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

Contenu

Introduction

Ce document examine ce qui se produit concernant le marquage et la classification d'un paquet à différents endroits pendant son voyage dans le châssis du Catalyst 6000. Il mentionne des cas particuliers, des restrictions, et fournit les études de cas courtes.

Ce document n'est pas destiné pour être une liste exhaustive de toutes les commandes de

SYSTÈME D'EXPLOITATION de Catalyst (CatOS) concernant le Qualité de service (QoS) ou le marquage. Pour plus d'informations sur l'interface de ligne de commande de CatOS (CLI), référez-vous au document suivant :

- Configuration QoS

Remarque: Ce document considère seulement 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.

Composants utilisés

Ce document est valide pour des Commutateurs de famille du Catalyst 6000 exécutant le logiciel de CatOS, et utilisant une des engines suivantes de superviseur :

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

Tous échantillonnent des commandes, cependant, ont été essayés sur un Catalyst 6506 avec la version de logiciel courante 6.3 SUP1A/PFC.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Terminologie

Ce qui suit est une liste de terminologie utilisée dans ce document :

- Differentiated Services Code Point (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:** Vous assignez également un DSCP interne à chaque paquet (IP ou non IP), cette affectation de DSCP interne serez détaillé plus tard dans ce document.
- 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). Il se compose de l'un des suivant trois bits :Les trois bits dot1p dans la balise

dot1q pour le paquet d'IEEE dot1q.Les trois bits appelés le « champ d'utilisateur » dans l'en-tête de Liaison inter-commutateurs (ISL) pour un paquet encapsulé ISL.Il n'y a pas de cos présent à l'intérieur d'un non-dot1q ou d'un paquet ISL.
- Classification : Le processus utilisé pour sélectionner le trafic à marquer.
- Repérage : Le processus de placer une valeur DSCP de la couche 3 (L3) dans un paquet. Dans ce document, la définition du marquage est étendue pour inclure placer les valeurs CoS L2.

Les Commutateurs de famille du Catalyst 6000 peuvent faire des classifications basées sur les trois paramètres suivants :

- DSCP
- Priorité IP
- Cos

Les Commutateurs de famille du Catalyst 6000 font la classification et la marquent à différents endroits. Ce qui suit est un regarder ce qui se produit à ces différents endroits :

- Port d'entrée (circuit intégré spécifique (ASIC) d'entrée)
- Moteur de commutation (carte de fonctionnalité de stratégie (PFC))
- Port de sortie (de sortie ASIC)

Activation de QoS

Par défaut, QoS est désactivé sur des Commutateurs du Catalyst 6000. QoS peut être activé en émettant l'**enable de set qos de** commande de CatOS.

Quand QoS est désactivé il n'y a aucune classification ou le marquage fait par le commutateur, et en tant que, chaque paquet laisse le commutateur avec la priorité DSCP/IP qu'il a eue en écrivant le commutateur.

Manipulation de port d'entrée

Le paramètre de configuration principale pour le port d'entrée, concernant la classification, est l'état de confiance du port. Chaque port du système peut avoir un des états suivants de confiance :

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

Le reste de cette section décrit comment la confiance de port énonce des influences la classification finale du paquet. L'état de confiance de port peut être placé ou changé utilisant la commande suivante de CatOS :

modèle de **set port qos/confiance de** *port* **{non approuvée | confiance-cos | confiance-ipprec | confiance-dscp}**

Remarque: Par défaut tous les ports sont dans l'état non approuvé quand QoS est activé.

Au port d'entrée nivelez-vous peut également appliquer le cos par défaut par port, comme dans l'exemple suivant :

modèle de **set port qos***/cos-valeur* **cos de** *port*

Si le port est placé à l'état non approuvé, marquez simplement 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, appliquez le cos par défaut de port (si la trame n'a pas le cos reçu (dot1q ou ISL)), ou gardez le cos comme il est (pour dot1q et trames ISL) et passez la trame au moteur de commutation. La classification des entrées est illustrée dans l'organigramme suivant :

Remarque: Suivant les indications de l'organigramme ci-dessus, chaque trame aura le cos interne assigné (le cos reçu, ou le cos par défaut de port), y compris les trames non marquées qui ne portent aucun vrai cos. Ce le cos interne et le DSCP reçu sont écrits dans une en-tête de paquet spéciale (appelée une en-tête de bus de données) et envoyés au-dessus du bus de données au moteur de commutation. Ceci se produit à la carte de ligne d'entrée et en ce moment on ne le connaît pas encore si ce le cos interne sera porté aux egresss ASIC et inséré dans la trame sortante. Ce tout dépend de ce que le PFC fait et est encore décrit dans la section suivante.

Moteur de commutation (PFC)

Une fois que l'en-tête a atteint le moteur de commutation, la logique de reconnaissance d'adresses encodées de moteur de commutation (EARL) assignera à chaque trame un DSCP interne. Ce DSCP interne est une priorité interne assignée à la trame par le PFC en tant que lui transite le commutateur. Ce n'est pas le DSCP dans l'en-tête d'ipv4. Il 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 commutées (ou a conduit) par le PFC, même les trames non-IP.

Quatre sources possibles pour le DSCP interne

Le DSCP interne sera dérivé d'un de ce qui suit :

1. Une valeur DSCP existante, positionnement avant la trame écrivant le commutateur.
2. Les bits reçus de Priorité IP ont déjà placé dans l'en-tête d'ipv4. Puisqu'il y a 64 valeurs DSCP et seulement huit valeurs de Priorité IP, l'administrateur configurera un mappage qui est utilisé par le commutateur pour dériver le DSCP. Les mappages par défaut sont en place, si l'administrateur ne configure pas les cartes.
3. Les bits reçus de cos ont déjà placé avant la trame écrivant le commutateur, ou du cos par défaut du port d'entrée s'il n'y avait aucun cos dans la trame entrante. Comme avec la Priorité IP, il y a un maximum de huit valeurs CoS, qui doivent être tracées à 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 placé de la trame utilisant une valeur par défaut de DSCP typiquement assignée cependant une entrée de liste de contrôle d'accès (ACL).

Pour no. 2 et 3 dans la liste ci-dessus, le mappage statique utilisé est par défaut, comme suit :

- Le DSCP a dérivé des égaux huit cos de périodes, pour le cos à la cartographie de DSCP.
- Le DSCP a dérivé des égaux huit Priorités IP de périodes, pour la Priorité IP à la cartographie de DSCP.

Ce mappage statique peut être ignoré par l'utilisateur en émettant les commandes suivantes :

ipprec-dscp-MAP <dscp1> <dscp2>...<dscp8> de **set qos**

cos-dscp-MAP <dscp1> <dscp2>...<dscp8> de **set qos**

La première valeur du DSCP correspondant au mappage pour le cos (ou la Priorité IP) est "0", la deuxième pour le cos (ou Priorité IP) est "1", et continuation dans ce modèle.

Lesquelles des quatre sources possibles pour le DSCP interne seront utilisées ?

Cette section décrit les règles qui déterminent lesquelles des quatre sources possibles ont décrit ci-dessus seront utilisées pour chaque paquet. Cela dépend des paramètres suivants :

1. Quel ACL de QoS sera appliqué au paquet ? Ceci est déterminé par les règles suivantes :**Remarque:** Chaque paquet passe par un rubrique de liste ACL.S'il n'y a aucun ACL relié au port d'entrée ou au VLAN, appliquez l'ACL par défaut.S'il y a un ACL relié au port d'entrée ou au VLAN, et si le trafic apparie une des entrées dans l'ACL, utilisez cette entrée.S'il y a un ACL relié au port d'entrée ou au VLAN, et si le trafic n'apparie pas une des entrées dans l'ACL, utilisez l'ACL par défaut.
2. Chaque entrée contient un mot clé de classification. Ce qui suit est une liste de mots clé possibles et de leurs descriptions :confiance-ipprec : Le DSCP interne sera dérivé de la Priorité IP reçue selon le mappage statique indépendamment de ce qu'être l'état de confiance de port peut.confiance-dscp : Le DSCP interne sera dérivé du DSCP reçu indépendamment de ce qu'être l'état de confiance de port peut.confiance-cos : Le DSCP interne sera dérivé du cos reçu selon le mappage statique, si l'état de confiance de port est de confiance (confiance-cos, confiance-dscp, confiance-ipprec). Si l'état de confiance de port est confiance-xx, le DSCP sera dérivé du cos par défaut de port selon le même mappage statique.dscp *xx* : Le DSCP interne dépendra des états suivants de confiance de port d'entrée :Si le port est non approuvé, le DSCP interne sera placé à *xx*.Si le port est confiance-dscp, le DSCP interne sera le DSCP reçu dans le paquet entrant.Si le port est confiance-cos, le DSCP interne sera dérivé du cos du paquet reçu.Si le port est confiance-ipprec, le DSCP interne sera dérivé de la Priorité IP du paquet reçu.
3. Chaque ACL de QoS peut être appliqué à un port ou à un VLAN, mais il y a un paramètre de configuration supplémentaire à prendre en considération ; le type de port d'ACL. Un port peut être configuré pour être basé sur VLAN ou basé sur port. Ce qui suit est une description des deux types de configurations :Un port configuré pour être basé sur VLAN regardera seulement à l'ACL appliqué au VLAN auquel le port appartient. S'il y a un ACL relié au port, l'ACL sera ignoré pour le paquet étant livré dedans sur ce port.Si un port appartenant à un VLAN est configuré comme basé sur port, même s'il y a un ACL relié à ce VLAN, il ne sera pas pris en compte pour le trafic étant livré dedans de ce port.

Ce qui suit est une syntaxe pour créer un ACL de QoS pour marquer le trafic IP :

acl_name d'**IP d'acl de set qos [dscp xx | confiance-cos | confiance-dscp |** *règle de rubrique de liste ACL de* **confiance-ipprec]**

L'ACL suivant, marquera tout le trafic IP dirigé héberger 1.1.1.1 avec un DSCP de "40" et confiance-dscp pour tout autre trafic IP :

IP quel du dscp 40 de l'**acl** TEST_ACL de **set qos** hôte 1.1.1.1

IP tout quel de confiance-dscp de l'**acl** TEST_ACL de **set qos**

Une fois que l'ACL a été créé vous devez le tracer à un port ou un VLAN, ceci peut être fait en émettant la commande suivante :

acl_name de **carte d'acl de set qos [module/port | VLAN]**

Par défaut, chaque port est basé sur port pour l'ACL, ainsi si vous voulez relier un ACL à un VLAN, vous devez configurer les ports de ce VLAN comme basés sur VLAN. Ceci peut être fait en émettant la commande suivante :

module/port de **set port qos basé sur VLAN**

Ce peut également être mode basé sur port revenu à en émettant la commande suivante :

module/port de **set port qos basé sur port**

Résumé : Comment le DSCP interne est-il choisi ?

Le DSCP interne dépend des facteurs suivants :

- état de confiance de port
- ACL relié au port
- ACL par défaut
- basé sur VLAN ou basé sur port en vue de l'ACL

L'organigramme suivant récapitule comment le DSCP interne est choisi selon la configuration :

Le PFC peut également faire le maintien de l'ordre. Ceci pourrait par la suite avoir comme conséquence une réduction du DSCP interne. Pour plus de détails sur maintenir l'ordre, référez-vous au document suivant :

- Réglementation QoS sur la gamme Catalyst 6000

L'organigramme suivant affiche comment le régulateur est appliqué :

Manipulation de port de sortie

Il n'y a rien qui peut être fait au niveau de port de sortie pour changer la classification, mais dans cette section vous marquerez le paquet accordant les règles suivantes :

- Si le paquet est un paquet d'ipv4, copiez le DSCP interne assigné en le moteur de commutation dans l'octet de tos de l'en-tête d'ipv4.
- Si le port de sortie est configuré pour un ISL ou l'encapsulation dot1q, utilisez le cos dérivé du DSCP interne, et copiez-le dans l'ISL ou la trame dot1q.

Remarque: Le cos est dérivé du DSCP interne selon une charge statique configurée par l'utilisateur émettant la commande suivante :

Remarque: *dscp_list de dscp-cos*-**MAP de set qos** *: cos_value*

Remarque: Ce qui suit sont les configurations par défaut. Par défaut le cos sera la pièce d'entier du DSCP divisé 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 le cos est dérivé du DSCP, le paquet sera envoyé à une des files d'attente de sortie pour la planification de sortie basée sur son cos (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 au document suivant :

- QoS sur des Commutateurs de gamme Catalyst 6000 : Planification de sortie sur le Catalyst 6000 avec le PFC ou le PFC2 utilisant le logiciel de CatOS

L'organigramme suivant récapitule le traitement du paquet concernant le marquage dans le port de sortie :

Notes et limites

L'ACL par défaut

Par défaut, l'ACL par défaut utilise le « dscp 0" comme mot clé de classification. Cela signifie que tout le trafic entrant le commutateur par un port non approuvé sera identifié par un DSCP de "0" si QoS est activé. Vous pouvez vérifier l'ACL par défaut pour l'IP en émettant la commande suivante :

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

L'ACL par défaut peut également être changé en émettant la commande suivante :

IP d'action par défaut d'acl de set qos [dscp xx | Confiance-cos | confiance-dscp | confiance-ipprec]

confiance-cos dans des limites de rubrique de liste ACL

Il y a une limite supplémentaire qui apparaît quand vous utilisez le mot clé de confiance-cos dans une entrée. Le cos met en boîte est de confiance seulement dans une entrée si l'état de confiance de réception n'est pas non approuvé. Tenter pour configurer une entrée avec le confiance-cos affichera 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 limite est une conséquence de ce qui a été vu plus tôt dans le port d'entrée traitant la section. Comme vu dans l'organigramme de cette section, si le port est non approuvé, la trame est immédiatement assignée le cos par défaut de port. Par conséquent, le cos entrant n'est pas préservé et n'est pas envoyé au moteur de commutation, ayant pour résultat une incapacité de faire confiance au cos même avec un ACL spécifique.

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

Cette section concerne seulement les linecards suivants :

- WS-X6224-100FX-MT : CATALYST 6000 24 PORTS 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 100FX, ENH QOS, LA TA
- WS-X6324-100FX-SM : CATALYST 6000 24-PORT 100FX, ENH QOS, LA TA
- WS-X6348-RJ-45 : CATALYST 6000 48-PORT 10/100, QO AMÉLIORÉ
- WS-X6348-RJ21V : CATALYST 6000 48-PORT 10/100, ALIMENTATION EN LIGNE
- WS-X6348-RJ45V : CATALYST 6000 48-PORT 10/100, ENH QOS, ALIMENTATION NE INLI

Ces linecards, cependant, ont quelques limites supplémentaires :

- Au niveau, à vous de port ne peut pas le confiance-dscp ou la confiance-ipprec.
- Au niveau de port, si l'état de confiance de port est confiance-cos, les déclarations suivantes s'appliquent :Le seuil de réception pour l'établissement du programme d'entrée est activé. En outre, le cos dans le paquet de réception est utilisé pour donner la priorité à des paquets pour accéder au bus.Le cos pas est de confiance et ne sera pas utilisé pour dériver le DSCP interne, à moins que vous ayez également configuré l'ACL pour ce trafic au confiance-cos. En outre, il n'est pas assez pour les linecards au confiance-cos sur le port, vous doit également avoir un ACL avec le confiance-cos pour ce trafic.
- Si l'état de confiance de port est non approuvé, le marquage normal se produira (comme avec le cas standard). Ceci dépend de l'ACL appliqué au trafic.

N'importe quelle tentative de configurer un état de confiance sur un de ces ports affichera 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 classification

Les tables ci-dessous affichent le DSCP en résultant classifié par ce qui suit :

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

Le tableau récapitulatif générique pour tous les ports excepté WS-X62XX et WS-X63XX

Mot clé	dscp	confiance-	confiance-	Confiance-

d'ACL État de confiance de port	xx	dscp	ipprec	cos
Non approuvé	xx (1)	Dscp de Rx	dérivé de l'ipprec de Rx	0
confiance-dscp	Rx-dscp	Dscp de Rx	dérivé de l'ipprec de Rx	dérivé du cos 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) c'est la seule manière de faire un nouveau marquage d'une trame.

Tableau récapitulatif pour WS-X62XX ou WS-X63XX

Mot clé d'ACL État de confiance de port	dscp 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	xx	Dscp de Rx	dérivé de l'ipprec de Rx	dérivé du cos de Rx ou du cos

				de port (2)

(2) c'est la seule manière de préserver le cos entrant pour le trafic provenant un linecard 62*xx* ou 63*xx*.

Surveillant et vérifiant une configuration

Vérifier la configuration des ports

Les configurations et les configurations de port mettent en boîte vérifié en émettant la commande suivante :

module/port de **show port qos**

En émettant cette commande, vous pouvez vérifier, entre d'autres paramètres, les paramètres suivants de classification :

- basé sur port ou basé sur VLAN
- type de port de confiance
- ACL relié au port

Ce qui suit est un échantillon de cette sortie de commande avec les importants champs concernant la classification mise en valeur :

```
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.

Vérifier l'ACL

Vous pouvez vérifier l'ACL appliqué et vu dans des commandes précédentes en émettant la commande suivante :

acl_name de **délai d'exécution de l'information d'acl de show qos**

```
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
```

Études de cas témoin

Les exemples suivants sont des configurations d'échantillon des cas communs qui pourraient apparaître dans un réseau.

Cas 1 : Marquage à la périphérie

Supposez que vous configurez un Catalyst 6000 utilisé comme un commutateur d'accès avec beaucoup d'utilisateurs s'est connecté pour rainer 2, qui est un linecard WS-X6348 (10/100M). Les utilisateurs peuvent envoyer ce qui suit :

- Le trafic de données normal : C'est toujours dans VLAN 100, et doit obtenir un DSCP de "0."
- Le trafic vocal d'un téléphone IP : C'est toujours dans le VLAN auxiliaire 101 de Voix, et doit obtenir un DSCP de "40."
- Le trafic d'application stratégique de mission : Ceci est livré également dans 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, donc vous quitterez le port en tant que non approuvé et configurerez un ACL spécifique pour classifier le trafic. Un ACL sera appliqué à l'ACL VLAN 100 et un sera appliqué à VLAN 101. Vous devez également configurer tous les ports comme basés sur VLAN. Ce qui suit est un exemple de la configuration en résultant :

```
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 au centre pour seulement une interface de gigabit

Supposez que vous configurez un principal Catalyst 6000 avec seulement une interface de gigabit dans l'emplacement 1 et l'emplacement 2 (aucun linecard 62xx ou 63xx dans le châssis). Le trafic a été correctement marqué précédemment par les commutateurs d'accès, donc vous n'avez pas besoin de faire la remarque, mais vous devez s'assurer que vous faites confiance au DSCP entrant. C'est le cas le plus facile, car tous les ports seront marqués comme confiance-dscp et ce devrait être suffisant :

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

Affaire 3 : La confiance au centre pour un 62xx ou les 63xx mettent en communication dans le châssis

Supposez que vous configurez périphérique un principal/distribution avec une liaison Gigabit sur un linecard WS-X6416-GBIC (dans emplacement 2), et un lien de 10/100 sur un linecard WS-X6348 (dans emplacement 3). Vous devez également faire confiance à tout le trafic entrant car il a été marqué plus tôt au niveau de commutateur d'accès. Puisque vous ne pouvez pas confiance-dscp sur le linecard 6348, la méthode facile dans ce cas serait de quitter tous les ports en tant que non approuvé et de changer l'ACL par défaut au confiance-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