurs Tc. Puisque le saut à jetons est réapprovisionné tous les Tc avec Bc jetons, vous pouvez accumuler les jetons inutilisés pour une utilisation ultérieure jusqu'à Bc + Be.

En revanche, la réglementation basée sur les classes et la limitation du débit ajoutent continuellement des jetons au saut. Spécifiquement, le débit d'arrivée des jetons est calculé comme suit :

$(\text{time between packets} < \text{which is equal to } t - t_1 > * \text{ policer rate}) / 8 \text{ bits per byte}$

En d'autres termes, si l'arrivée précédente du paquet était à t1 et l'heure actuelle est t, le saut est mis à jour avec la valeur t-t1 des octets selon le débit d'arrivée des jetons. Notez qu'un régulateur de trafic utilise des valeurs de rafale spécifiées en octets, et la formule ci-dessus convertit les bits en octets.

Examinons un exemple utilisant un CIR (ou débit de régulateur) de 8 000 bits/s et une rafale normale de 1 000 octets.

```
Router(config)# policy-map police-setting Router(config-pmap)# class access-match Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
```

Les sauts à jetons sont pleins à 1 000 octets. Si un paquet de 450 octets arrive, le paquet est conforme parce qu'assez d'octets sont disponibles dans le saut à jetons. La mesure conform (transmit) est prise par le paquet et 450 octets sont retirés du saut à jetons (en y laissant 550 octets). Si le paquet suivant arrive 25 secondes plus tard, 250 octets sont ajoutés dans le saut à jetons selon la formule suivante :

(0.25 * 8000) / 8

Le calcul laisse 700 octets dans le saut à jetons. Si le paquet suivant est de 800 octets, le paquet dépasse et la mesure exceed (drop) est prise. Aucun octet n'est pris du saut à jetons.

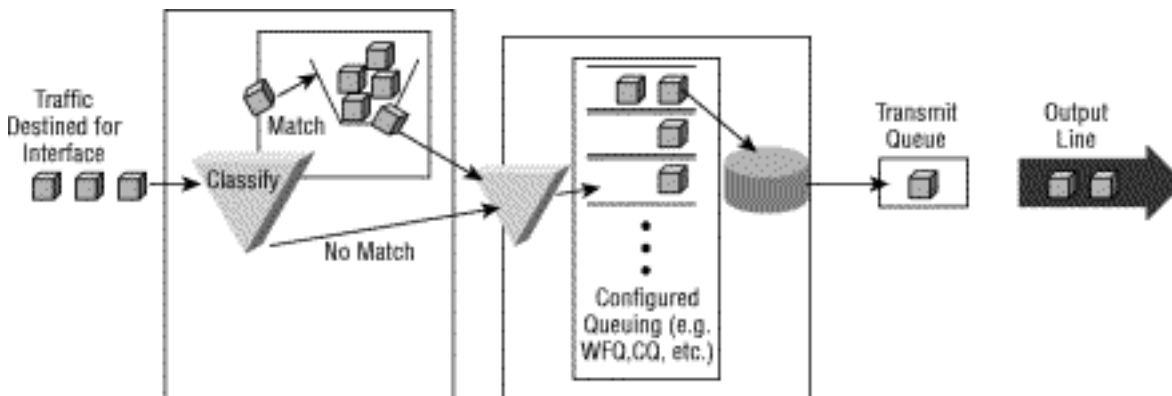
Formation du trafic

Cisco IOS prend en charge les méthodes suivantes de formatage de trafic :

- [Generic Traffic Shaping](#)
- [Formatage de trafic de relais de trame](#)
- [Formatage basé sur les classes](#) et [Formatage basé sur les classes distribuées](#)

Toutes les méthodes de formatage de trafic sont semblables dans la mise en place, bien que leur interface de ligne de commande (CLI) diffère un peu, et elles emploient différents types de files d'attente pour contenir et formater le trafic qui est reporté. Cisco recommande le formatage basé sur les classes et le formatage distribué, qui sont configurés à l'aide de la CLI QoS modulaire.

Le diagramme suivant illustre comment une stratégie QoS trie le trafic en classes et met en file d'attente les paquets qui dépassent les débits de formatage configurés.



Réglementation du trafic

Cisco IOS prend en charge les méthodes suivantes de réglementation de trafic :

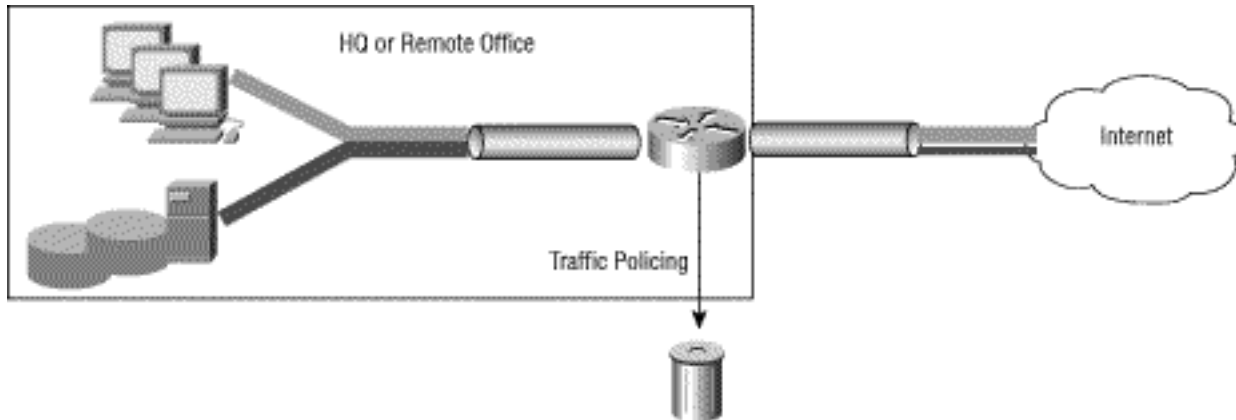
- [Committed Access Rate](#)
- [Réglementation basée sur les classes](#)

Les deux mécanismes ont des différences fonctionnelles importantes, comme expliqué dans [Comparaison entre la réglementation basée sur les classes et Committed Access Rate](#). Cisco recommande la réglementation basée sur les classes et d'autres fonctionnalités de la CLI QoS modulaire lors de l'application de stratégies QoS.

Utilisez la commande **police** pour spécifier qu'une classe de trafic devrait avoir un débit maximal imposé et, si ce débit est dépassé, une action immédiate devrait être prise. En d'autres termes, avec la commande **police**, ce n'est pas une option de mettre en mémoire tampon le paquet pour l'envoyer plus tard, comme c'est le cas pour la commande **shape**.

En outre, avec la réglementation, le saut à jetons détermine si un paquet dépasse le débit appliqué ou est conforme. Dans l'un ou l'autre cas, la réglementation met en application une action configurable, qui inclut la définition de la priorité IP ou de DSCP (Differentiated Services Code Point).

Le diagramme suivant illustre une application courante de réglementation de trafic à un point d'encombrement, où les fonctionnalités QoS s'appliquent généralement.



Contrôles de bande passante minimum et maximum

Les deux commandes **shape** et **police** limitent le débit en sortie à une valeur maximale en Kbits/s. Essentiellement, aucun mécanisme ne fournit une garantie de bande passante minimale au cours des périodes d'encombrement. Utilisez la commande **bandwidth** ou **priority** pour fournir de telles garanties.

Une politique hiérarchique emploie deux stratégies de service – une stratégie de parent pour appliquer un mécanisme de QoS à un agrégat du trafic et à une stratégie enfant pour appliquer un mécanisme de QoS à un écoulement ou à un sous-ensemble de l'agrégat. Les interfaces logiques, telles que des sous-interfaces et interfaces de tunnel, exigent une stratégie hiérarchique avec la fonction de limitation du trafic au niveau parent et une mise en file d'attente à des niveaux inférieurs. La fonction de limitation du trafic réduit le débit en sortie et (vraisemblablement) crée l'encombrement, comme illustré par la mise en file d'attente des paquets en excès.

La configuration suivante est suboptimale et est affichée pour illustrer la différence entre la **police** contre la commande de **forme** en limitant un agrégat du trafic – dans ce cas classe-par défaut – à un débit maximum. Dans cette configuration, la commande **police** envoie des paquets des classes enfants basés sur la taille du paquet et le nombre d'octets restants dans les sauts à jetons conform et exceed. (Référez-vous à [Réglementation du trafic](#).) Le résultat est que des débits indiqués aux classes Voix sur IP (VoIP) et IP (Internet Protocol) ne peuvent être garantis puisque la fonctionnalité **police** remplace les garanties faites par la fonctionnalité **priority**.

Cependant, si la commande **shape** est utilisée, le résultat est un système de mise en file d'attente hiérarchique, et toutes les garanties sont faites. En d'autres termes, quand la charge offerte dépasse le débit de format, les classes VoIP et IP ont leur débit garanti, et le trafic class-default (au niveau enfant) n'encourt aucune extraction.

Attention : Cette configuration n'est pas recommandée et est montrée pour illustrer la différence entre les commandes **police** et **shape** lors de la limitation d'un agrégat de trafic.

```
class-map match-all IP
  match ip precedence 3
class-map match-all VoIP
  match ip precedence 5

policy-map child
  class VoIP
    priority 128
```



```
class IP
  priority 1000
```

```
policy-map parent
  class class-default
    police 3300000 103000 103000 conform-action transmit exceed-action drop
  service-policy child
```

Pour que la configuration ci-dessus ait un sens, la réglementation doit être remplacée par le formatage. Exemple :

```
policy-map parent
  class class-default
    shape average 3300000 103000 0
  service-policy child
```

Afin de se renseigner plus sur le parent et les stratégies enfant, référez-vous s'il vous plaît à la [stratégie de service d'enfant de QoS pour la classe prioritaire](#).

Informations connexes

- [Assistance technique sur la technologie QoS](#)
- [Support technique - Cisco Systems](#)