Classification et signalisation QoS sur les commutateurs des gammes Catalyst 6500/6000 qui exécutent le logiciel Cisco IOS

Contenu

Introduction

Ce document examine ce qui se produit pour le marquage et la classification d'un paquet à diverses étapes au sein du Cisco Catalyst 6500/6000 qui exécute le logiciel Cisco IOS®. Ce document décrit des cas particuliers et des restrictions, et il aborde quelques études de cas.

Ce document ne fournit pas une liste exhaustive de toutes les commandes du logiciel Cisco IOS relatives à la qualité de service ou au marquage. Pour plus d'informations sur l'interface de ligne de commande (CLI) du logiciel Cisco IOS, référez-vous à Configuration de la QoS PFC.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel suivantes :

- Commutateurs de la gamme Catalyst 6500/6000 qui exécutent le logiciel Cisco IOS et utilisent l'un des moteurs de supervision suivants :Un Supervisor Engine 1A avec une carte PFC (Policy Feature Card) et une carte MSFC (Multilayer Switch Feature Card)Un Supervisor Engine 1A avec une carte PFC et une carte MSFC2Un Supervisor Engine 2 avec une carte PFC2 et une carte MSFC2

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.

Terminologie

La liste fournit la terminologie utilisée par ce document :

- DSCP (Differentiated Services Code Point) : les six premiers bits du type d'octet de service (ToS) de l'en-tête IP. DSCP est présent uniquement dans le paquet IP.**Remarque :** le commutateur attribue également un DSCP interne à chaque paquet, qu'il soit IP ou non IP. La section Quatre sources possibles pour DSCP interne de ce document détaille cette affectation DSCP interne.
- Priorité IP : les trois premiers bits de l'octet ToS de l'en-tête IP.
- Classe de service (CoS) : le seul champ pouvant être utilisé pour marquer un paquet au niveau de la couche 2 (L2). CoS se compose de l'un des trois bits suivants :Les trois bits IEEE 802.1p (dot1p) de la balise IEEE 802.1Q (dot1q) pour le paquet dot1q.**Remarque :** Par défaut, les commutateurs Cisco n'étiquettent pas les paquets VLAN natifs.Les trois bits appelés « Champ utilisateur » dans l'en-tête ISL (Inter-Switch Link) pour un paquet encapsulé ISL.**Remarque :** la CoS n'est pas présente dans un paquet non dot1q ou ISL.
- Classification : processus utilisé pour sélectionner le trafic à marquer.
- Marquage : processus qui définit une valeur DSCP de couche 3 (L3) dans un paquet. Ce document étend la définition du marquage pour inclure la définition des valeurs CoS L2.

Les commutateurs de la gamme Catalyst 6500/6000 peuvent effectuer des classifications sur la base de ces trois paramètres :

- DSCP
- Priorité IP
- CoS

Les commutateurs de la gamme Catalyst 6500/6000 effectuent la classification et le marquage à différentes étapes. Voici ce qui se passe à différents endroits :

- Port d'entrée (circuit intégré spécifique à l'application d'entrée [ASIC])
- Moteur de commutation (PFC)
- Port de sortie (ASIC de sortie)

Gestion des ports d'entrée

Le paramètre de configuration principal pour le port d'entrée, en ce qui concerne la classification, est l'état `d'approbation` du port. Chaque port du système peut avoir l'un de ces états `d'approbation` :

- `trust-ip-priority`
- `trust-dscp`
- `trust-cos`
- `non fiable`

Afin de définir ou de modifier l'état `d'approbation des` ports, émettez cette commande du logiciel Cisco IOS en mode `interface` :

```
6k(config-if)#mls qos trust ?
  cos            cos keyword
  dscp           dscp keyword
  ip-precedence  ip-precedence keyword
  <cr>
```

Remarque : Par défaut, tous les ports sont dans l'état `non approuvé` lorsque QoS est activé. Afin d'activer la QoS sur le Catalyst 6500 qui exécute le logiciel Cisco IOS, émettez la commande **mls qos** en mode de configuration principal.

Au niveau du port d'entrée, vous pouvez également appliquer une CoS par défaut par port. Voici un exemple :

```
6k(config-if)#mls qos cos cos-value
```

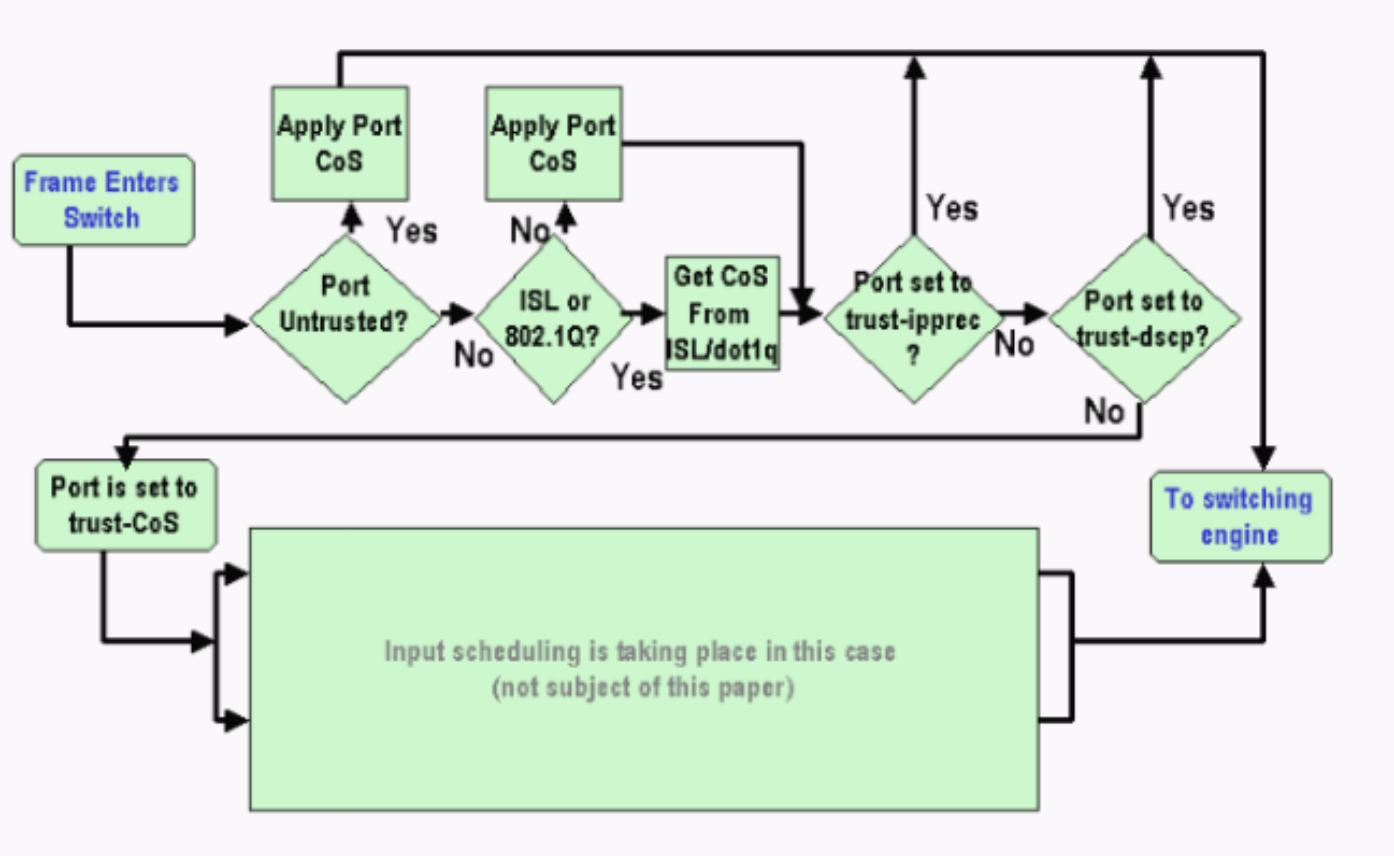
Cette CoS par défaut s'applique à tous les paquets, tels que IP et IPX (Internetwork Packet Exchange). Vous pouvez appliquer la CoS par défaut à n'importe quel port physique.

Si le port est dans l'état `non approuvé`, marquez la trame avec la CoS par défaut du port et passez l'en-tête au moteur de commutation (PFC). Si le port est défini sur l'un des états `d'approbation`, exécutez l'une des deux options suivantes :

- Si la trame n'a pas de CoS reçu (dot1q ou ISL), appliquez la CoS du port par défaut.
- Pour les trames dot1q et ISL, conservez la CoS telle quelle.

Puis, passez la trame au moteur de commutation.

Cet exemple illustre la classification et le marquage des entrées. L'exemple montre comment attribuer une CoS interne à chaque trame :



Remarque : Comme le montre cet exemple, chaque trame est affectée à une CoS interne. L'affectation est basée sur la CoS reçue ou la CoS du port par défaut. La CoS interne inclut des trames non étiquetées qui ne transportent aucune CoS réelle. La CoS interne est écrite dans un en-tête de paquet spécial, appelé en-tête de bus de données, et envoyée par le bus de données au moteur de commutation.

PFC (Switching Engine)

Lorsque l'en-tête atteint le moteur de commutation, la logique EARL (Enhanced Address Recognition Logic) du moteur de commutation attribue à chaque trame un DSCP interne. Ce DSCP interne est une priorité interne qui est attribuée à la trame par la carte PFC lorsque la trame transite le commutateur. Il ne s'agit pas du DSCP dans l'en-tête IP version 4 (IPv4). Le DSCP interne provient d'un paramètre CoS ou ToS existant et est utilisé pour réinitialiser la CoS ou ToS lorsque la trame quitte le commutateur. Ce DSCP interne est attribué à toutes les trames qui sont commutées ou routées par la carte PFC, même les trames non IP.

Cette section explique comment affecter une stratégie de service à l'interface afin d'effectuer un marquage. La section traite également du paramètre final du DSCP interne, qui dépend de l'état `d'approbation` du port et de la stratégie de service appliquée.

Configurer la stratégie de service pour classer ou marquer un paquet dans le logiciel Cisco IOS Version 12.1(12c)E et ultérieure

Complétez ces étapes afin de configurer la stratégie de service :

1. Configurez une liste de contrôle d'accès (ACL) pour définir le trafic que vous voulez prendre en compte.La liste de contrôle d’accès peut être numérotée ou nommée et le Catalyst 6500/6000 prend en charge une liste de contrôle d’accès étendue. Émettez la commande **access-list *xxx*** du logiciel Cisco IOS, comme le montre cet exemple :
```
(config)#access-list 101 permit ip any host 10.1.1.1
```

2. Configurez une classe de trafic (class map) pour qu'elle corresponde au trafic sur la base de la liste de contrôle d'accès que vous avez définie ou sur la base du DSCP reçu.Émettez la commande **class-map** du logiciel Cisco IOS. La QoS PFC ne prend pas en charge plus d'une instruction de correspondance par mappage de classe. En outre, la QoS PFC prend uniquement en charge ces instructions de correspondance :**match ip access-groupmatch ip dscpmatch ip prioritymatch protocolRemarque :** La commande **match protocol** permet d'utiliser la reconnaissance d'application basée sur le réseau (NBAR) pour faire correspondre le trafic.**Remarque :** Parmi ces options, seules les instructions **match ip dscp** et **match ip priority** sont prises en charge et fonctionnent. Ces instructions ne sont toutefois pas utiles pour le marquage ou la classification des paquets. Vous pouvez utiliser ces instructions, par exemple, pour appliquer des règles à tous les paquets qui correspondent à un certain DSCP. Cependant, cette action dépasse le cadre de ce document.
```
(config)#class-map class-name
(config-cmap)#match {access-group | input-interface | ip dscp}
```
Remarque : Cet exemple montre seulement trois options pour la commande **match**. Mais vous pouvez configurer beaucoup plus d'options à cette invite de commandes.**Remarque :** Toutes les options de cette commande **match** sont prises pour les critères match et les autres options sont laissées de côté, selon les paquets entrants.Voici un exemple :

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. Configurez une carte de stratégie pour appliquer une stratégie à une classe que vous avez précédemment définie.La carte de stratégie contient :Un nomEnsemble d'instructions de classePour chaque instruction de classe, l'action qui doit être effectuée pour cette classeLes actions prises en charge dans la QoS PFC1 et PFC2 sont les suivantes :**trust dscptrust ip priorityTRUST COset ip dscp** dans le logiciel Cisco IOS Version 12.1(12c)E1 et ultérieure**définir la priorité ip** dans le logiciel Cisco IOS Version 12.1(12c)E1 et ultérieure**policeRemarque :** Cette action dépasse le cadre de ce document.
```
(config)#policy-map policy-name
(config-pmap)#class class-name
(config-pmap-c)#{police | set ip dscp}
```

Remarque : Cet exemple montre seulement deux options, mais vous pouvez configurer beaucoup plus d'options à l'invite de commande `(config-pmap-c)#`.Voici un exemple :

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   set ip dscp 16
```

4. Configurez une entrée de stratégie de service pour appliquer une carte de stratégie que vous

avez précédemment définie à une ou plusieurs interfaces.**Remarque :** Vous pouvez associer une stratégie de service à l'interface physique ou à l'interface virtuelle commutée (SVI) ou VLAN. Si vous associez une stratégie de service à une interface VLAN, les seuls ports qui utilisent cette stratégie de service sont les ports qui appartiennent à ce VLAN et sont configurés pour la QoS basée sur VLAN. Si le port n'est pas défini pour la QoS basée sur VLAN, le port utilise toujours la QoS basée sur le port par défaut et ne regarde que la politique de service qui est connectée à l'interface physique.Cet exemple applique la stratégie de service `test_policy` au port Gigabit Ethernet 1/1 :

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Cet exemple applique la stratégie de service `test_policy` à tous les ports du VLAN 10 qui ont une configuration basée sur VLAN du point de vue de la QoS :

```
(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Remarque : Vous pouvez combiner les étapes 2 et 3 de cette procédure si vous ignorez la définition spécifique de la classe et joignez directement la liste de contrôle d'accès dans la définition de la carte de stratégie. Dans cet exemple, lorsque la `police TEST` de classe n'a pas été définie avant la configuration de la carte de stratégie, la classe est définie dans la carte de stratégie :

```
(config)#policy-map policy-name
(config-pmap)#class class_name {access-group acl_index_or_name | dscp dscp_1 [dscp_2
[dscp_N]] | precedence ipp_1 [ipp_2 [ipp_N]]}
!--- Note: This command should be on one line.

policy-map TEST
class TEST police access-group 101
```

Configurer la stratégie de service pour classer ou marquer un paquet dans les versions du logiciel Cisco IOS antérieures à la version 12.1(12c)E du logiciel Cisco IOS

Dans les versions du logiciel Cisco IOS antérieures à la version 12.1(12c)E1 du logiciel Cisco IOS, vous ne pouvez pas utiliser l'action **set ip dscp** ou **set ip priority** dans une carte de stratégie. Par conséquent, le seul moyen de marquer un trafic spécifique défini par une classe est de configurer un régulateur avec un taux très élevé. Ce débit doit être, par exemple, au moins le débit de ligne du port ou quelque chose de suffisamment élevé pour permettre à tout le trafic de toucher ce régulateur. Ensuite, utilisez **set-dscp-transmit *xx*** comme action de conformité. Pour configurer cette configuration, procédez comme suit :

1. Configurez une liste de contrôle d’accès pour définir le trafic à prendre en compte.La liste de contrôle d’accès peut être numérotée ou nommée et le Catalyst 6500/6000 prend en charge une liste de contrôle d’accès étendue. Émettez la commande **access-list *xxx*** du logiciel Cisco IOS, comme le montre cet exemple :

   ```
   (config)#access-list 101 permit ip any host 10.1.1.1
   ```

2. Configurez une classe de trafic (class map) pour qu'elle corresponde au trafic sur la base de la liste de contrôle d'accès que vous avez définie ou sur la base du DSCP reçu.Émettez la commande **class-map** du logiciel Cisco IOS. La QoS PFC ne prend pas en charge plus d'une instruction de correspondance par mappage de classe. En outre, la QoS PFC prend uniquement en charge ces instructions de correspondance :**match ip access-groupmatch ip dscpmatch ip prioritymatch protocolRemarque :** La commande **match protocol** permet d'utiliser NBAR pour faire correspondre le trafic.**Remarque :** Parmi ces instructions, seules les instructions **match ip dscp** et **match ip priority** sont prises en charge et fonctionnent. Ces instructions, cependant, ne sont pas utiles pour le marquage ou la classification des paquets. Vous pouvez utiliser ces instructions, par exemple, pour appliquer des règles à tous les paquets qui correspondent à un certain DSCP. Cependant, cette action dépasse le cadre de ce document.

```
(config)#class-map  class-name
(config-cmap)#match {access-group | input-interface | ip dscp}
```

   Remarque : Cet exemple montre seulement trois options pour la commande **match**. Mais vous pouvez configurer beaucoup plus d'options à cette invite de commandes.Voici un exemple :

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. Configurez une carte de stratégie pour appliquer une stratégie à une classe que vous avez précédemment définie.La carte de stratégie contient :Un nomEnsemble d'instructions de classePour chaque instruction de classe, l'action qui doit être effectuée pour cette classeLes actions prises en charge dans la QoS PFC1 ou PFC2 sont les suivantes :**trust dscptrust ip priorityTRUST COpolice**Vous devez utiliser l'instruction **police** car les actions **set ip dscp** et **set ip priority** ne sont pas prises en charge. Puisque vous ne voulez pas vraiment contrôler le trafic, mais simplement le marquer, utilisez un régulateur défini pour autoriser tout le trafic. Par conséquent, configurez le régulateur avec un débit élevé et une rafale. Par exemple, vous pouvez configurer le régulateur avec le débit maximal autorisé et la rafale. Voici un exemple :

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   police  4000000000 31250000 conform-action
   set-dscp-transmit 16 exceed-action policed-dscp-transmit
```

4. Configurez une entrée de stratégie de service pour appliquer une carte de stratégie que vous avez précédemment définie à une ou plusieurs interfaces.**Remarque :** La stratégie de service peut être associée à une interface physique ou à l'interface SVI ou VLAN. Si une stratégie de service est associée à une interface VLAN, seuls les ports qui appartiennent à ce VLAN et qui sont configurés pour la QoS basée sur VLAN utilisent cette stratégie de service. Si le port n'est pas défini pour la QoS basée sur VLAN, le port utilise toujours la QoS basée sur le port par défaut et ne regarde qu'une politique de service qui est connectée à l'interface

physique.Cet exemple applique la stratégie de service `test_policy` au port Gigabit Ethernet 1/1 :

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

Cet exemple applique la stratégie de service `test_policy` à tous les ports du VLAN 10 qui ont une configuration basée sur VLAN du point de vue de la QoS :

```
(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Quatre sources possibles pour le DSCP interne

Le DSCP interne est dérivé de l'une des valeurs suivantes :

1. Valeur DSCP reçue existante, définie avant que la trame n'entre dans le commutateurUn exemple est **trust dscp**.
2. Bits de priorité IP reçus qui sont déjà définis dans l'en-tête IPv4Comme il existe 64 valeurs DSCP et seulement huit valeurs de priorité IP, l'administrateur configure un mappage que le commutateur utilise pour dériver le DSCP. Les mappages par défaut sont en place, dans le cas où l'administrateur ne configure pas les mappages. Un exemple est **trust ip priority**.
3. Les bits CoS reçus qui sont déjà définis avant que la trame n'entre dans le commutateur et qui sont stockés dans l'en-tête du bus de données, ou s'il n'y avait pas de CoS dans la trame entrante, à partir de la CoS par défaut du port entrantComme pour la priorité IP, il existe un maximum de huit valeurs CoS, chacune devant être mappée à l'une des 64 valeurs DSCP. L'administrateur peut configurer cette carte ou le commutateur peut utiliser la carte par défaut qui est déjà en place.
4. La stratégie de service peut définir une valeur spécifique pour le DSCP interne.

Pour les numéros 2 et 3 de cette liste, le mappage statique est par défaut, de la manière suivante :

- Pour le mappage CoS-DSCP, le DSCP dérivé équivaut à huit fois le CoS.
- Pour le mappage de priorité IP à DSCP, le DSCP dérivé est égal à huit fois la priorité IP.

Vous pouvez émettre ces commandes afin de remplacer et vérifier ce mappage statique :

- **mls qos map ip-cipp-dscp** *dscp_1 dscp_2 dscp_3 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*
- **mls qos map cos-dscp** *dscp_1 dscp_2 dscp_3 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*

La première valeur du DSCP qui correspond au mappage de la CoS (ou priorité IP) est 0. La deuxième valeur pour la CoS (ou priorité IP) est 1 et le modèle se poursuit de cette manière. Par exemple, cette commande modifie le mappage de sorte que la CoS 0 soit mappée au DSCP de 0 et que la CoS de 1 soit mappée au DSCP de 8, etc. :

```
Cat65(config)#mls qos map cos-dscp 0 8 16 26 32 46 48 54
Cat65#show mls qos maps
```

```
CoS-dscp map:
 cos:     0 1  2   3   4   5   6   7
  ---------------------------------
 dscp:    0 8 16  26  32  46  48  54
```

Comment le DSCP interne est-il sélectionné ?

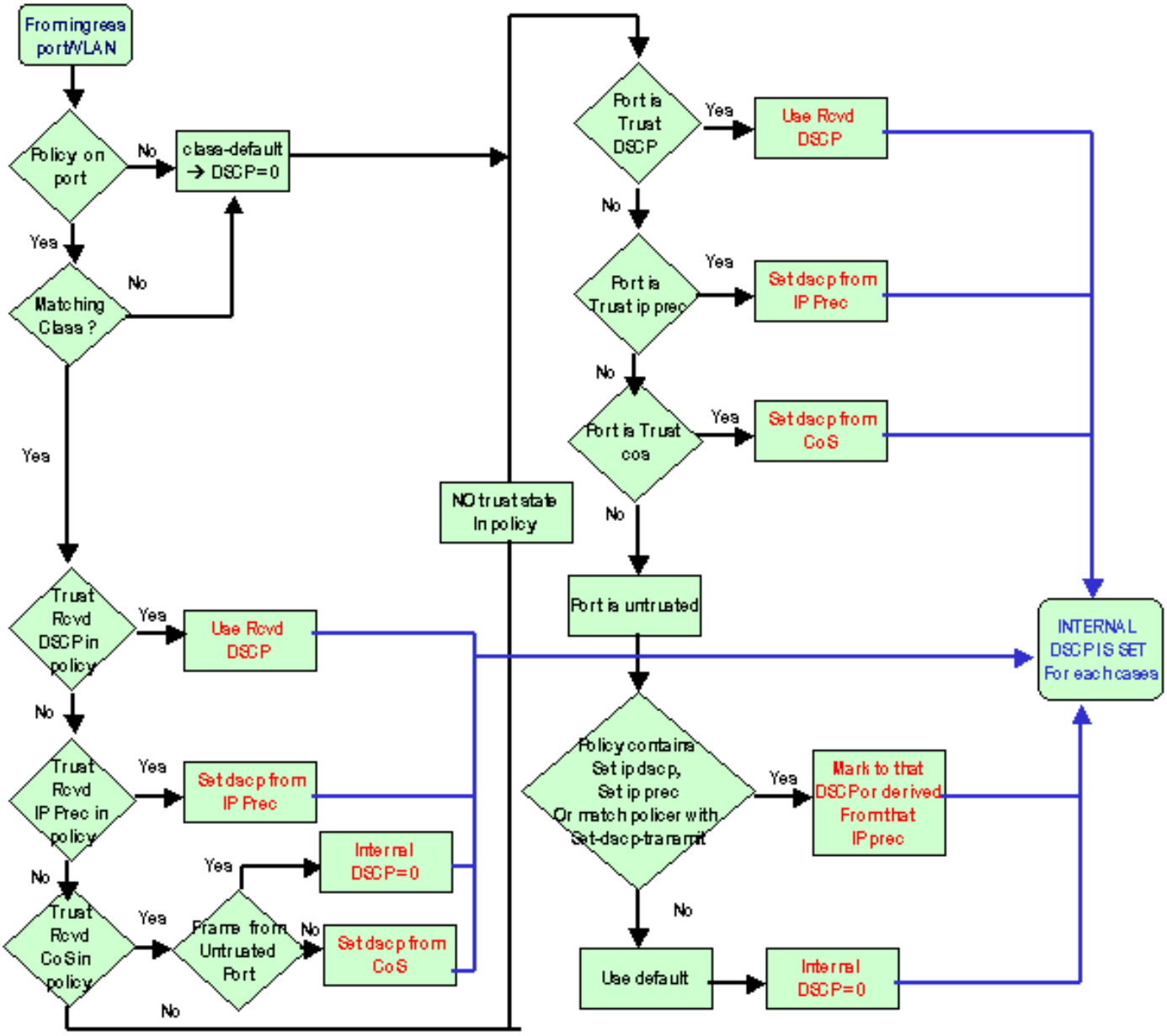
Le DSCP interne est choisi sur la base de ces paramètres :

- Mappage de stratégie QoS appliqué au paquetLa carte de stratégie QoS est déterminée par les règles suivantes :Si aucune stratégie de service n'est associée au port ou au VLAN entrant, utilisez la valeur par défaut.**Remarque :** cette action par défaut consiste à définir le DSCP interne sur 0.Si une stratégie de service est associée au port ou au VLAN entrant, et si le trafic correspond à l'une des classes définies par la stratégie, utilisez cette entrée.Si une stratégie de service est associée au port ou au VLAN entrant, et si le trafic ne correspond pas à l'une des classes définies par la stratégie, utilisez la valeur par défaut.
- L'état `d'approbation` du port et l'action de la carte de stratégieLorsque le port a un état de `confiance` spécifique et une politique avec une certaine marque (action de confiance en même temps), ces règles s'appliquent :La commande **set ip dscp** ou DSCP définie par agent de contrôle dans une carte de stratégie n'est appliquée que si le port est laissé dans l'état `non approuvé`.Si le port a un état `d'approbation`, cet état `d'approbation` est utilisé pour dériver le DSCP interne. L'état `d'approbation` du port prime toujours sur la commande **set ip dscp**.La commande **trust *xx dans une carte de stratégie a priorité sur l'***état `trust` du port.Si le port et la stratégie contiennent un état `d'approbation` différent, l'état `d'approbation` qui provient de la carte de stratégie est pris en compte.

Par conséquent, le DSCP interne dépend de ces facteurs :

- L'état `d'approbation` du port
- Stratégie de service (avec l'utilisation d'une liste de contrôle d'accès) connectée au port
- La carte de stratégie par défaut**Remarque :** la valeur par défaut du DSCP est 0.
- Basé sur VLAN ou sur port en ce qui concerne la liste de contrôle d’accès

Ce schéma résume la manière dont le DSCP interne est choisi sur la base de la configuration :



La carte PFC est également capable de contrôler. Cela peut éventuellement entraîner une démarcation du DSCP interne. Pour plus d'informations sur la réglementation, référez-vous à Contrôle QoS sur les commutateurs de la gamme Catalyst 6500/6000.

Gestion des ports de sortie

Vous ne pouvez rien faire au niveau du port de sortie afin de modifier la classification. Cependant, marquez le paquet sur la base de ces règles :

- Si le paquet est un paquet IPv4, copiez le DSCP interne que le moteur de commutation attribue dans l'octet ToS de l'en-tête IPv4.
- Si le port de sortie est configuré pour une encapsulation ISL ou dot1q, utilisez une CoS dérivée du DSCP interne. Copiez la CoS dans la trame ISL ou dot1q.

Remarque : La CoS est dérivée du DSCP interne selon une valeur statique. Émettez cette commande afin de configurer la statique :

```
Router(config)#mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7
```

```
[dscp8]]]]]]] to cos_value
!--- Note: This command should be on one line.
```

Les configurations par défaut apparaissent ici. Par défaut, la CoS est la partie entière du DSCP, divisée par huit. Émettez cette commande afin de voir et vérifier le mappage :

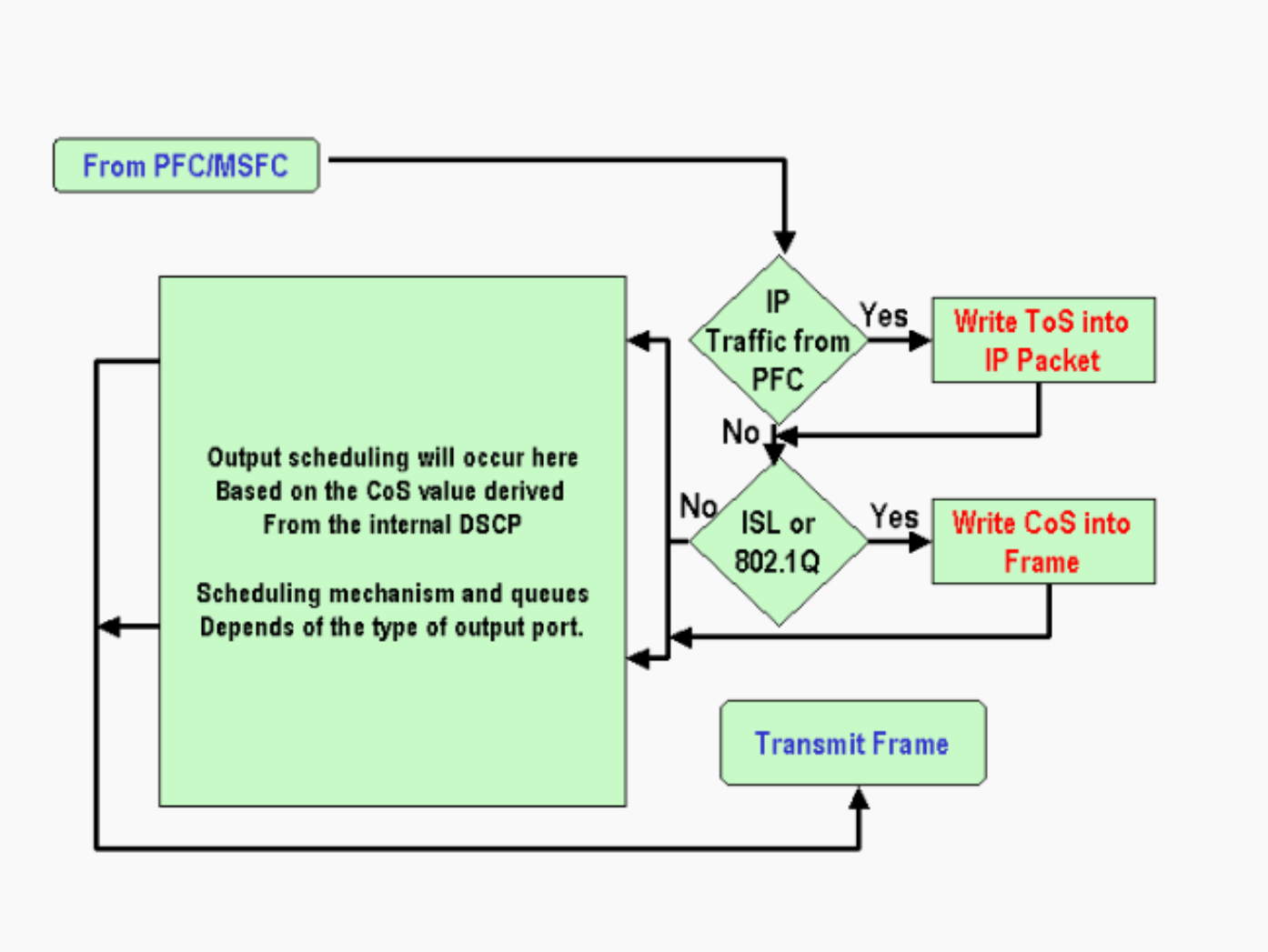
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Afin de modifier ce mappage, émettez cette commande de configuration en mode de configuration normal :

```
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 8 9 10 11 12 13 14 15 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
...
```

Une fois que le DSCP est écrit dans l'en-tête IP et que la CoS est dérivée du DSCP, le paquet est envoyé à l'une des files d'attente de sortie pour la planification de sortie sur la base de la CoS. Cela se produit même si le paquet n'est pas un dot1q ou un ISL. Pour plus d'informations sur la planification des files d'attente de sortie, référez-vous à Planification des sorties QoS sur les commutateurs de la gamme Catalyst 6500/6000 exécutant le logiciel système Cisco IOS.

Ce schéma résume le traitement du paquet en ce qui concerne le marquage dans le port de sortie :



Remarques et limitations

La liste de contrôle d'accès par défaut

La liste de contrôle d'accès par défaut utilise « dscp 0 » comme mot clé de classification. Tout le trafic qui entre dans le commutateur via un port non approuvé et qui ne touche pas une entrée de stratégie de service est marqué par un DSCP de 0 si QoS est activé. Actuellement, vous ne pouvez pas modifier la liste de contrôle d'accès par défaut dans le logiciel Cisco IOS.

Remarque : Dans le logiciel Catalyst OS (CatOS), vous pouvez configurer et modifier ce comportement par défaut. Pour plus d'informations, consultez la section *Liste de contrôle d'accès par défaut* de la classification et du marquage QoS sur les commutateurs de la gamme Catalyst 6500/6000 exécutant le logiciel CatOS.

Limitations des cartes de ligne WS-X61xx, WS-X6248-xx, WS-X6224-xx et WS-X6348-xx

Cette section concerne uniquement les cartes de ligne suivantes :

- WS-X6224-100FX-MT : Catalyst 6000 Multimode 100 FX 24 ports
- WS-X6248-RJ-45 : Module RJ-45 Catalyst 6000 48 ports 10/100
- WS-X6248-TEL : Module Telco 48 ports 10/100 du Catalyst 6000

- WS-X6248A-RJ-45 : Catalyst 6000 48 ports 10/100, qualité de service améliorée
- WS-X6248A-TEL : Catalyst 6000 48 ports 10/100, qualité de service améliorée
- WS-X6324-100FX-MM : Catalyst 6000 24 ports 100 FX, qualité de service améliorée, MT
- WS-X6324-100FX-SM : Catalyst 6000 24 ports 100 FX, qualité de service améliorée, MT
- WS-X6348-RJ-45 : Catalyst 6000 48 ports 10/100, qualité de service améliorée
- WS-X6348-RJ21V : Catalyst 6000 48 ports 10/100, alimentation en ligne
- WS-X6348-RJ45V : Catalyst 6000 48 ports 10/100, qualité de service améliorée, alimentation en ligne
- WS-X6148-RJ21V : Alimentation en ligne Catalyst 6500 48 ports 10/100
- WS-X6148-RJ45V : Alimentation en ligne Catalyst 6500 48 ports 10/100

Ces cartes de ligne ont une limite. Au niveau du port, vous ne pouvez pas configurer l'état `d'approbation` avec l'utilisation de l'un des mots clés suivants :

- `trust-dscp`
- `trust-ipcipy`
- `trust-cos`

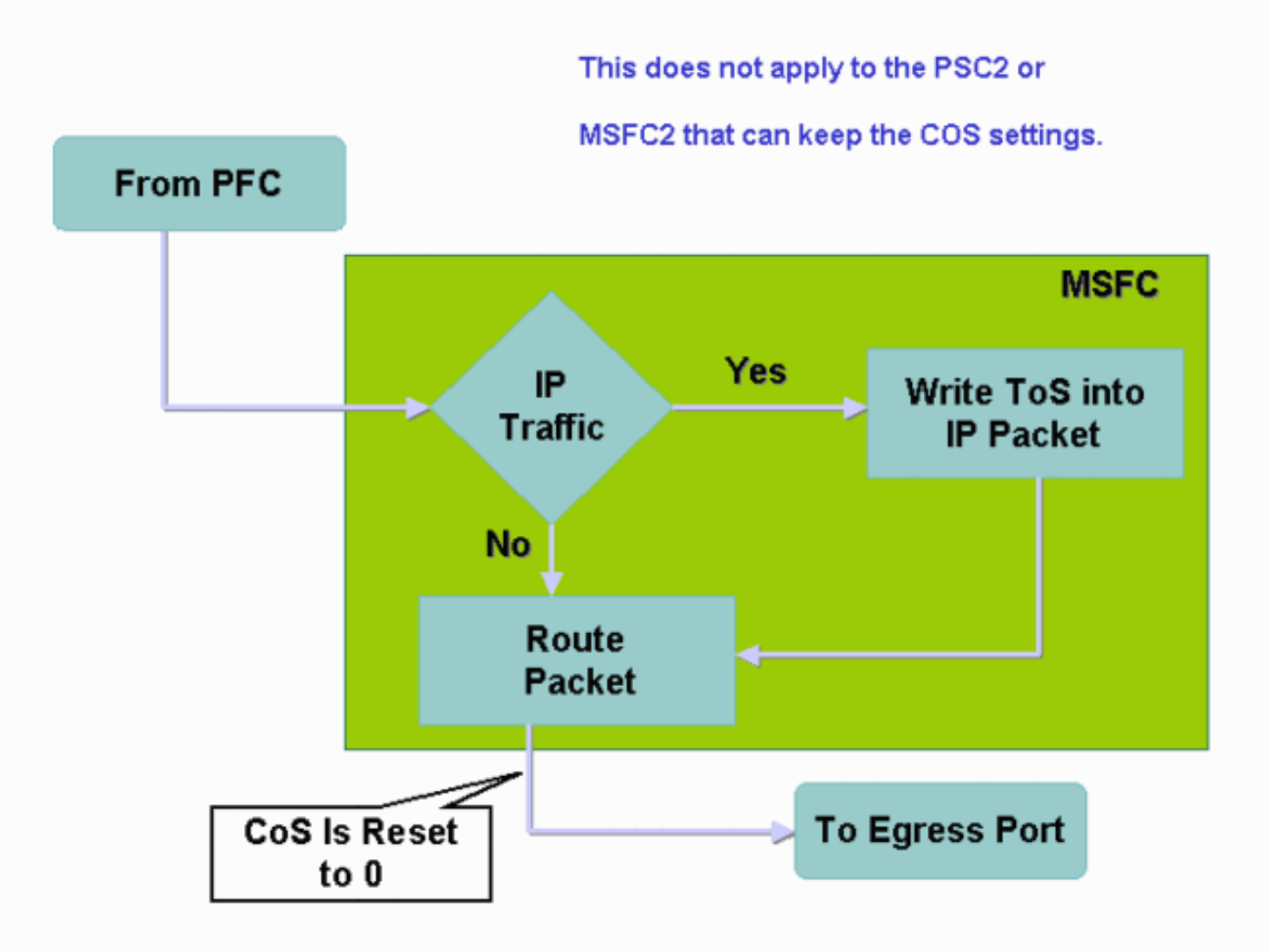
Vous ne pouvez utiliser que l'état `non approuvé`. Toute tentative de configuration d'un état `d'approbation` sur l'un de ces ports affiche l'un des messages d'avertissement suivants :

```
Tank(config-if)#mls qos trust ?
  extend  extend keyword
Tank(config-if)#mls qos trust
% Incomplete command.
Tank(config-if)#mls qos trust cos
                              ^
% Invalid input detected at '^' marker.
Tank(config-if)#mls qos trust ip-pre
                              ^
% Invalid input detected at '^' marker.
```

Vous devez associer une stratégie de service au port ou au VLAN si vous voulez qu'une trame de confiance arrive sur une telle carte de ligne. Utilisez la méthode dans le cas 1 : Marquage dans la section Périphérie de ce document.

Paquets provenant de MSFC1 ou MSFC2 sur Supervisor Engine 1A/PFC

Tous les paquets provenant de MSFC1 ou MSFC2 ont une CoS de 0. Le paquet peut être un paquet routé par logiciel ou un paquet que la carte MSFC émet. Il s'agit d'une limitation de la carte PFC car elle réinitialise la classe de service de tous les paquets qui proviennent de la carte MSFC. La priorité DSCP et IP est conservée. La carte PFC2 n'a pas cette limite. La CoS sortante de la carte PFC2 est égale à la priorité IP du paquet.



Résumé de la classification

Les tableaux de cette section indiquent le DSCP qui résulte de ces classifications :

- L'état `d'approbation` du port entrant
- Mot clé de classification dans la liste de contrôle d'accès appliquée

Ce tableau fournit un résumé générique pour tous les ports, à l'exception de WS-X62xx et WS-X63xx :

Mot clé de la carte de stratégie État de la confiance du port	set-ip-dscp xx ou set-dscp-transmit xx	trust-dscp	trust-ipcipy	trust-cos
non fiable	xx[1]	Rx[2] DSCP	Provient de Rx ipcipp	0
trust-dscp	Rx DSCP	Rx DSCP	Provient de Rx ipcipp	Provient de la CoS Rx ou de la CoS du port

trust-ipcipy	Provient de Rx ipcipp	Rx DSCP	Provient de Rx ipcipp	Provient de la CoS Rx ou de la CoS du port
trust-cos	Provient de la CoS Rx ou de la CoS du port	Rx DSCP	Provient de Rx ipcipp	Provient de la CoS Rx ou de la CoS du port

[1] C'est la seule façon de faire un nouveau marquage d'une trame.

[2] Rx = réception

Ce tableau fournit un résumé des ports WS-X61xx, WS-X62xx et WS-X63xx :

Mot clé de la carte de stratégie **État de la confiance du port**	**set-ip-dscp xx ou set-dscp-transmit xx**	**trust-dscp**	**trust-ipcipy**	**trust-cos**
non fiable	xx	Rx DSCP	Provient de Rx ipcipp	0
trust-dscp	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
trust-ipcipy	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
trust-cos	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge

Surveillance et vérification d'une configuration

Vérifier la configuration des ports

Émettez la commande **show queuing interface** *id-interface* afin de vérifier les paramètres et les configurations des ports.

Lorsque vous émettez cette commande, vous pouvez vérifier ces paramètres de classification, entre autres paramètres :

- Basé sur les ports ou sur les VLAN
- Le type de port `d'approbation`
- Liste de contrôle d’accès connectée au port

Voici un exemple de cette sortie de commande. Les champs importants relatifs à la classification apparaissent en caractères gras :

```
6500#show queuing interface gigabitethernet 3/2
Interface GigabitEthernet3/2 queuing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust COS
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
```

Le résultat montre que la configuration de ce port spécifique est avec `des cos d'approbation` au niveau du port. En outre, la CoS du port par défaut est 0.

Vérifier les classes définies

Émettez la commande **show class-map** afin de vérifier les classes définies. Voici un exemple :

```
Boris#show class-map
 Class Map match-all test (id 3)
   Match access-group  112

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all voice (id 4)
```

Vérifier la carte de stratégie appliquée à une interface

Émettez ces commandes afin de vérifier la carte de stratégie qui est appliquée et vue dans les commandes précédentes :

- **show mls qos ip interface** *interface-id*
- **show policy-map interface** *interface-id*

Voici des exemples des résultats de l'émission de ces commandes :

```
Boris#show mls qos ip gigabitethernet 1/1
   [In] Default.   [Out] Default.
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

 Int  Mod Dir  Class-map  DSCP AgId Trust FlId AgForward-Pk AgPoliced-k
 ---------------------------------------------------------------------
 Gi1/1 1  In   TEST       0    0*   No    0    1242120099             0
```

Remarque : Vous pouvez consulter les champs suivants relatifs à la classification :

- `Class-map` : indique quelle classe est associée à la stratégie de service associée à cette interface.
- `Trust` : indique si l'action de police dans cette classe contient une commande **trust** et ce qui est approuvé dans la classe.
- `DSCP` : indique le DSCP qui est transmis pour les paquets qui atteignent cette classe.

```
Tank#show policy-map interface fastethernet 4/4

 FastEthernet4/4

  service-policy input: TEST_aggre2

    class-map: Test_marking (match-all)
      27315332 packets
```

```
5 minute offered rate 25726 pps
match: access-group 101
police :
  10000000 bps 10000 limit 10000 extended limit
  aggregate-forwarded 20155529 packets action: transmit
  exceeded 7159803 packets action: drop
  aggregate-forward 19498 pps exceed 6926 pps
```

Exemples d'études de cas

Cette section fournit des exemples de configurations de cas courants qui peuvent apparaître dans un réseau.

Cas 1 : Marquage au bord

Supposez que vous configurez un Catalyst 6000 utilisé comme commutateur d'accès. De nombreux utilisateurs se connectent au logement de commutation 2, qui est une carte de ligne WS-X6348 (10/100 Mbits/s). Les utilisateurs peuvent envoyer :

- Trafic de données normal : ce trafic se trouve toujours dans le VLAN 100 et doit obtenir un DSCP de 0.
- Trafic vocal depuis un téléphone IP : ce trafic se trouve toujours dans le VLAN auxiliaire voix 101 et doit obtenir un DSCP de 46.
- Trafic d'applications stratégiques : ce trafic est également acheminé vers le serveur 10.10.10.20 via le VLAN 100. Ce trafic doit obtenir un DSCP de 32.

L'application ne marque aucun de ces trafics. Par conséquent, laissez le port comme `non approuvé` et configurez une liste de contrôle d'accès spécifique pour classifier le trafic. Une liste de contrôle d'accès est appliquée au VLAN 100 et une autre au VLAN 101. Vous devez également configurer tous les ports en tant que VLAN. Voici un exemple de configuration qui donne les résultats suivants :

```
Boris(config)#mls qos
Boris(config)#interface range fastethernet 2/1-48
Boris(config-if)#mls qos vlan-based
Boris(config-if)#exit
Boris(config)#ip access-list extended Mission_critical
Boris(config-ext-nacl)#permit ip any host 10.10.10.20
Boris(config)#ip access-list extended Voice_traffic
Boris(config-ext-nacl)#permit ip any any
Boris(config)#class-map voice

Boris(config-cmap)#match access-group Voice_traffic
Boris(config)#class-map Critical

Boris(config-cmap)#match access-group Mission_critical
Boris(config)#policy-map Voice_vlan
Boris(config-pmap)#class voice
Boris(config-pmap-c)#set ip dscp 46
Boris(config)#policy-map Data_vlan
Boris(config-pmap)#class Critical
Boris(config-pmap-c)#set ip dscp 32
Boris(config)#interface vlan 100
Boris(config-if)#service-policy input Data_vlan
Boris(config)#interface vlan 101
Boris(config-if)#service-policy input Voice_vlan
```

Cas 2 : Confiance dans le coeur de réseau avec des interfaces Gigabit Ethernet uniquement

Supposez que vous configurez un commutateur Catalyst 6000 principal avec une interface Gigabit Ethernet uniquement dans les logements 1 et 2. Les commutateurs d'accès ont marqué correctement le trafic précédemment. Par conséquent, vous n'avez pas besoin de faire de remarques. Cependant, vous devez vous assurer que le commutateur principal fait confiance au DSCP entrant. Ce cas est plus facile car tous les ports sont marqués comme `trust-dscp`, ce qui devrait suffire :

```
6k(config)#mls qos
6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-2
6k(config-if)#mls qos trust dscp
```

Informations connexes

- Présentation de Qos (Qualité de service) sur les commutateurs de la gamme Catalyst 6000
- Classification et signalisation QoS sur les commutateurs des gammes Catalyst 6500/6000 exécutant le logiciel CatOS
- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems