Classification et signalisation QoS sur les commutateurs des gammes Catalyst 6500/6000 exécutant le logiciel CatOS

Contenu

Introduction

Ce document examine ce qui se passe en ce qui concerne le marquage et la classification d'un paquet à différents endroits au cours de son parcours dans le châssis Catalyst 6000. Il mentionne des cas particuliers, des restrictions et fournit de brèves études de cas.

Ce document n'est pas destiné à être une liste exhaustive de toutes les commandes Catalyst OS (CatOS) concernant la qualité de service (QoS) ou le marquage. Pour plus d'informations sur

l'interface de ligne de commande (CLI) de CatOS, reportez-vous au document suivant :

- Configuration QoS

Remarque : ce document ne prend en compte que le trafic IP.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Ce document est valide pour les commutateurs de la gamme Catalyst 6000 exécutant le logiciel CatOS et utilisant l'un des moteurs de supervision suivants :

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2 + PFC2
- SUP2 + PFC2 + MSFC2

Cependant, tous les exemples de commandes ont été essayés sur un Catalyst 6506 avec SUP1A/PFC exécutant le logiciel version 6.3.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Terminologie

Voici une liste de termes utilisés dans ce document :

- DSCP (Differentiated Services Code Point) : Les six premiers bits de l'octet ToS (Type of Service) de l'en-tête IP. DSCP est présent uniquement dans le paquet IP.**Remarque :** Vous affectez également un DSCP interne à chaque paquet (IP ou non IP), cette affectation DSCP interne sera détaillée plus loin dans ce document.
- Priorité IP: Les trois premiers bits de l'octet ToS dans 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). Il se compose de l'un des trois bits suivants :Les trois bits dot1p de la balise dot1q pour le paquet IEEE dot1q.Les trois bits appelés « Champ utilisateur » dans l'en-tête ISL (Inter-Switch Link) pour un paquet encapsulé ISL.Il n'y a pas de CoS présent dans un paquet non dot1q ou ISL.

- Classification : Processus utilisé pour sélectionner le trafic à marquer.
- Marquage : Processus de définition d'une valeur DSCP de couche 3 (L3) dans un paquet. Dans ce document, la définition du marquage est étendue pour inclure la définition des valeurs CoS L2.

Les commutateurs de la gamme Catalyst 6000 peuvent effectuer des classifications basées sur les trois paramètres suivants :

- DSCP
- Priorité IP
- CoS

Les commutateurs de la gamme Catalyst 6000 effectuent la classification et le marquage à différents endroits. Voici un aperçu de ce qui se passe à ces différents endroits :

- Port d'entrée (circuit intégré spécifique à l'application d'entrée (ASIC))
- Moteur de commutation (PFC (Policy Feature Card))
- Port de sortie (ASIC de sortie)

Activation de la QoS

Par défaut, la QoS est désactivée sur les commutateurs Catalyst 6000. La QoS peut être activée en exécutant la commande CatOS **set qos enable**.

Lorsque QoS est désactivé, il n'y a aucune classification ou marquage effectuée par le commutateur et, en tant que tel, chaque paquet quitte le commutateur avec la priorité DSCP/IP qu'il avait lors de l'entrée dans le commutateur.

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 des états d'approbation suivants :

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

Le reste de cette section décrit comment les états de confiance des ports influencent la classification finale du paquet. L'état d'approbation des ports peut être défini ou modifié à l'aide de la commande CatOS suivante :

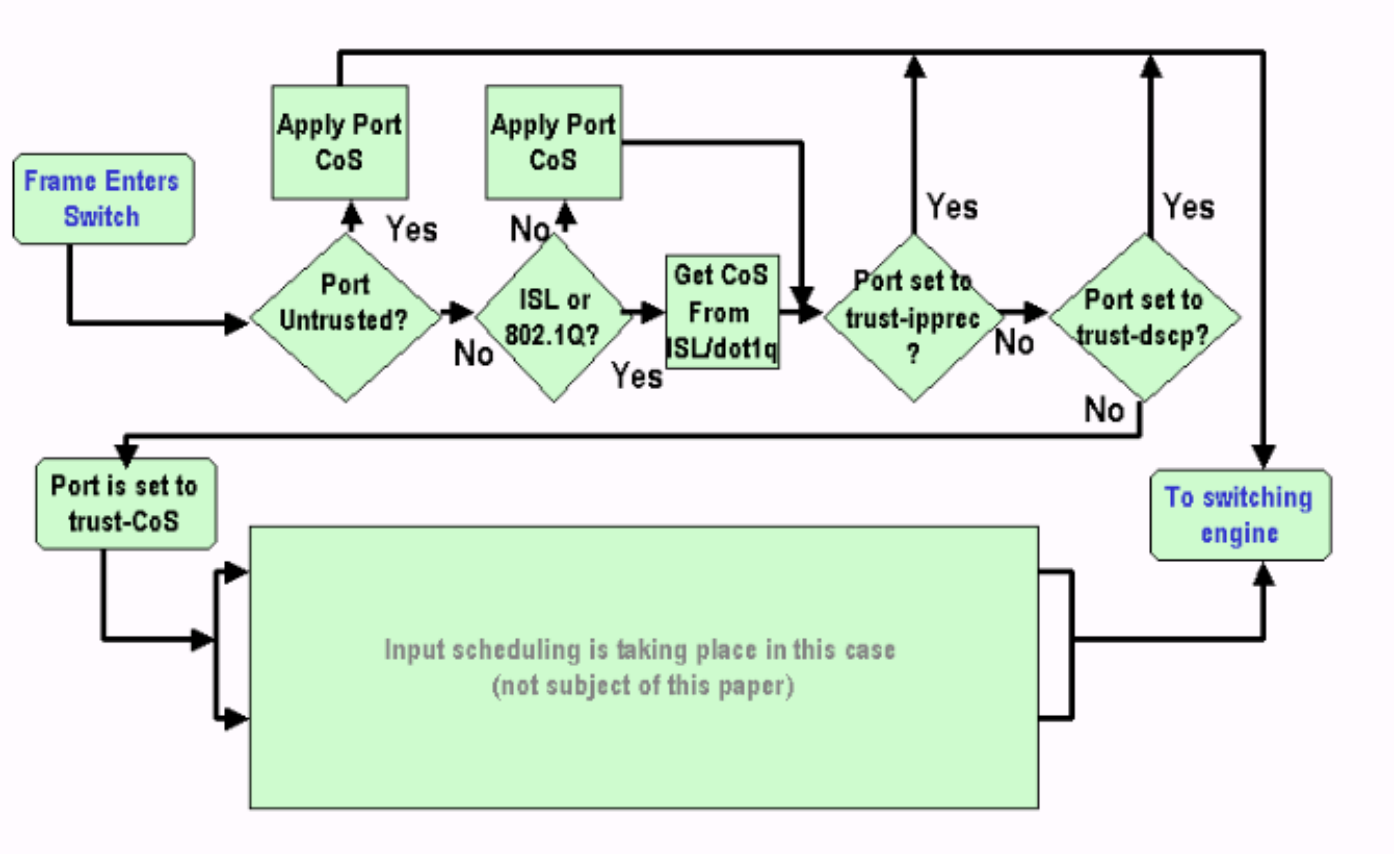
set port qos *mod/port* **trust {untrust | trust-cos | trust-ipcipp | trust-dscp }**

Remarque : par défaut, tous les ports sont à l'état non approuvé lorsque QoS est activé.

Au niveau du port d'entrée, vous pouvez également appliquer une CoS par défaut par port, comme dans l'exemple suivant :

set port qos *mod/port* **cos** *cos-value*

Si le port est défini sur l'état non approuvé, il suffit de marquer la trame avec la CoS par défaut du port et de passer l'en-tête au moteur de commutation (PFC). Si le port est défini sur l'un des états d'approbation, appliquez la CoS du port par défaut (si la trame n'a pas de CoS reçu (dot1q ou ISL)), ou conservez la CoS telle qu'elle est (pour les trames dot1q et ISL) et passez la trame au moteur de commutation. La classification des entrées est illustrée dans l'organigramme suivant :



Remarque : Comme indiqué dans l'organigramme ci-dessus, chaque trame aura une CoS interne affectée (soit la CoS reçue, soit la CoS du port par défaut), y compris les trames non étiquetées qui ne portent aucune CoS réelle. Cette CoS interne et le DSCP reçu sont écrits dans un en-tête de paquet spécial (appelé en-tête de bus de données) et envoyés par le bus de données au moteur de commutation. Cela se produit sur la carte de ligne d'entrée et à ce stade, on ne sait pas encore si cette CoS interne sera portée à l'ASIC de sortie et insérée dans la trame sortante. Tout cela dépend de ce que fait la carte PFC et est décrit plus en détail dans la section suivante.

PFC (Switching Engine)

Une fois que l'en-tête a atteint le moteur de commutation, la logique EARL (Encoded Address Recognition Logic) du moteur de commutation attribue à chaque trame un DSCP interne. Ce DSCP interne est une priorité interne attribuée à la trame par la carte PFC lors de la transmission du commutateur. Il ne s'agit pas du DSCP dans l'en-tête IPv4. Il 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 commutées (ou routées) par la carte PFC, même les trames non IP.

Quatre sources possibles pour le DSCP interne

Le DSCP interne provient de l'une des sources suivantes :

1. Valeur DSCP existante, définie avant la trame entrant dans le commutateur.
2. Les bits de priorité IP reçus qui sont déjà définis dans l'en-tête IPV4. Comme il existe 64 valeurs DSCP et seulement huit valeurs de priorité IP, l'administrateur configure un mappage utilisé par le commutateur pour dériver le DSCP. Les mappages par défaut sont en place, si l'administrateur ne configure pas les mappages.
3. Les bits CoS reçus sont déjà définis avant la trame entrant dans le commutateur, ou à partir de la CoS par défaut du port entrant s'il n'y avait pas de CoS dans la trame entrante. Comme pour la priorité IP, il existe un maximum de huit valeurs CoS, chacune devant être mappée à l'une des 64 valeurs DSCP. Cette carte peut être configurée ou le commutateur peut utiliser la carte par défaut déjà en place.
4. Le DSCP peut être défini pour la trame à l'aide d'une valeur par défaut DSCP généralement attribuée via une entrée de liste de contrôle d'accès (ACL).

Pour les numéros 2 et 3 dans la liste ci-dessus, le mappage statique utilisé est par défaut, comme suit :

- DSCP dérivé égale huit fois CoS, pour le mappage CoS à DSCP.
- Le DSCP dérivé est égal à huit fois la priorité IP, pour la priorité IP au mappage DSCP.

Ce mappage statique peut être remplacé par l'utilisateur en exécutant les commandes suivantes :

set qos ipcipp-dscp-map <dscp1> <dscp2>...<dscp8>

set qos cos-dscp-map <dscp1> <dscp2>...<dscp8>

La première valeur du DSCP correspondant au mappage de la CoS (ou priorité IP) est « 0 », la seconde valeur de la CoS (ou priorité IP) est « 1 » et continue dans ce modèle.

Parmi les quatre sources possibles pour le DSCP interne, laquelle sera utilisée ?

Cette section décrit les règles qui déterminent laquelle des quatre sources possibles décrites ci-dessus sera utilisée pour chaque paquet. Cela dépend des paramètres suivants :

1. Quelle liste de contrôle d'accès QoS sera appliquée au paquet ? Ceci est déterminé par les règles suivantes :**Remarque :** chaque paquet passe par une entrée de liste de contrôle d'accès.Si aucune liste de contrôle d'accès n'est connectée au port ou au VLAN entrant, appliquez la liste de contrôle d'accès par défaut.Si une liste de contrôle d'accès est connectée au port ou au VLAN entrant, et si le trafic correspond à l'une des entrées de la liste de contrôle d'accès, utilisez cette entrée.Si une liste de contrôle d'accès est connectée au port ou au VLAN entrant et si le trafic *ne* correspond *pas* à l'une des entrées de la liste de contrôle d'accès, utilisez la liste de contrôle d'accès par défaut.
2. Chaque entrée contient un mot clé de classification. Voici une liste de mots clés possibles et leurs descriptions :trust-ipcipe : Le DSCP interne est dérivé de la priorité IP reçue en fonction du mappage statique, quel que soit l'état d'approbation du port.trust-dscp : Le DSCP interne sera dérivé du DSCP reçu, quel que soit l'état d'approbation du port.trust-cos : Le DSCP interne sera dérivé de la CoS reçue selon le mappage statique, si l'état d'approbation du port est approuvé (trust-cos, trust-dscp, trust-ipcip). Si l'état d'approbation du port est trust-xx, le DSCP sera dérivé de la CoS du port par défaut selon le même mappage statique.dscp *xx* : Le DSCP interne dépend des états d'approbation de port entrants suivants :Si le port n'est pas approuvé, le DSCP interne sera défini sur *xx*.Si le port est trust-dscp, le DSCP interne sera le DSCP reçu dans le paquet entrant.Si le port est trust-CoS, le DSCP interne sera

dérivé de la CoS du paquet reçu.Si le port est trust-ipcipp, le DSCP interne est dérivé de la priorité IP du paquet reçu.

3. Chaque liste de contrôle d'accès QoS peut être appliquée à un port ou à un VLAN, mais il existe un paramètre de configuration supplémentaire à prendre en compte ; le type de port ACL. Un port peut être configuré pour être basé sur VLAN ou sur port. Voici une description des deux types de configuration :Un port configuré pour être basé sur un VLAN ne regarde que la liste de contrôle d'accès appliquée au VLAN auquel le port appartient. Si une liste de contrôle d'accès est connectée au port, elle sera ignorée pour le paquet entrant sur ce port.Si un port appartenant à un VLAN est configuré en tant que port, même s'il y a une liste de contrôle d'accès connectée à ce VLAN, il ne sera pas pris en compte pour le trafic entrant de ce port.

Voici une syntaxe permettant de créer une liste de contrôle d'accès QoS pour marquer le trafic IP :

set qos acl ip ***acl_name*** **[dscp xx | trust-cos | trust-dscp | trust-ipcipp]** ***règle d'entrée acl***

La liste de contrôle d'accès suivante marque tout le trafic IP dirigé vers l'hôte 1.1.1.1 avec un DSCP de « 40 » et fait confiance à dscp pour tout autre trafic IP :

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

Une fois que la liste de contrôle d'accès a été créée, vous devez la mapper à un port ou à un VLAN. Pour ce faire, exécutez la commande suivante :

set qos acl map ***acl_name*** **[module/port | VLAN]**

Par défaut, chaque port est basé sur les ports de la liste de contrôle d'accès. Par conséquent, si vous voulez connecter une liste de contrôle d'accès à un VLAN, vous devez configurer les ports de ce VLAN en tant que VLAN. Pour ce faire, exécutez la commande suivante :

set port qos ***module/port*** **vlan**

Vous pouvez également revenir au mode basé sur les ports en exécutant la commande suivante :

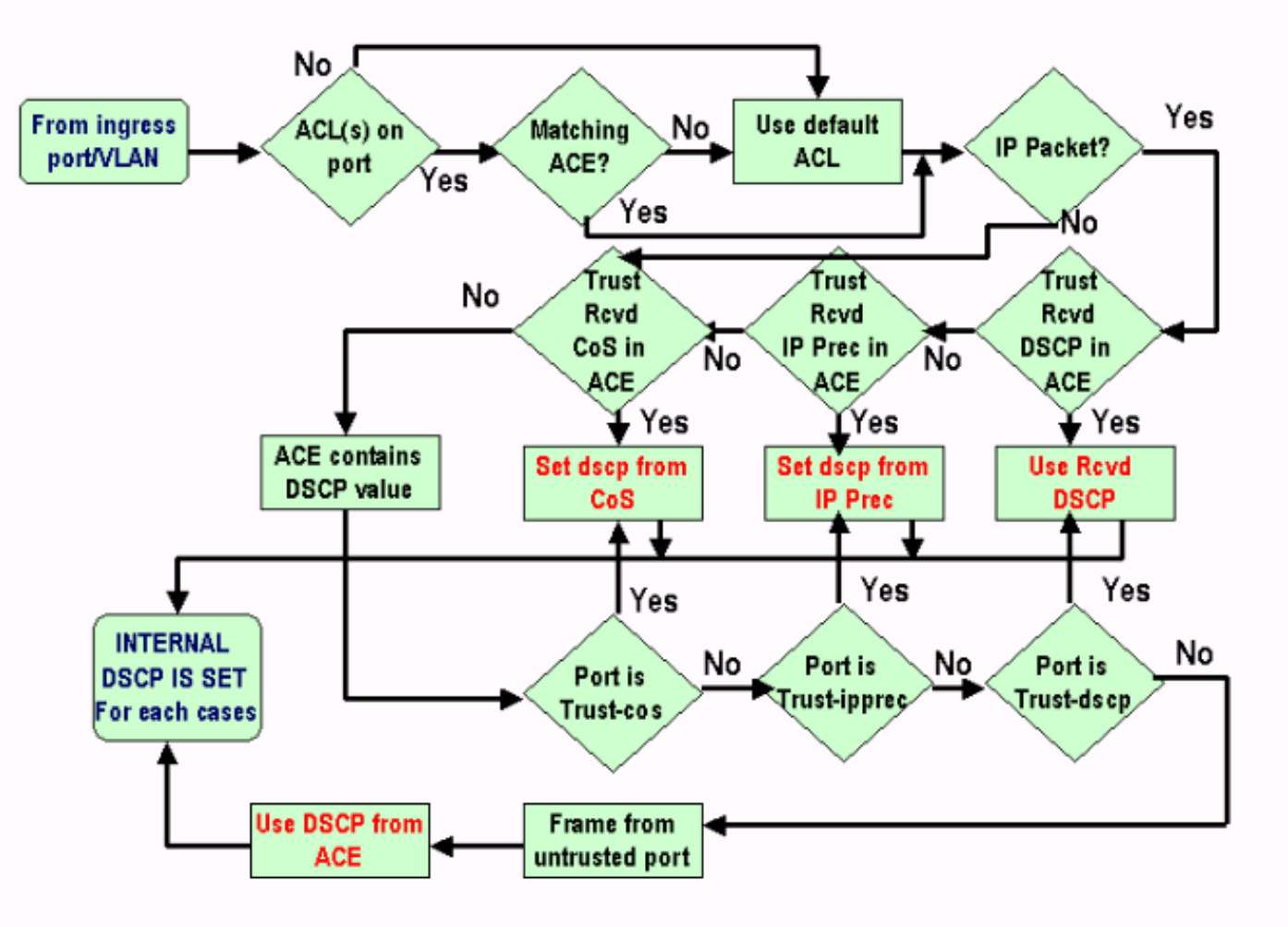
set port qos ***module/port*** **port-based**

Résumé: Comment le DSCP interne est-il sélectionné ?

Le DSCP interne dépend des facteurs suivants :

- état de confiance des ports
- ACL connectée au port
- ACL par défaut
- Basé sur VLAN ou sur port en ce qui concerne la liste de contrôle d'accès

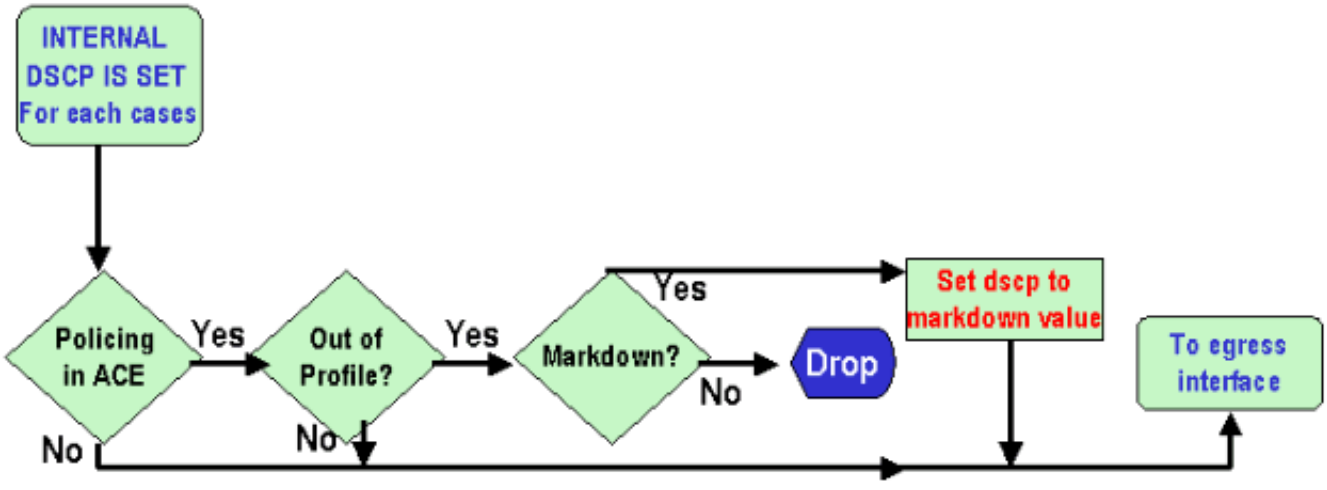
Le diagramme de flux suivant résume la manière dont le DSCP interne est choisi en fonction de la configuration :



La carte PFC est également capable de contrôler. Cela pourrait éventuellement aboutir à un blocage du DSCP interne. Pour plus d'informations sur la réglementation, reportez-vous au document suivant :

- Réglementation QoS sur la gamme Catalyst 6000

Le diagramme de flux suivant montre comment le régulateur est appliqué :



Gestion des ports de sortie

Rien ne peut être fait au niveau du port de sortie pour modifier la classification, mais dans cette section, vous allez marquer le paquet selon les règles suivantes :

- Si le paquet est un paquet IPv4, copiez le DSCP interne attribué par le moteur de commutation 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 et copiez-la dans la trame ISL ou dot1q.

Remarque : La CoS est dérivée du DSCP interne en fonction d'une valeur statique configurée par l'utilisateur qui exécute la commande suivante :

Note: set qos dscp-cos-map ***dscp_list:cos_value***

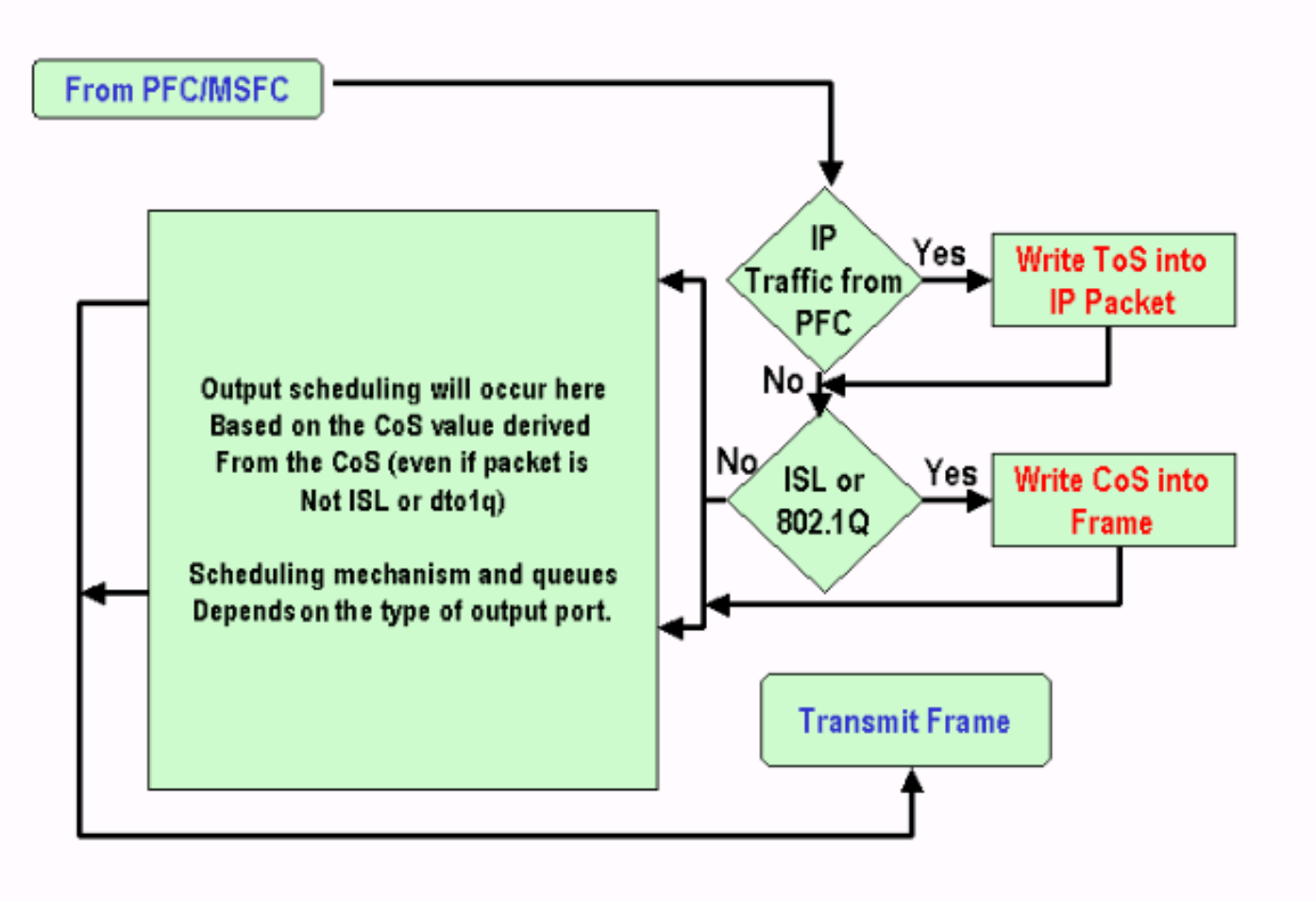
Remarque : Les configurations par défaut sont les suivantes. Par défaut, la CoS sera la partie entière du DSCP divisée par huit :

```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

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 basée sur sa CoS (même si le paquet n'est pas un dot1q ou un ISL). Pour plus d'informations sur la planification de la file d'attente de sortie, reportez-vous au document suivant :

- QoS sur les commutateurs de la gamme Catalyst 6000 : Planification des sorties sur le Catalyst 6000 avec PFC ou PFC 2 à l'aide du logiciel CatOS

Le diagramme de flux suivant récapitule le traitement du paquet concernant le marquage dans le port de sortie :



Remarques et limitations

La liste de contrôle d'accès par défaut

Par défaut, la liste de contrôle d'accès par défaut utilise « dscp 0 » comme mot clé de classification. Cela signifie que tout le trafic entrant dans le commutateur via un port non approuvé sera marqué par un DSCP de « 0 » si QoS est activé. Vous pouvez vérifier la liste de contrôle d'accès par défaut pour l'adresse IP en exécutant la commande suivante :

```
Boris-1> (enable) show qos acl  info default-action  ip
set qos acl default-action
-------------------------
ip dscp 0
```

Vous pouvez également modifier la liste de contrôle d'accès par défaut en exécutant la commande suivante :

set qos acl default-action ip [dscp xx | trust-CoS | trust-dscp | trust-ipcipp]

confiance cos dans les limites d'entrée de liste de contrôle d'accès

Il y a une limite supplémentaire qui apparaît lorsque vous utilisez le mot clé trust-CoS dans une entrée. La CoS ne peut être approuvée que dans une entrée si l'état d'approbation de réception n'est pas non approuvé. La tentative de configuration d'une entrée avec trust-CoS affiche l'avertissement suivant :

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any
Warning: ACL trust-CoS should only be used with ports that are also configured with port
trust=trust-CoS
test_2 editbuffer modified. Use 'commit' command to apply changes.
```

Cette limitation est une conséquence de ce qui a été vu précédemment dans la section Gestion des ports d'entrée. Comme le montre l'organigramme de cette section, si le port n'est pas approuvé, la trame se voit immédiatement attribuer la CoS du port par défaut. Par conséquent, la CoS entrante n'est pas conservée et n'est pas envoyée au moteur de commutation, ce qui entraîne une incapacité à faire confiance à la CoS même avec une liste de contrôle d'accès spécifique.

Limitations des cartes de ligne 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 24 PORTS 100 FX
- WS-X6248-RJ-45 : MODULE CATALYST 6000 48 PORTS 10/100 RJ-45
- WS-X6248-TEL : MODULE TELCO 48 PORTS 10/100 CATALYST 6000
- WS-X6248A-RJ-45 : CATALYST 6000 48 PORTS 10/100, QOS AMÉLIORÉ
- WS-X6248A-TEL : CATALYST 6000 48 PORTS 10/100, QOS AMÉLIORÉ
- WS-X6324-100FX-MM : CATALYST 6000 24 PORTS 100FX, QOS ENH, MT
- WS-X6324-100FX-SM : CATALYST 6000 24 PORTS 100FX, QOS ENH, MT
- WS-X6348-RJ-45 : CATALYST 6000 48 PORTS 10/100, QO AMÉLIORÉE
- WS-X6348-RJ21V : CATALYST 6000 48 PORTS 10/100, ALIMENTATION EN LIGNE
- WS-X6348-RJ45V : CATALYST 6000 48 PORTS 10/100, QOS ENH, ALIMENTATION NE INLI

Cependant, ces cartes de ligne présentent des limitations supplémentaires :

- Au niveau du port, vous ne pouvez pas faire confiance à trust-dscp ou trust-ipcip.
- Au niveau du port, si l'état de confiance du port est trust-CoS, les instructions suivantes s'appliquent :Le seuil de réception pour la planification des entrées est activé. En outre, la CoS du paquet de réception est utilisée pour donner la priorité aux paquets pour accéder au bus.La CoS ne sera pas approuvée et ne sera pas utilisée pour dériver le DSCP interne, à moins que vous n'ayez également configuré la liste de contrôle d'accès pour ce trafic vers des cos de confiance. En outre, il ne suffit pas que les cartes de ligne utilisent des cos de confiance sur le port, vous devez également disposer d'une liste de contrôle d'accès avec des cos de confiance pour ce trafic.
- Si l'état d'approbation du port n'est pas approuvé, un marquage normal se produit (comme dans le cas standard). Cela dépend de la liste de contrôle d’accès appliquée au trafic.

Toute tentative de configuration d'un état d'approbation sur l'un de ces ports affichera l'un des messages d'avertissement suivants :

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
```

```
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

Résumé de la classification

Les tableaux ci-dessous indiquent le DSCP résultant classé par :

- État d'approbation du port entrant.
- Mot clé de classification dans la liste de contrôle d'accès appliquée.

Résumé de la table générique pour tous les ports, à l'exception de WS-X62*xx* et WS-X63*xx*

Mot clé ACL État de la confiance du port	dscp xx	trust-dscp	trust-ipcipy	trust-CoS
Non approuvé	xx (1)	Rx dscp	provient de Rx ipcipt	0
trust-dscp	Rx-dscp	Rx dscp	provient de Rx ipcipt	provient de la CoS Rx ou de la CoS du port
trust-ipcipy	provient de Rx ipcipt	Rx dscp	provient de Rx ipcipt	provient de la CoS Rx ou de la CoS du port
trust-CoS	provient de cos Rx ou CoS de port	Rx dscp	provient de Rx ipcipt	provient de la CoS Rx ou de la CoS du port

(1) Il s'agit de la seule façon de faire un nouveau marquage d'une trame.

Résumé du tableau pour WS-X62*xx* ou WS-X63*xx*

Mot clé ACL État de la confiance du port	dscp xx	trust-dscp	trust-ipcipy	trust-CoS
Non approuvé	xx	Rx dscp	provient de Rx ipcipt	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	xx	Rx dscp	provient de Rx ipcipt	provient de la CoS Rx ou de la CoS du port (2)

(2) Il s'agit de la seule façon de préserver la CoS entrante pour le trafic provenant d'une carte de ligne 62*xx* ou 63*xx*.

Surveillance et vérification d'une configuration

Vérification de la configuration du port

Les paramètres et les configurations des ports peuvent être vérifiés en exécutant la commande suivante :

show port qos ***module/port***

En exécutant cette commande, vous pouvez vérifier, entre autres paramètres, les paramètres de classification suivants :

- basé sur les ports ou VLAN
- type de port de confiance
- ACL connectée au port

Voici un exemple de cette sortie de commande avec les champs importants concernant la classification mis en surbrillance :

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 1/1    port-based     port-based      COPS           local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 1/1     1p2q2t       1p1q4t     untrusted     untrusted      0       0

(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                           IP

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
 1/1  test_2                            IP
```

Remarque : Pour chaque champ, il y a le paramètre configuré et le paramètre d'exécution. Celui qui sera appliqué au paquet est le paramètre d'exécution.

Vérification de la liste de contrôle d’accès

Vous pouvez vérifier la liste de contrôle d’accès appliquée et vue dans les commandes précédentes en exécutant la commande suivante :

show qos acl info runtime *acl_name*

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
---------------------------------------------
1. dscp 32 ip any host 1.1.1.1
2. trust-dscp any
```

Exemples d'études de cas

Les exemples suivants sont des exemples de configurations de cas courants qui peuvent apparaître dans un réseau.

Cas 1 : Marquage au bord

Supposons que vous configurez un Catalyst 6000 utilisé comme commutateur d'accès avec de nombreux utilisateurs connectés au logement 2, qui est une carte de ligne WS-X6348 (10/100M). Les utilisateurs peuvent envoyer les informations suivantes :

- Trafic de données normal : Ceci est toujours dans le VLAN 100, et doit obtenir un DSCP de « 0 ».
- Trafic vocal à partir d'un téléphone IP : Il est toujours dans le VLAN auxiliaire voix 101, et doit obtenir un DSCP de « 40 ».
- Trafic d'applications stratégiques : Cela arrive également dans le VLAN 100 et est dirigé vers le serveur 10.10.10.20. Ce trafic doit obtenir un DSCP de « 32 ».

Aucun de ce trafic n'est marqué par l'application. Par conséquent, vous quitterez le port comme non approuvé et configurerez une liste de contrôle d'accès spécifique pour classer le trafic. Une liste de contrôle d’accès sera 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 la configuration résultante :

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

Cas 2 : Confiance dans le coeur de réseau avec une interface Gigabit uniquement

Supposons que vous configurez un commutateur Catalyst 6000 principal avec une interface Gigabit uniquement dans les logements 1 et 2 (pas de carte de ligne 62xx ou 63xx dans le châssis). Le trafic a été correctement marqué précédemment par les commutateurs d'accès. Par conséquent, vous n'avez pas besoin d'effectuer de marquage, mais vous devez vous assurer que vous faites confiance au DSCP entrant. C'est le cas le plus simple, car tous les ports seront marqués comme trust-dscp et devraient être suffisants :

```
set qos enable
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

Cas 3 : Confiance dans le coeur avec un port 62xx ou 63xx dans le châssis

Supposons que vous configurez un périphérique de coeur/distribution avec une liaison Gigabit sur une carte de ligne WS-X6416-GBIC (dans le logement 2) et une liaison 10/100 sur une carte de ligne WS-X6348 (dans le logement 3). Vous devez également faire confiance à tout le trafic entrant, car il a été marqué précédemment au niveau du commutateur d'accès. Comme vous ne pouvez pas faire confiance à dscp sur la carte de ligne 6348, la méthode la plus simple dans ce cas serait de laisser tous les ports comme non approuvés et de changer la liste de contrôle d'accès par défaut en trust-dscp, comme dans l'exemple suivant :

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
set qos acl default-action ip trust-dscp
```

Informations connexes

- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support technique - Cisco Systems