Signalisation et réglementation QoS (Qualité de service) avec les moteurs de superviseur IOS Catalyst 4000/4500

Contenu

Introduction

La fonction de contrôle détermine si le niveau de trafic se trouve dans le profil spécifié (contrat). La fonction de réglementation permet de supprimer le trafic hors profil ou de marquer le trafic jusqu'à une valeur DSCP (Differential Services Code Point) différente pour appliquer le niveau de service contractuel. 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 pour transmettre le niveau de QoS du paquet.

La réglementation ne doit pas être confondue avec le formatage du trafic, bien que les deux garantissent que le trafic reste dans le profil (contrat). La réglementation ne met pas en mémoire tampon le trafic, de sorte que le délai de transmission n'est pas affecté. Au lieu de mettre en mémoire tampon des paquets hors profil, la réglementation les supprime ou les marque avec un niveau de QoS différent (marquage DSCP vers le bas). La mise en forme du trafic met en mémoire tampon le trafic hors profil et atténue les rafales de trafic, mais affecte les variations de délai et de délai. Le formatage ne peut être appliqué que sur une interface sortante, tandis que la réglementation peut être appliquée sur les interfaces entrantes et sortantes.

Catalyst 4000/4500 avec Supervisor Engine 3, 4 et 2+ (SE3, SE4, SE2+ désormais dans ce document) prend en charge la réglementation dans les directions entrantes et sortantes. Le formatage du trafic est également pris en charge, mais ce document ne traitera que de la réglementation et du marquage. Le marquage est un processus de modification du 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.

Paramètres de contrôle et de marquage QoS

La réglementation est établie en définissant les cartes de stratégie QoS et en les appliquant aux ports (QoS basée sur les ports) ou aux VLAN (QoS basée sur les VLAN). Le régulateur est défini par des paramètres de débit et de rafale, ainsi que par des actions pour le trafic dans le profil et hors profil.

Deux types de contrôleurs sont pris en charge : agrégé et par interface. Chaque régulateur peut être appliqué à plusieurs ports ou VLAN.

Le régulateur agrégé agit sur le trafic sur tous les ports/VLAN appliqués. Par exemple, nous appliquons le régulateur agrégé pour limiter le trafic TFTP (Trivial File Transfer Protocol) à 1 Mbits/s sur les VLAN 1 et 3. Un tel régulateur autorise 1 Mbits/s de trafic TFTP dans les VLAN 1 et 3 ensemble. Si nous appliquons un régulateur par interface, il limitera le trafic TFTP sur les VLAN 1 et 3 à 1 Mbits/s chacun.

Remarque : Si la réglementation d'entrée et de sortie est appliquée à un paquet, la décision la plus sévère sera prise. Autrement dit, si le régulateur d'entrée spécifie de supprimer le paquet et que le régulateur de sortie spécifie de marquer le paquet vers le bas, le paquet sera supprimé. Le tableau 1 récapitule l'action QoS sur le paquet lorsqu'il est traité à la fois par des stratégies d'entrée et de sortie.

Tableau 1 : Action QoS en fonction de la politique 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$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

Le matériel QoS du Catalyst 4000 SE3, SE4, SE2+ est mis en oeuvre de telle sorte que le marquage réel du paquet se produit après le régulateur de sortie. Cela signifie que même si la stratégie d'entrée remarque le paquet (par marquage par le régulateur ou par marquage normal), la stratégie de sortie verra toujours les paquets marqués avec le niveau QoS d'origine. La stratégie de sortie voit le paquet comme s'il n'avait pas été marqué par la stratégie d'entrée. Cela signifie que :

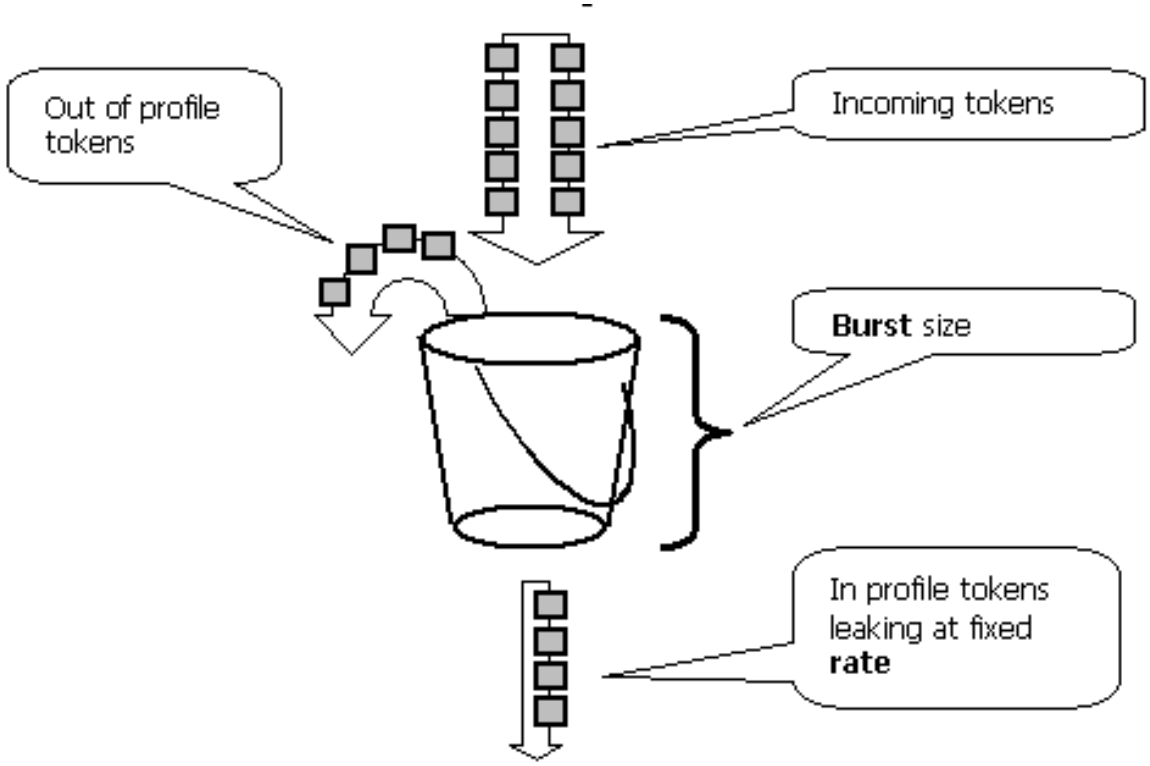
- Le marquage de sortie remplace le marquage d'entrée.

- La stratégie de sortie ne peut pas correspondre aux nouveaux niveaux de QoS modifiés par le marquage d'entrée.

Les autres conséquences importantes sont les suivantes :

- Il n'est pas possible de marquer et de marquer dans la même classe de trafic dans la même politique.
- Les régulateurs agrégés sont par direction. En d'autres termes, si un régulateur d'agrégat est appliqué à la fois en entrée et en sortie, il y aura deux régulateurs d'agrégat, l'un sur les entrées et l'autre sur les sorties.
- Lorsqu'un régulateur d'agrégation est appliqué dans la stratégie aux VLAN et à l'interface physique, il y a effectivement deux régulateurs d'agrégat - l'un pour les interfaces VLAN et l'autre pour les interfaces physiques. Actuellement, il n'est pas possible de contrôler ensemble les interfaces VLAN et physiques.

La réglementation dans les commutateurs Catalyst 4000 SE3, SE4, SE2+ est conforme au concept de seau fuité, comme le montre le modèle ci-dessous. Les jetons correspondant aux paquets de trafic entrants sont placés dans un compartiment (# de jetons = taille du paquet). À intervalles réguliers, un nombre défini de jetons (dérivé du taux 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 abandonné ou marqué vers le bas, conformément à l'action de réglementation configurée.



Il est à noter que le trafic n'est pas mis en mémoire tampon dans le compartiment, comme il peut apparaître dans le modèle ci-dessus. Le trafic réel ne passe pas du tout par le seau. Le compartiment est seulement utilisé pour décider si le paquet est dans le profil ou hors profil.

Notez que la mise en oeuvre matérielle exacte de la réglementation peut être différente, fonctionnellement elle est conforme au modèle ci-dessus.

Les paramètres suivants contrôlent le fonctionnement de la réglementation :

- Rate définit le nombre de jetons supprimés à chaque intervalle. Ceci définit effectivement le débit de réglementation. Tout le trafic au-dessous du débit est considéré comme dans le profil.
- L'intervalle définit la fréquence à laquelle les jetons sont supprimés du compartiment. L'intervalle est fixé à 16 nanosecondes (16 sec *10-9). Impossible de modifier l'intervalle.
- Burst définit la quantité maximale de jetons que le compartiment peut contenir à tout moment.

Référez-vous à la section Comparer la réglementation et le marquage sur les moteurs de supervision basés sur IOS Catalyst 6000 et Catalyst 4000/4500 à la fin de ce document pour connaître les différences de rafales entre Catalyst 6000 et Catalyst 4000 SE3, SE4, SE2+.

Le régulateur s'assure que si vous examinez une période quelconque (de zéro à infini) que le régulateur n'autorisera jamais plus de

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

de trafic par le policier pendant cette période.

Le matériel QoS Catalyst 4000 SE3, SE4, SE2+ présente une certaine granularité pour la réglementation. Selon le taux configuré, l'écart maximal par rapport au taux est de 1,5 %.

Lors de la configuration du débit de rafale, vous devez tenir compte du fait que certains protocoles (tels que TCP) implémentent des mécanismes de contrôle de flux qui réagissent en cas de perte de paquets. Par exemple, TCP réduit la fenêtre de moitié pour chaque paquet perdu. Lorsque le débit est contrôlé à un certain débit, l'utilisation effective de la liaison est inférieure au débit configuré. On peut augmenter la rafale afin d'obtenir une meilleure utilisation. Un bon début pour un tel trafic serait de définir la rafale comme égale au double de la quantité de trafic envoyée avec le débit souhaité pendant le temps de trajet aller-retour (RTT). Pour la même raison, il n'est pas recommandé de comparer le fonctionnement du régulateur par le trafic orienté connexion, car il affichera généralement des performances inférieures à celles autorisées par le régulateur.

Remarque : 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 (bloc entier).

Par exemple, voici un calcul de la rafale pour une session TCP, avec un débit de réglementation de 64 Kbits/s et un RTT TCP de 0,05 secondes :

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

Remarque : <burst**>** concerne une session TCP, il doit donc être mis à l'échelle pour indiquer le nombre moyen de sessions devant passer par le régulateur. Il s'agit uniquement d'un exemple, donc dans chaque cas, il faut évaluer les exigences et le comportement du trafic/application par rapport aux ressources disponibles afin de choisir les paramètres de réglementation.

L'action de réglementation consiste à supprimer le paquet (abandonner) ou à modifier le DSCP du paquet (marquer vers le bas). Afin de marquer le paquet en aval, la carte DSCP contrôlée doit être modifiée. Le DSCP réglementé par défaut indique le paquet au même DSCP, c'est-à-dire qu'aucun signe de désactivation ne se produit.

Remarque : les paquets peuvent être envoyés hors de l'ordre lorsqu'un paquet hors profil est marqué vers un DSCP vers une file d'attente de sortie différente de celle du DSCP d'origine. Pour

cette raison, si l'ordre des paquets est important, il est recommandé de marquer les paquets hors profil vers DSCP mappés à la même file d'attente de sortie que les paquets de profil.

Fonctions de contrôle et de marquage prises en charge par les moteurs de supervision Catalyst 4000/4500 basés sur IOS

La réglementation des entrées (interface entrante) et des sorties (interface sortante) est prise en charge sur Catalyst 4000 SE3, SE4, SE2+. Le commutateur prend en charge les régulateurs d'entrée et de sortie 1024. Deux régulateurs d'entrée et deux régulateurs de sortie sont utilisés par le système pour le comportement de non-réglementation par défaut.

Notez que lorsque le régulateur d'agrégation est appliqué dans la stratégie à un VLAN et à une interface physique, une entrée supplémentaire de régulateur matériel est utilisée. Actuellement, il n'est pas possible de contrôler ensemble les interfaces VLAN et physiques. Cela pourrait être modifié dans les versions ultérieures du logiciel.

Toutes les versions logicielles prennent en charge la réglementation. Le Catalyst 4000 prend en charge jusqu'à 8 instructions de correspondance valides par classe et jusqu'à 8 classes sont prises en charge par policy-map. Les instructions de correspondance valides sont les suivantes :

- match access-group
- match ip dscp
- match ip priority
- correspondent à

Remarque : Pour les paquets V4 non IP, l'instruction **match ip dscp** est la seule méthode de classification, à condition que les paquets entrent dans des ports d'agrégation faisant confiance à CoS. Ne vous laissez pas induire en erreur par le mot clé ip dans la commande **match ip dscp**, car le DSCP interne est mis en correspondance, cela s'applique à tous les paquets, pas seulement à IP. Lorsqu'un port est configuré pour faire confiance à CoS, ce dernier est extrait de la trame L2 (802.1Q ou étiquetée ISL) et converti en DSCP interne à l'aide d'une carte CoS vers DSCP QoS. Cette valeur DSCP interne peut ensuite être mise en correspondance dans la stratégie à l'aide de **match ip dscp**.

Les actions de stratégie valides sont les suivantes :

- police
- set ip dscp
- set ip priority
- trust dscp
- TRUST CO

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 de critères définis. Afin de correspondre à la priorité IP ou DSCP, l'interface entrante correspondante doit être définie sur le mode approuvé. Le commutateur prend en charge la CoS de confiance, le DSCP de confiance et les interfaces non fiables. Trust spécifie le champ à partir duquel le niveau de QoS du paquet sera dérivé.

Lorsque vous configurez CoS, le niveau QoS est dérivé de l'en-tête L2 du paquet encapsulé ISL ou 802.1Q. Lors de la confiance en DSCP, le commutateur dérive le niveau QoS du champ DSCP du paquet. La confiance en CoS n'a de sens que sur les interfaces d'agrégation, et la confiance en

DSCP est valide pour les paquets IP V4 uniquement.

Lorsqu'une interface n'est pas approuvée (il s'agit de l'état par défaut lorsque QoS est activé), le DSCP interne est dérivé de la CoS ou du DSCP par défaut configurable pour l'interface correspondante. Si aucune CoS ou DSCP par défaut n'est configurée, la valeur par défaut sera zéro (0). Une fois que le niveau de QoS initial du paquet est déterminé, il est mappé dans le DSCP interne. Le DSCP interne peut être conservé ou modifié par marquage ou réglementation.

Après le traitement QoS du paquet, les champs de niveau QoS (dans le champ IP DSCP pour IP et dans l'en-tête ISL/802.1Q, le cas échéant) seront mis à jour à partir du DSCP interne.

Il existe des cartes spéciales utilisées pour convertir les métriques de QoS de confiance du paquet en DSCP interne et vice versa. Ces cartes sont les suivantes :

- DSCP vers DSCP réglementé ; utilisé pour dériver le DSCP réglementé lors du marquage du paquet.
- DSCP vers CoS : utilisé pour dériver le niveau CoS du DSCP interne pour mettre à jour l'en-tête ISL/802.1Q du paquet sortant.
- CoS vers DSCP : utilisé pour dériver le DSCP interne de CoS entrant (en-tête ISL/802.1Q) lorsque l'interface est en mode CoS de confiance.

Notez que lorsqu'une interface est en mode CoS approuvé, la CoS sortante sera toujours la même que la CoS entrante. Ceci est spécifique à la mise en oeuvre de QoS dans Catalyst 4000 SE3, SE4, SE2+.

Configuration et surveillance de la réglementation

La configuration de la réglementation dans IOS implique les étapes suivantes :

1. Définition d'un régulateur.
2. Définition de critères pour sélectionner le trafic à contrôler.
3. Définition de stratégie de service à l'aide de la classe et application d'un régulateur à une classe spécifiée.
4. Application d'une stratégie de service à un port ou à un VLAN.

Prenons l’exemple suivant : Un générateur de trafic est connecté au port 5/14, envoyant ~17 Mbits/s de trafic UDP avec une destination du port 111. Nous voulons que ce trafic soit contrôlé jusqu'à 1 Mbit/s et qu'un trafic excessif soit abandonné.

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
```

```
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
interface Vlan 2
service-policy output po_test
!
```

Notez que lorsqu'un port est en mode QoS basé sur VLAN, mais qu'aucune stratégie de service n'est appliquée au VLAN correspondant, le commutateur suit la stratégie de service (le cas échéant) appliquée à un port physique. Cela permet une plus grande flexibilité dans la combinaison de la qualité de service basée sur les ports et sur les VLAN.

Deux types de contrôleurs sont pris en charge : agrégat nommé et par interface. Un régulateur d'agrégation nommé contrôle le trafic combiné de toutes les interfaces auxquelles il est appliqué. L'exemple ci-dessus a utilisé un régulateur nommé. Un régulateur par interface, contrairement à un régulateur nommé, contrôle le trafic séparément sur chaque interface où il est appliqué. Un régulateur par interface est défini dans la configuration de mappage de réglementation. Prenons l'exemple suivant avec un régulateur d'agrégation par interface :

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

La commande suivante est utilisée pour surveiller les opérations de réglementation :

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
```

```
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
```

Le compteur près de class-map compte le nombre de paquets correspondant à la classe correspondante.

Tenez compte des considérations spécifiques à la mise en oeuvre suivantes :

- Le compteur de paquets par classe n'est pas par interface. Autrement dit, il compte tous les paquets correspondant à la classe parmi toutes les interfaces où cette classe est appliquée dans la stratégie de service.
- Les régulateurs ne gèrent pas les compteurs de paquets, seuls les compteurs d'octets sont pris en charge.
- Il n'existe aucune commande spécifique permettant de vérifier le débit de trafic offert ou sortant par agent de contrôle.
- Les compteurs sont mis à jour périodiquement. Si vous exécutez la commande ci-dessus à plusieurs reprises, les compteurs peuvent toujours apparaître à un moment donné.

Configuration et surveillance du marquage

La configuration du marquage implique les étapes suivantes :

1. Définissez les critères de classification du trafic - liste d'accès, DSCP, priorité IP, etc.
2. Définissez les classes de trafic à classifier à l'aide de critères précédemment définis.
3. Créez une carte de stratégie associant des actions de marquage et/ou de réglementation aux classes définies.
4. Configuration du mode de confiance sur les interfaces correspondantes.
5. Appliquer la carte de stratégie à une interface.

Prenons l'exemple suivant où nous voulons que le trafic entrant ayant la priorité IP 3 soit mappé à l'hôte 192.168.196.3, le port UDP 777 est mappé à la priorité IP 6. Tout autre trafic de priorité IP 3 est réglementé à 1 Mbit/s et le trafic excédentaire doit être marqué à la priorité IP 2.

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
```

```
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

La commande **sh policy interface** permet de surveiller le marquage. L'exemple de résultat et les implications sont documentés dans la configuration de la réglementation ci-dessus.

Comparaison de la réglementation et du marquage sur les moteurs de supervision IOS Catalyst 6000 et Catalyst 4000/4500

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

Informations connexes

- Présentation et configuration de la QoS

- Support technique - Cisco Systems