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

Contenu

Introduction

La fonction de réglementation détermine si le niveau de trafic se trouve dans le profil ou le contrat spécifié et vous permet d'abandonner le trafic hors profil ou de le marquer à une valeur DSCP (Differential Services Code Point) différente. Ceci impose un niveau de service contracté.

DSCP est une mesure du niveau de qualité de service (QoS) du paquet. En plus du DSCP, la priorité IP et la classe de service (CoS) sont également utilisées afin de transmettre le niveau de QoS du paquet.

La réglementation ne doit pas être confondue avec le formatage du trafic, bien que les deux s'assurent que le trafic reste dans le profil ou le contrat.

La réglementation ne met pas en mémoire tampon le trafic, de sorte qu'elle n'affecte pas le délai de transmission. Au lieu de mettre en mémoire tampon des paquets hors profil, la réglementation les supprime ou les marque avec différents niveaux de QoS (marquage DSCP).

La mise en forme du trafic met en mémoire tampon le trafic hors profil et ajuste les rafales de trafic, mais affecte les variations de délai et de délai. Le formatage ne peut être appliqué que sur l'interface sortante, tandis que la réglementation peut être appliquée à la fois sur l'interface entrante et sortante.

Le Catalyst 3550 prend en charge la réglementation des directions entrantes et sortantes. Le formatage du trafic n'est pas pris en charge.

Le marquage modifie le niveau de QoS du paquet en fonction d'une stratégie.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Versions matérielles et logicielles

La réglementation et le marquage sur le Catalyst 3550 sont pris en charge avec toutes les versions logicielles. Le dernier guide de configuration est répertorié ici. Reportez-vous à cette documentation pour toutes les fonctionnalités prises en charge.

- Configuration QoS

Paramètres de contrôle et de marquage QoS

Pour configurer la réglementation, vous devez définir les cartes de stratégie QoS et les appliquer aux ports. Il s'agit également de la QoS basée sur les ports.

Remarque : la QoS basée sur VLAN n'est actuellement pas prise en charge par le Catalyst 3550.

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

Ces deux types de contrôleurs sont pris en charge :

- Agréger
- Individuel

Le régulateur d'agrégation agit sur le trafic dans toutes les instances où il est appliqué. Chaque régulateur agit séparément sur le trafic de chaque instance où il est appliqué.

Remarque : sur Catalyst 3550, le régulateur d'agrégation ne peut être appliqué qu'à différentes classes de la même stratégie. La réglementation agrégée sur plusieurs interfaces ou stratégies

n'est pas prise en charge.

Par exemple, appliquez le régulateur agrégé afin de limiter le trafic des classes customer1 et class customer2 dans la même carte de stratégie à 1 Mbits/s. Un tel régulateur autorise 1 Mbit/s de trafic dans la classe customer1 et customer2 ensemble. Si vous appliquez le régulateur individuel, le régulateur limite le trafic pour la classe customer1 à 1 Mbits/s et pour la classe customer2 à 1 Mbits/s. Par conséquent, chaque instance du régulateur est distincte.

Ce tableau récapitule l'action QoS sur le paquet lorsqu'elle est traitée par les politiques d'entrée et de sortie :

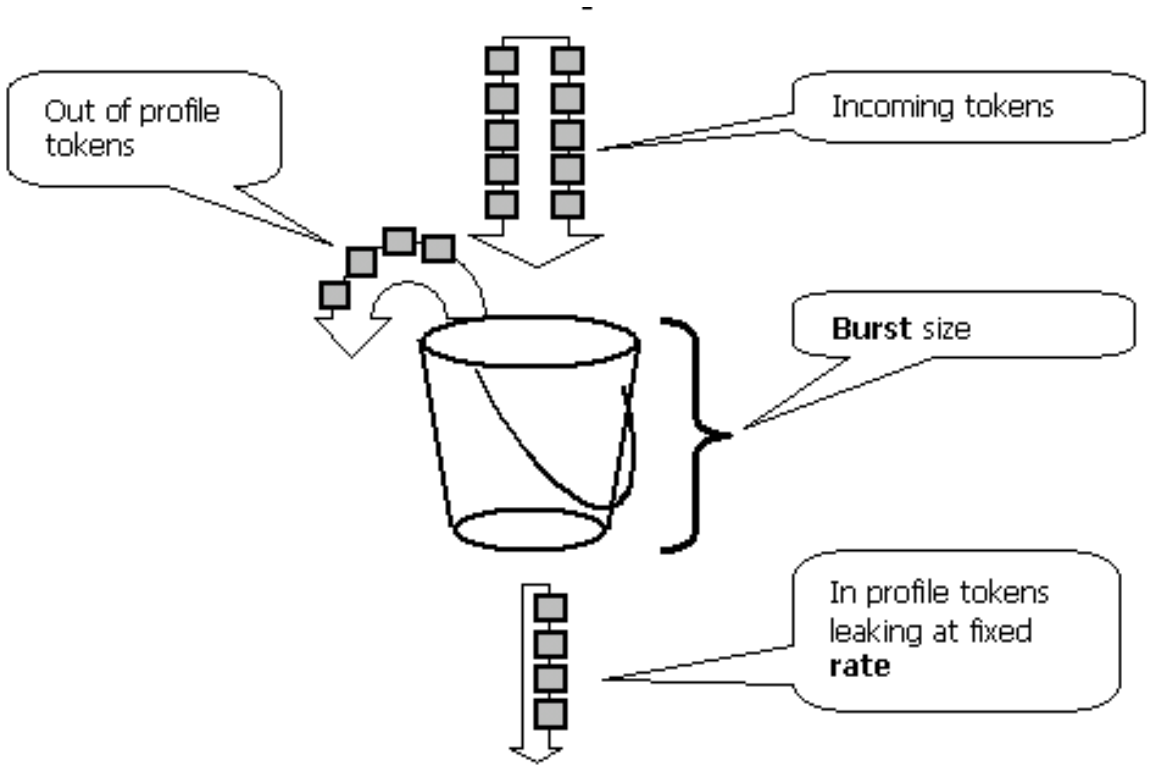
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

Remarque : Il est possible de marquer et de marquer dans la même classe de trafic de la même stratégie. Dans ce cas, tout le trafic de la classe particulière est marqué en premier. La réglementation et le balisage se produisent sur le trafic déjà marqué.

La réglementation QoS dans le Catalyst 3550 est conforme à ce concept de seau fuité :

Le nombre de jetons proportionnel à la taille des paquets de trafic entrants est placé dans un compartiment de jetons ; le nombre de jetons équivaut à la taille du paquet. À un intervalle régulier, un nombre défini de jetons dérivés du débit configuré est supprimé du compartiment. S'il n'y a pas d'emplacement dans le compartiment pour accueillir un paquet entrant, le paquet est considéré comme hors profil et est abandonné ou marqué en fonction de l'action de réglementation configurée.

Ce concept est illustré dans cet exemple :



Remarque : Le trafic n'est pas mis en mémoire tampon dans le compartiment comme il peut apparaître dans cet exemple. Le trafic réel ne traverse pas du tout le compartiment ; le compartiment est uniquement utilisé pour déterminer si le paquet est dans le profil ou hors profil.

Remarque : La mise en oeuvre matérielle de la réglementation peut varier, mais elle reste fonctionnelle et conforme à ce modèle.

Ces paramètres contrôlent le fonctionnement de la réglementation :

- **Débit - définit combien de tokens sont supprimés à chaque intervalle.** Ceci définit effectivement le débit de réglementation. Tout le trafic inférieur au débit est pris en compte dans le profil. Les débits pris en charge varient de 8 Kbits/s à 2 Gbits/s et augmentent de 8 Kbits/s.
- **Intervalle - définit à quelle fréquence les tokens sont supprimés du compartiment.** L'intervalle est fixé à 0,125 millisecondes (soit 8 000 fois par seconde). Cet intervalle ne peut pas être modifié.
- **Burst** : définit la quantité maximale de jetons que le compartiment peut contenir à tout moment. Les rafales prises en charge vont de 8 000 octets à 2 000 000 octets et s'incrémentent de 64 octets.

Remarque : bien que les chaînes d'aide de la ligne de commande affichent une grande plage de valeurs, l'option rate-bps ne peut pas dépasser la vitesse de port configurée et l'option burst-byte ne peut pas dépasser 200000 octets. Si vous entrez une valeur plus grande, le commutateur rejette la carte de stratégie lorsque vous la reliez à une interface.

Pour supporter le débit de trafic spécifié, la rafale doit être au moins égale à la somme de cette équation :

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

Par exemple, calculez la valeur de rafale minimale afin de maintenir un débit de 1 Mbit/s. La vitesse est définie comme étant de 1 000 Kbits/s, la rafale minimale requise est donc la somme de cette équation :

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

La taille minimale de rafale prise en charge est de 8 000 octets, ce qui est supérieur à la taille minimale de rafale calculée.

Remarque : en raison de la granularité de la réglementation matérielle, le taux exact et la rafale sont arrondis à la valeur prise en charge la plus proche.

Lorsque vous configurez le débit de rafale, vous devez tenir compte du fait que certains protocoles implémentent des mécanismes qui réagissent à la perte de paquets. Par exemple, le protocole TCP (Transmission Control Protocol) réduit la fenêtre de moitié pour chaque paquet perdu. Cela provoque un effet de dents de scie dans le trafic TCP lorsque le protocole TCP tente d'accélérer jusqu'au débit de ligne et est limité par le régulateur. Si le taux moyen du trafic de dents de scie est calculé, ce taux est beaucoup plus bas que le taux réglementé. Cependant, vous pouvez augmenter la rafale afin d'obtenir une meilleure utilisation. Un bon début consiste à définir la rafale égale à deux fois la quantité de trafic envoyée avec le débit souhaité pendant le temps de trajet aller-retour TCP (RTT). Si RTT n'est pas connu, vous pouvez doubler la valeur du paramètre de rafale.

Pour la même raison, il n'est pas recommandé de comparer le fonctionnement du régulateur par le trafic orienté connexion. Ce scénario affiche généralement des performances inférieures à celles autorisées par le régulateur.

Le trafic sans connexion peut également réagir différemment à la réglementation. Par exemple, le système de fichiers réseau (NFS) utilise des blocs qui peuvent être constitués de plusieurs paquets UDP (User Datagram Protocol). Un paquet abandonné peut déclencher la retransmission de nombreux paquets, même du bloc entier.

Cet exemple calcule la rafale d'une session TCP avec un débit de réglementation de 64 Kbits/s et étant donné que le TCP RTT est de 0,05 secondes :

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

Dans cet exemple, `<burst>` correspond à une session TCP. Faites évoluer ce chiffre pour indiquer la moyenne du nombre prévu de sessions passant par le régulateur.

Remarque : Il s'agit uniquement d'un exemple. Dans chaque cas, vous devez évaluer les exigences et le comportement du trafic et des applications par rapport aux ressources disponibles afin de choisir les paramètres de réglementation.

L'action de réglementation peut consister à supprimer le paquet ou à modifier le DSCP du paquet (marquage). Afin de marquer le paquet, un mappage DSCP réglementé doit être modifié. Une carte DSCP contrôlée par défaut indique le paquet au même DSCP. Par conséquent, il n'y a pas de démarcation.

Les paquets peuvent être envoyés dans le désordre lorsqu'un paquet hors profil est marqué vers un DSCP mappé dans une file d'attente de sortie différente de celle du DSCP d'origine. Si l'ordre des paquets est important, marquez les paquets hors profil vers le DSCP mappés à la même file d'attente de sortie que les paquets dans le profil.

Fonctions de contrôle et de marquage prises en charge par le Catalyst 3550

Ce tableau fournit un résumé des fonctions de contrôle et de marquage prises en charge par le Catalyst 3550, ventilé par 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 instruction match est prise en charge par class-map. Voici des instructions de correspondance valides pour la stratégie d'entrée :

- match access-group
- match ip dscp
- match ip priority

Remarque : Sur le Catalyst 3550, la commande **match interface** n'est pas prise en charge et une seule commande match est autorisée dans une class-map. Par conséquent, il est difficile de classer tout le trafic qui entre par une interface et de contrôler tout le trafic avec un seul régulateur. Voir Comment classifier tout le trafic d'interface avec un seul régulateur de ce document.

Il s'agit de l'instruction de correspondance valide pour la stratégie de sortie :

- match ip dscp

Il s'agit d'actions de stratégie valides pour la stratégie d'entrée :

- police
- set ip dscp (marquage)
- set ip priority (marquage)
- trust dscp
- trust ip-precedence
- TRUST CO

Ce tableau présente la matrice des politiques QoS d'entrée prises en charge :

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 la priorité IP de correspondance.
2. Cette option couvre la CoS de confiance, la priorité IP et le DSCP.
3. Cette option couvre également la définition de la priorité IP.

Il s'agit de l'action de stratégie valide pour la stratégie de sortie :

- police

Ce tableau présente la matrice des stratégies QoS de sortie prises en charge :

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 de modifier le niveau de QoS du paquet en fonction de la classification ou de la réglementation. La classification divise le trafic en différentes classes pour le traitement QoS en fonction des critères définis.

Le traitement QoS est basé sur le DSCP interne ; mesure du niveau de QoS du paquet. Le DSCP interne est dérivé en fonction de la configuration de confiance. Le système prend en charge les interfaces CoS, DSCP, de priorité IP et non approuvées. Trust spécifie le champ à partir duquel le DSCP interne est dérivé pour chaque paquet, comme suit :

- Lors de la confiance en CoS, le niveau QoS est dérivé de l'en-tête de couche 2 (L2) du protocole ISL (Inter-Switch Link Protocol) ou du paquet encapsulé 802.1Q.
- Lorsque vous configurez la priorité DSCP ou IP, le système déduit le niveau QoS du champ DSCP ou de priorité IP du paquet en conséquence.

La confiance en CoS n'a de sens que sur les interfaces d'agrégation, et la confiance en DSCP (ou la priorité IP) n'a de sens que pour les paquets IP.

Lorsqu'une interface n'est pas approuvée, le DSCP interne est dérivé de la CoS par défaut configurable pour l'interface correspondante. Il s'agit de l'état par défaut lorsque QoS est activé. Si aucune CoS par défaut n'est configurée, la valeur par défaut est zéro.

Une fois le DSCP interne déterminé, il peut être modifié par marquage et contrôle, ou conservé.

Une fois que le paquet a subi le traitement QoS, ses champs de niveau QoS (dans le champ IP/DSCP pour IP et dans l'en-tête ISL/802.1Q, le cas échéant) sont mis à jour à partir du DSCP interne. Il existe ces cartes QoS spéciales pertinentes pour la réglementation :

- **DSCP-to-Policed DSCP** : utilisé pour dériver le DSCP réglementé lorsque vous démarrez le paquet.
- **DSCP-to-CoS** : utilisé afin de dériver le niveau CoS du DSCP interne pour mettre à jour l'en-tête ISL/802.1Q du paquet sortant.
- **CoS-to-DSCP** : utilisé pour dériver le DSCP interne de la CoS entrante (en-tête ISL/802.1Q) lorsque l'interface est en mode CoS de confiance.

Il s'agit de considérations spécifiques à la mise en oeuvre :

- La stratégie de service d'entrée ne peut pas être associée à l'interface lorsque celle-ci est configurée pour faire confiance à l'une des métriques de QoS, telles que CoS/DSCP ou la priorité IP. Afin de faire correspondre la priorité DSCP/IP et la police en entrée, vous devez configurer l'approbation pour la classe particulière dans la stratégie, et non sur l'interface. Pour marquer en fonction de la priorité DSCP/IP, aucune approbation ne doit être configurée.
- Seul le trafic IPv4 sans options IP et l'encapsulation ARPA (Advanced Research Projects Agency) Ethernet II sont considérés comme du trafic IP du point de vue du matériel et de la

qualité de service. Tout autre trafic est considéré comme non-IP, y compris IP avec des options, telles que SNAP (SubNetwork Access Protocol) encapsulé IP et IPv6.
- Pour les paquets non IP, « match access group » est la seule méthode de classification car vous ne pouvez pas faire correspondre DSCP au trafic non IP. Une liste de contrôle d'accès au support (MAC) est utilisée à cette fin ; les paquets peuvent être mis en correspondance en fonction de l'adresse MAC source, de l'adresse MAC de destination et de l'EtherType. Il n'est pas possible de faire correspondre le trafic IP à la liste de contrôle d'accès MAC, car le commutateur fait une distinction entre le trafic IP et le trafic non IP.

Configurer et surveiller la réglementation

Ces étapes sont nécessaires pour configurer la réglementation dans Cisco IOS :

1. Définir un régulateur (pour les régulateurs agrégés)
2. Définir des critères pour sélectionner le trafic à contrôler
3. Définir une carte de classe pour sélectionner le trafic à l'aide de critères définis
4. Définissez une stratégie de service à l'aide de la classe et appliquez une stratégie à la classe spécifiée
5. Appliquer une stratégie de service à un port

Ces deux types de contrôleurs sont pris en charge :

- Agrégation nommée
- Individuel

Le régulateur d'agrégation nommé règle le trafic combiné de toutes les classes de la même stratégie à l'endroit où il est appliqué. La réglementation agrégée sur différentes interfaces n'est pas prise en charge.

Remarque : Le régulateur d'agrégation ne peut pas être appliqué à plusieurs stratégies. Si tel est le cas, ce message d'erreur s'affiche :

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

Considérez cet exemple :

Il existe un générateur de trafic connecté au port GigabitEthernet0/3 qui envoie environ 17 Mbits/s de trafic UDP avec le port de destination 111. Il y a également du trafic TCP à partir du port 20. Vous voulez que ces deux flux de trafic soient contrôlés jusqu'à 1 Mbit/s et que le trafic excessif soit abandonné. Cet exemple montre comment cela se 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 nommé. Contrairement au régulateur nommé, le régulateur individuel règle le trafic séparément sur chaque classe où il est appliqué. Le régulateur individuel est défini dans la configuration de la carte de stratégie. Dans cet exemple, deux classes de trafic sont contrôlées par deux contrôleurs individuels ; cl_udp11 est réglementé à 1 Mbit/s par rafale de 8 Ko et cl_tcp20 à 512 Kbits/s par rafale de 32 Ko :

```
!--- 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'opération de réglementation :

```
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
```

Remarque : Par défaut, il n'existe aucune statistique par DSCP. Le Catalyst 3550 prend en charge une collecte de statistiques par interface et par direction pour un maximum de huit valeurs DSCP différentes. Ceci est configuré lorsque vous émettez la commande **mls qos monitor**. Pour surveiller les statistiques des DSCP 8, 16, 24 et 32, vous devez émettre cette commande **par interface** :

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

Remarque : La **commande mls qos monitor dscp 8 16 24 32** modifie la sortie de la commande **show mls qos int g0/3 statistics** 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
```

Description des champs de l'exemple :

- **Incoming** : indique le nombre de paquets qui arrivent de chaque direction.
- **NO_change** : indique le nombre de paquets approuvés (niveau QoS non modifié, par exemple)
- **Classified** - indique le nombre de paquets auxquels ce DSCP interne a été affecté après classification
- **Policed** - indique le nombre de paquets marqués en bas par la police ; DSCP affiché avant le marquage.
- **Abandonné** : indique le nombre de paquets abandonnés par la réglementation.

Tenez compte de ces considérations spécifiques à la mise en oeuvre :

- Si huit valeurs DSCP sont configurées lorsque vous émettez la commande **mls qos monitor**, les autres compteurs affichés lors de l'émission de la commande **show mls qos int statistics** peuvent afficher des informations inadéquates.
- Il n'existe aucune commande spécifique afin de vérifier le débit de trafic offert ou sortant par agent de contrôle.
- Puisque les compteurs sont récupérés du matériel de manière séquentielle, il est possible que les compteurs ne s'additionnent pas correctement. Par exemple, la quantité de paquets contrôlés, classifiés ou abandonnés peut être légèrement différente du nombre de paquets entrants.

Configurer et surveiller le marquage

Ces étapes sont nécessaires pour configurer le marquage :

1. Définir les critères de classification du trafic
2. Définir les classes de trafic à classer avec les critères précédemment définis
3. Créer une carte de stratégie qui associe les actions de marquage et de réglementation aux classes définies

4. Configurer les interfaces correspondantes en mode approbation
5. Appliquer la carte de stratégie à une interface

Dans cet exemple, vous voulez que le trafic IP entrant soit l'hôte 192.168.192.168 marqué par la priorité IP 6 et réglementé à 1 Mbits/s ; le trafic excédentaire doit être marqué sur 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 **show mls qos interface statistics** est émise afin de surveiller le marquage. Les résultats et les implications des exemples sont documentés dans la section de ce document.

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

Sur le Catalyst 3550, la commande **match interface** n'est pas prise en charge et une seule commande match est autorisée par class-map. En outre, le Catalyst 3550 ne permet pas de faire correspondre le trafic IP aux ACL MAC. Le trafic IP et le trafic non IP doivent donc être classés avec deux cartes de classe distinctes. Il est donc difficile de classer tout le trafic entrant dans une interface et de contrôler tout le trafic avec un seul régulateur. L'exemple de configuration vous permet d'accomplir ceci. Dans cette configuration, le trafic IP et le trafic non-IP sont associés à deux cartes-classes différentes. Cependant, chacun utilise un régulateur commun pour les deux trafics.

```
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

- Configuration de la qualité de service sur Catalyst 3550
- Pages d'assistance pour la qualité de service
- Page de support sur la commutation LAN
- Pages de support pour les produits LAN
- Support et documentation techniques - Cisco Systems