Présentation de la réglementation et de la signalisation QoS (Qualité de service) sur Catalyst 3550

Contenu

Introduction

La fonction policière détermine si le niveau du trafic est dans le profil ou le contrat spécifié, et vous permet à l'un ou l'autre de trafic hors profil de baisse ou le marque vers le bas à une valeur différentielle différente de point de code de service (DSCP). Ceci impose un niveau de service contracté.

Le DSCP est une mesure du niveau de Qualité de service (QoS) du paquet. Avec le DSCP, la Priorité IP et le Classe de service (Cos) sont également utilisés afin de donner le niveau de QoS du paquet.

Le maintien de l'ordre ne doit pas être confondu avec le trafic formant, bien que chacun des deux s'assurent les séjours du trafic dans le profil ou le contrat.

Le maintien de l'ordre ne met pas en mémoire tampon le trafic, ainsi le maintien de l'ordre n'affecte pas le retard de transmission. Au lieu des paquets hors profil de mise en mémoire tampon, le maintien de l'ordre les relâche ou les identifie par différents niveaux de QoS (baisse de DSCP).

Trafiquez en formant le trafic hors profil de mémoires tampons et lissez les rafales du trafic, mais affectez le retard et la variation de délai. La formation peut seulement être appliquée sur l'interface sortante, alors que le maintien de l'ordre peut être appliqué sur chacun des deux l'interface d'entrée et de sortie.

Le Catalyst 3550 prend en charge le maintien de l'ordre pour des directions entrantes et sortantes. La formation du trafic n'est pas prise en charge.

Le repérage change le niveau de QoS de paquet selon une stratégie.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Matériel et versions de logiciel

Le maintien de l'ordre et le repérage sur le Catalyst 3550 est pris en charge avec toutes les versions de logiciel. Le dernier guide de configuration est répertorié ici. Référez-vous à cette documentation pour toutes les caractéristiques prises en charge.

- Configuration QoS

Paramètres de Réglementation QoS et de marquage

Afin d'installer le maintien de l'ordre, vous devez définir les cartes de stratégie QoS et les appliquer aux ports. Ceci est autrement connu en tant que QoS basé sur port.

Note: QoS basé sur VLAN n'est pas actuellement pris en charge par le Catalyst 3550.

Le régulateur est défini par le débit et les paramètres de rafale aussi bien que l'action pour le trafic hors profil.

Ces deux types de régulateurs sont pris en charge :

- Agrégat
- Individuel

Le régulateur d'agrégation agit sur le trafic à travers tous les exemples où il est appliqué. Les

différents actes de régulateur séparément sur le trafic à travers chaque exemple où il est appliqué.

Note: Sur le Catalyst 3550, le régulateur d'agrégation peut seulement être appliqué aux classes différentes de la même stratégie. Le maintien de l'ordre d'agrégat à travers des plusieurs interfaces ou des stratégies n'est pas pris en charge.

Par exemple, appliquez le régulateur d'agrégation afin de limiter le trafic de la classe customer1 et classer customer2 dans le même policy-map au Mbits/s 1. Un tel régulateur permet le Mbits/s 1 du trafic dans la classe customer1 et customer2 ensemble. Si vous appliquez le régulateur individuel, le régulateur limite le trafic pour la classe customer1 au Mbits/s 1 et pour la classe customer2 au Mbits/s 1. Par conséquent, chaque exemple du régulateur est distinct.

Cette table récapitule l'action de QoS sur le paquet une fois traité par des stratégies d'entrée et de sortie :

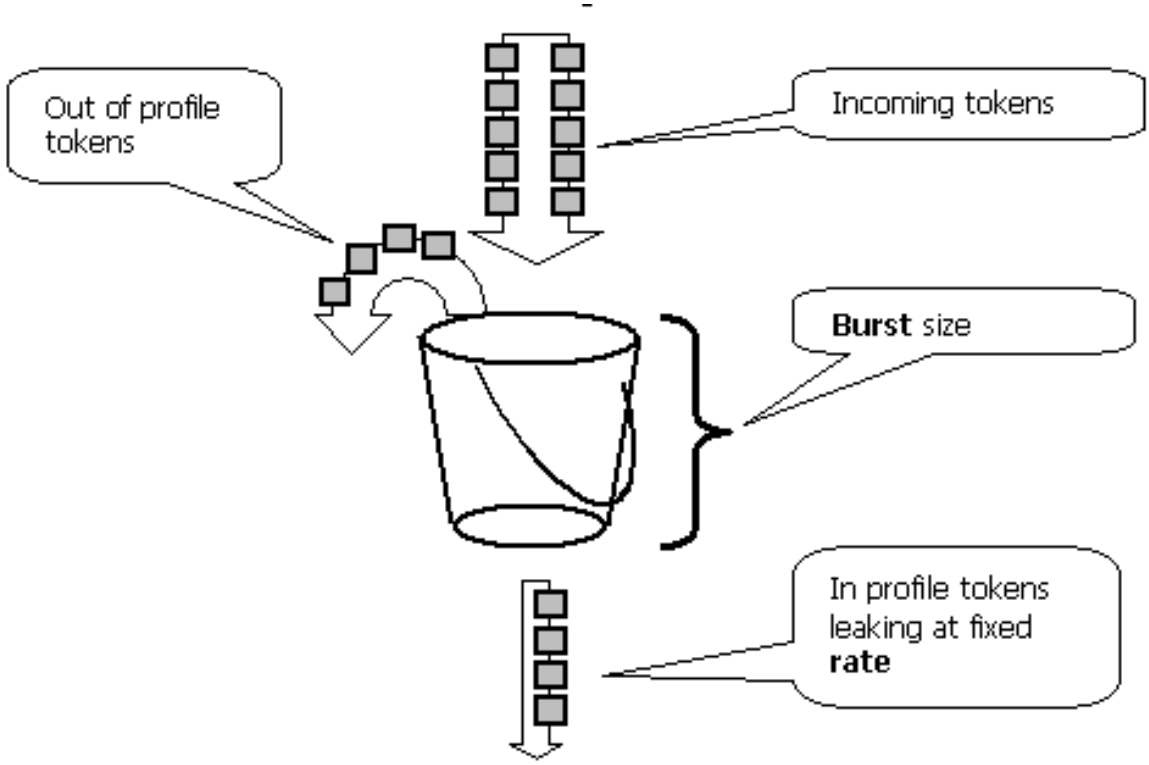
	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_i$ then Markdown$_e$	Mark$_i$ then Markdown$_e$

Note: Il est possible de marquer et baisse dans la même classe du trafic de la même stratégie. En pareil cas, tout le trafic pour la classe particulière est marqué d'abord. Le maintien de l'ordre et la baisse se produit sur le trafic déjà marqué.

La Réglementation QoS dans le Catalyst 3550 est conforme à ce concept de saut percé :

Le nombre de jetons proportionnels aux longueurs de paquet du trafic entrant sont placés dans un seau à jetons ; le nombre de jetons égale la taille du paquet. À un intervalle régulier, un nombre défini de jetons dérivés du débit configuré est retiré de la position. S'il n'y a aucun endroit dans la position pour faciliter un paquet entrant, le paquet est considéré -de-profil et est lâché ou marqué vers le bas selon l'action de réglementation configurée.

Ce concept est affiché dans cet exemple :



Note: Le trafic n'est pas mis en mémoire tampon dans la position pendant qu'il peut apparaître dans cet exemple. Le trafic réel ne traverse pas la position du tout ; la position est seulement utilisée afin de décider si le paquet est dans le profil ou le -de-profil.

Note: L'implémentation de matériel du maintien de l'ordre peut varier, mais fonctionellement elle se conforme toujours à ce modèle.

Ces paramètres contrôlent l'exécution du maintien de l'ordre :

- **Débit** - définit combien de tokens sont supprimés à chaque intervalle. Ceci définit effectivement le débit de réglementation. Tout le trafic au-dessous du débit est considéré dans le profil. Les débits pris en charge s'étendent de 8 Kbps à 2 GBP, et à incrément par 8 Kbps.
- **Intervalle** - définit à quelle fréquence les tokens sont supprimés du compartiment. L'intervalle est réparé à 0.125 milliseconde (ou à 8000 fois par seconde). Cet intervalle ne peut pas être changé.
- **Rafale** — définit la quantité maximale de jetons que la position peut se tenir à tout moment. Plage de rafales prise en charge de 8000 octets à 2000000 octets, et à incrément par 64 octets.

Note: Bien que les chaînes d'aide de ligne de commande affichent une gamme étendue de valeurs, l'option débit-bps ne peut pas dépasser la vitesse du port configurée, et l'option de rafale-octet ne peut pas dépasser 2000000 octets. Si vous écrivez une plus grande valeur, le commutateur rejette la carte de stratégie quand vous le reliez à une interface.

Afin de soutenir le débit du trafic indiqué, la rafale doit être aucune moins que la somme de cette équation :

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

Par exemple, calculez la valeur minimale de rafale afin de soutenir un débit de Mbits/s 1. Le débit est défini en tant que 1000 Kbps, ainsi la rafale minimum requise est la somme de cette équation :

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

La taille de rafale prise en charge par minimum est de 8000 octets, qui est plus que la rafale minimum calculée.

Note: En raison de la granularité de la réglementation de matériel, le débit et la rafale exacts sont arrondis à la valeur prise en charge la plus proche.

Quand vous configurez le débit de rafales, vous devez prendre en considération que quelques protocoles implémentent les mécanismes qui réagissent à la perte de paquets. Par exemple, le Protocole TCP (Transmission Control Protocol) réduit la fenêtre par moitié pour chaque paquet perdu. Ceci fait accélérer un effet « de dent de scie » dans le trafic TCP quand des essais de TCP à la ligne débit et est étranglé par le régulateur. Si le débit moyen du trafic de dent de scie est calculé, ce débit est beaucoup inférieur au débit maintenu l'ordre. Cependant, vous pouvez augmenter la rafale afin de réaliser une meilleure utilisation. Un bon début est de placer la rafale égale deux fois à la quantité du trafic envoyé avec du débit désiré pendant le Round-Trip Time (DURÉE DE TRANSMISSION de TCP). Si la DURÉE DE TRANSMISSION n'est pas connue, vous pouvez doubler la valeur du paramètre de rafale.

Pour la même raison, il n'est pas recommandé pour évaluer l'exécution de régulateur par le trafic connecté. Ce scénario affiche généralement la performance inférieure qu'autorisée par le régulateur.

Le trafic sans connexion peut également réagir au maintien de l'ordre différemment. Par exemple, le Systèmes de fichiers en réseau (NFS) utilise les blocs, qui pourraient se composer de plus d'un paquet de Protocole UDP (User Datagram Protocol). Un paquet lâché peut déclencher beaucoup de paquets, même le bloc entier, pour être retransmis.

Cet exemple calcule la rafale pour une session TCP avec du débit de maintien de l'ordre de 64 Kbits/s et donné la DURÉE DE TRANSMISSION de TCP est, 0.05 seconde :

```
<burst> = 2*  *  = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800    [bytes]
```

Dans cet exemple, le `<burst>` est pour une session TCP. Mesurez cette figure pour faire la moyenne du nombre prévu de sessions voyageant par le régulateur.

Note: C'est un exemple seulement, dans chaque cas vous devez évaluer le trafic et des conditions requises et comportement d'application contre des ressources disponibles afin de choisir des paramètres de réglementation.

L'action de réglementation peut être de relâcher le paquet ou de changer le DSCP du paquet (baisse). La baisse le paquet, une carte maintenue l'ordre de DSCP doit être modifiée. Un par défaut a maintenu l'ordre la carte de DSCP remarque le paquet au même DSCP. Par conséquent, aucune baisse ne se produit.

Des paquets peuvent être envoyés à en panne quand un paquet hors profil est marqué vers le bas à un DSCP tracé dans une file d'attente de sortie différente que le DSCP d'origine. Si la commande des paquets est importante, les paquets hors profil de baisse au DSCP ont tracé à la même file d'attente de sortie que des paquets de dans-profil.

Maintien de l'ordre et fonctionnalités de marquage pris en charge par le Catalyst 3550

Cette table fournit un résumé des caractéristiques relatives de maintien de l'ordre et de repérage prises en charge par le Catalyst 3550, décomposé par la direction :

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

Une déclaration de correspondance est prise en charge par class-map. Ce sont des déclarations valides de correspondance pour la stratégie d'entrée :

- match access-group
- match ip dscp
- match ip precedence

Note: Sur le Catalyst 3550, la commande de **match interface** n'est pas prise en charge et seulement une commande match est permise dans un class-map. Par conséquent, il est délicat pour classifier tout le trafic qui entre par une interface et maintient l'ordre tout le trafic avec un régulateur simple. Voyez comment classifier tout le trafic d'interface avec une seule section de régulateur de ce document.

C'est la déclaration valide de correspondance pour la stratégie de sortie :

- match ip dscp

Ce sont des actions valides de stratégie pour la stratégie d'entrée :

- police
- set ip dscp (marquage)
- placez la Priorité IP (le marquage)
- dscp de confiance
- Priorité IP de confiance
- cos de confiance

Cette table affiche la matrice prise en charge de stratégies QoS d'entrée :

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. Cette option couvre également le match ip precedence.
2. Cette option couvre faire confiance au cos, à la Priorité IP, et au DSCP.
3. Cette option couvre également placer la Priorité IP.

C'est l'action valide de stratégie pour la stratégie de sortie :

- police

Cette table affiche la matrice prise en charge de stratégies QoS de sortie :

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

Le marquage permet au niveau de QoS du paquet pour changer basé lors de la classification ou du maintien de l'ordre. Les fractionnements de classification trafiquent dans des classes différentes pour le traitement de QoS basé sur les critères définis.

Le traitement de QoS est basé sur le DSCP interne ; la mesure du niveau de QoS du paquet. Le DSCP interne est dérivé selon la configuration de confiance. Les assistances techniques faisant confiance au cos, au DSCP, à la Priorité IP, et aux interfaces non approuvées. La confiance spécifie le champ dont le DSCP interne est dérivé pour chaque paquet, comme suit :

- En faisant confiance au cos, le niveau de QoS est dérivé de l'en-tête de la couche 2 (L2) de la liaison Inter-Switch Link le protocole (ISL) ou du paquet encapsulé de 802.1Q.
- En faisant confiance au DSCP ou à la Priorité IP, le système dérive le niveau de QoS du DSCP ou du champ de priorité IP du paquet en conséquence.

La confiance du cos est seulement signicative sur des interfaces d'agrégation, et la confiance du DSCP (ou de la Priorité IP) semble raisonnable pour des paquets IP seulement.

Quand une interface n'est pas faite confiance, le DSCP interne est dérivé du cos par défaut configurable pour l'interface correspondante. C'est l'état par défaut quand QoS est activé. Si aucun cos par défaut n'est configuré, la valeur par défaut est zéro.

Une fois que le DSCP interne est déterminé, il peut être changé par le repérage et le maintien de l'ordre, ou être retenu.

Après que le paquet subisse le QoS traitant, ses champs de niveau de QoS (dans le champ IP/DSCP pour l'IP, et dans l'en-tête ISL/802.1Q, si quel) sont mis à jour du DSCP interne. Il y a ces cartes spéciales de QoS concernant le maintien de l'ordre :

- **DSCP Dscp-à-maintenu l'ordre** — utilisé afin de dériver le DSCP maintenu l'ordre quand vous baisse avalez le paquet.
- **Dscp-à-cos** — utilisé afin de dériver le cos de niveau du DSCP interne pour mettre à jour l'en-tête sortante du paquet ISL/802.1Q.
- **CoS-to-DSCP** — utilisé afin de dériver le DSCP interne du cos entrant (en-tête ISL/802.1Q) quand l'interface est en mode de cos de confiance.

Ce sont d'importantes considérations d'implémentation-particularité :

- La stratégie de service d'entrée ne peut pas être reliée à l'interface quand l'interface est configurée pour faire confiance à des mesures l'unes des de QoS, telles que CoS/DSCP ou Priorité IP. Afin d'apparier sur la priorité et la police DSCP/IP sur le d'entrée, vous devez configurer la confiance pour la classe particulière dans la stratégie, pas sur l'interface. Afin de marquer a basé sur la priorité DSCP/IP, aucune confiance doit être configuré.
- Seulement le trafic d'ipv4 sans des options IP et l'encapsulation d'Advanced Research Projects Agency d'Ethernet II (ARPA) est considéré le trafic IP du matériel et du point de vue

de QoS. Tout autre trafic est considéré non-IP comprenant, IP avec des options, telles que l'IP encapsulé de protocole d'accès de sous-réseau (SNAP) et l'IPv6.
- Pour les paquets non-IP, « le groupe d'accès de correspondance » est la seule méthode de classification parce que vous ne pouvez pas match dscp pour le trafic non-IP. Une liste d'accès de Contrôle d'accès au support (MAC) (ACL) est utilisée dans ce but ; des paquets peuvent être appariés ont basé sur l'adresse MAC source, l'adresse MAC de destination, et EtherType. Il n'est pas possible d'apparier le trafic IP avec l'ACL de MAC, puisque le commutateur fait une distinction entre le trafic IP et non-IP.

Configurez et surveillez le maintien de l'ordre

Ces étapes sont nécessaires afin de configurer le maintien de l'ordre dans le Cisco IOS :

1. Définissez un régulateur (pour des régulateurs d'agrégation)
2. Définissez les critères pour sélectionner le trafic pour le maintien de l'ordre
3. Définissez un class-map pour sélectionner le trafic utilisant des critères définis
4. Définissez une service-stratégie utilisant la classe et appliquer un régulateur à la classe spécifiée
5. Appliquez-vous une service-stratégie à un port

Ces deux types de régulateurs sont pris en charge :

- Agrégat Désigné
- Individuel

Le régulateur d'agrégation Désigné maintient l'ordre le trafic combiné de toutes les classes dans la même stratégie à où il est appliqué. Le maintien de l'ordre d'agrégat à travers différentes interfaces n'est pas pris en charge.

Note: Le régulateur d'agrégation ne peut pas être appliqué à plus d'une stratégie. S'il est, ce message d'erreur est affiché :

```
QoS: Cannot allocate policer for policy map <policy name>
```

Considérez cet exemple :

Il y a un générateur du trafic relié pour mettre en communication GigabitEthernet0/3 qui envoie approximativement 17 Mbits/s du trafic UDP avec la destination port 111. Il y a également du trafic TCP du port 20. Vous voulez que ces deux flux de trafic soient maintenus l'ordre vers le bas au Mbits/s 1, et le trafic excessif doit être abandonné. Cet exemple affiche comment ceci est fait :

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
```

```
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

Le premier exemple a utilisé le régulateur d'agrégation Désigné. Le régulateur individuel, à la différence de l'agent de contrôle nommé, maintient l'ordre le trafic séparément sur chaque classe où il est appliqué. Le régulateur individuel est défini dans le configuration de policy-map. Dans cet exemple, deux classes du trafic sont maintenues l'ordre par deux différents régulateurs ; cl_udp111 est maintenu l'ordre au Mbits/s 1 par rafale 8K, et cl_tcp20 est maintenu l'ordre à 512 Kbps par 32K éclaté :

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

Cette commande est utilisée afin de surveiller l'exécution de maintien de l'ordre :

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a       n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

Note: Par défaut, il n'y a aucune statistiques de par-DSCP. Le Catalyst 3550 prend en charge une par-interface, collecte de statistiques de par-direction pour jusqu'à huit valeurs DSCP différentes. Ceci est configuré quand vous émettez la commande de **mls qos monitor**. Afin de surveiller des statistiques pour DSCPs 8, 16, 24, et 32, vous devez émettre cette commande de par-**interface** :

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

Note: **Le dscp 8 de mls qos monitor** commandes **16 24 32** change la sortie de la commande de

statistiques du show mls qos international g0/3 à ceci :

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a       n/a      0          0
    16: 0             n/a       n/a      0          0         ? per DSCP statistics
    24: 15239542      n/a       n/a      0          0
    32: 539289117     n/a       n/a      536486430  0
Others: 1983055       n/a       n/a      1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

C'est une description des champs dans l'exemple :

- **Entrant** — affiche combien de paquets arrivent de chaque direction
- **NO_change** — affiche combien de paquets ont été de confiance (comme le niveau de QoS non changé)
- **Classifié** — affiche combien des paquets ont été assignés à ce DSCP interne après classification
- **Maintenu l'ordre** — affiche combien des paquets ont été marqués vers le bas par le maintien de l'ordre ; DSCP affiché avant baisse.
- **Relâché** — affiche combien de paquets ont été lâchés par le maintien de l'ordre

Rendez-vous compte de ces considérations d'implémentation-particularité :

- Si huit valeurs DSCP sont configurées quand vous émettez la commande de **mls qos monitor**, les autres compteur vu quand vous émettez la commande de **statistiques du show mls qos international** pourraient afficher les informations insuffisantes.
- Il n'y a aucune commande spécifique afin de vérifier le par-régulateur offerte ou du trafic sortant de débit.
- Puisque les compteurs sont récupérés du matériel séquentiellement, il est possible que les compteurs n'ajoutent pas correctement. Par exemple, la quantité de paquets maintenus l'ordre, classifiés, ou abandonnés peut être légèrement différente que le nombre de paquets entrant.

Configurez et surveillez le marquage

Ces étapes sont nécessaires afin de configurer le marquage :

1. Définissez les critères pour classifier le trafic
2. Définissez les classes du trafic à classifier avec les critères précédemment définis

3. Créez une carte de stratégie qui relie des actions et des actions de réglementation de marquage aux classes définies
4. Configurez l'interface correspondante pour faire confiance au mode
5. Appliquez la carte de stratégie à une interface

Dans cet exemple, vous voulez que le trafic IP en entrée héberge 192.168.192.168 identifié par la Priorité IP 6 et maintenu l'ordre vers le bas au Mbits/s 1 ; le trafic excédentaire doit être marqué vers le bas à la Priorité IP 2 :

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

La même commande de **statistiques de show mls qos interface** est émise afin de surveiller le marquage. La sortie et les implications d'échantillon sont documentées dans la section de ce document.

Comment classifier tout le trafic d'interface avec un régulateur simple

Sur le Catalyst 3550, la commande de **match interface** n'est pas prise en charge, et seulement une commande match est permise par class-map. D'ailleurs, le Catalyst 3550 ne permet pas le trafic IP à apparier par le MAC ACLs. Ainsi le trafic IP et non-IP doit être classifié avec deux class-map distincts. Ceci le rend délicat pour classifier tout le trafic qui entre dans une interface et maintient l'ordre tout le trafic avec un régulateur simple. La configuration d'échantillon ici vous permet d'accomplir ceci. Dans ces configuration, trafic IP et non-IP sont appariés avec deux class-map différents. Cependant, chacun utilise un régulateur commun pour le les deux le trafic.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic
```

```
interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

Informations connexes

- Configurer QoS sur le Catalyst 3550
- Pages de support de qualité de service
- Page de support sur la commutation LAN
- Pages de support pour les produits LAN
- Support et documentation techniques - Cisco Systems