# Comprendre la qualité de service sur les commutateurs de la gamme Catalyst 6000

---

## Contenu



---

## Introduction

Ce document explique les capacités en matière de qualité de service (QoS) offertes par les commutateurs de la gamme Catalyst 6000. Ce document couvre les capacités de configuration de QoS et donne des exemples de mise en œuvre de la QoS.

Le présent document n'est pas destiné à servir de guide de configuration. Des exemples de configuration sont présentés tout au long du document pour soutenir les explications des caractéristiques de QoS du matériel et du logiciel de la gamme Catalyst 6000. Pour savoir quelle syntaxe utilisée pour la structure des commandes de QoS, consultez les guides de configuration et de commandes suivants concernant la gamme Catalyst 6000 :

- Commutateurs de la gamme Catalyst 6500

## Définition de la QoS de couche 2

Bien des gens peuvent penser que la QoS dans les commutateurs de couche 2 (L2) consiste simplement à donner priorité aux trames Ethernet, mais ce processus va beaucoup plus loin. La QoS de L2 comporte ce qui suit :

1. **La planification des files d'attente d'entrée :** Lorsque la trame entre dans le port, elle peut être affectée à l'une des nombreuses files d'attente basées sur les ports avant que sa commutation vers un port de sortie soit programmée. Généralement, plusieurs files

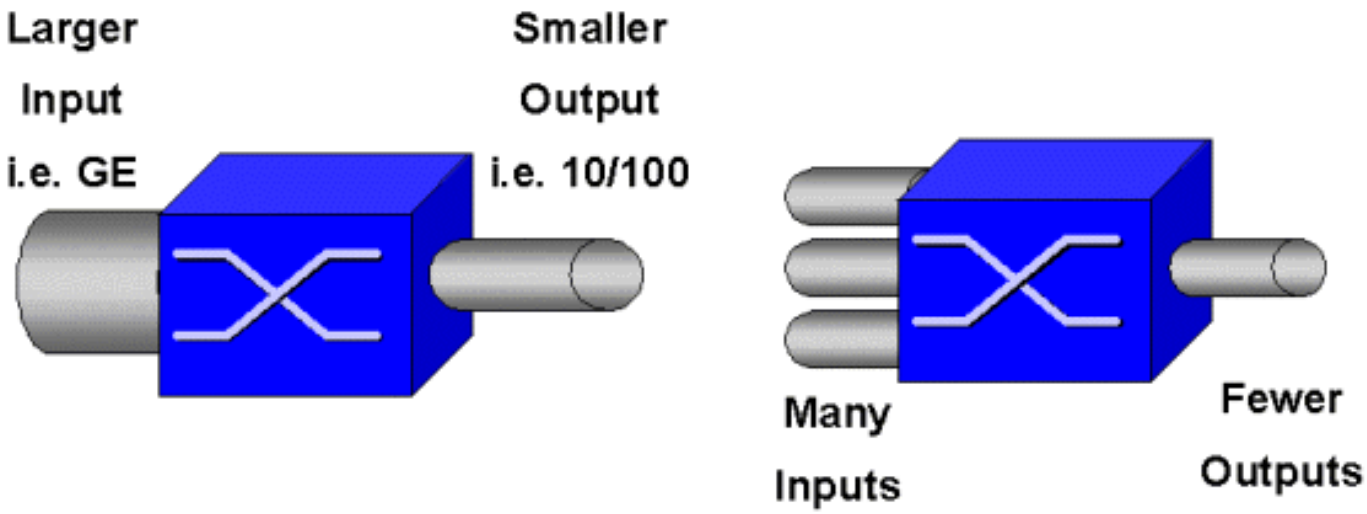
d’attente sont utilisées lorsque le trafic nécessite différents niveaux de service ou lorsque la latence du commutateur doit être réduite au minimum. Par exemple, les données vidéo et vocales reposant sur l’IP nécessitent une faible latence. Ainsi, il faudra peut-être changer ces données avant de passer à d’autres données, comme FTP (File Transfer Protocol), Web, courriel ou Telnet.

2. **Classification :** le processus de classification consiste à inspecter différents champs de l’en-tête Ethernet L2, ainsi que les champs de l’en-tête IP (couche 3 (L3)) et de l’en-tête TCP/UDP (Transmission Control Protocol/User Datagram Protocol) (couche 4 (L4)) pour déterminer le niveau de service qui sera appliqué à la trame lors de sa transmission du commutateur.
3. **Contrôle :** le contrôle s’entend du processus d’inspection d’une trame Ethernet visant à déterminer si celle-ci a dépassé un débit de trafic prédéfini dans un laps de temps donné (en général, ce laps de temps est déterminé par un nombre fixe interne au commutateur). Si cette trame est hors profil (c’est-à-dire qu’elle fait partie d’un train de données dépassant la limite de débit prédéfinie), soit la trame peut être supprimée, soit la valeur de classe de service (CoS) peut être réduite.
4. **Réécriture :** Le processus de réécriture consiste en la capacité du commutateur à modifier la CoS dans l’en-tête Ethernet ou les bits de type de service (ToS) dans l’en-tête IPV4.
5. **La planification de la sortie des files d’attente :** Après les processus de réécriture, le commutateur placera la trame Ethernet dans une file d’attente sortante (sortie) appropriée pour la commutation. C’est dans cette file d’attente que le commutateur gérera le tampon, en veillant à ce que celui-ci ne déborde pas. Pour ce faire, il utilise généralement un algorithme RED (Random Early Discard), qui supprime de la file d’attente les trames aléatoires. WRED est un dérivé de RED (qu’utilisent certains modules de la gamme Catalyst 6000), qui inspecte les valeurs CoS pour déterminer les trames à supprimer. Lorsque les tampons atteignent des seuils prédéfinis, les trames de priorité inférieure sont généralement supprimées, ce qui permet de conserver les trames de priorité supérieure dans la file d’attente.

Les sections suivantes de ce document expliquent plus en détail chaque mécanisme mentionné ci-dessus et leur relation avec la gamme Catalyst 6000.

# Le besoin relatif à une QoS dans un commutateur

Énormes fonds de panier, millions de paquets commutés par seconde et commutateurs non bloquants sont tous des synonymes des nombreux commutateurs offerts aujourd’hui. Pourquoi la QoS est-elle nécessaire? C’est en raison de la congestion.




Un commutateur peut être le plus rapide au monde, mais si un des deux scénarios présentés dans la figure ci-dessus survient, ce commutateur sera tout de même congestionné. En cas de congestion, si les fonctionnalités de gestion appropriées ne sont pas mises en place, les paquets seront supprimés. Lorsque des paquets sont supprimés surviennent alors des retransmissions. Le cas échéant, la charge du réseau peut augmenter. Dans les réseaux déjà congestionnés, cela peut aggraver les problèmes de performance actuels, voire dégrader davantage la performance.

Grâce aux réseaux convergents, la gestion de la congestion est encore plus critique. Le trafic sensible à la latence, comme la voix et la vidéo, peut être sérieusement touché en cas de retard. L'ajout de tampons à un commutateur n'atténuera pas forcément les problèmes de congestion. Le trafic sensible à la latence doit être commuté le plus rapidement possible. Vous devez d'abord cibler cet important trafic au moyen de techniques de classification, puis mettre en œuvre des techniques de gestion de la mémoire tampon pour éviter la perte du trafic de priorité supérieure pendant la congestion. Enfin, vous devez intégrer des techniques de planification pour commuter le plus rapidement possible les paquets importants des files d'attente. Comme vous le verrez dans ce document, la gamme Catalyst 6000 met en œuvre toutes ces techniques, ce qui fait de son sous-système de QoS l'un des plus complets de l'industrie actuellement.

Les techniques de QoS décrites dans la section précédente seront examinées plus en détail dans le présent document.

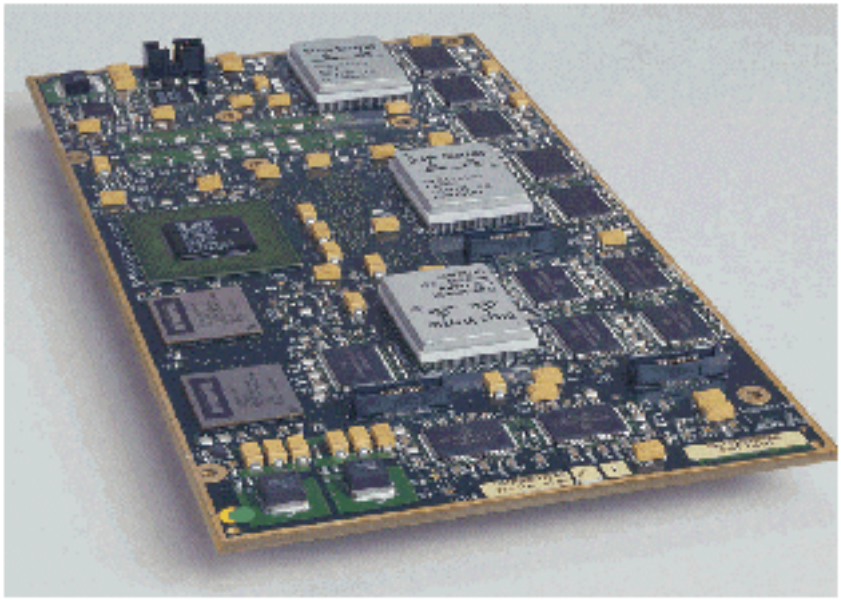
## Soutien matériel pour la QoS relative à la gamme de produits Catalyst 6000

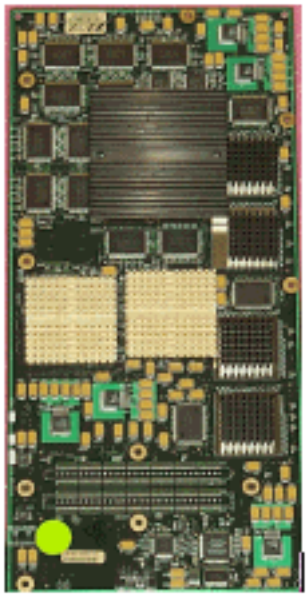
Pour prendre en charge la QoS de la gamme Catalyst 6000, un soutien matériel est requis. Parmi le matériel qui prend en charge la QoS, mentionnons la carte de commutation multicouche (MSFC), la carte de fonctionnalité stratégique (PFC) et les circuits intégrés à application spécifique (ASIC) des ports sur les cartes de ligne. Ce document n'explorera pas les capacités de la MSFC en matière de QoS, mais plutôt celles de la PFC et des ASIC sur les cartes de ligne.

### PFC

La version 1 de la PFC est une carte fille qui repose sur le Supervisor I (SupI) et le Supervisor IA (SupIA) de la gamme Catalyst 6000. La PFC2 constitue une nouvelle version de la PFC1 et est livrée avec le nouveau Supervisor II (SupII) et des nouveaux ASIC intégrés. Alors que la PFC1 et la PFC2 sont principalement connues pour leur programme d'accélération par matériel L3, la QoS

fait également partie de leurs objectifs. Les PFC sont illustrées ci-dessous.





Alors que les PFC1 et PFC2 sont essentiellement identiques, il existe quelques différences dans la fonctionnalité de QoS. Notamment, la PFC2 ajoute ce qui suit :

1. La capacité de réduire le contrôle de la QoS à une carte de transfert distribué (DFC).

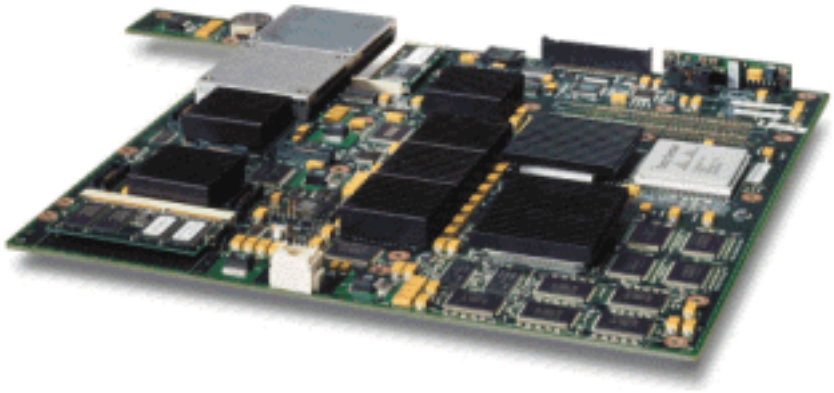
2. Les décisions en matière de contrôle sont légèrement différentes. La PFC1 et la PFC2 prennent en charge un contrôle normal, qui fait en sorte que les trames sont supprimées ou réduites si un contrôle d'agrégation ou de microflux renvoie une décision hors profil. Toutefois, la PFC2 ajoute la prise en charge d'un débit excédentaire, ce qui indique un deuxième niveau de contrôle pouvant s'appliquer.

Lorsqu'un contrôle de débit excédentaire est défini, les paquets peuvent être supprimés ou réduits quand ils dépassent la limite établie. Si un niveau de contrôle excédentaire est fixé, le mappage DSCP excédentaire est utilisé pour remplacer la valeur DSCP d'origine par une valeur réduite. Si seul un niveau de contrôle normal est fixé, le mappage DSCP normal est alors utilisé. Le niveau de contrôle excédentaire aura préséance lors de la sélection des règles de mappage si les deux niveaux de contrôle sont fixés.

Il est important de noter que les fonctions de QoS décrites dans ce document et exécutées par les ASIC mentionnés offrent des performances élevées. La performance de la QoS dans une gamme de base Catalyst 6000 (sans module de trame de commutation) génère 15 Mbit/s. Des gains de performance supplémentaires peuvent être obtenus pour la QoS si des DFC sont utilisées.

## DFC

La DFC peut être connectée au WS-X6516-GBIC en option. Cependant, il s'agit d'un appareil standard de la carte WS-X6816-GBIC. Il peut également être pris en charge sur des prochaines cartes de ligne de la trame, telles que la récente carte de ligne 10/100 (WS-X6548-RJ45) de la trame, la carte de ligne RJ21 (WS-X6548-RJ21) de la trame ainsi que la carte de ligne 100FX (WS- X6524-MM-FX). La DFC est illustrée ci-dessous.



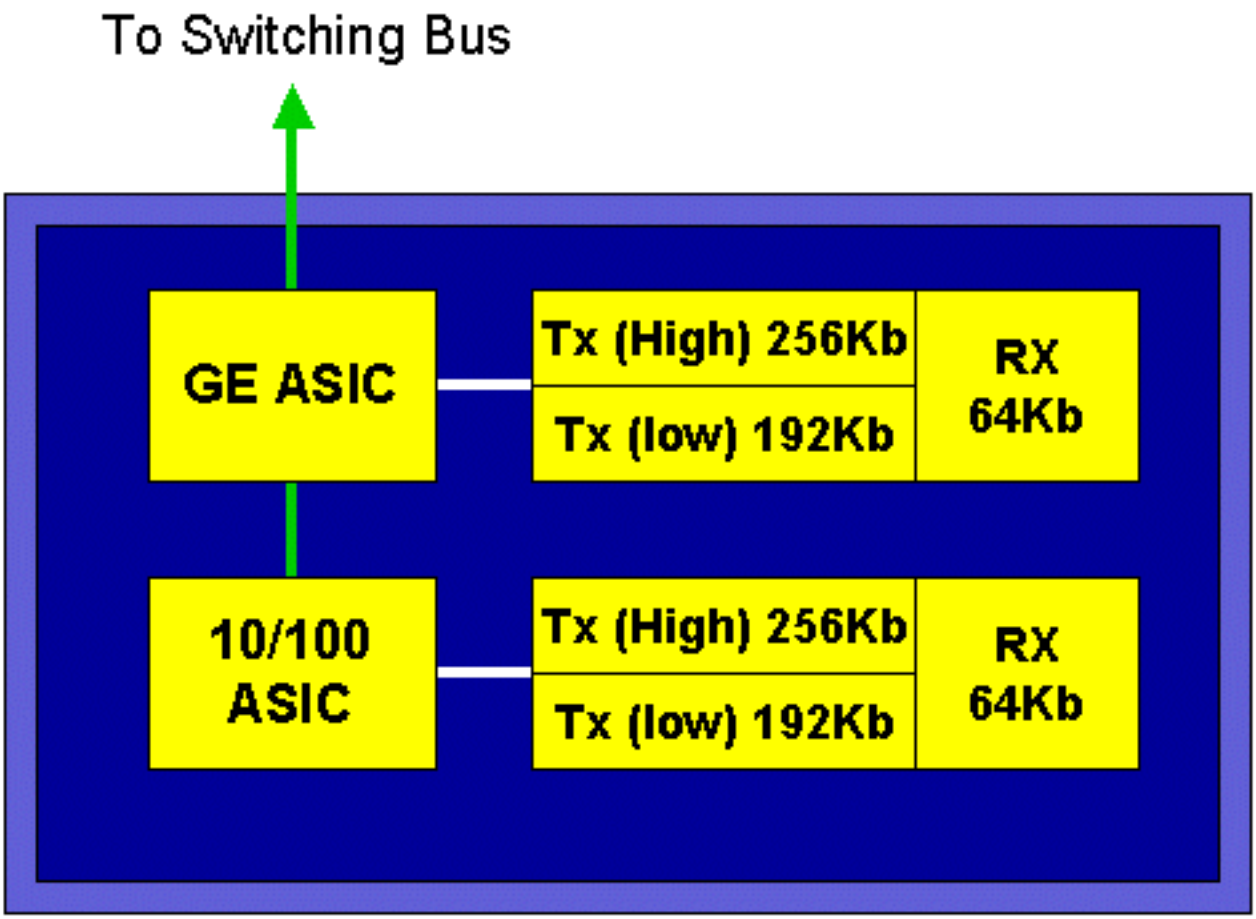
La DFC permet à la carte de ligne de la trame (connectée au distributeur) d'effectuer la commutation locale. Pour ce faire, elle doit également prendre en charge n'importe quel contrôle de QoS défini pour le commutateur. L'administrateur ne peut pas configurer directement la DFC; il doit plutôt passer par la MSFC/PFC principale sur le superviseur actif. La PFC principale générera un tableau de la base d'informations de transfert (FIB), qui donne à la DFC ses tableaux de transfert L2 et L3. Elle fera de même pour une copie des contrôles de QoS afin qu'ils servent également de contrôles locaux pour la carte de ligne. Par la suite, les décisions de commutation locale peuvent référencer la copie locale de tout contrôle de QoS, fournissant ainsi des vitesses de traitement de QoS matériel et offrant des niveaux de performance supérieurs grâce à la commutation répartie.

## ASIC de port

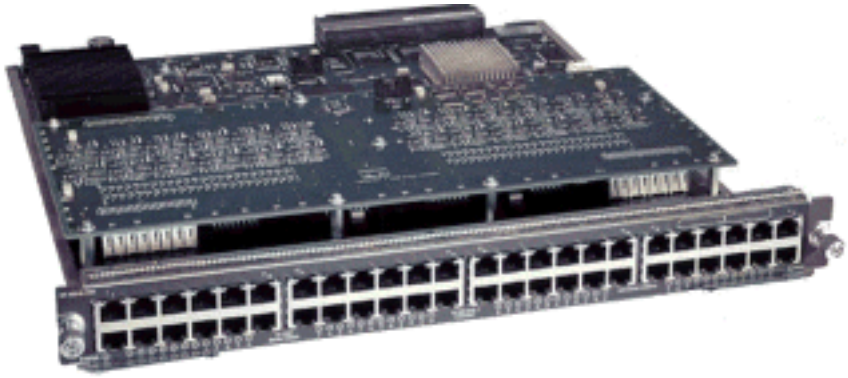
Pour avoir un tableau complet du matériel, chaque carte de ligne met en œuvre un certain nombre d'ASIC. Ces ASIC mettent en œuvre les files d'attente, la mise en mémoire tampon ainsi que les seuils utilisés pour le stockage temporaire des trames lorsque celles-ci transitent par le commutateur. Sur les cartes 10/100, une combinaison d'ASIC est utilisée pour approvisionner les 48 ports 10/100.

### Cartes de lignes 10/100 d'origine (WS-X6348-RJ45)

Les ASIC 10/100 fournissent une série de files d'attente de réception (Rx) et de transmission (TX) pour chaque port 10/100. Les ASIC procurent une mise en mémoire tampon de 128 Ko par port 10/100. Consultez les notes de version pour en savoir plus sur la mise en mémoire tampon par port qu'offre chaque carte de ligne. Chaque port de la carte de ligne prend en charge une file d'attente Rx ainsi que deux files d'attente TX désignées à haute et à basse priorité. Voir le schéma ci-dessous à cet effet.




Dans le schéma ci-dessus, chaque ASIC 10/100 fournit une ventilation pour 12 ports 10/100. Pour chaque port 10/100, des tampons de 128 Ko sont fournis. Les 128 Ko de tampons sont répartis entre chacune des trois files d'attente. Les figures présentées dans la file d'attente ci-dessus n'illustrent pas les valeurs par défaut; elles sont plutôt une représentation des configurations possibles. La seule file d'attente Rx obtient 16 Ko, et la mémoire restante (112 Ko) est répartie entre les deux files d'attente Tx. Par défaut (dans CatOS), la file d'attente à haute priorité reçoit 20 % de cet espace, tandis que la file d'attente à basse priorité en reçoit 80 %. Dans Catalyst IOS, la valeur par défaut est de donner 10 % à la file d'attente à haute priorité et 90 % à la file d'attente à basse priorité.

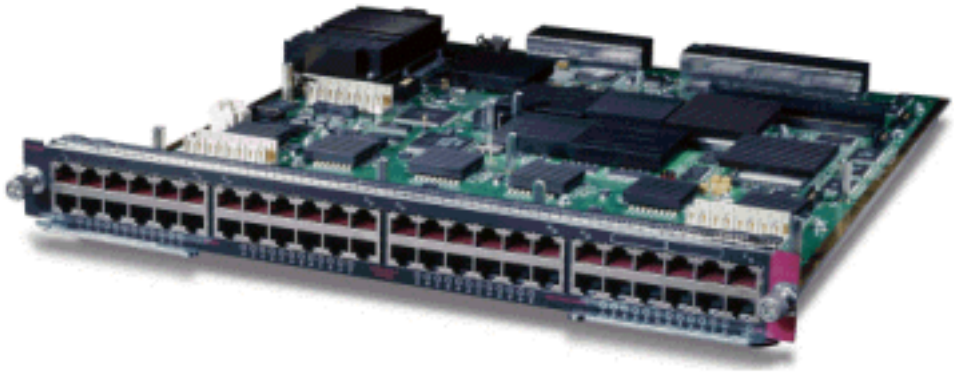


Bien que la carte offre une mise en mémoire tampon en deux étapes, seule la mise en mémoire tampon axée sur ASIC 10/100 peut être manipulée pendant la configuration de la QoS.

### Cartes de lignes 10/100 (WS-X6548-RJ45) de la trame

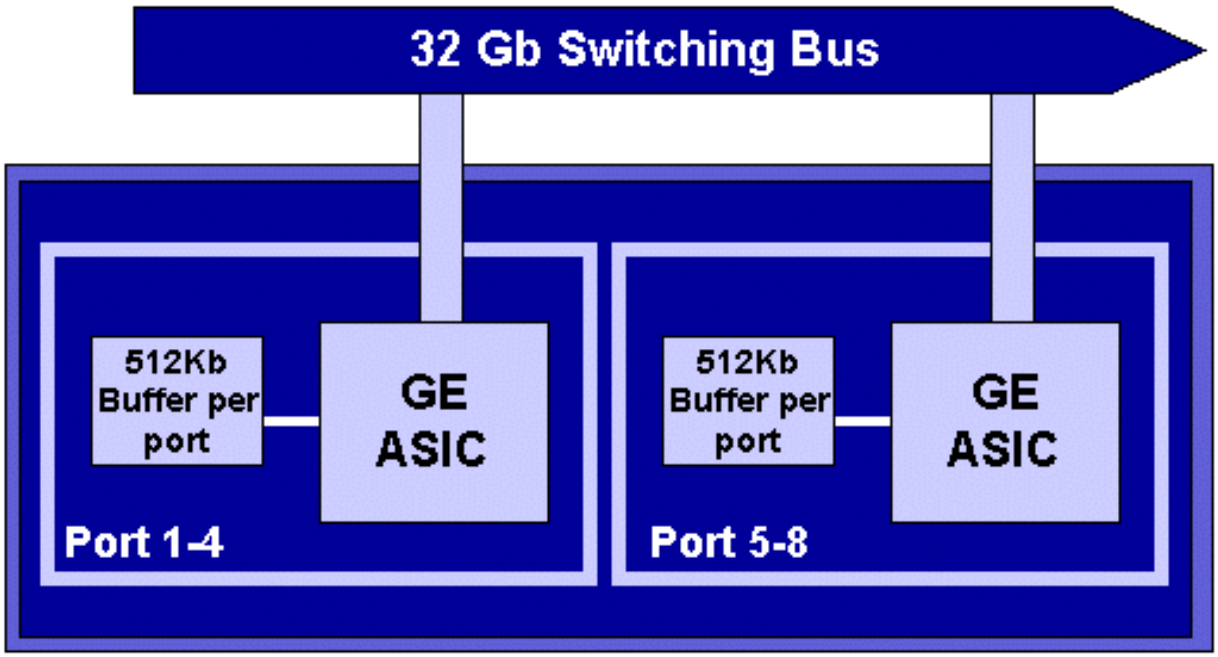
Les nouveaux ASIC 10/100 fournissent une série de files d'attente Rx et TX pour chaque port 10/100. Les ASIC fournissent un ensemble partagé de la mémoire offerte sur les ports 10/100.

Consultez les notes de version pour en savoir plus sur la mise en mémoire tampon par port qu'offre chaque carte de ligne. Chaque port de cette carte de ligne prend en charge deux files d'attente Rx et trois files d'attente TX. Une file d'attente Rx et une file d'attente TX sont considérées comme une file d'attente à priorité absolue. Elle agit comme une file d'attente à faible latence, ce qui est idéal pour le trafic sensible à la latence comme le trafic de voix sur IP (VoIP).

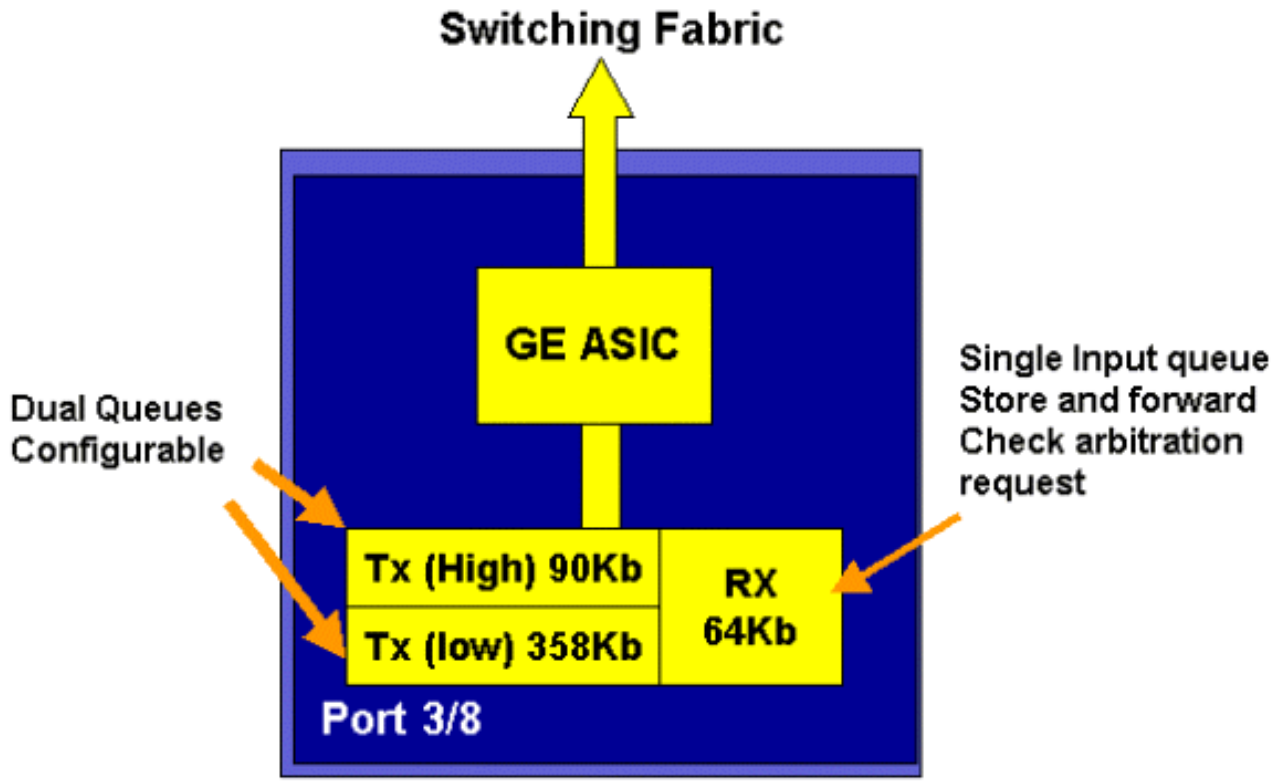


### Cartes de lignes GE (WS-X6408A, WS-X6516, WS-X6816)

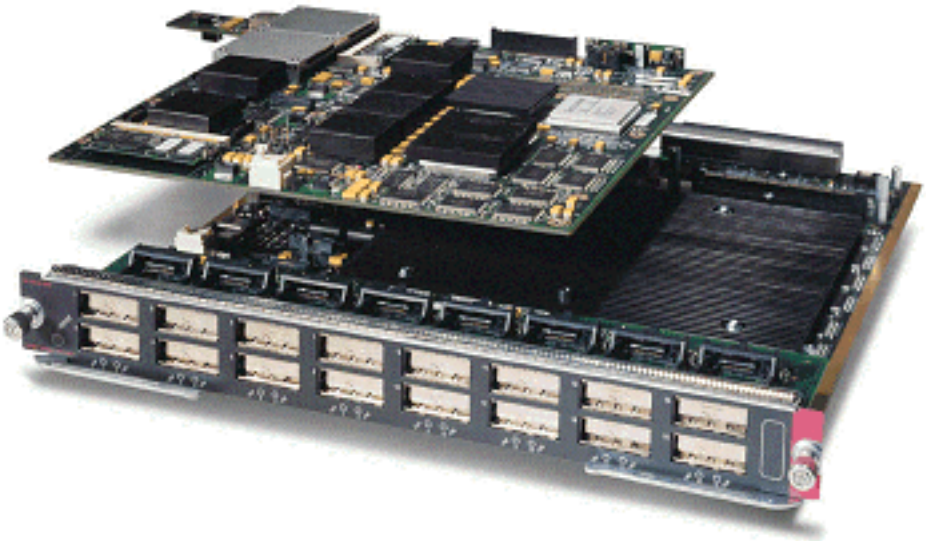
Pour les cartes de ligne GE, l'ASIC fournit 512 Ko de mise en mémoire tampon par port. Une représentation de la carte de ligne GE à huit ports est illustrée dans le schéma ci-dessous.




Comme pour les ports 10/100, chaque port GE comporte trois files d'attente, soit une Rx et deux TX. Il s'agit de la valeur par défaut sur la carte de ligne WS-X6408-GBIC. Elle est illustrée dans le schéma ci-dessous.



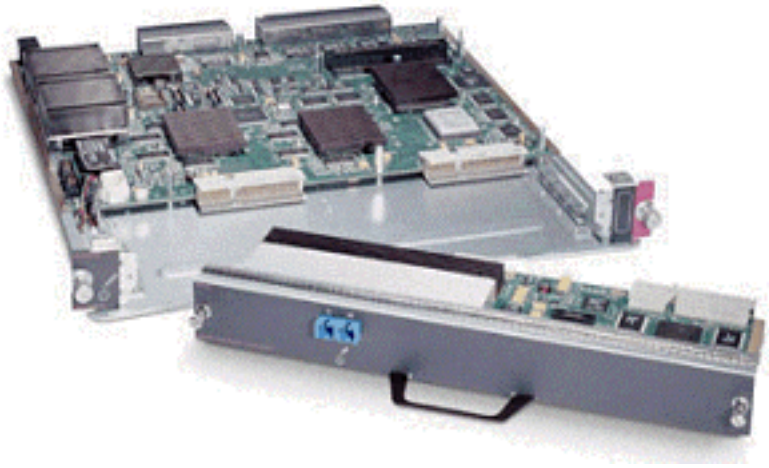

Sur les récentes cartes de ligne GE à 16 ports, les ports GBIC des SupIA et SupII ainsi que la carte GE WS-X6408A-GBIC à 8 ports, deux autres files d'attente de priorité stricte (SP) sont fournies. Une file d'attente SP est affectée comme file d'attente Rx, et l'autre, comme file d'attente TX. Cette file d'attente SP est utilisée principalement pour la mise en file d'attente du trafic sensible à la latence, comme la voix. Avec la file d'attente SP, les données qui y sont envoyées seront traitées avant les données des files d'attente à haute et à basse priorité. Les files d'attente de haute et de basse priorité ne seront traitées que lorsque la file d'attente SP sera vide.



### 10 cartes de lignes GE (WS-X6502-10GE)

Au cours du dernier semestre de 2001, Cisco a lancé un ensemble de 10 cartes de ligne GE offrant un port de 10 GE par carte de ligne. Ce module prend un logement du châssis 6000. La carte de ligne 10 GE prend en charge la QoS. Quant au port 10 GE, il procure deux files d'attente Rx et trois files d'attente TX. Une file d'attente Rx et une file d'attente TX sont désignées en tant

que file d'attente SP. La mise en mémoire tampon est également fournie pour le port, procurant un total de 256 Ko de mise en mémoire tampon Rx et 64 Mo de mise en mémoire tampon TX. Ce port met en œuvre une structure de file d'attente 1p1q8t pour le côté Rx et 1p2q1t pour le côté TX. Les structures de file d'attente sont expliquées en détail ultérieurement dans ce document.



### Résumé du matériel QoS de la gamme Catalyst 6000

Les composants matériels qui exécutent les fonctions QoS ci-dessus dans la gamme Catalyst 6000 sont expliqués en détail dans le tableau suivant.

| QoS Process | Catalyst 6500 Component that performs function |
|---|---|
| Input Scheduling | Performed by port ASIC's<br>L2 only with or without the PFC |
| Classification | Performed by Supervisor or PFC<br>L2 only is done by Supervisor<br>L2/3 is done by PFC |
| Policing | Done by PFC via L3 forwarding Engine |
| Packet Re-write | Done by port ASIC's<br>L2/L3 based on classification done in point 2 above |
| Output Scheduling | Done by port ASIC's<br>L2/L3 based on classification done in point 2 above |

## Soutien logiciel pour la QoS relative à la gamme de produits Catalyst 6000

La gamme Catalyst 6000 prend en charge deux systèmes d'exploitation. La plateforme logicielle d'origine, CatOS, est issue de la base de code utilisée sur la plateforme Catalyst 5000. Dernièrement, Cisco a introduit Cisco IOS® intégré [mode natif] (appelé auparavant IOS natif), qui utilise une base de code issue du routeur Cisco IOS. Les deux plates-formes de système d'exploitation (CatOS et Cisco IOS intégré (mode natif)) implémentent la prise en charge logicielle pour activer la QoS sur la plate-forme de la gamme de commutateurs Catalyst 6000 à l'aide du matériel décrit dans les sections précédentes.

**Note:** Ce document montre des exemples de configuration pour les deux plateformes de système

d’exploitation.

## Mécanismes prioritaires dans l’IP et l’Ethernet

Pour que des services de QoS soient appliqués aux données, il doit y avoir un moyen d’étiqueter ou de hiérarchiser un paquet IP ou une trame Ethernet. Les champs ToS et CoS sont utilisés pour y parvenir.

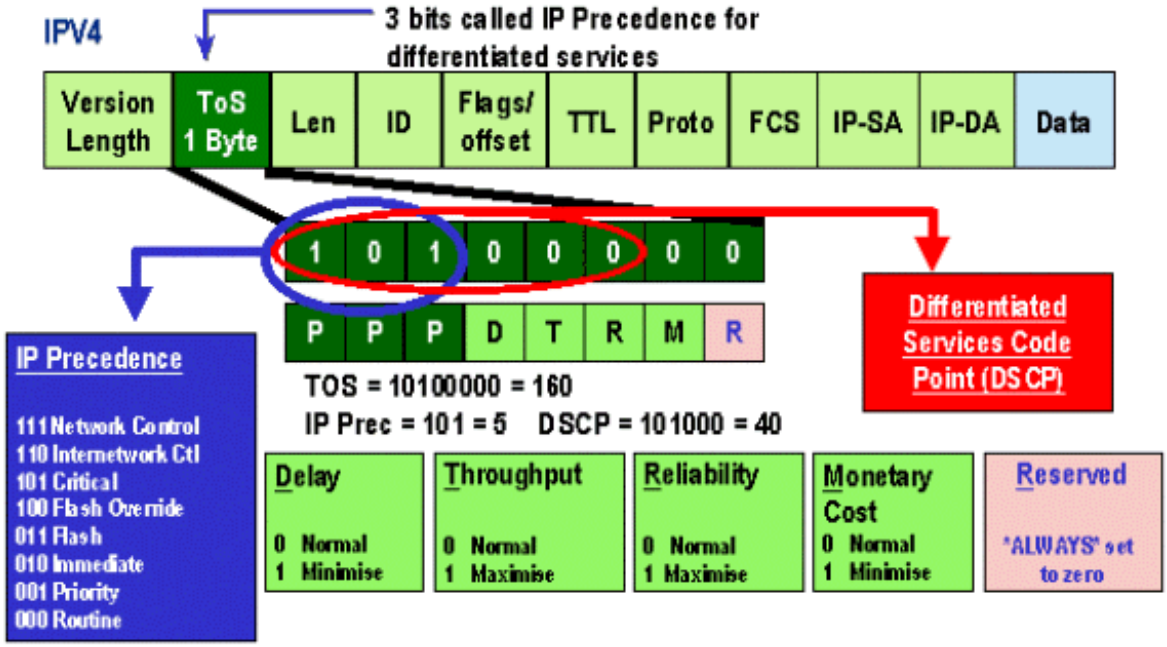
### ToS

ToS est un champ d’un octet qui existe dans un en-tête IPV4. Le champ ToS comporte huit bits, dont les trois premiers sont utilisés pour indiquer la priorité du paquet IP. Ces trois premiers bits sont appelés bits de priorité IP. Ces bits peuvent être réglés de zéro à sept, zéro étant la priorité la plus basse et sept la priorité la plus élevée. Depuis plusieurs années, le réglage des priorités IP dans IOS est pris en charge. La réinitialisation de la priorité IP peut être prise en charge par la MSFC ou la PFC (indépendante de la MSFC). Un paramètre de confiance indiquant « untrusted » (non fiable) peut également effacer n’importe quel paramètre de priorité IP sur une trame entrante.

Les valeurs possibles pour les priorités IP sont les suivantes :

| IP Precedence bits | IP Precedence Value |
|---|---|
| 000 | Routine |
| 001 | Priority |
| 010 | Intermediate |
| 011 | Flash |
| 100 | Flash Override |
| 101 | Critical |
| 110 | Internetwork Control |
| 111 | Network Control |

Le schéma ci-dessous est une représentation des bits de priorité IP dans l’en-tête ToS. Les trois bits les plus significatifs (MSB) sont interprétés comme les bits de priorité IP.



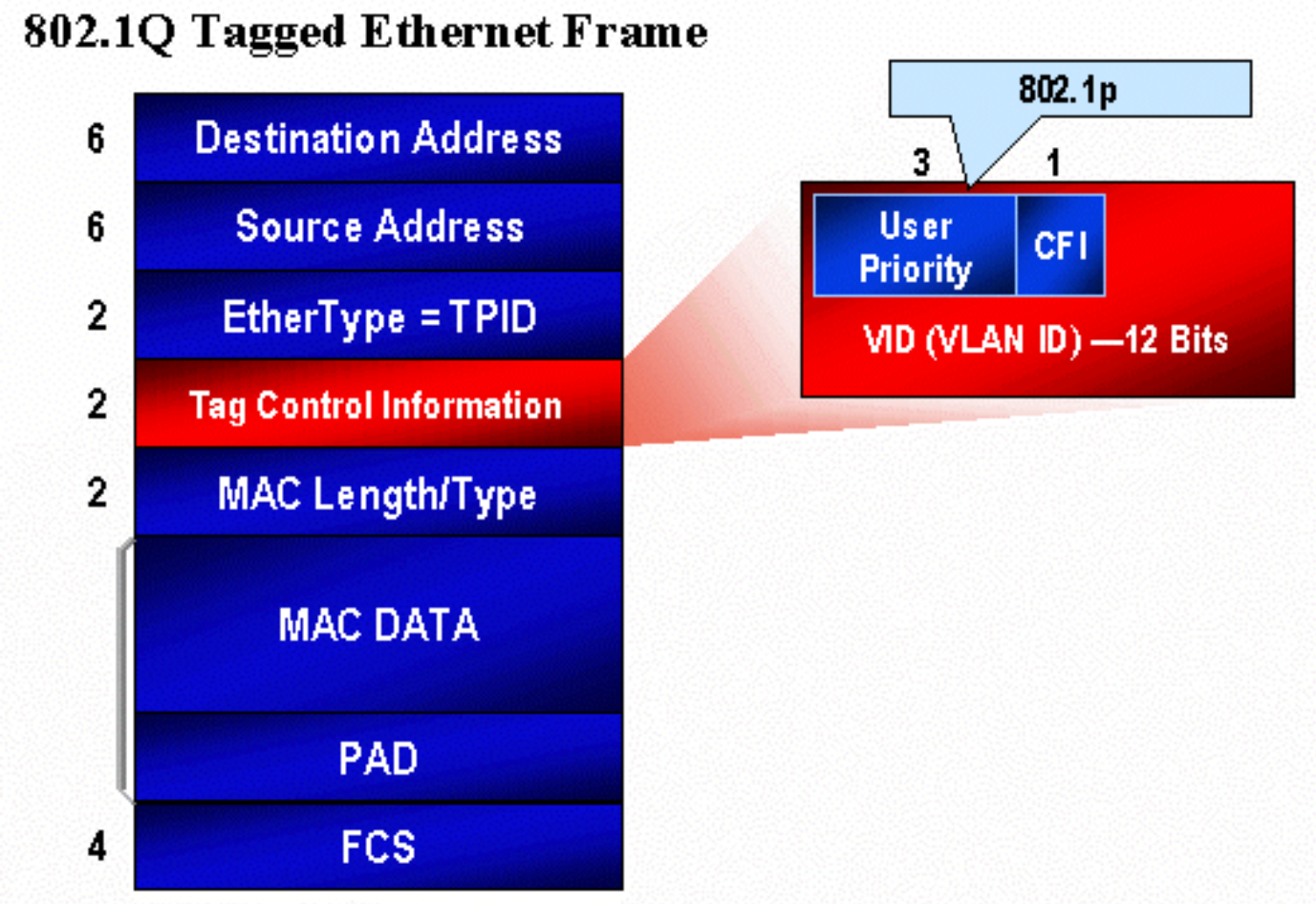

Dernièrement, l'utilisation du champ ToS a été élargie de manière à englober les six MSB, ou « DSCP ». Le DSCP donne 64 valeurs de priorité (deux à la puissance de six) qui peuvent être octroyées au paquet IP.

La gamme Catalyst 6000 peut manipuler le ToS. C'est possible en utilisant à la fois la PFC et la MSFC. Si une trame entre dans le commutateur, elle se voit attribuer une valeur DSCP. Cette valeur DSCP est utilisée à l'interne, dans le commutateur, pour affecter des niveaux de service (contrôles de QoS) définis par l'administrateur. Le DSCP peut déjà exister dans une trame et être utilisé, ou il peut provenir de la CoS existante, de la priorité IP ou du DSCP dans la trame (si le port est fiable). Une carte est utilisée à l'interne, dans le commutateur, pour obtenir le DSCP. Avec huit valeurs de CoS/priorité IP possibles et 64 valeurs de DSCP proposées, la carte par défaut mappera la CoS/priorité IP 0 à DSCP 0, la CoS/priorité IP 1 à DSCP 7, la CoS/priorité IP 2 à DSCP 15, etc. Ces mappages par défaut peuvent être remplacés par l'administrateur. Lorsque la trame est programmée vers un port sortant, la CoS peut être réécrite, et la valeur DSCP sert alors à obtenir la nouvelle CoS.

## CoS

La CoS fait référence à trois bits dans un en-tête ISL ou un en-tête 802.1Q, qui sont employés pour indiquer la priorité de la trame Ethernet lors de son passage dans un réseau commuté. Aux fins du présent document, nous tiendrons compte uniquement de l'utilisation de l'en-tête 802.1Q. Les bits de CoS dans l'en-tête 802.1Q sont communément appelés les « bits 802.1p ». Comme il fallait s'y attendre, il y a trois bits de CoS, ce qui correspond au nombre de bits utilisés pour la priorité IP. Dans de nombreux réseaux, afin de maintenir la QoS de bout en bout, un paquet peut traverser les domaines L2 et L3. Pour maintenir la QoS, le ToS peut être mappé au CoS, et le CoS peut être mappé au ToS.

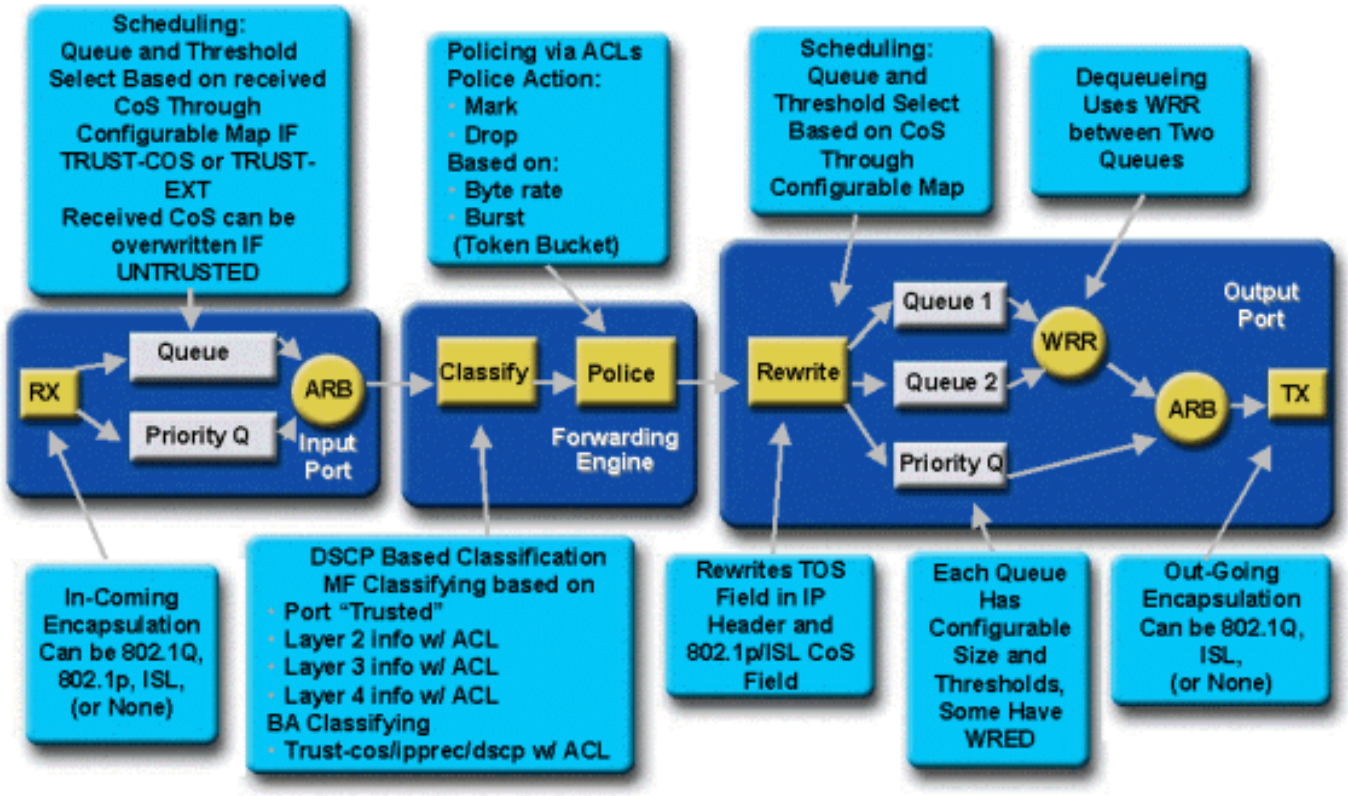
Le schéma suivant représente une trame Ethernet étiquetée et assortie d'un champ 802.1Q, lequel est composé d'un Ethertype et d'une étiquette tous deux à deux octets. Dans l'étiquette à deux octets figurent les bits de priorité d'utilisateur (appelés « 802.1p »).




## Flux QoS dans la gamme Catalyst 6000

La QoS dans la gamme Catalyst 6000 constitue la mise en œuvre la plus complète de la QoS dans l'ensemble des commutateurs Cisco Catalyst actuels. Les sections suivantes décrivent comment les divers processus de QoS sont appliqués à une trame lorsqu'elle transite par le commutateur.

Comme il a été mentionné précédemment dans ce document, de nombreux commutateurs L2 et L3 peuvent offrir divers éléments de QoS. Ces éléments sont la classification, la planification de files d'attente d'entrée, le contrôle, la réécriture et la planification des files d'attente de sortie. La différence avec la gamme Catalyst 6000, c'est que ces éléments de QoS sont appliqués par un moteur L2 qui a un aperçu des détails L3 et L4 ainsi que des informations sur l'en-tête L2. Le schéma suivant résume comment la gamme Catalyst 6000 met en œuvre ces éléments.




Une trame entre dans le commutateur et est traitée initialement par le port ASIC qui a reçu la trame. Il enverra la trame dans une file d'attente Rx. Selon la carte de ligne de la gamme Catalyst 6000, il y aura une ou deux files d'attente Rx.

L'ASIC de port utilisera les bits CoS pour indiquer dans quelle file d'attente placer la trame (en présence de plusieurs files d'attente d'entrée). Si le port est classé comme « untrusted » (non fiable), l'ASIC de port peut remplacer les bits CoS existants en fonction d'une valeur prédéfinie.

La trame est ensuite redirigée vers le moteur de transfert L2/L3 (PFC), qui classifie et facultativement contrôle la trame. La classification consiste à attribuer à la trame une valeur DSCP, qui est utilisée à l'interne par le commutateur aux fins de traitement de la trame. La valeur DSCP sera obtenue d'un des éléments suivants :

1. Une valeur DSCP existante définie avant l'entrée de la trame dans le commutateur;
2. Les bits de priorité IP reçus qui sont déjà définis dans l'en-tête IPV4. Étant donné qu'il existe 64 valeurs DSCP et seulement huit valeurs de priorité IP, l'administrateur configurera un mappage qu'utilisera le commutateur pour obtenir la valeur DSCP. Des mappages par défaut sont mis en place si l'administrateur ne configure pas les cartes.
3. Les bits CoS reçus sont déjà définis avant l'entrée de la trame dans le commutateur. Comme pour la priorité IP, il existe un maximum de huit valeurs CoS, chacune devant être mappée à une des 64 valeurs DSCP. Cette carte peut être configurée, ou le commutateur peut utiliser la carte par défaut mise en place.
4. Le paramètre de la trame est fixé à l'aide d'une valeur DSCP par défaut qui est généralement octroyée en passant par une entrée ACL (liste de contrôle d'accès).

Après l'octroi d'une valeur DSCP à la trame, le contrôle (limitation de débit) est appliqué, s'il existe une configuration de contrôle. Le contrôle limitera le flux de données par la PFC en supprimant ou en réduisant le trafic qui est hors profil. Le terme « hors profil » est utilisé pour indiquer que le trafic a dépassé une limite définie par l'administrateur, comme la quantité de bits par seconde qu'enverra la PFC. Le trafic hors profil peut être supprimé, ou la valeur CoS, diminuée. Les PFC1

et PFC2 prennent actuellement en charge le contrôle d'entrée (limitation de débit) seulement. La prise en charge du contrôle des entrées et des sorties sera possible lors du lancement d'une nouvelle PFC.

La PFC transmettra ensuite la trame au port de sortie aux fins de traitement. À ce stade, un processus de réécriture est employé pour modifier les valeurs CoS de la trame et la valeur ToS dans l'en-tête IPV4. Cela provient du DSCP interne. La trame sera ensuite placée dans une file d'attente de transmission selon sa valeur CoS, prête pour la transmission. Pendant que la trame est dans la file d'attente, l'ASIC de port surveillera les tampons et mettra en œuvre WRED pour éviter le débordement des tampons. Un algorithme de planification WRR est ensuite utilisé pour planifier et transmettre des trames à partir du port de sortie.

Les sections suivantes exploreront ce flux plus en détail et donneront des exemples de configuration pour chaque étape décrite ci-dessus.

# Files d'attente, tampons, seuils et mappages

Avant que la configuration de la QoS soit approfondie, certains termes doivent être expliqués davantage pour que vous compreniez bien les capacités de configuration de la QoS du commutateur.

### Files d'attente

Chaque port du commutateur comporte une série de files d'attente d'entrée et de sortie qui servent comme zones de stockage temporaire pour les données. Les cartes de ligne de la gamme Catalyst 6000 mettent en œuvre un nombre différent de files d'attente pour chaque port. En général, les files d'attente sont mises en œuvre dans des ASIC matériels pour chaque port. Sur les cartes de ligne de la gamme Catalyst 6000 de première génération, la configuration type était une file d'attente d'entrée et deux de sortie. Sur les récentes cartes de ligne (10/100 et GE), l'ASIC met en œuvre un ensemble supplémentaire de deux files d'attente (une d'entrée et une de sortie), pour un total de deux files d'attente d'entrée et trois files d'attente de sortie. Ces deux files d'attente supplémentaires sont des files d'attente SP spéciales qui sont utilisées pour le trafic sensible à la latence, comme la VoIP. Elles sont effectuées en mode SP. Autrement dit, si une trame entre dans la file d'attente SP, la planification des trames des files d'attente inférieures est interrompue afin que soit traitée la trame dans la file d'attente SP. Ce n'est que lorsque la file d'attente SP est vide que reprend la planification des paquets à partir des files d'attente inférieures.

Lorsqu'une trame arrive à un port (pour l'entrée ou la sortie) en période de congestion, elle est placée dans une file d'attente. La décision concernant la file d'attente où sera placée la trame est généralement prise en fonction de la valeur CoS dans l'en-tête Ethernet de la trame entrante.

Àla sortie, un algorithme de planification sera employé pour que soit vidée la file d'attente TX (sortie). WRR est la technique utilisée pour y parvenir. Pour chaque file d'attente, une pondération permet de déterminer la quantité de données qui sera retirée de la file d'attente avant de passer à la suivante. La pondération qu'attribue l'administrateur à chaque file d'attente TX est un nombre de 1 à 255.

### Tampons

Chaque file d'attente reçoit une certaine quantité d'espace tampon pour stocker les données de transit. La mémoire réside dans l'ASIC du port. Elle est répartie et octroyée par port. Pour chaque port GE, l'ASIC GE attribue 512 Ko d'espace tampon. Pour les ports 10/100, l'ASIC du port

réserve 64 Ko ou 128 Ko (selon la carte de ligne) de mise en mémoire tampon par port. Cet espace tampon est ensuite réparti entre les files d'attente Rx (entrée) et TX (sortie).

### Seuils

Un aspect de la transmission normale de données est que si un paquet est supprimé, celui-ci sera alors retransmis (flux TCP). En cas de congestion, la charge sur le réseau peut ainsi augmenter et éventuellement entraîner la surcharge des tampons. Le commutateur de la gamme Catalyst 6000 utilise un certain nombre de techniques pour éviter le débordement des tampons.

Les seuils sont des niveaux imaginaires qu'attribue le commutateur (ou l'administrateur). Ils définissent les points d'utilisation qui régissent le moment où l'algorithme de gestion de la congestion commence à supprimer des données de la file d'attente. Sur les ports de la gamme Catalyst 6000, il y a généralement quatre seuils associés aux files d'attente d'entrée. En général, deux seuils sont associés aux files d'attente de sortie.

Ces seuils sont également déployés, dans le contexte de la QoS, afin que leur soient attribuées des trames ayant des priorités différentes. Lorsque la mémoire tampon commence à se remplir et que les seuils sont franchis, l'administrateur peut mapper différentes priorités à différents seuils, tout en indiquant au commutateur les trames à supprimer au moment où un seuil est franchi.

### Mappages

Les sections ci-dessus portant sur les files d'attente et les seuils mentionnent que la valeur CoS de la trame Ethernet sert à déterminer dans quelle file d'attente envoyer la trame et à quel moment lors du remplissage de la mémoire tampon la trame peut être supprimée. C'est le but d'un mappage.

Lorsque la QoS est configurée sur la gamme Catalyst 6000, les mappages par défaut sont activés et définissent ce qui suit :

- àquels seuils peuvent être supprimées les trames ayant des valeurs CoS précises;
- dans quelle file d'attente est placée une trame (selon sa valeur CoS).

Malgré l'existence de mappages par défaut, ces derniers peuvent être remplacés par l'administrateur. Le mappage est offert pour les éléments suivants :

- Valeurs CoS sur une trame entrante vers une valeur DSCP
- Valeurs de priorité IP sur une trame entrante vers une valeur DSCP
- Valeurs DSCP vers une valeur CoS pour une trame sortante
- Valeurs CoS pour supprimer les seuils des files d'attente de réception
- Valeurs CoS pour supprimer les seuils des files d'attente de transmission
- Valeurs de réduction du DSCP pour les trames qui dépassent les instructions de contrôle
- Valeurs de CoS vers une trame ayant une adresse MAC de destination bien précise

## WRED et WRR

WRED et WRR sont deux algorithmes extrêmement puissants qui résident dans la gamme Catalyst 6000. WRED et WRR utilisent tous deux l'étiquette de priorité (CoS) dans une trame Ethernet afin d'améliorer la gestion du tampon et la planification de la sortie. B

## WRED

WRED est un algorithme de gestion de la mémoire tampon utilisé par la gamme Catalyst 6000 pour réduire au minimum les répercussions liées à la suppression du trafic à priorité élevée en cas de congestion. WRED repose sur l'algorithme RED.

Afin de comprendre RED et WRED, consultez de nouveau la section sur le concept de gestion de flux TCP. La gestion de flux empêche l'expéditeur TCP de surcharger le réseau. L'algorithme TCP slowstart fait partie de la solution pour remédier à cette situation. Cela signifie que si un flux commence, un seul paquet est envoyé avant l'attente d'un accusé de réception (ACK). Deux paquets sont ensuite envoyés, avant la réception d'un ACK, ce qui augmente progressivement le nombre de paquets transmis avant la réception de chaque ACK. Ce processus se poursuivra jusqu'à ce que le flux atteigne un niveau de transmission (c'est-à-dire qu'il envoie un nombre *x de paquets) que peut gérer le réseau sans que la charge cause un encombrement.* Si une congestion survient, l'algorithme slowstart limitera la taille de la fenêtre (c'est-à-dire le nombre de paquets transmis avant l'attente d'un accusé de réception), réduisant ainsi les performances globales pour la session TCP (flux).

RED surveillera une file d'attente dès qu'elle commence à se remplir. Une fois qu'un certain seuil a été franchi, les paquets commencent à être supprimés aléatoirement. Aucune considération n'est donnée à des flux en particulier; plutôt, les paquets aléatoires seront supprimés. Ces paquets peuvent provenir de flux à priorité élevée ou faible. Les paquets supprimés peuvent faire partie d'un seul flux ou de plusieurs flux TCP. Si plusieurs flux sont touchés, comme il est décrit ci-dessus, les répercussions sur la taille de chaque fenêtre de flux peuvent être considérables.

Contrairement à RED, WRED n'est pas aussi aléatoire lors de la suppression de trames. WRED prend en compte la priorité des trames (dans son cas, la gamme Catalyst 6000 utilise la valeur CoS). Avec WRED, l'administrateur attribue des trames ayant certaines valeurs CoS à des seuils précis. Lorsque ces seuils sont franchis, les trames ayant des valeurs CoS mappées à ces seuils peuvent être supprimées. Les autres trames dont les valeurs CoS sont octroyées à des seuils supérieurs sont conservées dans la file d'attente. Ce processus permet aux flux de priorité supérieure de rester intacts tout en conservant la taille agrandie de leurs fenêtres et en réduisant au minimum la latence nécessaire pour transférer les paquets de l'émetteur au récepteur.

Comment savoir si votre carte de ligne prend en charge WRED? Utilisez la commande suivante. Dans la sortie, vérifiez la section indiquant la prise en charge de WRED sur ce port.

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
```

```
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        40% 100%
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
--------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ---------------------------------- 1 100 2 255 Console> (enable)
```

Dans le cas où WRED ne serait pas disponible sur un port, ce port utilisera alors une méthode d'élimination pour la gestion de la mémoire tampon. Cette méthode d'élimination, ou « tail drop », supprime simplement les trames entrantes une fois que les tampons ont été entièrement utilisés.

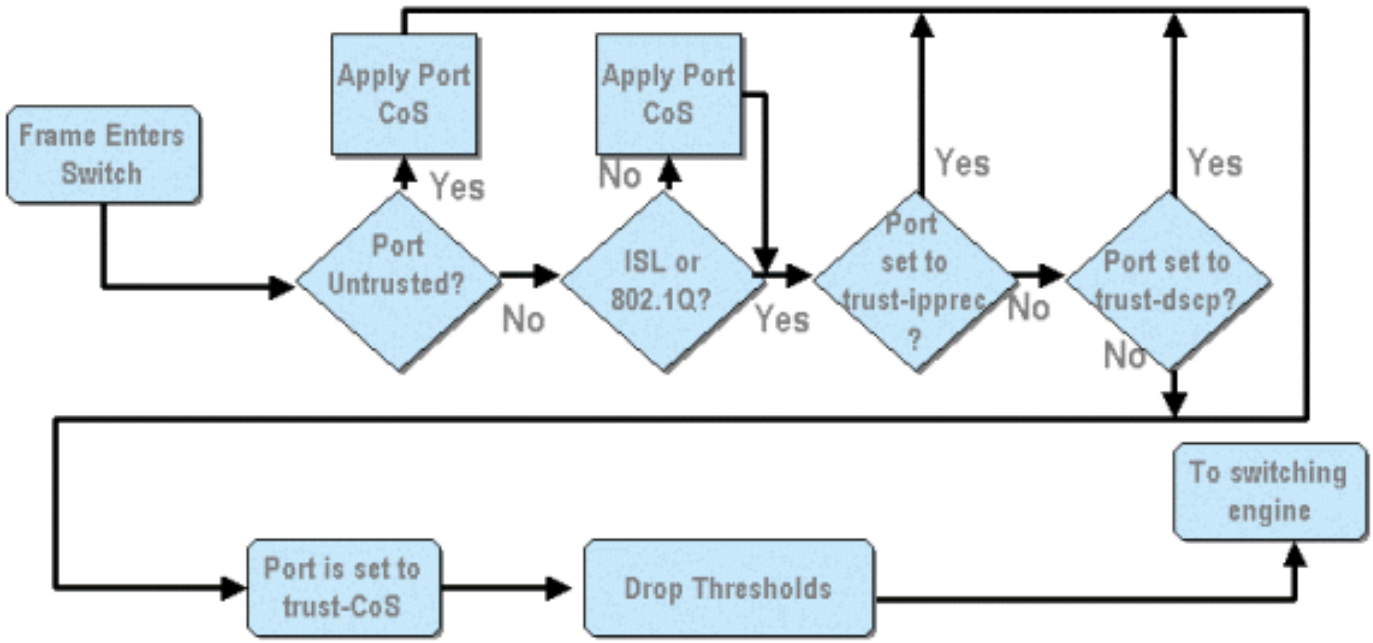
### WRR

WRR est utilisé pour programmer le trafic sortant des files d'attente TX. Un algorithme normal qui intervient en séquence périodiquement alternera entre les files d'attente TX, envoyant un nombre égal de paquets à partir de chaque file d'attente avant de passer à la prochaine. L'aspect pondéré de WRR permet à l'algorithme de planification d'inspecter une pondération qui est affectée à la file d'attente. Ainsi, les files d'attente d'accès qui sont définies peuvent accéder à une plus grande partie de la bande passante. L'algorithme de planification WRR retirera plus de données des files d'attente ciblées que des autres files d'attente, créant ainsi un biais pour les files d'attente désignées.

La configuration de WRR et les autres aspects des éléments décrits ci-dessus sont expliqués dans les prochaines sections.

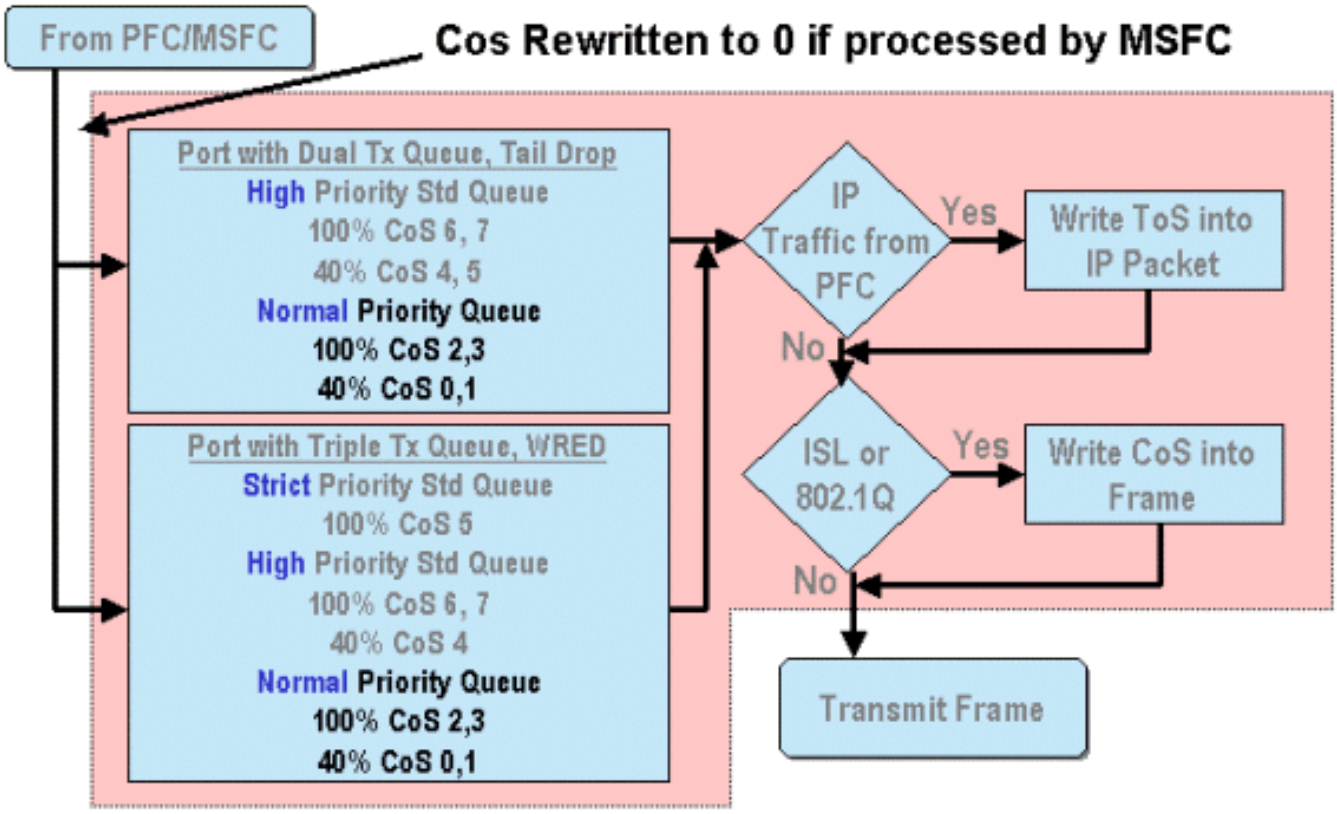
## Configuration de la QoS basée sur ASIC pour les ports de la gamme Catalyst 6000

La configuration de la QoS demande à l'ASIC du port ou à la PFC d'effectuer une QoS. Les sections suivantes aborderont la configuration de la QoS pour ces deux processus. Sur l'ASIC du port, la configuration de la QoS a une incidence sur les flux de trafic entrant et sortant.




Le schéma ci-dessus montre que les processus suivants de configuration de la QoS s'appliquent :

1. états de confiance des ports
2. application de la CoS basée sur les ports
3. attribution du seuil de suppression de Rx
4 mappages des seuils de suppression de CoS à Rx




Lorsqu'une trame est traitée par la MSFC ou la PFC, elle est transmise à l'ASIC du port sortant aux fins de traitement ultérieur. Toutes les trames traitées par la MSFC verront leurs valeurs CoS réinitialisées à zéro. Ce résultat doit être pris en compte pour le traitement de la QoS sur les ports sortants.

Le schéma ci-dessus illustre le traitement de la QoS effectuée par l'ASIC du port pour le trafic sortant. Certains processus mentionnés lors du traitement de la QoS sortante comprennent les suivants :

1. Méthode d'élimination pour la file d'attente TX et attribution du seuil de WRED
2. Mappages de CoS à la méthode d'élimination pour la file d'attente TX et à WRED

Bien qu'il ne soit pas illustré dans le schéma ci-dessus, il existe un processus de réaffectation de la CoS à la trame sortante au moyen d'un mappage DSCP à CoS.

Les sections suivantes traitent plus en détail les capacités de configuration de la QoS des ASIC basés sur les ports.

**Note:** Soulignons que lorsque les commandes de QoS sont utilisées avec CatOS, elles s'appliquent généralement à tous les ports associés au type de file d'attente indiqué. Par exemple, si un seuil de suppression WRED est appliqué aux ports avec le type de file d'attente 1p2q2t, ce seuil de suppression est alors appliqué à tous les ports sur l'ensemble des cartes de ligne prenant en charge ce type de file d'attente. Avec Cat IOS, les commandes de QoS sont généralement appliquées au niveau de l'interface.

## Activation de la QoS

Avant qu'une configuration de QoS puisse avoir lieu sur la gamme Catalyst 6000, la QoS doit d'abord être activée sur le commutateur. Pour ce faire, exécutez la commande suivante :

### CatOS

```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

### Cisco IOS intégré (mode natif)

```
Cat6500(config)# mls qos
```

Lorsque la QoS est activée dans la gamme Catalyst 6000, le commutateur définira une série de valeurs QoS par défaut pour le commutateur. Ces paramètres par défaut comprennent les suivants :

| QoS Feature | Default setting |
|---|---|
| Trust state of each port | Un-trusted |
| Receive Queue drop threshold percentages | Threshold 1 – 50%<br>Threshold 2 – 60%<br>Threshold 3 – 80%<br>Threshold 4 – 100% |
| Transmit Queue drop threshold percentages | Low priority queue threshold 1 – 80%<br>Low priority queue threshold 2 – 100%<br>High priority queue threshold 1 – 80%<br>High priority queue threshold 2 – 100% |
| CoS value to Drop threshold mapping | Receive queue 1/drop threshold 1: CoS 0 and 1<br>Transmit queue 1/drop threshold 1: CoS 0 and 1<br>Receive queue 1/drop threshold 2: CoS 2 and 3<br>Transmit queue 1/drop threshold 2: CoS 2 and 3<br>Receive queue 1/drop threshold 3: CoS 4 and 5<br>Transmit queue 2/drop threshold 1: CoS 4 and 5<br>Receive queue 1/drop threshold 4: CoS 6 and 7 |
| | Transmit queue 2/drop threshold 2: CoS 6 and 7 |
| CoS to DSCP Mapping<br>(DSCP set from CoS value) | CoS 0 = DSCP 0<br>CoS 1 = DSCP 8<br>CoS 2 = DSCP 16<br>CoS 3 = DSCP 24<br>CoS 4 = DSCP 32<br>CoS 5 = DSCP 40<br>CoS 6 = DSCP 48<br>CoS 7 = DSCP 56 |
| IP Precedence to DSCP Map<br>(DSCP set from IP Precedence value) | IP precedence 0 = DSCP 0<br>IP precedence 1 = DSCP 8<br>IP precedence 2 = DSCP 16<br>IP precedence 3 = DSCP 24<br>IP precedence 4 = DSCP 32<br>IP precedence 5 = DSCP 40<br>IP precedence 6 = DSCP 48<br>IP precedence 7 = DSCP 56 |
| DSCP to CoS map<br>(CoS set from DSCP values) | DSCP 0-7 = CoS 0<br>DSCP 8-15 = CoS 1<br>DSCP 16-23 = CoS 2<br>DSCP 24-31 = CoS 3<br>DSCP 32-39 = CoS 4<br>DSCP 40-47 = CoS 5<br>DSCP 48-55 = CoS 6<br>DSCP 56-63 = CoS 7 |

## Ports sécurisés et non sécurisés

Tous les ports de la gamme Catalyst 6000 peuvent être configurés comme des ports sécurisés ou non sécurisés. Le port fiable représente comment celui-ci marque, classe et planifie la trame lorsqu'elle transite par le commutateur. Par défaut, tous les ports sont réglés à l'état non sécurisé.

### Ports non sécurisés (paramètre par défaut pour les ports)

Si le port doit être configuré comme un port non sécurisé, lors de la première entrée du port, une trame aura sa valeur CoS et ToS remise à zéro par l'ASIC du port. Cela signifie que la trame se verra attribuée le service de priorité inférieur sur son chemin à travers le commutateur.

Sinon, l'administrateur peut réinitialiser la valeur CoS de toute trame Ethernet qui entre dans un port non sécurisé à une valeur prédéterminée. Cette configuration sera abordée dans une section ultérieure.

Si vous définissez le port comme non sécurisé, le commutateur ne fera rien pour prévenir la congestion. La prévention de la congestion est la méthode utilisée pour supprimer les trames en fonction de leurs valeurs CoS une fois qu'elles franchissent les seuils définis pour la file d'attente. Toutes les trames qui entrent dans ce port pourront également être suspendues lorsque les tampons atteindront 100 %.

Dans CatOS, un port 10/100 ou GE peut être configuré comme non sécurisé au moyen de la commande suivante :

### CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

Cette commande règle le port 16 du module 3 à un état non sécurisé.

**Note:** En ce qui concerne Cisco IOS intégré (mode natif), le logiciel ne prend en charge actuellement que la configuration « sécurisée » pour les ports GE.

### Cisco IOS intégré (mode natif)

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

Dans l'exemple ci-dessus, nous saisissons la configuration de l'interface pour appliquer la commande **no form et ainsi régler le port comme non sécurisé, étant donné qu'il s'agit d'IOS.**

### Ports sécurisés

Parfois, les trames Ethernet entrant dans un commutateur ont un paramètre CoS ou ToS que l'administrateur veut maintenir dans le commutateur lorsque la trame transite par celui-ci. L'administrateur peut définir l'état sécurisé d'un port à l'endroit considéré comme sécurisé, où le trafic entre dans le commutateur.

Comme mentionné précédemment, le commutateur utilise une valeur DSCP à l'interne pour attribuer un niveau de service prédéterminé à cette trame. Lorsqu'une trame entre dans un port sécurisé, l'administrateur peut configurer le port afin qu'il examine la valeur CoS, la priorité IP, ou la valeur DSCP existante afin de définir la valeur DSCP interne. Sinon, l'administrateur peut régler un DSCP prédéfini pour chaque paquet qui entre dans le port.

Il est possible de configurer un port à l'état sécurisé au moyen de la commande suivante :

### CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

Cette commande s'applique à la carte de ligne WS-X6548-RJ45 et paramètre l'état du port 3/16 à « sécurisé ». Le commutateur utilisera la valeur CoS définie dans la trame entrante pour configurer le DSCP interne. Le DSCP est obtenu d'une carte par défaut créée lors de l'activation de la QoS sur le commutateur ou d'une carte définie par l'administrateur. Au lieu du mot clé « trust-COs », l'administrateur peut également utiliser les mots clés « trust-dscp » ou « trust-ipprec ».

Sur les cartes de ligne 10/100 précédentes (WS-X6348-RJ45 et WS-X6248-RJ45), l'état sécurisé du port doit être configuré au moyen de la commande **set qos acl.** Dans cette commande, un état de confiance peut être octroyé par un sous-paramètre de la commande **set qos acl.** La configuration d'une CoS sécurisée sur les ports de ces cartes de ligne n'est pas prise en charge, comme il est illustré ci-dessous.

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so port is set to untrusted.
```

La commande précédente indique qu'elle est nécessaire pour activer la planification de la file d'attente d'entrée. Ainsi, en ce qui concerne les ports 10/100 sur les cartes de lignes WS-X6248-RJ45 et WS-X6348-RJ45, la commande **set port qos x/y trust trust-COs doit toujours être configurée, même si l'ACL doit être utilisée pour définir l'état sécurisé.**

Avec Cisco IOS intégré (mode natif), le réglage de l'état sécurisé peut être effectué sur une interface GE et des ports 10/100 sur la nouvelle carte de ligne WS-X6548-RJ45.

### Cisco IOS intégré (mode natif)

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

Cet exemple définit l'état sécurisé du port GE 5/4. La valeur de priorité IP de la trame sera utilisée pour générer la valeur DSCP.

## Classification des entrées et configuration de la CoS basée sur les ports

En entrant dans un port de commutation, une trame Ethernet peut changer sa CoS si elle répond à l'un des deux critères suivants :

1. le port est configuré comme port non sécurisé,
2. la trame Ethernet n'a pas encore de valeur CoS.

Si vous souhaitez reconfigurer la CoS d'une trame Ethernet entrante, vous devez utiliser la commande suivante :

### CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

Cette commande définit les CO des trames Ethernet entrantes sur le port 16 du module 3 à une valeur de 3 si une trame sans marque arrive ou si le port est configuré comme non sécurisé.

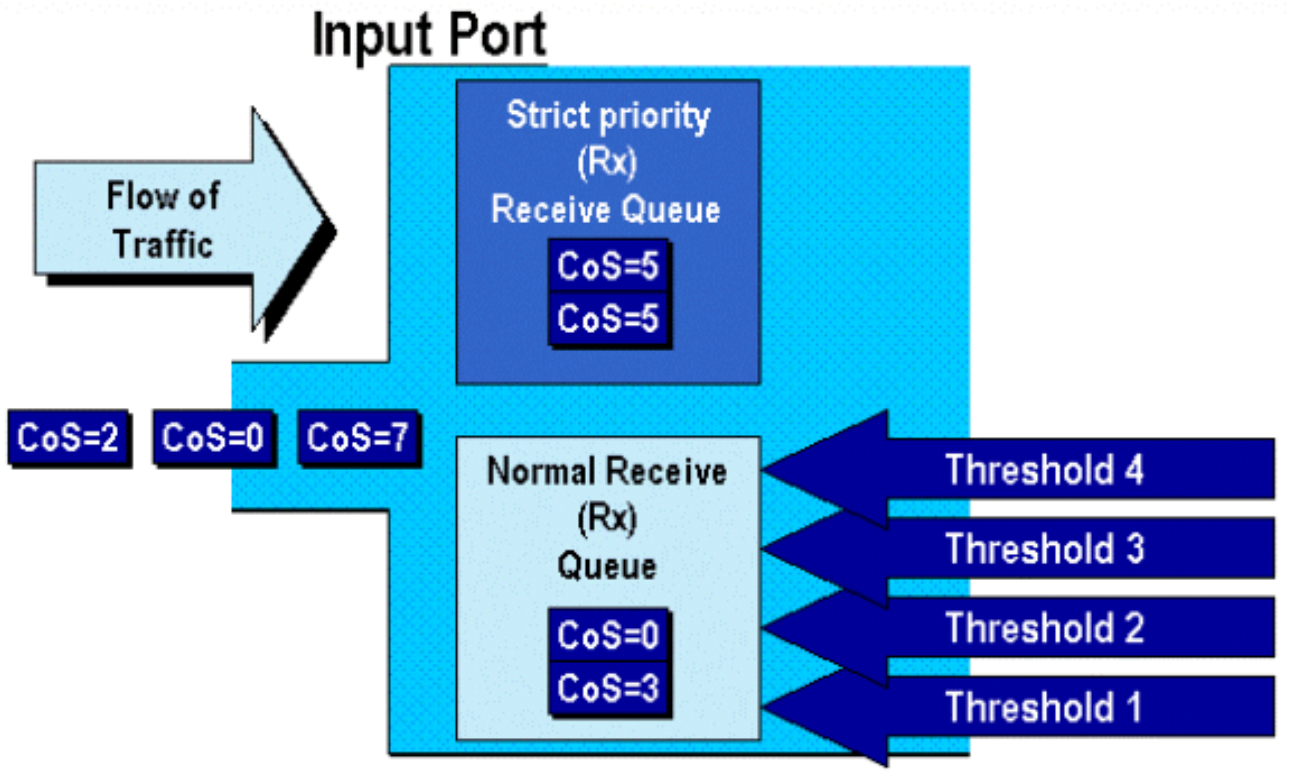
### Cisco IOS intégré (mode natif)

```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

Cette commande définit les CO des trames Ethernet entrantes sur le port 13 du module 5 à une valeur de 4 si une trame sans marque arrive ou si le port est configuré comme non sécurisé.

## Configurer les seuils de suppression pour la file d'attente Rx

En entrant dans le port de commutation, la trame sera placée dans une file d'attente Rx. Pour éviter les débordements des tampons, l'ASIC du port met en œuvre quatre seuils sur chaque file d'attente Rx et utilise ces seuils pour cibler les trames pouvant être supprimées lorsque ces seuils auront été franchis. L'ASIC du port utilisera la valeur des CO des trames pour déterminer quelles trames peuvent être supprimées lorsqu'un seuil est franchi. Cette fonctionnalité permet aux trames de priorité supérieure de rester dans la mémoire tampon plus longtemps en cas de congestion.




Comme le montre le schéma ci-dessus, les trames arrivent et sont ensuite placées dans la file d'attente. Lorsque la file d'attente commence à se remplir, les seuils sont surveillés par l'ASIC du port. Lorsqu'un seuil est franchi, les trames ayant des valeurs CO déterminées par l'administrateur

sont supprimées aléatoirement de la file d'attente. Les mappages des seuils par défaut pour une file d'attente 1q4t (figurant sur les cartes de lignes WS-X6248-RJ45 et WS-X6348-RJ45) vont comme suit :

- le seuil 1 est fixé à 50 %, et les valeurs CO 0 et 1 sont mappées avec ce seuil;
- le seuil 2 est fixé à 60 %, et les valeurs CO 2 et 3 sont mappées avec ce seuil;
- le seuil 3 est fixé à 80 %, et les valeurs CO 4 et 5 sont mappées avec ce seuil;
- le seuil 4 est fixé à 100 %, et les valeurs CO 6 et 7 sont mappées avec ce seuil;

Pour une file d'attente 1P1q4t (qui se situe sur les ports GE), les mappages par défaut sont les suivants :

- le seuil 1 est fixé à 50 %, et les valeurs CO 0 et 1 sont mappées avec ce seuil;
- le seuil 2 est fixé à 60 %, et les valeurs CO 2 et 3 sont mappées avec ce seuil;
- le seuil 3 est fixé à 80 %, et les valeurs CO 4 sont mappées avec ce seuil;
- le seuil 4 est fixé à 100 %, et les valeurs CO 6 et 7 sont mappées avec ce seuil;
- la valeur CO 5 est mappée avec la file d'attente à priorité stricte.

Pour un 1p1q0t (figurant sur les ports 10/100 de la carte de ligne WS-X6548-RJ45), les mappages par défaut sont les suivants :

- Les trames assorties de CO 5 vont dans la file d'attente SP Rx (file d'attente 2), où le commutateur supprime les trames entrantes seulement si la mémoire tampon de la file d'attente de réception SP est pleine à 100 %.
- Les trames ayant des valeurs CO 0, 1, 2, 3, 4, 6 ou 7 sont acheminées vers la file d'attente Rx standard. Le commutateur supprime alors les trames entrantes lorsque la mémoire tampon de la file d'attente Rx est pleine à 100 %.

Ces seuils de suppression peuvent être modifiés par l'administrateur. De plus, les valeurs CO par défaut qui sont mappées avec chaque seuil peuvent également être modifiées. Différentes cartes de ligne mettent en œuvre diverses files d'attente Rx. Un résumé des types de files d'attente est présenté ci-dessous.

### CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

Cette commande fixe les seuils de suppression Rx pour les ports d'entrée ayant une file d'attente et quatre seuils (soit 1q4t) à 20 %, 40 %, 75 % et 100 %.

La commande utilisée dans Cisco IOS intégré (mode natif) est illustrée ci-dessous.

### Cisco IOS intégré (mode natif)

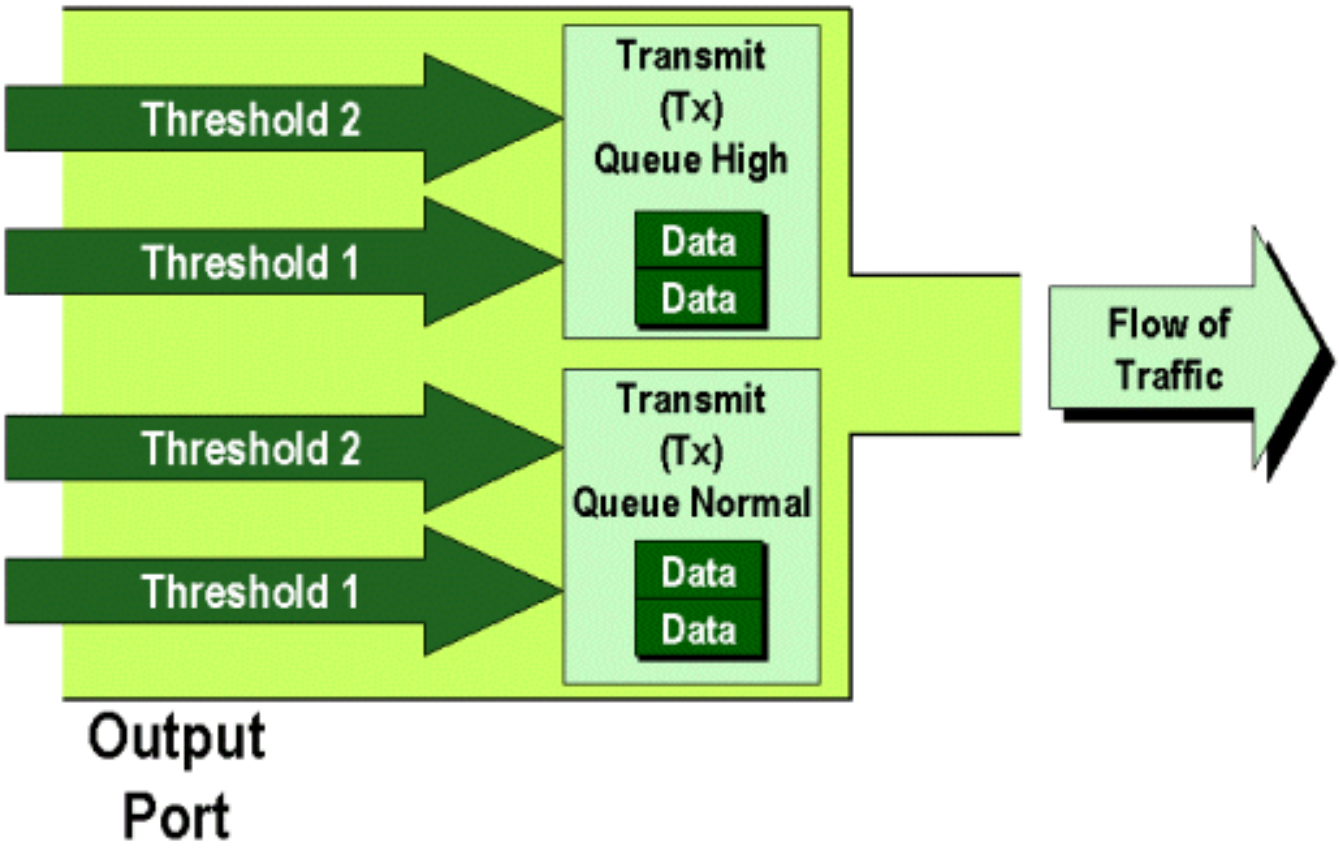
```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100
```

```
!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line card.
```

Les seuils de suppression Rx doivent être activés par l'administrateur. Actuellement, la commande **set port qos x/y trust trust-COs doit être utilisée pour activer les seuils de suppression Rx (où** *x est le numéro de module, et y est le port du module).*

## Configuration des seuils de suppression TX

Sur un port de sortie, le port aura deux seuils TX qui sont utilisés dans le cadre du mécanisme d'évitement de congestion, la file d'attente 1 et la file d'attente 2. La file d'attente 1 est désignée comme file d'attente de priorité basse standard et la file d'attente 2 comme file d'attente de priorité haute standard. Selon les cartes de ligne employées, une méthode d'élimination ou un algorithme de gestion du seuil WRED sera utilisé. Les deux algorithmes utilisent deux seuils pour chaque file d'attente TX.




Voici comment l'administrateur peut régler manuellement ces seuils :

### CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

Cette commande fixe les seuils de suppression TX pour la file d'attente 1 à tous les ports de sortie ayant deux files d'attente et deux seuils (soit 2q2t) à 40 % et à 100 %.

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
```

```
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

Cette commande fixe les seuils de suppression WRED pour la file d'attente 1 à tous les ports de sortie ayant deux files d'attente SP, deux files d'attente normales et deux seuils (soit 1p2q2t) à 60 % et à 100 %. La file d'attente 1 est désignée comme la file d'attente normale de faible priorité et a la plus basse priorité. La file d'attente 2 est la file d'attente normale de priorité élevée et a une priorité plus élevée que la file d'attente 1. La file d'attente 3 est la file d'attente SP et est traitée avant toutes les autres files d'attente sur ce port.

La commande équivalente utilisée dans Cisco IOS intégré (mode natif) est indiquée ci-dessous.

### Cisco IOS intégré (mode natif)

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
Cat6500(config-if)#
```

Cette commande fixe les seuils de suppression WRED de la file d'attente 1 d'un port 1p2q2t à 40 % pour le seuil 1 (TX) et à 100 % pour le seuil 2 (TX).

WRED peut également être désactivé, s'il y a lieu, dans Cisco IOS intégré (mode natif). Il faut, pour ce faire, se servir de la méthode consistant à utiliser la forme **n" de la commande.** Voici un exemple de désactivation de WRED :

### Cisco IOS intégré (mode natif)

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

## Mappage de l'adresse MAC aux valeurs CO

En plus de définir les CO en fonction d'une définition de port globale, le commutateur permet à l'administrateur de fixer des valeurs CO selon l'adresse MAC de destination et l'identifiant du VLAN. Ainsi, les trames destinées à des cibles précises peuvent être étiquetées à une valeur CO prédéterminée. Cette configuration peut être obtenue au moyen de la commande suivante :

### CatOS

```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

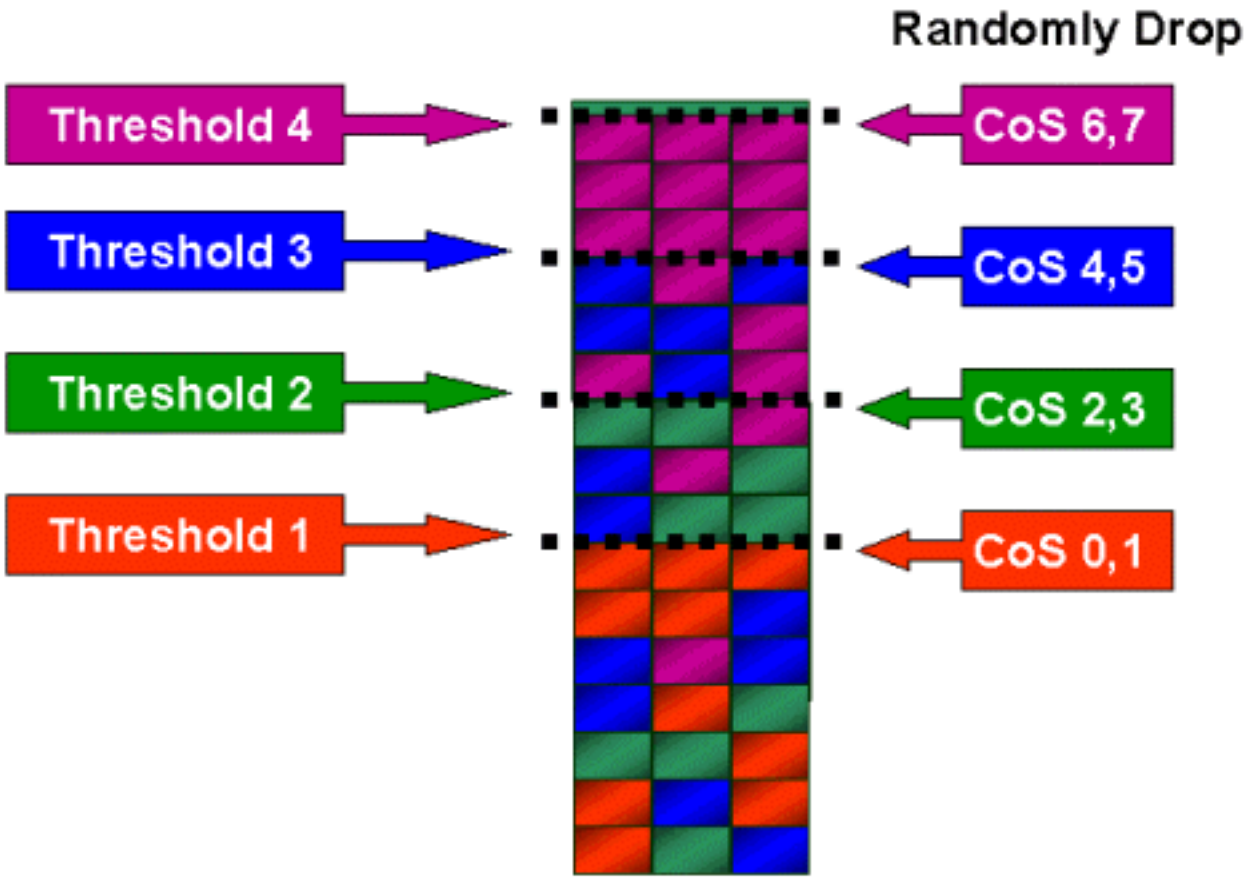
Cette commande définit un CO de 5 pour toute trame dont l'adresse MAC de destination est 00-00-0c-33-2a-4e provenant du VLAN 200.

Cisco IOS intégré (mode natif) n'offre pas de commande équivalente. En effet, cette commande est prise en charge seulement si aucune PFC n'est présente et si Cisco IOS intégré (mode natif) nécessite une PFC pour fonctionner.

## Mappage des CO avec les seuils

Après la configuration des seuils, l'administrateur peut alors leur octroyer des valeurs CO. Ainsi, lorsque le seuil est franchi, les trames assorties de valeurs CO précises peuvent être supprimées.

En général, l'administrateur attribuera des trames à faible priorité aux seuils inférieurs, maintenant ainsi le trafic à priorité élevée dans la file d'attente en cas de congestion.




La figure ci-dessus illustre une file d'attente d'entrée ayant quatre seuils et montre comment les valeurs de CO ont été octroyées à chaque seuil.

La sortie suivante illustre comment les valeurs de CO peuvent être mappées à des seuils :

### CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

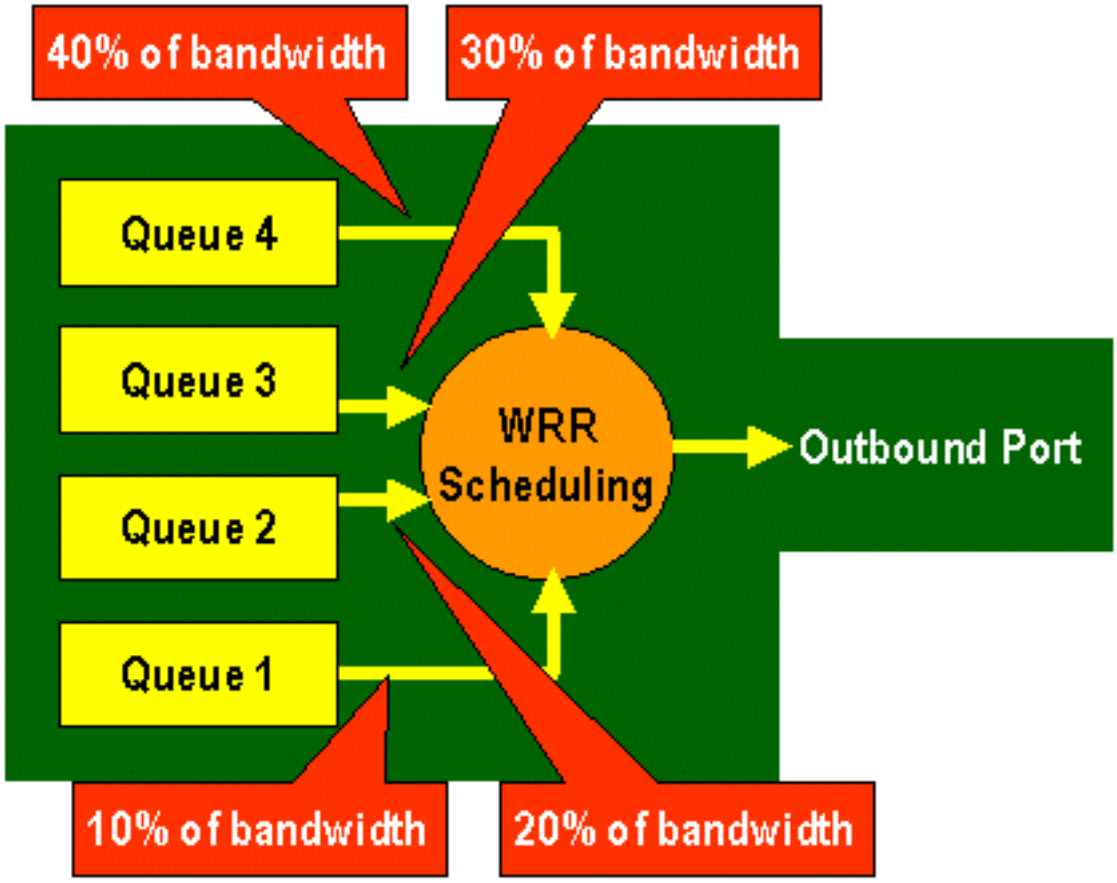
Cette commande octroie des valeurs CO de 0 et 1 à la file d'attente 1, seuil 1. La commande équivalente dans Cisco IOS intégré (mode natif) est illustrée ci-dessous.

### Cisco IOS intégré (mode natif)

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

## Configurer la bande passante sur les files d'attente TX

Lorsqu'une trame est placée dans une file d'attente de sortie, elle est transmise à l'aide d'un algorithme de planification de sortie. Le processus du planificateur de sortie utilise WRR pour transmettre les trames à partir des files d'attente de sortie. Selon le matériel de carte de ligne utilisé, il y a deux, trois ou quatre files d'attente de transmission par port.




Sur les cartes de ligne WS-X6248 et WS-X6348 (utilisant des structures de file d'attente 2q2t), deux files d'attente TX sont utilisées par le mécanisme WRR pour la planification. Sur les cartes de ligne WS-X6548 (utilisant une structure de file d'attente 1p3q1t) figurent quatre files d'attente TX. Parmi ces quatre files d'attente, trois sont traitées selon l'algorithme WRR (la dernière est une file d'attente SP). Sur les cartes de ligne GE figurent trois files d'attente TX (utilisant une structure de file d'attente 1p2q2t). L'une d'elles représente une file d'attente SP, et donc l'algorithme WRR ne dessert que deux files d'attente TX.

Généralement, l'administrateur attribuera une pondération à la file d'attente TX. WRR fonctionne en examinant la pondération attribuée à la file d'attente de port, qui est utilisée à l'interne par le commutateur pour déterminer la quantité de trafic qui sera transmise avant de passer à la file d'attente suivante. Une valeur de pondération comprise entre 1 et 255 peut être octroyée à chaque file d'attente de port.

### CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

Cette commande attribue une pondération de 40 à la file d'attente 1 et de 80 à la file d'attente 2. À toutes fins utiles, cela représente un rapport de deux pour un (80 à 40 = 2 à 1) de bande passante attribuée entre les deux files d'attente. Cette commande agit sur tous les ports dotés de deux files d'attente et de deux seuils.

La commande équivalente utilisée dans Cisco IOS intégré (mode natif) est indiquée ci-dessous.

### Cisco IOS intégré (mode natif)

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

Ce qui précède représente un rapport de trois pour un entre les deux files d'attente. Vous constaterez que la version Cat IOS de cette commande s'applique seulement à une interface donnée.

### Mappage de DSCP vers les CO

Lorsque la trame a été placée dans le port de sortie, l'ASIC du port utilisera les CO applicables pour éviter la congestion (c'est-à-dire WRED) et également pour déterminer la planification de la trame (sa transmission). À ce stade, le commutateur se servira d'une carte par défaut pour prendre le DSCP attribué et le mapper à une valeur CO. Cette carte par défaut est affichée dans ce tableau.

Sinon, l'administrateur peut créer une carte qu'utilisera le commutateur pour prendre la valeur DSCP interne attribuée et créer une nouvelle valeur CO pour la trame. Voici des exemples de l'utilisation de CatOS et de Cisco IOS intégré (mode natif) pour y parvenir.

#### CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

La commande ci-dessus fait correspondre les valeurs DSCP de 20 à 30 avec une valeur CO de 5, les valeurs DSCP de 10 à 15 avec une valeur CO de 3, et les valeurs DSCP de 45 à 52 avec une valeur CO de 7. Toutes les autres valeurs DSCP utilisent la carte par défaut créée lorsque la QoS a été activée sur le commutateur.

La commande équivalente utilisée dans Cisco IOS intégré (mode natif) est indiquée ci-dessous.

#### Cisco IOS intégré (mode natif)

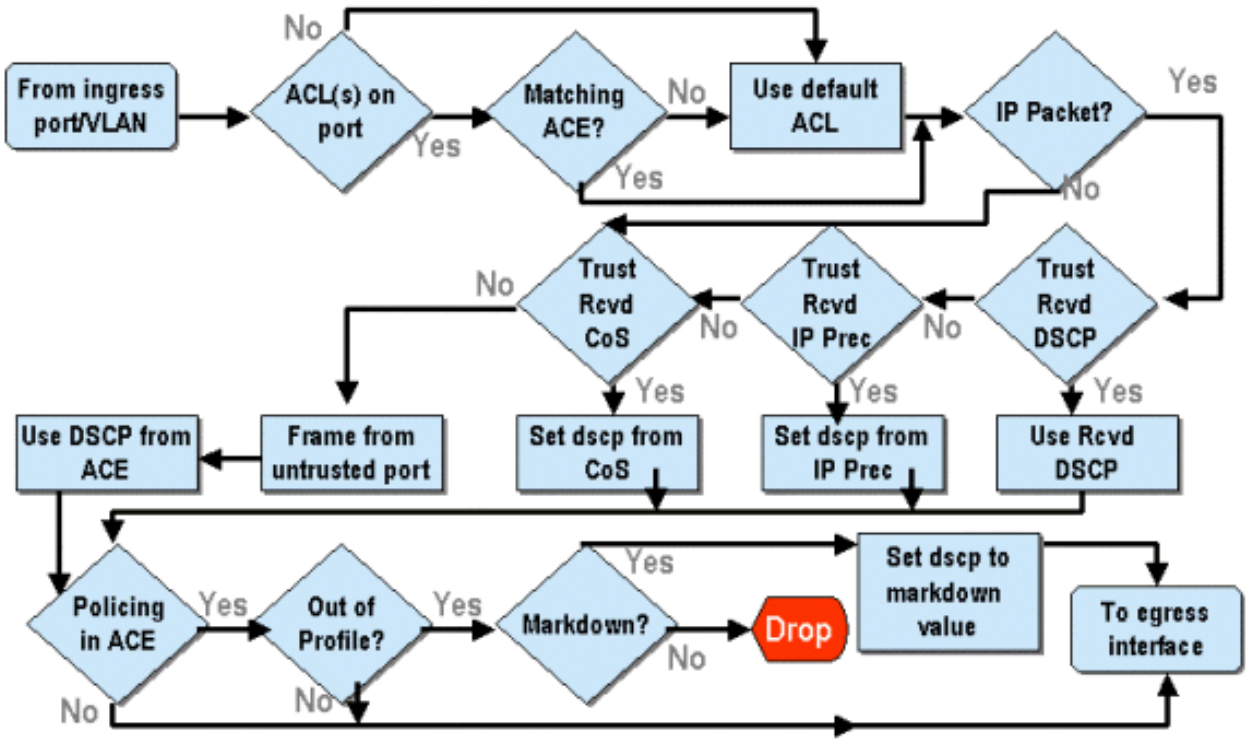
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

Les valeurs DSCP 20, 30, 40, 50, 52, 10 et 1 sont ainsi réglées à une valeur CO de 3.

## Classification et contrôle grâce à la carte PFC

La PFC prend en charge la classification et le contrôle des trames. La classification peut utiliser une ACL pour attribuer (marquer) une priorité (DSCP) à une trame entrante. Le contrôle permet de limiter un flux de trafic à une certaine quantité de bande passante.

Les sections suivantes décrivent ces fonctionnalités sur la PFC du point de vue de la plateforme CatOS et du système d'exploitation Cisco IOS intégré (mode natif). Les processus appliqués par la PFC sont illustrés dans le schéma suivant :




## Configurer le contrôle sur la gamme Catalyst 6000 avec CatOS

La fonction de contrôle est divisée en deux sections : une pour CatOS et une pour Cisco IOS intégré (mode natif). Les deux obtiennent le même résultat, mais leur configuration et leur mise en œuvre sont différentes.

### Contrôle

La PFC prend en charge la capacité de limiter (ou de contrôler) le débit du trafic entrant vers le commutateur et peut réduire le flux du trafic à une limite prédéterminée. Le trafic dépassant cette limite peut être supprimé, ou la valeur DSCP dans la trame peut être réduite à une valeur inférieure.

La limitation du débit de sortie n'est actuellement pas prise en charge dans la PFC1 ou la PFC2. Cette fonction sera ajoutée dans une nouvelle révision de la PFC prévue pour le deuxième semestre de 2002, qui prendra en charge le contrôle de sortie.

Le contrôle est pris en charge dans CatOS et la nouvelle version de Cisco IOS intégré (mode natif), bien que la configuration de ces fonctionnalités soit très différente. Les sections suivantes expliqueront la configuration du contrôle sur les deux plateformes de système d'exploitation.

### Agrégats et microflux (CatOS)

Les agrégats et les microflux sont des termes utilisés pour définir la portée des contrôles qu'effectue la PFC.

Un microflux détermine le contrôle d'un seul flux. Un flux est défini par une session dotée d'une adresse MAC SA/DA unique, d'une adresse IP SA/DA et des numéros de port TCP/UDP. Pour chaque nouveau flux amorcé par un port de réseau VLAN, le microflux peut être utilisé pour limiter la quantité de données que reçoit le commutateur pour ce flux. Dans la définition du microflux, les paquets qui franchissent la limite de débit prescrite peuvent être supprimés ou voir leur valeur DSCP diminuée.

De façon comparable à un microflux, un agrégat peut être utilisé pour évaluer la limite de débit du trafic. Toutefois, le débit de l'agrégat s'applique à l'ensemble du trafic entrant sur un port ou un VLAN, qui correspond à une ACL de QoS donnée. Vous pouvez considérer l'agrégat comme le contrôle du trafic cumulé correspondant au profil dans l'entrée de contrôle d'accès (ACE).

L'agrégat et le microflux définissent tous deux la quantité de trafic pouvant être acceptée dans le commutateur. Un agrégat et un microflux peuvent être affectés simultanément à un port ou à un réseau VLAN.

Un maximum de 63 microflux et de 1 023 agrégats peuvent être définis.

### Entrées de contrôle d'accès et ACL de QoS (CatOS)

Une ACL de QoS se compose d'ACE définissant un ensemble de règles de QoS que la PFC utilise pour traiter les trames entrantes. Les ACE sont comparables à une liste de contrôle d'accès du routeur (RACL). L'ACE définit les critères de classification, de marquage et de contrôle pour une trame entrante. Si une trame entrante correspond aux critères établis dans l'ACE, le moteur de QoS traitera la trame (comme le juge l'ACE).

Tout le traitement de la QoS est réalisé au niveau du matériel, et donc l'activation du contrôle de la QoS n'a aucune incidence sur la performance du commutateur.

La carte PFC2 peut actuellement prendre en charge 500 ACL et être composée de 32 000 ACE (au total). Le nombre d'ACE réel dépendra des autres services définis et de la mémoire utilisable dans la PFC.

Trois types d'ACE peuvent être définis. Il s'agit des types IP, IPX et MAC. Les ACE IP et IPX inspectent les informations de l'en-tête L3, tandis que les ACE MAC ne vérifient que celles de l'en-tête L2. Soulignons que les ACE MAC peuvent être appliquées seulement au trafic sans IP et sans IPX.

### Création des règles de contrôle

Le processus de création d'une règle de contrôle comprend la création d'un agrégat (ou microflux), puis le mappage de l'agrégat (ou microflux) avec une ACE.

S'il fallait, par exemple, limiter tout le trafic IP entrant sur le port 5/3 à un maximum de 20 Mbit, les deux étapes mentionnées ci-dessus devraient être configurées.

D'abord, dans l'exemple, tout le trafic IP entrant doit être limité. Par conséquent, un contrôleur d'agrégat doit être défini. En voici un exemple :

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

Nous avons créé un agrégat appelé « flux de test ». Il définit un débit de 20 000 kbit/s (20 Mbit/s) et une rafale de 13. Le mot clé « policed-dscp » indique que toutes données dépassant ce contrôle verront leur valeur DSCP réduite comme il est mentionné dans une carte de diminution DSCP (une valeur un par défaut existe ou peut être modifiée par l'administrateur). Un autre moyen d'utiliser le mot clé « policed-dscp » est d'utiliser le mot clé « drop ». Le mot clé « drop » supprimera simplement tout le trafic hors profil (le trafic qui ne correspond pas à la valeur de rafale attribuée).

Le contrôle fonctionne sur un schéma de seau à jetons qui fuit (seau percé), et par conséquent vous définissez une rafale (qui représente la quantité de données en bits par seconde que vous accepterez dans un intervalle donné [fixe]), puis le débit (soit la quantité de données que vous retirez de ce compartiment en une seconde). Toutes les données qui débordent du seau sont supprimées ou verront leur valeur DSCP réduite. La période (ou l'intervalle) indiquée ci-dessus est de 0,00025 seconde (ou 1/4000e de seconde) et est fixe (c'est-à-dire qu'aucune commande de configuration ne vous permettra de modifier ce nombre).

Le nombre 13 de l'exemple ci-dessus représente un seau qui acceptera tout au plus 13 000 bits de données tous les 1/4000e de seconde. Cela correspond à 52 Mbit par seconde (13 Ko * [1/0,00025] ou 13 Ko * 4 000). Vous devez toujours vous assurer que votre rafale est configurée de manière à être égale ou supérieure à la vitesse souhaitée de l'envoi des données. Autrement dit, la rafale doit être supérieure ou égale à la quantité minimale de données que vous souhaitez transmettre pour une période donnée. Si la rafale donne un nombre inférieur au débit que vous avez précisé, la limite de débit sera alors égale à la rafale. En d'autres mots, si vous établissez un débit de 20 Mbit/s et une rafale qui calcule à 15 Mbit/s, votre débit ne sera jamais que de 15 Mbit/s. La prochaine question que vous pourriez vous poser est « pourquoi 13 »? Rappelez-vous que la rafale définit la profondeur du seau à jetons, soit la profondeur du seau utilisé pour recevoir les données entrantes tous les 1/4000e de seconde. Ainsi, la rafale pourrait être n'importe quel nombre pris en charge sur un débit de données d'arrivée supérieur ou égal à 20 Mbit par seconde. La rafale minimale pouvant être utilisée pour une limite de débit de 20 Mbit est de 20 000/4 000 = 5.

Lors du traitement du contrôleur, l'algorithme de contrôle commence par remplir le seau à jetons avec un ensemble complet de jetons. Le nombre de jetons équivaut à la valeur de la rafale. Par conséquent, si la valeur de la rafale est de 13, le nombre de jetons dans le seau est égal à 13 000. Pour chaque 1/4000e de seconde, l'algorithme de contrôle enverra une quantité de données équivalant au débit établi divisé par 4 000. Pour chaque bit (chiffre binaire) de données envoyé, un jeton du compartiment est consommé. À la fin de l'intervalle, le seau est réapprovisionné en jetons issus d'un nouvel ensemble. Le nombre de jetons qu'il remplace est défini par le débit / 4 000. Prenons l'exemple ci-dessus pour comprendre ce qui suit :

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

Supposons qu'il s'agisse d'un port à 100 Mbit/s et que nous envoyions un flux constant de 100 Mbit/s dans le port. Nous savons que la valeur équivaudra alors à un débit entrant de 100 000 000 bits par seconde. Les paramètres ici représentent un débit de 20 000 et une rafale de 13. À l'intervalle de temps t0, le seau contient un ensemble complet de jetons (soit 13 000). À un intervalle de temps t0, le premier ensemble de données arrivera dans le port. Pour cet intervalle, le débit d'arrivée sera de 100 000 000/4 000 = 25 000 bits par seconde. Comme notre seau à jetons a seulement une profondeur de 13 000 jetons, seuls 13 000 bits des 25 000 bits arrivant dans le port à cet intervalle peuvent être envoyés, et 12 000 bits sont supprimés.

Le débit indiqué établit un débit de transfert de 20 000 000 de bits par seconde, ce qui équivaut à 5 000 bits envoyés par intervalle de 1/4000e. Pour chaque tranche de 5 000 bits envoyés, 5 000 jetons sont utilisés. À un intervalle de temps T1, ce sont 25 000 bits de données supplémentaires qui arrivent, mais le seau supprime 12 000 bits. Le seau est réapprovisionné en jetons selon la valeur définie par le débit / 4 000 (ce qui équivaut à 5 000 nouveaux jetons). L'algorithme envoie ensuite l'ensemble de données suivant, équivalant à 5 000 bits de données supplémentaires (pour une consommation de 5 000 jetons supplémentaires), et ainsi de suite pour chaque intervalle.

Essentiellement, toute donnée excédant la profondeur du seau (rafale définie) est supprimée. Les données restantes après l'envoi des données (correspondant au débit indiqué) sont également supprimées, ce qui fait place à l'autre ensemble de données d'arrivée. Un paquet incomplet est un

paquet qui n'a pas été entièrement reçu pendant l'intervalle de temps. Au lieu d'être supprimé, il est conservé jusqu'à ce que le port l'ait entièrement reçu.

Ce nombre lié à la rafale suppose un flux de trafic constant. Cependant, dans les réseaux réels, les données ne sont pas constantes, et leur flux est déterminé par la taille des fenêtres TCP, où sont intégrés les accusés TCP dans la séquence de transmission. Pour prendre en considération les problèmes liés à la taille des fenêtres TCP, il est recommandé que soit doublée la valeur de rafale. Dans l'exemple ci-dessus, la valeur suggérée de 13 serait alors de 26.

Autre point important à souligner, à l'intervalle de temps 0 (c'est-à-dire au début d'un cycle de contrôle), le seau à jetons est rempli de jetons.

Ce contrôle d'agrégat doit maintenant être intégré dans une ACE de QoS. L'ACE représente l'endroit où est effectuée la spécification afin de faire correspondre un ensemble de critères à une trame entrante. Prenons l'exemple suivant : Vous souhaitez appliquer l'agrégat défini ci-dessus à tout le trafic IP, mais surtout au trafic provenant du sous-réseau 10.5.x.x et destiné au sous-réseau 203.100.45.x. L'ACE ressemblerait à ceci :

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

La commande ci-dessus a créé une ACE IP (désignée par l'utilisation de la commande **set qos acl ip), qui est maintenant associée à une ACL de QoS appelée « test-acl ».** Les ACE subséquentes qui sont associées à l'ACL « test-acl » sont ajoutés à la fin de la liste de l'ACE. L'ACE est associée à l'agrégat du flux de test. Un flux TCP ayant un sous-réseau source de 10.5.0.0 et un sous-réseau de destination de 203.100.45.0 appliqueront ce contrôle.

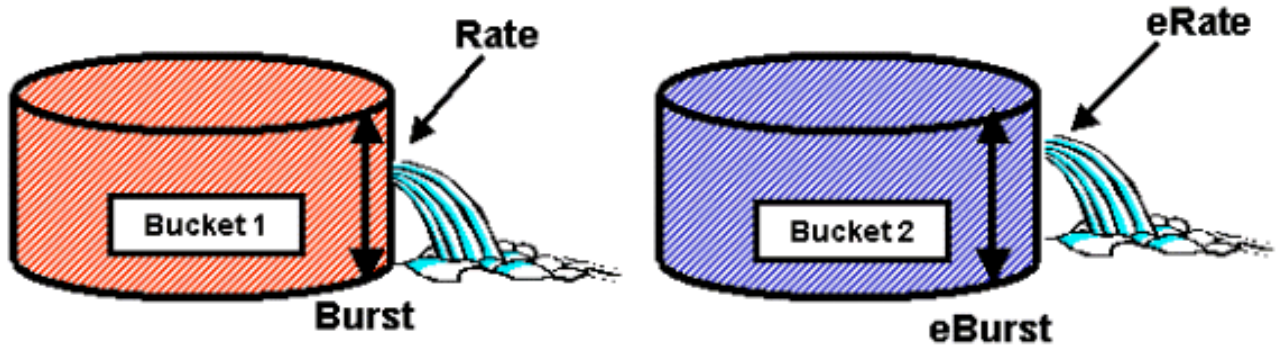
Les ACL (et les ACE connexes) offrent une flexibilité de configuration très granulaire que peuvent utiliser les administrateurs. Une ACL peut comprendre une ou plusieurs ACE, et les adresses source et de destination peuvent être utilisées ainsi que les valeurs du port L4 afin de cibler les flux à contrôler.

Toutefois, avant qu'un contrôle soit appliqué, l'ACL doit être mappée à un port physique ou à un VLAN.

### Décisions liées au contrôle de la PFC2

En ce qui concerne la PFC2, une modification a été apportée à CatOS 7.1 et CatOS 7.2, qui ont introduit un algorithme du double seau percé aux fins de contrôle. Grâce à ce nouvel algorithme, les deux niveaux suivants s'ajoutent :

1. **Niveau de contrôle normal :** Ce niveau équivaut au premier seau et définit les paramètres précisant la profondeur du seau (rafale) et la vitesse de l'envoi des données à partir du seau (débit).
2. **Niveau de contrôle excédentaire :** Ce niveau équivaut au deuxième seau et définit les paramètres précisant la profondeur du seau (rafale excédentaire) et la vitesse de l'envoi des données à partir du seau (débit excédentaire).




Dans ce processus, les données commencent à remplir le premier seau. La PFC2 accepte un flux entrant de données qui est inférieur ou égal à la profondeur (valeur de la rafale) du premier seau. Les données qui débordent du premier seau peuvent être réduites, puis transmises au deuxième seau. Le deuxième seau peut accepter un débit entrant de données provenant du premier seau, à une valeur inférieure ou égale à celle de la rafale excédentaire. Les données du deuxième seau sont envoyées à un débit déterminé par le paramètre de débit excédentaire moins le paramètre de débit. Les données qui débordent du deuxième seau peuvent également être réduites ou supprimées.

Voici un exemple de contrôleur du double seau percé :

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

Cet exemple met en place un agrégat appelé « AGG1 », dont le débit de trafic supérieur à 10 Mbit/s sera réduit en fonction de la carte DSCP contrôlée. Le trafic dépassant le débit (fixé à 12 Mbit/s) sera supprimé au moyen du mot clé « drop ».

### Application des contrôleurs d'agrégat aux modules compatibles avec la DFC

Notons que les contrôleurs d'agrégats peuvent être appliqués sur les cartes de lignes non compatibles avec la DFC en fonction de l'utilisation par les commutateurs 6000 d'un moteur de retransmission centralisé (PFC) pour réacheminer le trafic. La mise en œuvre d'un moteur de retransmission centralisé permet le suivi des statistiques concernant le trafic pour un réseau VLAN donné. Ce processus peut être utile pour l'application d'un contrôleur d'agrégat à un réseau VLAN.

Sur une carte de ligne compatible avec la DFC, cependant, les décisions de retransmission sont distribuées à cette carte. La DFC ne détecte que les ports de sa carte de ligne immédiate et non les mouvements du trafic sur les autres cartes de ligne. Pour cette raison, si un contrôleur d'agrégat est appliqué à un réseau VLAN qui a des ports membres sur plusieurs modules de la DFC, des résultats incohérents pourraient alors se produire. La raison réside dans le fait que la DFC peut seulement suivre les statistiques portant sur le port local et qu'elle ne tient pas compte des statistiques concernant les ports des autres cartes de ligne. Ainsi, un contrôleur d'agrégat qui est appliqué à un réseau VLAN doté de ports membres sur une carte de ligne compatible avec la DFC entraînera un trafic de contrôle de la DFC à la limite établie pour les ports du réseau VLAN résidant sur la carte de ligne DFC uniquement.

### Cartes de réduction DSCP (CatOS)

Les cartes de réduction DSCP sont utilisées lorsque le contrôleur est configuré pour réduire le trafic hors profil au lieu de le supprimer. On entend par « trafic hors profil » le trafic qui excède le paramètre de rafale établi.

Une carte de réduction DSCP utilisée par défaut est configurée lorsque la QoS est activée. Cette carte par défaut figure dans ce tableau, présenté précédemment. Grâce à l'interface de ligne de commande (CLI), un administrateur peut modifier la carte de réduction par défaut au moyen de la commande **set qos policed-dscp-map.** Un exemple est fourni ci-dessous.

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

Cet exemple vient modifier la carte DSCP contrôlée afin d'indiquer que les valeurs DSCP 20 à 25 seront réduites à une valeur DSCP de 7 et que les valeurs DSCP de 33 à 38 passeront à une valeur DSCP de 3.

### Mappage des contrôles avec les réseaux VLAN et les ports (CatOS)

Lorsqu'une ACL est créée, celle-ci doit être mappée avec un port ou un réseau VLAN pour prendre effet.

Une commande intéressante, qui évite bien des surprises, concerne le paramètre de QoS par défaut qui axe la QoS sur les ports. Si vous appliquez un agrégat (ou un microflux) à un réseau VLAN, il ne prendra effet sur un port que si ce dernier a été configuré pour une QoS basée sur le VLAN.

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

Le passage de la QoS basée sur les ports à la QoS basée sur les VLAN consiste à détacher immédiatement toutes les ACL associées à ce port pour lui attribuer toutes les ACL basées sur un VLAN.

Le mappage de l'ACL avec un port (ou un réseau VLAN) se fait au moyen de la commande suivante :

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

Même après avoir mappé l'ACL avec un port (ou un réseau VLAN), l'ACL en question ne prendra effet que lorsqu'elle sera affectée au matériel. Voir la section suivante à ce sujet. À ce stade, l'ACL se trouve dans une mémoire tampon d'édition temporaire. Dans ce tampon, l'ACL peut être modifiée.

Si vous souhaitez supprimer des ACL non validées qui résident dans la mémoire tampon d'édition, il vous faut utiliser la commande **rollback.** Cette commande supprime essentiellement l'ACL de la mémoire tampon d'édition.

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

### Validation des ACL (CatOS)

Pour appliquer l'ACL de la QoS que vous avez définie (ci-dessus), l'ACL doit être affectée au

matériel. Le processus de validation vient copier l'ACL du tampon temporaire sur le matériel de la PFC. Une fois dans la mémoire de la PFC, le contrôle qui est défini dans l'ACL de la QoS peut être appliqué au trafic correspondant aux ACE.

Pour faciliter la configuration, la plupart des administrateurs appliquent la commande **commit all.** Cependant, vous pouvez valider une ACL donnée (une parmi plusieurs) qui peut se trouver actuellement dans la mémoire tampon d'édition. Un exemple de cette commande est présenté ci-dessous.

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

Si vous souhaitez supprimer une ACL d'un port (ou d'un VLAN), vous devez effacer la carte qui associe cette ACL au port (ou au VLAN) grâce à la commande suivante :

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

## Configurer la fonction de contrôle sur la gamme Catalyst 6000 grâce à Cisco IOS intégré (mode natif)

Le contrôle est pris en charge par Cisco IOS intégré (mode natif). Toutefois, la configuration et la mise en œuvre de la fonction de contrôle sont réalisées à l'aide de cartes de contrôle. Chaque carte de contrôle est composée de plusieurs classes de contrôle, qui peuvent être définies pour différents types de flux de trafic.

Les classes des cartes de contrôles, lors du filtre, utilisent des ACL basées sur IOS et des instructions de mise en correspondance des classes pour déterminer quel trafic doit être contrôlé. Une fois le trafic déterminé, les classes de contrôle peuvent utiliser des contrôleurs d'agrégat et de microflux pour appliquer les contrôles au trafic correspondant.

Les sections suivantes expliquent plus en détail la configuration du contrôle pour Cisco IOS intégré (mode natif).

### Agrégats et microflux (Cisco IOS intégré [mode natif])

Les agrégats et les microflux sont des termes utilisés pour définir la portée des contrôles qu'effectue la PFC. De façon comparable à CatOS, les agrégats et les microflux sont également utilisés dans Cisco IOS intégré (mode natif).

Un microflux détermine le contrôle d'un seul flux. Un flux est défini par une session dotée d'une adresse MAC SA/DA unique, d'une adresse IP SA/DA et des numéros de port TCP/UDP. Pour chaque nouveau flux amorcé par un port de réseau VLAN, le microflux peut être utilisé pour limiter la quantité de données que reçoit le commutateur pour ce flux. Dans la définition du microflux, les paquets qui franchissent la limite de débit prescrite peuvent être supprimés ou voir leur valeur DSCP diminuée. Les microflux sont appliqués au moyen de la commande « police flow », qui fait partie d'une classe de carte de contrôle.

Pour fonctionner, le contrôle des microflux dans Cisco IOS intégré (mode natif) doit être activé sur l'ensemble du commutateur. Pour ce faire, vous pouvez utiliser la commande suivante :

```
Cat6500(config)# mls qos flow-policing
```

Le contrôle des microflux peut également s'appliquer au trafic ponté, qui n'est pas commuté sur la couche 3. Pour que le commutateur prenne en charge le contrôle des microflux sur le trafic ponté, utilisez la commande suivante :

```
Cat6500(config)# mls qos bridged
```

Cette commande active également le contrôle des microflux pour le trafic de multidiffusion. Si un contrôle de microflux doit être appliqué au trafic de multidiffusion, il faut alors activer cette commande (**mls qos bridged**).

De façon comparable à un microflux, un agrégat peut être utilisé pour évaluer la limite de débit du trafic. Toutefois, le débit de l'agrégat s'applique à l'ensemble du trafic entrant sur un port ou un VLAN, qui correspond à une ACL de QoS donnée. Vous pouvez considérer l'agrégat comme le contrôle du trafic cumulé correspondant au profil du trafic défini.

Deux formes d'agrégats peuvent être indiquées dans Cisco IOS intégré (mode natif), comme suit :

- les contrôleurs d'agrégats par interface;
- les contrôleurs d'agrégats nommés.

Les agrégats par interface s'appliquent à une interface individuelle à l'aide de la commande **police dans une classe de carte de contrôle.** Ces classes de carte peuvent être appliquées à plusieurs interfaces, mais le contrôleur gère chaque interface séparément. Les agrégats nommés s'appliquent quant à eux à un groupe de ports et contrôlent le trafic sur l'ensemble des interfaces de façon cumulative. Les agrégats nommés s'appliquent grâce à la commande **mls qos aggregate policer.**

Un maximum de 63 microflux et de 1 023 agrégats peuvent être définis.

### Création de règles de contrôle (Cisco IOS intégré [mode natif])

Le processus de création de règles de contrôle comporte la formation d'un agrégat (ou microflux) au moyen d'une carte de contrôle, qui sera ensuite associée à une interface.

Prenons l'exemple créé pour le CatOS. La condition était de limiter tout le trafic IP entrant sur le port 5/3 à un maximum de 20 Mbit/s.

D'abord, une carte de contrôle doit être créée. Créez une carte de contrôle nommée « limit-traffic ». Procédez ainsi :

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

Vous remarquerez immédiatement que l'invite du commutateur change pour signaler que vous êtes en mode de configuration pour la création d'une classe de carte. Rappelez-vous qu'une carte de contrôle peut contenir plusieurs classes. Chaque classe contient un ensemble distinct de contrôles pouvant s'appliquer à différents flux de trafic.

Nous devrions créer une classe de trafic qui limiterait, en particulier, le trafic entrant à 20 Mbit/s.

Nous appellerons cette classe « limit-to-20 ». Voir ci-dessous.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

Une fois de plus, l'invite change, cette fois pour signaler que vous êtes désormais en mode de configuration pour la classe de la carte (indiqué par « -c » à la fin de l'invite). Si vous souhaitez appliquer la limite de débit pour que celui-ci corresponde à un trafic entrant en particulier, vous pouvez configurer une ACL, que vous appliquerez au nom de la classe. Si vous souhaitez appliquer la limite de 20 Mbit/s au trafic provenant du réseau 10.10.1.x, utilisez l'ACL suivante :

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

Vous pouvez ajouter cette ACL au nom de la classe comme suit :

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

Lorsque vous avez défini votre carte, vous pouvez désormais choisir des contrôleurs individuels pour la classe en question. Vous pouvez créer des agrégats (au moyen du mot clé « police ») ou des microflux (au moyen du mot clé « police flow »). Procédez comme suit pour créer l'agrégat.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

Les instructions de la classe ci-dessus (commande **police) fixent une limite de débit de 20 000 kbit/s (20 Mbit/s) avec une rafale de 52 Mbit/s (13 000 x 4 000 = 52 Mbit).** Si le trafic correspond au profil et se situe dans la limite établie, l'action doit alors être réglée grâce à l'instruction « confirme-action » pour que soit acheminé le trafic dans le profil. Si le trafic est hors profil (dans notre exemple, supérieur à la limite de 20 Mbit), l'instruction « exceed-action » est saisie pour supprimer le trafic (dans notre exemple, le trafic supérieur à 20 Mbit est supprimé).

Lors de la configuration d'un microflux, une action semblable est entreprise. Si nous voulions limiter à 200 kbit le débit de chaque flux dans un port correspondant à une classe de carte donnée, la configuration des flux ressemblerait à ceci :

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

### Cartes de réduction DSCP

Les cartes de réduction DSCP sont utilisées lorsque le contrôleur est configuré pour réduire le trafic hors profil au lieu de le supprimer. On entend par « trafic hors profil » le trafic qui excède le paramètre de rafale établi.

Une carte de réduction DSCP par défaut est établie lorsque la QoS est activée. Cette carte par défaut figure dans ce tableau. Grâce à l'interface de ligne de commande (CLI), un administrateur peut modifier la carte de réduction par défaut au moyen de la commande **set qos policed-dscp-map.** Un exemple est fourni ci-dessous.

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

Cet exemple illustre une modification de la carte DSCP contrôlée par défaut qui fait passer la valeur DSCP de 32 à 16. Pour un port assorti d'un tel contrôleur, les données entrantes qui ont cette valeur DSCP et qui font partie d'un bloc de données dépassant la rafale fixée verront leur valeur DSCP réduite à 16.

### Mappage des contrôles aux réseaux VLAN et aux ports (Cisco IOS intégré [mode natif])

Lorsqu'un contrôle est créé, celui-ci doit être mappé à un port ou à un réseau VLAN pour prendre effet. Contrairement au processus de validation dans CatOS, Cisco IOS intégré (mode natif) n'offre pas de commande équivalente. Lorsqu'un contrôle est mappé à une interface, ce contrôle entre en vigueur. Pour mapper le contrôle ci-dessus à une interface, utilisez la commande suivante :

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

Si un contrôle est mappé à un réseau VLAN, pour chaque port du réseau VLAN auquel vous souhaitez appliquer le contrôle, vous devez, à l'aide de la commande **mls qos vlan-based, informer l'interface que la QoS repose sur le VLAN.**

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

En supposant que l'interface 3/5 fasse partie du réseau VLAN 100, le contrôle « limit-traffic », qui était appliqué au réseau VLAN 100, s'appliquerait également à l'interface 3/5.

## Configurer la classification sur la gamme Catalyst 6000 avec CatOS

La PFC intègre la prise en charge de la classification des données au moyen des ACL pouvant afficher les informations d'en-tête L2, L3 et L4. Pour le SupI ou l'IA (sans la PFC), la classification est limitée à l'utilisation des mots clés sécurisés sur les ports.

La section suivante décrit les composants de configuration de la QoS utilisés par la PFC pour la classification dans CatOS.

### Mappage des CO avec DSCP (CatOS)

En entrant dans le commutateur, une trame aura une valeur DSCP définie par le commutateur. Si le port est dans un état sécurisé et si l'administrateur a utilisé le mot clé « trust-COs », la valeur des CO qui est définie dans la trame servira à déterminer la valeur DSCP fixée pour la trame. Comme il est mentionné précédemment, le commutateur peut attribuer, selon la valeur DSCP interne, des niveaux de service à la trame lorsqu'elle transite par le commutateur.

Ce mot clé sur certains modules 10/100 précédents (WS-X6248 et WS-X6348) n'est pas pris en charge. Pour ces modules, il est recommandé d'utiliser les ACL pour appliquer les paramètres CO sur les données entrantes.

Lorsque la QoS est activée, le commutateur crée une carte par défaut. Cette carte permettra de déterminer la valeur du DSCP qui sera fixée selon la valeur des CO. Ces cartes sont répertoriées dans ce tableau, vu précédemment dans le document. Sinon, l'administrateur peut configurer une carte unique. Un exemple est fourni ci-dessous.

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

La commande ci-dessus définit la carte suivante :

| CoS | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Bien qu'il soit très peu probable que la carte ci-dessus soit utilisée dans un réseau réel, elle sert à donner une idée de ce qui peut être réalisé lors de l'utilisation de cette commande.

### Mappage de la priorité IP avec DSCP (CatOS)

De façon comparable au mappage de CO avec DSCP, une trame peut avoir une valeur DSCP déterminée à partir du paramètre de priorité IP des paquets entrants. C'est possible seulement si l'administrateur a mis le port à l'état sécurisé et qu'il a utilisé le mot clé « trust-ipprec ».

Lorsque la QoS est activée, le commutateur crée une carte par défaut. Cette carte est référencée dans ce tableau, présenté précédemment. Cette carte permettra de déterminer la valeur du DSCP qui sera fixée selon la valeur de la priorité IP. Sinon, l'administrateur peut configurer une carte unique. Voici un exemple :

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

La commande ci-dessus définit la carte suivante :

| Priorité IP | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Bien qu'il soit très peu probable que la carte ci-dessus soit utilisée dans un réseau réel, elle sert à donner une idée de ce qui peut être réalisé lors de l'utilisation de cette commande.

## Classification (CatOS)

Lorsqu'une trame est transmise à la PFC aux fins de traitement, le processus de classification est alors exécuté sur la trame. La PFC utilisera une ACL préconfigurée (ou par défaut) pour attribuer un DSCP à la trame. Dans l'ACE, un des quatre mots clés est utilisé pour attribuer une valeur DSCP. Ces mots clés sont les suivants :

1. TRUST-DSCP (ACL IP uniquement)
2. TRUST-IPPREC (ACL IP seulement)
3. TRUST-COS (toutes les ACL sauf IPX et MAC sur une PFC2)
4. DSCP

Le mot clé TRUST-DSCP suppose que la trame arrivant dans la PFC a déjà une valeur DSCP définie avant d'entrer dans le commutateur. Le commutateur conservera cette valeur DSCP.

Avec TRUST-IPPREC, la PFC obtiendra une valeur DSCP à partir de la valeur de priorité IP existante qui figure dans le champ ToS. La PFC utilisera la priorité IP sur les cartes DSCP afin d'attribuer le bon DSCP. Une carte par défaut est créée lorsque la QoS est activée sur le commutateur. Vous pouvez également utiliser une carte créée par l'administrateur pour obtenir la valeur DSCP.

Comme c'est le cas pour TRUST-IPPREC, le mot clé TRUS-COS indique à la PFC de générer une valeur DSCP à partir des CO dans l'en-tête de la trame. Il y aura également un mappage des CO avec le DSCP (soit un mappage par défaut, soit un mappage attribué par un administrateur) pour aider la PFC à obtenir le DSCP.

Le mot clé DSCP est utilisé lorsqu'une trame provient d'un port non sécurisé. Une situation intéressante se présente pour l'obtention du DSCP. À ce stade, le DSCP configuré dans l'instruction « set qos acl » est utilisé pour obtenir le DSCP. Or, c'est à ce stade que les ACL peuvent servir à l'obtention d'un DSCP pour le trafic, en fonction des critères de classification établis dans l'ACE. Cela signifie que dans une ACE, on peut utiliser des critères de classification tels que l'adresse IP source et de destination, les numéros de port TCP/UDP, les codes ICMP, le type IGMP, les numéros de réseau et de protocole IPX, les adresses MAC source et de destination, ainsi que les Ethertypes (trafic sans IP et sans IPX seulement) pour cibler le trafic. Ainsi, une ACE pourrait être configurée de manière à attribuer une valeur DSCP précise pour déterminer le trafic HTTP sur le trafic FTP.

Prenons l'exemple suivant :

```
Console> (enable) set port qos 3/5 trust untrusted
```

Si vous configurez un port comme étant non sécurisé, la PFC utilisera une ACE pour obtenir le DSCP de la trame. Si l'ACE est configurée selon des critères de classification, les flux individuels du port peuvent être classés selon des priorités différentes. Voici ce qu'illustrent les ACE suivantes :

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

Dans cet exemple figurent deux instructions ACE. La première cible tout flux TCP (le mot clé « any » est utilisé pour déterminer le trafic source et de destination) dont le numéro de port est 80 (80 = HTTP) et qui doit recevoir une valeur DSCP de 32. La deuxième ACE cible le trafic

provenant de n'importe quel hôte et destiné à n'importe quel hôte dont le numéro de port TCP est 21 (FTP) et qui doit recevoir une valeur DSCP de 16.

## Configurer la classification sur la gamme Catalyst 6000 avec Cisco IOS intégré (mode natif)

La section suivante décrit les composants de configuration de QoS utilisés pour prendre en charge la classification sur la PFC au moyen de Cisco IOS intégré (mode natif).

### Mappage des CO avec le DSCP (Cisco IOS intégré [mode natif])

En entrant dans le commutateur, une trame aura une valeur DSCP définie par le commutateur. Si le port est dans un état sécurisé et si l'administrateur a utilisé le mot clé « mls qos trust-COs » (sur les ports GE ou les ports 10/100 des cartes de ligne WS-X6548), la valeur des CO qui est définie dans la trame servira à déterminer la valeur DSCP fixée pour la trame. Comme il est mentionné précédemment, le commutateur peut attribuer, selon la valeur DSCP interne, des niveaux de service à la trame lorsqu'elle transite par le commutateur.

Lorsque la QoS est activée, le commutateur crée une carte par défaut. Consultez ce tableau pour connaître les paramètres par défaut. Cette carte permettra de déterminer la valeur du DSCP qui sera fixée selon la valeur des CO. Sinon, l'administrateur peut configurer une carte unique. Un exemple est fourni ci-dessous.

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

La commande ci-dessus définit la carte suivante :

| CoS | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Bien qu'il soit très peu probable que la carte ci-dessus soit utilisée dans un réseau réel, elle sert à donner une idée de ce qui peut être réalisé lors de l'utilisation de cette commande.

### Mappage de la priorité IP avec le DSCP (Cisco IOS intégré [mode natif])

De façon comparable au mappage de CO avec DSCP, une trame peut avoir une valeur DSCP déterminée à partir du paramètre de priorité IP des paquets entrants. C'est possible seulement si l'administrateur a mis le port à l'état sécurisé et qu'il a utilisé le mot clé « mls qos trust-ipprec ». Ce mot clé est pris en charge seulement sur les ports GE et les ports 10/100 des cartes de ligne WS-X6548. Pour les ports 10/100 des cartes de ligne WS-X6348 et WS-X6248, les ACL doivent être utilisées pour attribuer la priorité IP aux données entrantes.

Lorsque la QoS est activée, le commutateur crée une carte par défaut. Consultez ce tableau pour connaître les paramètres par défaut. Cette carte permettra de déterminer la valeur du DSCP qui sera fixée selon la valeur de la priorité IP. Sinon, l'administrateur peut configurer une carte unique. Un exemple est fourni ci-dessous.

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

La commande ci-dessus définit la carte suivante :

| Priorité IP | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 20 | 30 | 1 | 43 | 63 | 12 | 13 | 8 |

Bien qu'il soit très peu probable que la carte ci-dessus soit utilisée dans un réseau réel, elle sert à donner une idée de ce qui peut être réalisé lors de l'utilisation de cette commande.

### Classification (Cisco IOS intégré [mode natif])

Lorsqu'une trame est transmise à la PFC, le processus de classification peut être effectué pour attribuer une nouvelle priorité à une trame entrante. Mise en garde : ce ne peut être fait que si la trame provient d'un port non sécurisé ou si elle a été classée comme non sécurisée.

Les classifications suivantes peuvent être utilisées pour la carte de contrôle :

1. TRUST CO
2. TRUST IP-PRECEDENCE
3. TRUST DSCP
4. NO TRUST

Le mot clé TRUST DSCP suppose que la trame qui arrive dans la PFC a déjà une valeur DSCP définie avant d'entrer dans le commutateur. Le commutateur conservera cette valeur DSCP.

Avec TRUST IP-PRECEDENCE, la PFC obtiendra une valeur DSCP à partir de la valeur de priorité IP existante qui figure dans le champ ToS. La PFC utilisera une priorité IP sur les cartes DSCP afin d'attribuer le bon DSCP. Une carte par défaut est créée lorsque la QoS est activée sur le commutateur. Vous pouvez également utiliser une carte créée par l'administrateur pour obtenir la valeur DSCP.

De façon semblable à TRUST IP-PRECEDENCE, le mot clé TRUST COs indique à la PFC qu'une valeur DSCP doit être obtenue à partir des CO de l'en-tête de la trame. Il y aura également un mappage des CO avec le DSCP (soit un mappage par défaut, soit un mappage attribué par un administrateur) pour aider la PFC à obtenir le DSCP.

Un exemple de l'obtention du DSCP à partir d'une priorité existante (DSCP, priorité IP ou CO) est présenté ci-dessous.

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

La carte de classification ci-dessus obtiendra la valeur DSCP à partir des CO de l'en-tête Ethernet.

La forme NO TRUST du mot clé est utilisée lorsqu'une trame arrive d'un port non sécurisé. Ainsi, la trame peut recevoir une valeur DSCP pendant le processus de contrôle.

Prenons l'exemple ci-dessous, qui montre comment une nouvelle priorité (DSCP) peut être attribuée à différents flux entrant dans la PFC par la définition de contrôle suivante.

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

L'exemple ci-dessus montre ce qui suit :

1. Une ACL est créée pour cibler les flux http entrant dans le port.
2. Une carte de contrôle est intitulée « new-dscp-for-flow ».
3. Une carte de classification (test de noms) utilise la liste d'accès 102 pour cibler le trafic où elle agira.
4. Le test de la carte de classification fixera l'état de la trame entrante à non sécurisé et attribuera un DSCP de 24 à ce flux.
5. Cette carte de classe limitera également l'agrégat des flux http à 1 Mbit tout au plus.

# Protocole COPS (Common Open Policy Server)

Le protocole COPS permet à la gamme Catalyst 6000 de configurer la QoS à partir d'un hôte distant. Actuellement, le protocole COPS est uniquement pris en charge à l'aide de CatOS et fait partie de l'architecture intserv pour la QoS. Il n'est actuellement pas pris en charge (à la date de rédaction de ce document) avec l'utilisation de Cisco IOS intégré (mode natif). Bien que le protocole COPS transmette les informations de configuration QoS au commutateur, il ne représente pas la source de ces informations. L'utilisation du protocole COPS nécessite un gestionnaire de QoS externe pour héberger les configurations de QoS du commutateur. Le gestionnaire de QoS externe amorcera la poussée vers le bas de ces configurations vers le commutateur à l'aide du protocole COPS. Le gestionnaire de contrôle de QoS (QPM) de Cisco est un exemple de gestionnaire de QoS externe.

L'objectif du présent document n'est pas d'expliquer le fonctionnement de QPM, mais d'expliquer la configuration requise sur le commutateur pour prendre en charge les configurations de QoS externes à partir de QPM.

## Configuration du protocole COPS

Par défaut, la prise en charge du protocole COPS est désactivée. Il doit être activé pour l'utiliser sur le commutateur. Pour ce faire, vous pouvez utiliser la commande suivante :

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

Lorsque cette commande est lancée, certaines valeurs de configuration QoS par défaut proviendront du serveur COPS. Ces valeurs comprennent les suivantes :

1. Les mappages des CO avec les files d'attente
2. L'octroi des seuils pour les files d'attente d'entrée et de sortie
3. L'attribution de la bande passante WRR

4. Tous les contrôles d'agrégat et de microflux
5. Les mappages des CO avec DSCP pour le trafic sortant
6. ACL
7. L'attribution des CO des ports par défaut

Lorsque la QoS est configurée à l'aide du protocole COPS, il est important de savoir que ces configurations s'appliquent différemment. Plutôt que de configurer directement les ports, le protocole COPS est utilisé pour configurer l'ASIC de port. L'ASIC de port contrôle généralement un groupe de ports, de sorte que la configuration de COPS soit appliquée à plusieurs ports à la fois.

L'ASIC de port configuré est l'ASIC GE. Sur les cartes de ligne GE figurent quatre ports par GE (ports 1-4, 5-8, 9-12, 13-16). Sur ces cartes de ligne, la configuration de COPS influe sur chaque groupe de ports. Sur les cartes de ligne 10/100 (comme nous avons vu précédemment dans ce document) se trouvent deux groupes d'ASIC : GE et ASIC 10/100. Un ASIC GE existe pour quatre ASIC 10/100. Chaque ASIC 10/100 prend en charge 12 ports 10/100. Le protocole COPS configure l'ASIC GE. Ainsi, lors de l'application de la configuration QoS aux cartes de ligne 10/100 par le protocole COPS, la configuration s'applique aux 48 ports 10/100.

Lorsque vous activez la prise en charge de COPS au moyen de la commande **set qos policy-source cops, la configuration de QoS par le protocole COPS est appliquée à l'ensemble des ASIC du châssis du commutateur.** Il est possible d'appliquer la configuration de COPS à des ASIC précis. Il suffit notamment d'utiliser la commande suivante :

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

Vous pouvez constater, à partir de l'application de la commande ci-dessus, que cette commande est utilisée sur un module GE, car quatre ports ont réagi à la commande.

## Serveurs Policy Decision Point et noms de domaine

Les serveurs PDPS (Policy Decision Point) sont les gestionnaires de contrôles externes qui sont utilisés pour stocker les détails de la configuration de la QoS transmis au commutateur. Si la fonction COPS est activée sur le commutateur, ce dernier doit être configuré selon l'adresse IP du gestionnaire externe qui fournira les détails de la configuration de la QoS au commutateur. Ce processus est semblable à celui utilisé lorsque le SNMP est activé et que l'adresse IP du gestionnaire SNMP est définie.

La commande servant à cibler le PDPS externe est exécutée ainsi :

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```

La commande ci-dessus cible le périphérique 192.168.1.1 comme le serveur PDPS principal.

Lorsque le commutateur communique avec le PDPS, il doit faire partie d'un domaine défini sur le PDPS. Le PDPS communiquera uniquement avec les commutateurs qui font partie de son domaine défini. Le commutateur doit donc être configuré de façon à déterminer le domaine COPS auquel il appartient. Pour ce faire, utilisez la commande suivante :

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

La commande ci-dessus indique que le commutateur est configuré pour faire partie du domaine « remote-cat6k ». Ce domaine doit être défini dans QPM, et le commutateur doit être ajouté à ce domaine.

---

# Informations connexes

- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems

---