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 de logiciel de Cisco IOS qui associent à QoS ou à marquage. Pour plus d'informations sur l'interface de ligne de commande de logiciel de Cisco IOS (CLI), référez-vous à configurer PFC QoS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Commutateurs de gamme Catalyst 6500/6000 qui exécutent le logiciel de Cisco IOS et utilisent une de ces engines de superviseur :Une engine 1A de superviseur avec une carte de fonctionnalité de stratégie (PFC) et une carte de commutation multicouche (MSFC)Une engine 1A de superviseur avec un PFC et un MSFC2Un Supervisor Engine 2 avec un PFC2 et un MSFC2

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.

Terminologie

La liste fournit la terminologie que ce document utilise :

- Point de code de Différenciation de services (DSCP) — Les six premiers bits de l'octet de Type de service (ToS) dans l'en-tête IP. Le DSCP est seulement présent dans le paquet IP.**Remarque:** Le commutateur assigne également un DSCP interne à chaque paquet, si IP ou non-IP. Les quatre sources possibles pour la section de DSCP interne de ce document détaille cette affectation de DSCP interne.
- Priorité IP — Les trois premiers bits de l'octet de tos dans l'en-tête IP.
- Classe de service (Cos) — Le seul champ qui peut être utilisé pour marquer un paquet à la couche 2 (L2). Le cos se compose de l'un de ces trois bits :Les trois bits de l'IEEE 802.1p (dot1p) dans la balise du 802.1Q d'IEEE (dot1q) pour le paquet dot1q.**Remarque:** Par défaut, les Commutateurs de Cisco n'étiquettent pas les paquets indigènes VLAN.Les trois bits appelés le « champ d'utilisateur » dans l'en-tête de Liaison inter-commutateurs (ISL) pour un paquet ISL-encapsulé.**Remarque:** Le cos n'est pas présent à l'intérieur d'un non-dot1q ou d'un paquet ISL.
- Classification — Le processus qui est utilisé pour sélectionner le trafic à marquer.

- Repérage — Le processus qui place une valeur DSCP de la couche 3 (L3) dans un paquet. Ce document étend la définition du marquage pour comporter la configuration des valeurs CoS L2.

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

- DSCP
- Priorité IP
- Cos

Les Commutateurs de gamme Catalyst 6500/6000 exécutent la classification et le marquage à de diverses étapes. C'est ce qui se produit à différents endroits :

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

Manipulation de port d'entrée

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

- `confiance-IP-priorité`
- `confiance-dscp`
- `confiance-cos`
- `non approuvé`

Afin de placer ou changer l'état de `confiance de` port, émettez cette commande de logiciel de Cisco IOS dans le `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` quand QoS est activé. Afin d'activer QoS sur le Catalyst 6500 qui exécute le Cisco IOS logiciel, émettez le **mls qos** commandent en mode de configuration principale.

Au niveau de port d'entrée, vous pouvez également appliquer le cos par défaut par port. Voici un exemple :

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

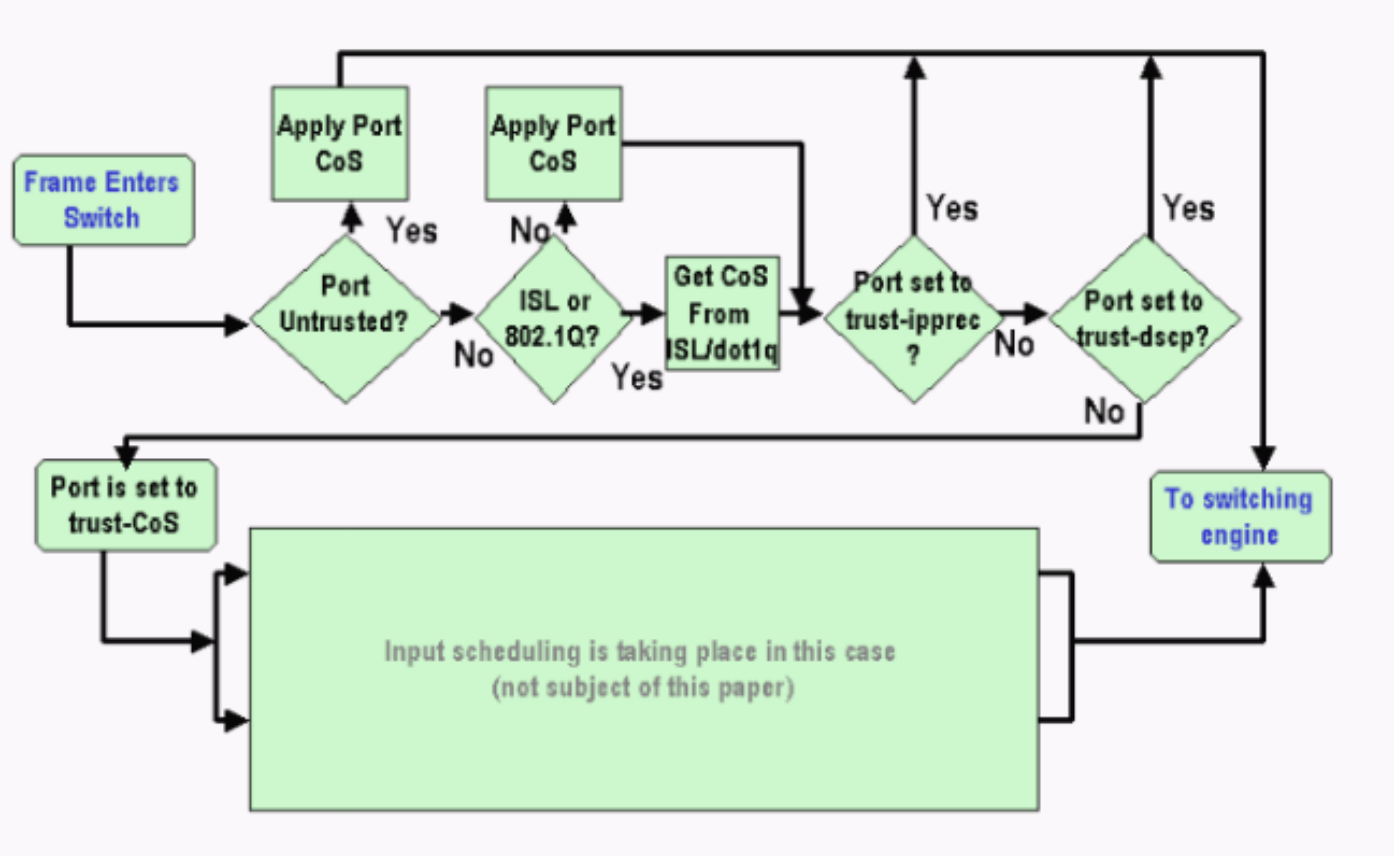
Ce le cos par défaut s'applique à tous les paquets, tels qu'IP et Internetwork Packet Exchange (IPX). Vous pouvez appliquer le cos par défaut à n'importe quel port physique.

Si le port est dans l'état `non approuvé`, marquez la trame avec le cos de par défaut de port et passez l'en-tête au moteur de commutation (PFC). Si le port est placé à un des états de `confiance`, exécutez une de ces deux options :

- Si la trame n'a pas le cos reçu (dot1q ou ISL), appliquez le cos par défaut de port.
- Pour dot1q et trames ISL, gardez le cos comme il est.

Puis, passez la trame au moteur de commutation.

Cet exemple montre la classification des entrées et le marquage. L'exemple affiche comment assigner le cos interne à chaque trame :



Remarque: Le comme indiqué dans cet exemple, chaque trame est assigné au cos interne. L'affectation est basée sur le cos reçu ou le cos par défaut de port. Le cos interne inclut les trames non marquées qui ne portent aucun vrai cos. Le cos interne est écrit dans une en-tête de paquet spéciale, qui s'appelle une en-tête de bus de données, et est envoyée au-dessus du bus de données au moteur de commutation.

Moteur de commutation (PFC)

Quand l'en-tête atteint le moteur de commutation, la logique de reconnaissance d'adresse améliorée par moteur de commutation (EARL) assigne à chaque trame un DSCP interne. Ce DSCP interne est une priorité interne qui est assignée à la trame par le PFC pendant que la trame transite le commutateur. Ce n'est pas le DSCP dans l'en-tête de la version d'IP 4 (ipv4). Le DSCP interne est dérivé de l'cos ou tos existant plaçant et est utilisé pour remettre à l'état initial le cos ou le tos pendant que la trame quitte le commutateur. Ce DSCP interne est assigné à toutes les trames qui sont commutées ou conduites par le PFC, même les trames non-IP.

Cette section discute comment vous pouvez assigner une stratégie de service à l'interface afin de faire un marquage. La section discute également la configuration finale du DSCP interne, qui dépend de l'état de `confiance de` port et de la stratégie de service qui est appliquée.

Configurez la stratégie de service pour classifier ou marquer un paquet dans le Logiciel Cisco IOS version 12.1(12c)E et plus tard

Terminez-vous 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 considérer.L'ACL peut être numéroté ou nommé, et le Catalyst 6500/6000 prend en charge un ACL étendu. Émettez la commande de logiciel de Cisco IOS de la **liste d'accès** *xxx*, comme indiqué dans cet exemple :`(config)#`**`access-list 101 permit ip any host 10.1.1.1`**
2. Configurez une classe du trafic (class map) pour apparier le trafic sur la base de l'ACL que vous avez défini ou sur la base du DSCP reçu.Émettez la commande de logiciel de Cisco IOS de **class-map**. PFC QoS ne prend en charge pas plus d'une déclaration de correspondance par class map. En outre, PFC QoS prend en charge seulement ces déclarations de correspondance :**ip access-group de correspondancematch ip dscpmatch ip precedencematch protocolRemarque:** Les commandes enables de **match protocol l'**utilisation du Reconnaissance d'application fondée sur le réseau (NBAR) d'apparier le trafic.**Remarque:** De ces options, seulement le **match ip dscp** et les déclarations de **match ip precedence** sont pris en charge et fonctionnent. Ces déclarations, cependant, ne sont pas utiles dans le marquage ou la classification des paquets. Vous pouvez employer ces déclarations, par exemple, pour faire le maintien de l'ordre sur tous les paquets qui apparient un certain DSCP. Cependant, cette action est hors de portée de ce document.`(config)#`**`class-map`** *`class-name`*
`(config-cmap)#`**`match {access-group | input-interface | ip dscp}`** **Remarque:** Cet exemple affiche seulement trois options pour la **commande match**. Mais vous pouvez configurer beaucoup plus d'options à cette invite de commande.**Remarque:** Des n'importe quelles des options dans cette **commande match** sont prises pour le critère de correspondance et les autres options sont laissées, selon les paquets entrant.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 s'appliquer une stratégie à une classe que vous avez précédemment définie.La carte de stratégie contient :Un nomUn ensemble de déclarations de classePour chaque déclaration de classe, la mesure qui doit être prise pour cette classeLes actions prises en charge dans PFC1 et PFC2 QoS sont :**dscp de confiancePriorité IP de confiancecos de confianceset ip dscp** dans la version du logiciel Cisco IOS 12.1(12c)E1 et plus tard**placez la Priorité IP** dans la version du logiciel Cisco IOS 12.1(12c)E1 et plus tard**policeRemarque:** Cette action est hors de portée de ce document.`(config)#`**`policy-map`** *`policy-name`*
`(config-pmap)#`**`class`** *`class-name`*
`(config-pmap-c)#`**`{police | set ip dscp}`**
Remarque: Cet exemple affiche seulement deux options, mais vous pouvez configurer beaucoup plus d'options à ceci `(config-pmap-C) #` invite de commande.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 défini à un ou plusieurs l'interface.**Remarque:** Vous pouvez relier une stratégie de service à l'interface physique ou à l'interface virtuelle commutée (SVI) ou à l'interface VLAN. Si vous reliez une stratégie de service à une interface VLAN, les seuls ports qui utilisent cette stratégie de service sont des ports qui appartiennent à ce VLAN et sont configurés pour QoS basé sur VLAN. Si le port n'est pas placé pour QoS basé sur VLAN, le port utilise toujours le QoS basé sur port par défaut et regarde seulement la

stratégie de service qui est reliée à l'interface physique.Cet exemple s'applique le `test_policy de` stratégie de service aux Gigabit Ethernet 1/1 de port :`(config)` **`interface gigabitethernet 1/1`**

```
(config-if)#service-policy input test_policy
```

Cet exemple s'applique le `test_policy de` stratégie de service à tous les ports dans le VLAN 10 qui ont une configuration basée sur VLAN du point de vue de 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 l'étape 2 et l'étape 3 de cette procédure si vous ignorez la définition spécifique de la classe et reliez l'ACL directement dans la définition de la carte de stratégie. Dans cet exemple, où la `police de 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
```

Configurez la stratégie de service pour classifier ou marquer un paquet dans des versions du logiciel Cisco IOS plus tôt que le Logiciel Cisco IOS version 12.1(12c)E

Dans des versions logicielles de Cisco IOS plus tôt que la version du logiciel Cisco IOS 12.1(12c)E1, vous ne pouvez pas utiliser le **set ip dscp** ou l'action de **Priorité IP de positionnement** dans une carte de stratégie. Par conséquent, la seule manière de faire un marquage du trafic spécifique qu'une classe définit est de configurer un régulateur avec très un haut débit. Ce débit devrait être, par exemple, au moins la ligne débit du port ou de quelque chose assez élevée pour permettre à tout le trafic pour frapper ce régulateur. Puis, l'utilisation positionnement-dscp-**transmettent** *xx* comme action de conformation. Suivez ces étapes afin d'installer cette configuration :

1. Configurez un ACL pour définir le trafic que vous voulez considérer.L'ACL peut être numéroté ou nommé, et le Catalyst 6500/6000 prend en charge un ACL étendu. Émettez la commande de logiciel de Cisco IOS de la **liste d'accès** *xxx*, comme indiqué dans cet exemple :`(config)#` **`access-list 101 permit ip any host 10.1.1.1`**
2. Configurez une classe du trafic (class map) pour apparier le trafic sur la base du l'un ou l'autre l'ACL que vous avez défini ou sur la base du DSCP reçu.Émettez la commande de logiciel de Cisco IOS de **class-map**. PFC QoS ne prend en charge pas plus d'une déclaration de correspondance par class map. En outre, PFC QoS prend en charge seulement ces déclarations de correspondance :**ip access-group de correspondancematch ip dscpmatch ip precedencematch protocolRemarque:** Les commandes enables de **match protocol l'**utilisation de NBAR d'apparier le trafic.**Remarque:** De ces déclarations, seulement le **match ip dscp** et les déclarations de **match ip precedence** sont pris en charge et fonctionnent. Ces déclarations, cependant, ne sont pas utiles dans le marquage ou la classification des paquets. Vous pouvez employer ces déclarations, par exemple, pour faire le maintien de l'ordre sur tous les paquets qui apparient un certain DSCP. Cependant, cette action est hors

de portée de ce document.`(config)#`**`class-map`** *`class-name`*
`(config-cmap)#`**`match {access-group | input-interface | ip dscp}`**
Remarque: Cet exemple affiche seulement trois options pour la **commande match**. Mais vous pouvez configurer beaucoup plus d'options à cette invite de commande.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 s'appliquer une stratégie à une classe que vous avez précédemment définie.La carte de stratégie contient :Un nomUn ensemble de déclarations de classePour chaque déclaration de classe, la mesure qui doit être prise pour cette classeLes actions prises en charge dans PFC1 ou PFC2 QoS sont :**dscp de confiancePriorité IP de confiancecos de confiancepolice**Vous devez utiliser la **déclaration de réglementation** parce que le **set ip dscp** et les actions de **Priorité IP de positionnement** ne sont pas pris en charge. Puisque vous ne voulez pas réellement maintenir l'ordre le trafic, mais le marquer juste, utilisez un régulateur qui est défini pour permettre tout le trafic. , Configurez par conséquent le régulateur avec du grands débit et rafale. Par exemple, vous pouvez configurer le régulateur avec du débit et la rafale de maximum autorisé. 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 un ou plusieurs interfaces.**Remarque:** La stratégie de service peut être reliée à une interface physique ou au SVI ou à l'interface VLAN. Si une stratégie de service est reliée à une interface VLAN, seulement les ports qui appartiennent à ce VLAN et qui sont configurés pour l'usage basé sur VLAN de QoS cette stratégie de service. Si le port n'est pas placé pour QoS basé sur VLAN, le port utilise toujours le QoS basé sur port par défaut et regarde seulement une stratégie de service qui est reliée à l'interface physique.Cet exemple s'applique le `test_policy de` stratégie de service aux Gigabit Ethernet 1/1 de port :`(config)` **`interface gigabitethernet 1/1`**
`(config-if)#`**`service-policy input test_policy`**
Cet exemple s'applique le `test_policy de` stratégie de service à tous les ports dans le VLAN 10 qui ont une configuration basée sur VLAN du point de vue de 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 d'un de ces derniers :

1. Exister a reçu la valeur DSCP, qui est placée avant que la trame écrive le commutateurUn exemple est **dscp de confiance**.
2. Les bits reçus de Priorité IP qui sont déjà placés dans l'en-tête d'ipv4Puisqu'il y a 64 valeurs

DSCP et seulement huit valeurs de Priorité IP, l'administrateur configure un mappage que le commutateur l'utilise pour dériver le DSCP. Les mappages par défaut sont en place, dans le cas que l'administrateur ne configure pas les cartes. Un exemple est **Priorité IP de confiance**.

3. Les bits reçus de cos qui sont déjà placés avant que la trame écrive le commutateur et qui sont enregistrés dans l'en-tête de bus de données, ou s'il n'y avait aucun cos dans la trame entrante, du cos par défaut du port d'entréeComme avec la Priorité IP, il y a un maximum de huit valeurs CoS, qui doivent être tracées à 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 placer le DSCP interne à une valeur spécifique.

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

- Pour le mappage de CoS-to-DSCP, le DSCP qui est les égaux dérivés huit fois le cos.
- Pour le priorité-à-DSCP IP traçant, le DSCP qui est les égaux dérivés huit fois la Priorité IP.

Vous pouvez émettre ces commandes afin d'ignorer et vérifier ce mappage statique :

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

La première valeur du DSCP qui correspond au mappage pour le cos (ou la Priorité IP) est 0. La deuxième valeur pour le cos (ou la Priorité IP) est 1, et le modèle continue de cette façon. Par exemple, cette commande change le mappage de sorte que le cos 0 soit tracé au DSCP de 0, et le cos de 1 est tracé au DSCP de 8, et ainsi de suite :

```
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 choisi ?

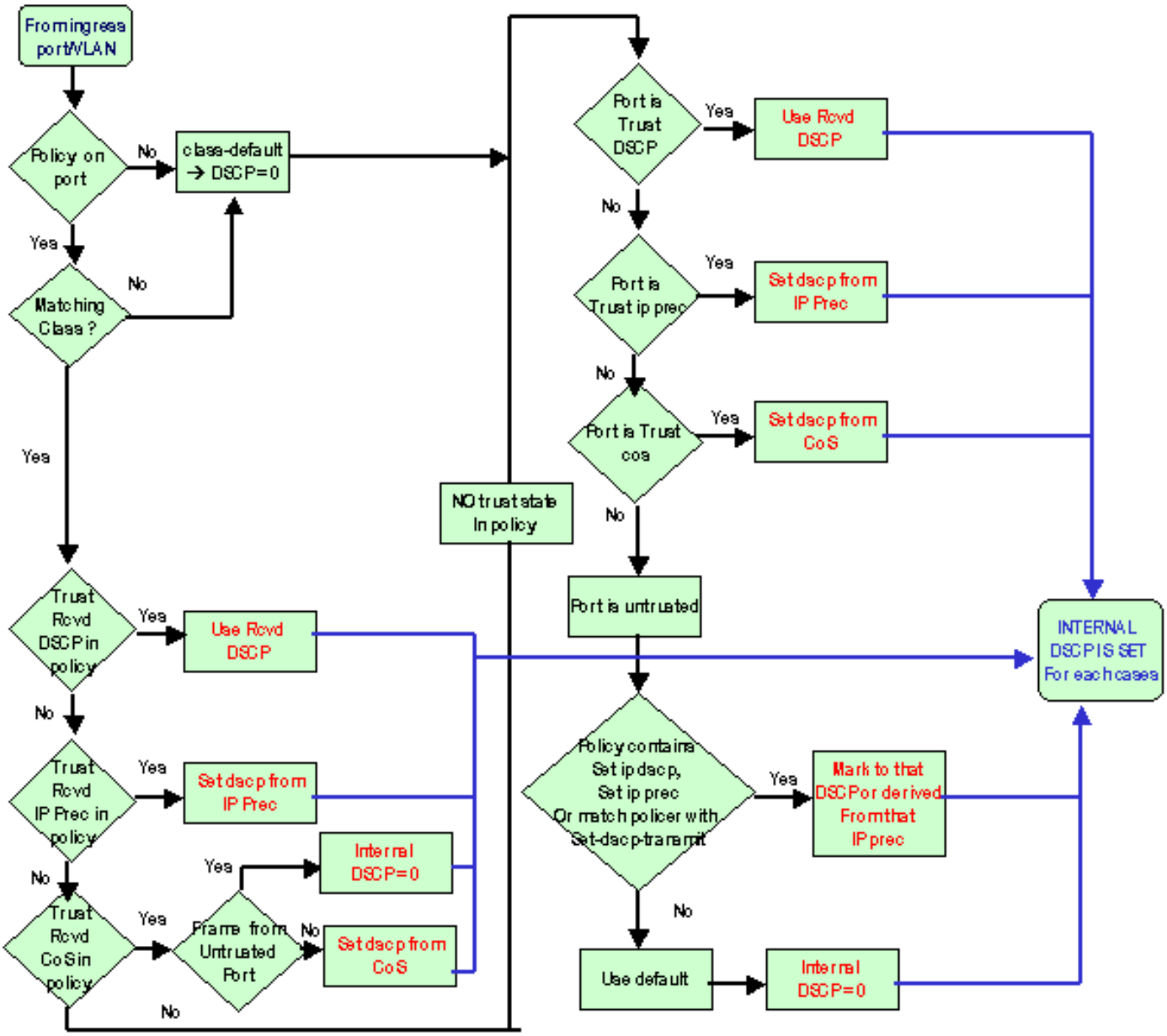
Le DSCP interne est choisi sur la base de ces paramètres :

- La carte de stratégie QoS qui est appliquée au paquetLa carte de stratégie QoS est déterminée par ces règles :Si aucune stratégie de service n'est reliée au port d'entrée ou au VLAN, utilisez le par défaut.**Remarque:** Cette action par défaut est de placer le DSCP interne à 0.Si une stratégie de service est reliée au port d'entrée ou au VLAN, et si le trafic apparie une des classes que la stratégie définit, utilisez cette entrée.Si une stratégie de service est reliée au port d'entrée ou au VLAN, et si le trafic n'apparie pas une des classes que la stratégie définit, utilisez le par défaut.
- L'état de `confiance du` port et l'action de la stratégie tracentQuand le port a un état spécifique de `confiance` et une stratégie avec un certain marquage (faisant confiance à l'action en même temps), ces règles s'appliquent :La commande de **set ip dscp** ou le DSCP qui est définie par régulateur dans une carte de stratégie est seulement appliqué si le port est parti dans l'état `non approuvé`.Si le port a un état de `confiance`, cet état de `confiance` est utilisé pour dériver le DSCP interne. L'état de `confiance de` port a toujours la priorité au-dessus de la commande de **set ip dscp**.La commande de la **confiance** *xx* dans une carte de stratégie a la priorité au-dessus de l'état de `confiance de` port.Si le port et la stratégie contiennent un état différent de `confiance`, le déclarer de `confiance` qui provient la carte de stratégie est considéré.

Par conséquent, le DSCP interne dépend de ces facteurs :

- L'état de `confiance de` port
- La stratégie de service (avec l'utilisation de l'ACL) qui est reliée au port
- La carte de stratégie par défaut**Remarque:** Le par défaut remet à l'état initial le DSCP à 0.
- Si basé sur VLAN ou basé sur port en ce qui concerne l'ACL

Ce diagramme récapitule comment le DSCP interne est choisi sur la base de la configuration :



Le PFC peut également faire le maintien de l'ordre. Ceci peut par la suite avoir comme conséquence une baisse du DSCP interne. Pour plus d'informations sur le maintien de l'ordre, référez-vous à la Réglementation QoS sur des Commutateurs de gamme Catalyst 6500/6000.

Manipulation de port de sortie

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

- Si le paquet est un paquet d'ipv4, copiez le DSCP interne que le moteur de commutation

assigne dans le tos à l'octet de l'en-tête d'ipv4.

- Si le port de sortie est configuré pour un ISL ou une encapsulation dot1q, utilisez le cos qui sont dérivés du DSCP interne. Copiez le cos dans l'ISL ou la trame dot1q.

Remarque: Le cos est dérivé du DSCP interne selon une charge statique. Émettez cette commande afin de configurer la charge 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, le cos est la pièce d'entier du DSCP, divisée par huit. Émettez cette commande afin de voir et vérifier le mappage :

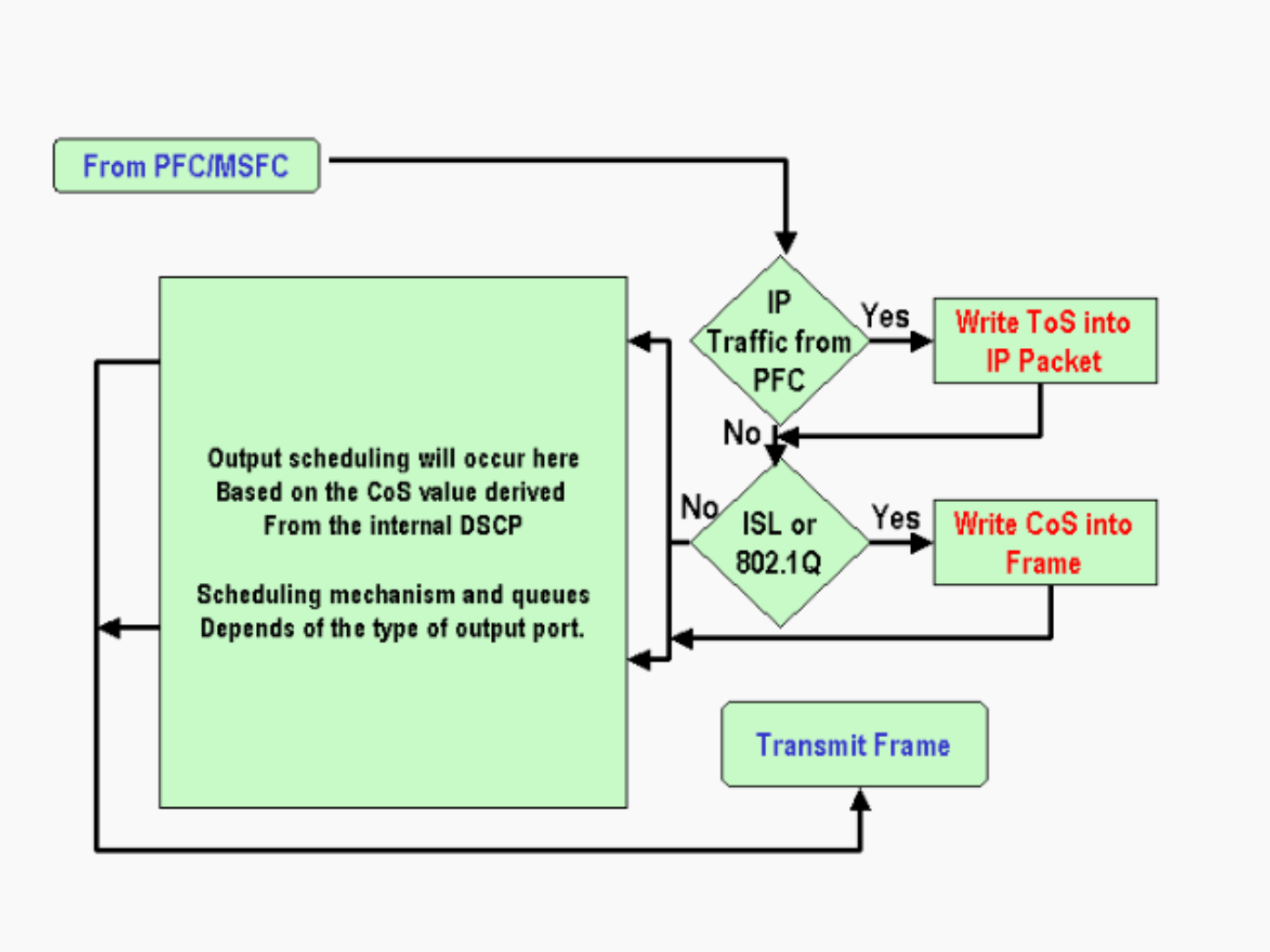
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 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 changer ce mappage, émettez cette commande de configuration dans le 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
...
```

Après que le DSCP soit écrit dans l'en-tête IP et le cos est dérivé du DSCP, le paquet est envoyé à une des files d'attente de sortie pour la planification de sortie sur la base du cos. Ceci se produit même si le paquet n'est pas un dot1q ou un ISL. Pour plus d'informations sur la file d'attente de sortie programmant, référez-vous à la planification de sortie de QoS sur des Commutateurs de gamme Catalyst 6500/6000 exécutant le logiciel système de Cisco IOS.

Ce diagramme récapitule le traitement du paquet en ce qui concerne le marquage dans le port de sortie :



Notes et limites

L'ACL par défaut

L'ACL par défaut utilise le « dscp 0" comme mot clé de classification. Tout le trafic qui écrit le commutateur par un port non approuvé et ne frappe pas une entrée de stratégie de service est identifié par un DSCP de 0 si QoS est activé. Actuellement, vous ne pouvez pas changer l'ACL par défaut en logiciel de Cisco IOS.

Remarque: En logiciel de SYSTÈME D'EXPLOITATION de Catalyst (CatOS), vous pouvez configurer et changer ce comportement par défaut. Le pour en savoir plus, se rapportent *l'à la* section *par défaut d'ACL de* classification QoS et de marquage sur des Commutateurs de gamme Catalyst 6500/6000 exécutant le logiciel de CatOS.

Limites des linecards WS-X61xx, WS-X6248-xx, WS-X6224-xx, et WS-X6348-xx

Cette section concerne seulement ces linecards :

- WS-X6224-100FX-MT : Catalyst 6000 24-Port 100 FX à plusieurs modes de fonctionnement
- WS-X6248-RJ-45 : Module du RJ-45 48-Port 10/100 du Catalyst 6000
- WS-X6248-TEL : Module de la compagnie de téléphone 48-Port 10/100 du Catalyst 6000
- WS-X6248A-RJ-45 : Catalyst 6000 48-Port 10/100, QoS amélioré

- WS-X6248A-TEL : Catalyst 6000 48-Port 10/100, QoS amélioré
- WS-X6324-100FX-MM : Catalyst 6000 24-Port 100 FX, QoS amélioré, la TA
- WS-X6324-100FX-SM : Catalyst 6000 24-Port 100 FX, QoS amélioré, la TA
- WS-X6348-RJ-45 : Catalyst 6000 48-Port 10/100, QoS amélioré
- WS-X6348-RJ21V : Catalyst 6000 48-Port 10/100, alimentation en ligne
- WS-X6348-RJ45V : Catalyst 6000 48-Port 10/100, QoS amélioré, alimentation en ligne
- WS-X6148-RJ21V : Alimentation en ligne du Catalyst 6500 48-Port 10/100
- WS-X6148-RJ45V : Alimentation en ligne du Catalyst 6500 48-Port 10/100

Ces linecards ont une limite. Au niveau de port, vous ne pouvez pas configurer l'état de `confiance` avec l'utilisation de l'un de ces mots clé :

- `confiance-dscp`
- `confiance-ipprec`
- `confiance-cos`

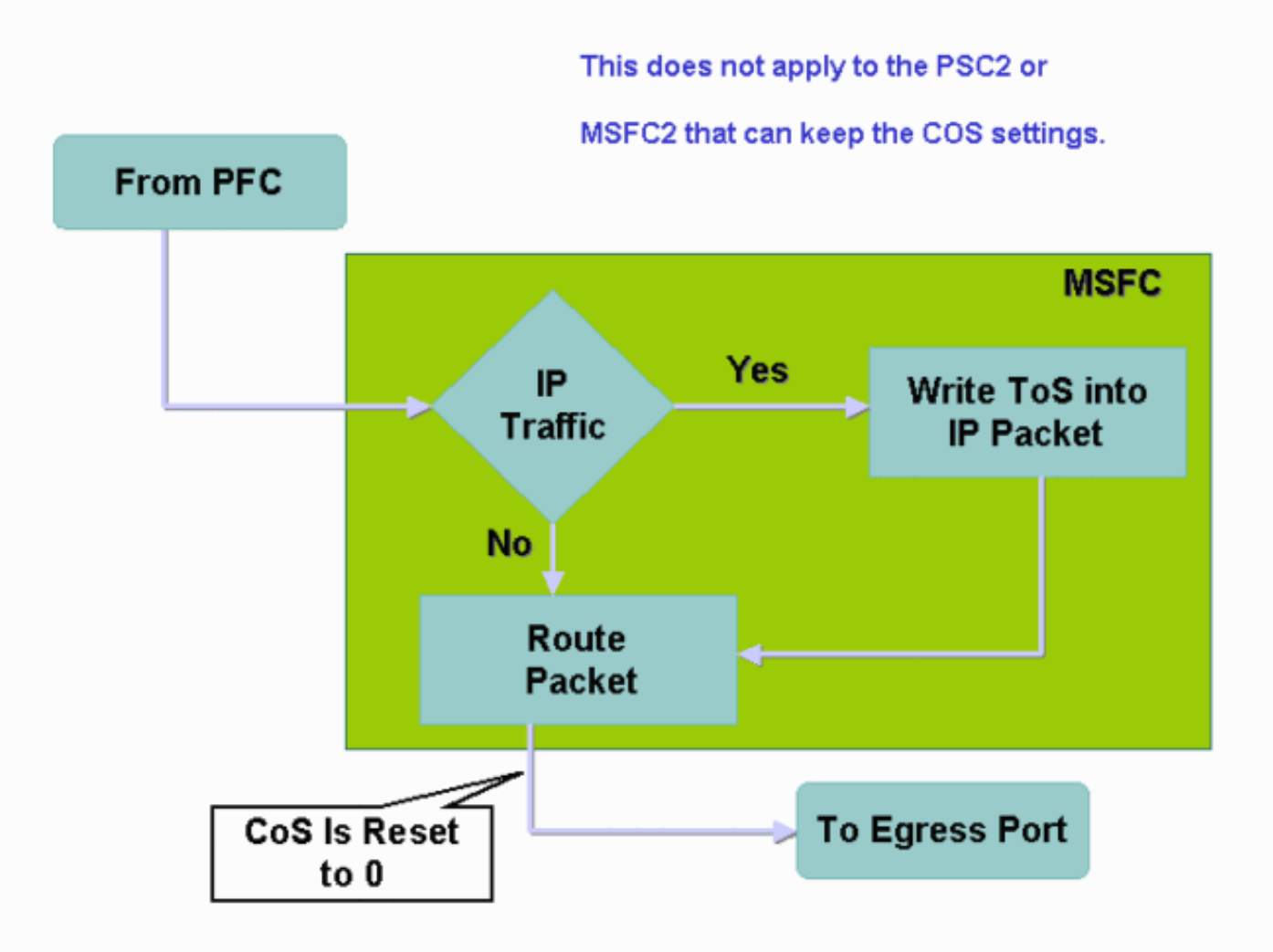
Vous pouvez seulement utiliser l'état `non approuvé`. N'importe quelle tentative de configurer un état de `confiance` sur un de ces ports affiche un de ces messages d'avertissement :

```
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 relier une stratégie de service au port ou au VLAN si vous voulez qu'une trame de confiance entre sur un tel linecard. Utilisez la méthode dans l'affaire 1 : Marquage à la section de périphérie de ce document.

Paquets qui proviennent le MSFC1 ou le MSFC2 sur l'engine 1A/PFC de superviseur

Tous les paquets qui proviennent le MSFC1 ou le MSFC2 ont le cos de 0. Le paquet peut être un paquet logiciel-conduit ou un paquet ce les questions MSFC. C'est une limite du PFC parce qu'il remet à l'état initial le cos de tous les paquets qui proviennent le MSFC. Le DSCP et la Priorité IP sont encore mis à jour. Le PFC2 n'a pas cette limite. Le cos quittant du PFC2 est égal à la Priorité IP du paquet.



Résumé de classification

Les tables dans cette section donnent au DSCP ce des résultats sur la base de ces classifications :

- L'état de `confiance de` port d'entrée
- Le mot clé de classification dans l'ACL appliqué

Cette table fournit est un résumé générique pour tous les ports excepté WS-X62xx et WS-X63xx :

Mot clé de carte de stratégie État de confiance de port	le set ip dscp xx ou positionnement-dscp-transmettent xx	confiance-dscp	confiance-ipprec	confiance-cos
non approuvé	xx[1]	DSCP de Rx[2]	Dérivé de l'ipprec de Rx	0
confiance-dscp	DSCP de Rx	DSCP de Rx	Dérivé de	Dérivé du cos

			l'ipprec de Rx	de Rx ou du cos de port
confiance-ipprec	Dérivé de l'ipprec de Rx	DSCP de Rx	Dérivé de l'ipprec de Rx	Dérivé du cos de Rx ou du cos de port
confiance-cos	Dérivé du cos de Rx ou du cos de port	DSCP de Rx	Dérivé de l'ipprec de Rx	Dérivé du cos de Rx ou du cos de port

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

[2] Rx = reçoivent

Cette table fournit un résumé pour les ports WS-X61xx, WS-X62xx, et WS-X63xx :

Mot clé de carte de stratégie **État de confiance de port**	**le set ip dscp xx ou positionnement-dscp-transmettent xx**	**confiance-dscp**	**confiance-ipprec**	**confiance-cos**
non approuvé	xx	DSCP de Rx	Dérivé de l'ipprec de Rx	0
confiance-dscp	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
confiance-ipprec	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge
confiance-cos	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge

Surveillez et vérifiez une configuration

Vérifiez la configuration des ports

Émettez la commande d'interface-*id de* **show queueing interface** afin de vérifier les configurations et les configurations de port.

Quand vous émettez cette commande, vous pouvez vérifier ces paramètres de classification, entre d'autres paramètres :

- Si basé sur port ou basé sur VLAN
- Le type de port de `confiance`
- L'ACL qui est relié au port

Voici un échantillon de cette sortie de commande. Les importants champs en ce qui concerne 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]:
```

La sortie prouve que la configuration de ce port spécifique est avec le `cos de confiance au` niveau de port. En outre, le cos par défaut de port est 0.

Classes définies par contrôle

Émettez la commande de **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)
```

Vérifiez la carte de stratégie qui est appliquée à une interface

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

- *interface-id d'***interface d'IP de show mls qos**
- *interface-id de* **show policy-map interface**

Voici les échantillons de la sortie de la question 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 regarder ces champs qui associent à la classification :

- `Class-map` — Te dit quelle classe est reliée à la stratégie de service qui est reliée à cette interface.
- `Confiance` — Te dit si l'action de police dans cette classe contient une commande de **confiance** et ce qui est de confiance dans la classe.

- `DSCP` — Te dit le DSCP qui est transmis pour les paquets qui frappent 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
```

Études de cas témoin

Cette section fournit des configurations d'échantillon des cas communs qui peuvent apparaître dans un réseau.

Cas 1 : Marquage à la périphérie

Supposez que vous configurez un Catalyst 6000 qui est utilisé comme commutateur d'accès. Beaucoup d'utilisateurs se connectent à l'emplacement 2 de commutateur, qui est un linecard WS-X6348 (10/100 de Mbits/s). Les utilisateurs peuvent envoyer :

- Le trafic de données normal — Ce trafic est toujours dans VLAN 100 et doit obtenir un DSCP de 0.
- Le trafic vocal d'un téléphone IP — Ce trafic est toujours dans le VLAN auxiliaire 101 de Voix et doit obtenir un DSCP de 46.
- Le trafic d'application stratégique — Ce trafic également est livré dans VLAN 100 et est dirigé vers le serveur 10.10.10.20. Ce trafic doit obtenir un DSCP de 32.

L'application ne marque pas de ce trafic. , Quittez par conséquent le port en tant que `non approuvé` et configurez un ACL spécifique pour classifier le trafic. Un ACL est appliqué au VLAN 100, et un ACL est appliqué à VLAN 101. Vous devez également configurer tous les ports comme basés sur VLAN. Voici un exemple de la configuration qui résulte :

```
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 au centre pour seulement des interfaces de Gigabit Ethernet

Supposez que vous configurez un principal Catalyst 6000 avec seulement une interface de Gigabit Ethernet dans l'emplacement 1 et l'emplacement 2. Le trafic correctement précédemment marqué de commutateurs d'accès. Par conséquent, vous n'avez pas besoin de faire la remarque. Cependant, vous devez s'assurer que le principal commutateur fait confiance au DSCP entrant. Ce cas est le cas plus facile parce que tous les ports sont marqués comme confiance-`dscp`, qui devrait être suffisant :

```
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