

CoPP sur des Commutateurs de gamme de Nexus 7000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[CoPP sur l'aperçu de commutateur de gamme de Nexus 7000](#)

[Pourquoi CoPP sur la gamme de Nexus 7000 commutent](#)

[Contrôlez le traitement plat sur le commutateur de gamme de Nexus 7000](#)

[Stratégie de pratiques recommandées de CoPP](#)

[Comment personnaliser une stratégie de CoPP](#)

[Étude de cas personnalisée de stratégie de CoPP](#)

[Structure de données de CoPP](#)

[Facteur d'échelle de CoPP](#)

[Surveillance et Gestion de CoPP](#)

[Compteurs de CoPP](#)

[Compteurs d'ACL](#)

[Pratiques recommandées de configuration de CoPP](#)

[Pratiques recommandées de surveillance de CoPP](#)

[Conclusions](#)

[Fonctions non prises en charge](#)

Introduction

Ce document décrit ce que, comment, et pourquoi la Réglementation du plan de commande (CoPP) est utilisée sur les Commutateurs de gamme de Nexus 7000, qui incluent le F1, F2, M1, et les modules de gamme M2 et les linecards (LCS). Il inclut également des stratégies de pratique recommandée, aussi bien que comment personnaliser une stratégie de CoPP.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du système d'exploitation CLI de Nexus.

Composants utilisés

Les informations dans ce document sont basées sur les Commutateurs de gamme de Nexus 7000 avec le module du superviseur 1.

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.

CoPP sur l'aperçu de commutateur de gamme de Nexus 7000

Le CoPP est essentiel à l'exploitation réseau. Une attaque du Déni de service (DOS) à l'avion de contrôle/Gestion, qui peut être commis par distraction ou avec malveillance, implique typiquement les hauts débits du trafic qui ont comme conséquence l'utilisation du processeur excessive. Le module de superviseur passe une durée excessive manipulant les paquets.

Les exemples de telles attaques incluent :

- Requêtes d'écho de Protocole ICMP (Internet Control Message Protocol).
- Paquets envoyés avec des IP-**options** réglées.

Ceci peut mener à :

- Perte de messages de keep-alive et de mises à jour de protocole de routage.
- Le remplissage du paquet s'aligne, qui a comme conséquence des baisses aveugles.
- Sessions interactives lentes ou insensibles.

Les attaques peuvent accabler la stabilité du réseau et la Disponibilité et mener aux pannes de réseau entreprise-les affectant.

CoPP est une caractéristique réalisée par matériel qui protège le superviseur contre des attaques DoS. Il contrôle le débit auquel on permet à des des paquets pour atteindre le superviseur. La caractéristique de CoPP est modelée comme une stratégie QoS d'entrée reliée à l'interface spéciale appelée le contrôle-**avion**. Cependant, CoPP est une fonctionnalité de sécurité et pas une partie de QoS. Afin de protéger le superviseur, le CoPP sépare des paquets de plan de données des paquets d'avion de contrôle (logique d'exception). Il identifie des paquets d'attaque DoS des paquets valides (classification). CoPP tient compte de la classification de ces paquets :

- Recevez les paquets
- Paquets de multidiffusion
- Paquets d'exception
- Réorientez les paquets
- MAC de diffusion + paquets non-IP
- MAC de diffusion + paquets IP (voir l'ID de bogue Cisco [CSCub47533](#) - des paquets dans le VLAN L2 (aucun SVI) frappant CoPP)
- MAC + paquets IP de Mcast

- MAC de routeur + paquets non-IP
- Paquets d'ARP

Après qu'un paquet soit classifié, le paquet peut également être marqué et utilisé pour assigner différentes priorités basées sur le type de paquets. Conformez-vous, dépassez, et violez les actions (transmettez, relâchez, réduction) peut être placé. Si aucun régulateur n'est relié à une classe, alors un régulateur par défaut est ajouté dont se conforment action sont baisse. Glanez les paquets sont maintenus l'ordre avec la classe par défaut. Un débit, deux colorent, et deux évaluez, maintien de l'ordre de trois couleurs sont pris en charge.

Trafiquez que frappe la CPU sur le superviseur que le module peut entrer par quatre chemins :

1. Interfaces intrabandes (port de panneau avant) pour le trafic envoyé par des linecards.
2. Interface de gestion (mgmt0) utilisée pour le trafic d'administration.
3. Interface du processeur de contrôle et de surveillance (CMP) utilisée pour la console.
4. Les Ethernets commutés réunissent la Manche (EOBC) pour contrôler les linecards du module de superviseur et pour permuter des messages d'état.

Seulement le trafic envoyé par l'interface intrabande est sujet à CoPP, parce que c'est le seul trafic qui accède le module de superviseur par les engines d'expédition (FEs) sur les linecards. L'implémentation de commutateur de gamme de Nexus 7000 de CoPP est réalisée par matériel seulement, ainsi il signifie que CoPP n'est pas exécuté dans le logiciel par le module de superviseur. La fonctionnalité de CoPP (maintien de l'ordre) est mise en application sur chaque technicien indépendamment. Quand les divers débits sont configurés pour le policy-map de CoPP, la considération doit être respect rentré au nombre de linecards dans le système.

Tout le trafic reçu par le superviseur est des temps $N X$, où N est le nombre de FEs sur le système de Nexus 7000, et X est le débit laissé pour la classe particulière. Les valeurs configurées de régulateur s'appliquent sur a par base technicien, et l'ensemble du trafic enclin a frappé la CPU est la somme du trafic conformé et transmis sur tout les FEs. En d'autres termes, trafiquez que frappe la CPU égale configuré se conforment débit multiplié par le nombre de FEs.

- N7K-M148GT-11/L LC a 1 technicien
- N7K-M148GS-11/L LC a 1 technicien
- N7K-M132XP-12/L LC a 1 technicien
- N7K-M108X2-12L LC a le technicien 2
- N7K-F248XP-15 LC a le technicien 12 (les SOC)
- N7K-M235XP-23L LC a le technicien 2
- N7K-M206FQ-23L LC a le technicien 2
- N7K-M202CF-23L LC a le technicien 2

La configuration de CoPP est seulement mise en application dans le contexte par défaut de périphérique virtuel (volts continu) ; cependant, les stratégies de CoPP s'appliquent pour tout le VDCs. La même stratégie globale est appliquée pour tous les linecards. CoPP applique le partage de ressource entre VDCs si les ports du même FEs appartiennent à VDCs différent (gamme M1 ou gamme M2 LC). Par exemple, ports d'un technicien, même dans VDCs différent, compte contre le même seuil pour CoPP.

Si le même technicien est partagé entre VDCs différent et une classe donnée du trafic d'avion de contrôle dépasse le seuil, ceci affecte tout le VDCs sur le même technicien. Il est recommandé

pour dédier un technicien par volts continu afin d'isoler l'application de CoPP, si possible.

Quand le commutateur est soulevé première fois, la stratégie par défaut doit être programmée pour protéger le contrôle-avion. CoPP fournit les stratégies par défaut, qui sont contrôle-avion appliqué en tant qu'élément de l'ordre de démarrage initial.

Pourquoi CoPP sur la gamme de Nexus 7000 commutent

Le commutateur de gamme de Nexus 7000 est déployé comme commutateur d'agrégation ou de noyau. Par conséquent, c'est l'oreille et le cerveau du réseau. Il manipule le chargement maximum dans le réseau. Il doit traiter des demandes fréquentes et de rafale. Certaines de demandes incluent :

- **Traitement du BPDU de spanning-tree (BPDU)** - Le par défaut est toutes les deux secondes.
- **D'abord Redondance de saut** - Ceci inclut le Protocole HSRP (Hot Standby Router Protocol), le Protocole VRRP (Virtual Router Redundancy Protocol), et l'Équilibrage de charge Protocol (GLBP) de passerelle - par défaut est toutes les trois secondes.
- **Address resolution** - Ceci inclut Address Resolution Protocol/Voisin-détection (ARP/ND), Forwarding Information Base (FIB) glanent - jusqu'à une demande par seconde, par hôte, tel que teaming du contrôleur d'interface réseau (NIC).
- **Dynamic Host Control Protocol (DHCP)** - Requête DHCP, relais - Jusqu'à une demande par seconde, par hôte.
- **Protocoles de routage** pour la couche 3 (L3).
- **Interconnexion de Data Center** - Virtualisation de transport de recouvrement (OTV), Commutation multiprotocole par étiquette (MPLS), et service privé virtuel de RÉSEAU LOCAL (VPLS).

CoPP est essentiel afin de protéger la CPU contre les serveurs misconfigured ou les attaques DoS de potentiel, qui permet à la CPU pour avoir assez de cycle pour traiter les messages essentiels d'avion de contrôle.

Contrôlez le traitement plat sur le commutateur de gamme de Nexus 7000

La gamme de Nexus 7000 commute adopte une approche d'avion de contrôle distribué. Il a un multinucléaire sur chaque module E/S, aussi bien qu'un multinucléaire pour l'avion de contrôle de commutateur sur le module de superviseur. Il débarque des tâches intensives à la CPU de module E/S pour des listes de contrôle d'accès (ACL) et la programmation de FIB. Il mesure la capacité d'avion de contrôle avec le nombre de linecards. Ceci évite l'étranglement CPU de superviseur, qui est vu dans une approche centralisée. Les bornes de débit de matériel et le CoPP réalisé par matériel protège l'avion de contrôle contre le mauvais ou l'action malveillante.

Stratégie de pratiques recommandées de CoPP

La stratégie de pratiques recommandées de CoPP (BPP) a été introduite dans la version 5.2 de Cisco NX-OS. La sortie de **commande show running-config** n'affiche pas le contenu du CoPP BPP. **L'exposition exécute toute la commande affiche le contenu de CoPP BPP.**

```
-----SNIP-----
SITE1-AGG1# show run copp

!! Command: show running-config copp
!! Time: Mon Nov 5 22:21:04 2012

version 5.2(7)
copp profile strict
```

```
SITE1-AGG1# show run copp all

!! Command: show running-config copp all
!! Time: Mon Nov 5 22:21:15 2012
```

```
version 5.2(7)
-----SNIP-----
control-plane
service-policy input copp-system-p-policy-strict
copp profile strict
```

CoPP fournit quatre options à l'utilisateur pour des stratégies par défaut :

- Strict
- Modéré
- Clément
- Dense (introduit dans version 6.0(1))

Si aucune option n'est sélectionnée ou si l'installation est ignorée, alors le maintien de l'ordre strict est appliqué. Toutes ces options des valeurs utilisent les mêmes class-map et classes, mais le débit de données garanti différent (CIR) et de rafale compte (BC) pour le maintien de l'ordre. Dans le Cisco NX-OS libère plus tôt que 5.2.1, la **commande setup** ont été utilisés pour changer l'option. La version 5.2.1 de Cisco NX-OS a introduit une amélioration au CoPP BPP de sorte que l'option puisse être changée sans **commande setup** ; utilisez la commande de **profil de copp**.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# copp profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1(config)# copp profile strict
SITE1-AGG1(config)# exit
```

Utilisez la commande de **<profile-type> de profil de copp d'exposition** de visualiser la configuration par défaut de CoPP BPP. Utilisez la commande de **show copp status** de vérifier que la stratégie de CoPP a été appliquée correctement.

```
SITE1-AGG1# show copp status
Last Config Operation: copp profile strict
Last Config Operation Timestamp: 20:40:27 PST Nov 5 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-system-p-policy-strict
```

Afin de visualiser la différence entre deux CoPP BPPs, utilisez la commande du <profile-type 2> de profil du <profile-type 1> de profil de diff de copp d'exposition :

```
SITE1-AGG1# show copp diff profile strict profile moderate
A '+' represents a line that has been added and
a '-' represents a line that has been removed.
-policy-map type control-plane copp-system-p-policy-strict
- class copp-system-p-class-critical
- set cos 7
- police cir 39600 kbps bc 250 ms conform transmit violate drop
- class copp-system-p-class-important
- set cos 6
- police cir 1060 kbps bc 1000 ms conform transmit violate drop
-----SNIP-----
+policy-map type control-plane copp-system-p-policy-moderate
+ class copp-system-p-class-critical
+ set cos 7
+ police cir 39600 kbps bc 310 ms conform transmit violate drop
+ class copp-system-p-class-important
+ set cos 6
+ police cir 1060 kbps bc 1250 ms conform transmit violate drop
-----SNIP-----
```

Comment personnaliser une stratégie de CoPP

Les utilisateurs peuvent créer une stratégie personnalisée de CoPP. Copiez le CoPP par défaut BPP, et reliez-le à l'interface de contrôle-avion parce que le CoPP BPP est en lecture seule.

```
SITE2-AGG1(config)# policy-map type control-plane copp-system-p-policy-strict
^
% String is invalid, 'copp-system-p-policy-strict' is not an allowed string at
'^' marker.
```

La commande de <prefix> de <profile-type> de profil de copie de copp [suffixe] crée un clone du CoPP BPP. Ceci est utilisé afin de modifier les configurations par défaut. La commande de **profil de copie de copp** est une commande de **mode d'exécution**. L'utilisateur peut choisir un préfixe ou un suffixe pour la liste d'accès, les class-map, et le nom de policy-map. Par exemple, copp-système-p-stratégie-strict est changé [préfixe] à copp-stratégie-strict [suffixe]. Des configurations copiées sont traitées comme configurations utilisateur et sont incluses dans la sortie de **passage d'exposition**.

```
SITE1-AGG1# copp copy profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1# copp copy profile strict ?
prefix Prefix for the copied policy
suffix Suffix for the copied policy
SITE1-AGG1# copp copy profile strict suffix ?
WORD Enter prefix/suffix for the copied policy (Max Size 20)
SITE1-AGG1# copp copy profile strict suffix CUSTOMIZED-COPP
SITE1-AGG1# show run copp | grep policy-map
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1#
```

Il est possible de marquer en bas du trafic qui dépasse et viole un taux d'informations laissé spécifié (PIR) avec ces commandes :

```
SITE1-AGG1(config)# policy-map type
control-plane copp-policy-strict-CUSTOMIZED-COPP
```

```

SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms ?
<CR>
conform Specify a conform action
pir Specify peak information rate

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir ?
<1-80000000000> Peak Information Rate in bps/kbps/mbps/gbps

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps ?
<CR>
<1-512000000> Peak Burst Size in bytes/kbytes/mbytes/packets/ms/us
be Specify extended burst
conform Specify a conform action

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform ?
drop Drop the packet
set-cos-transmit Set conform action cos val
set-dscp-transmit Set conform action dscp val
set-prec-transmit Set conform action precedence val
transmit Transmit the packet

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform
set-dscp-transmit ef exceed set dscp1 dscp2 table cir-markdown-map violate
set1 dscp3 dscp4 table1 pir-markdown-map
SITE1-AGG1(config-pmap-c)#

```

Appliquez la stratégie personnalisée de CoPP au contrôle-avion global d'interface. Employez la commande de **show copp status** afin de vérifier que la stratégie de CoPP a été appliquée correctement.

```

SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP

```

Étude de cas personnalisée de stratégie de CoPP

Cette section décrit un vrai exemple dans lequel le client exige de plusieurs périphériques de surveillance afin de cingler fréquemment les interfaces locales. La difficulté est rencontrée dans ce scénario quand le client veut modifier la stratégie de CoPP :

- Augmentez le CIR de sorte que ces adresses spécifiques puissent cingler le périphérique local et ne pas violer la stratégie.
- Permettez aux autres adresses IP pour mettre à jour la capacité de cingler le périphérique local, mais à un CIR inférieur pour dépannage des butts.

La solution est affichée dans l'exemple suivant, qui est de créer une stratégie personnalisée avec un class-map distinct. Le class-map distinct contient les adresses IP spécifiées des périphériques de surveillance et le class-map a un CIR plus élevé. Ceci part également de la *surveillance*

d'origine de class-map, qui capture le trafic d'ICMP pour toutes les autres adresses IP à un CIR inférieur.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

Structure de données de CoPP

La structure de données de CoPP BPP est construite en tant que :

- **Configuration d'ACL** : ACL IP et ACL de MAC.
- **Configuration de classificateur** : Class-map appariant l'ACL IP ou l'ACL de MAC.
- **Configuration de régulateur** : Placez le CIR, BC, se conformement action, et viole l'action. Le régulateur a deux débits (CIR et BC), et deux couleurs (conformez-vous et violez).

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

Facteur d'échelle de CoPP

La configuration de facteur d'échelle introduite dans la version 6.0 de Cisco NX-OS est utilisée pour mesurer le débit de régulateur de la stratégie appliquée de CoPP pour une carte de ligne particulière. Ceci augmente ou réduit le débit de régulateur pour une carte de ligne particulière, mais ne change pas la stratégie en cours de CoPP. Les modifications sont efficaces immédiatement, et il n'y a aucun besoin de réappliquer la stratégie de CoPP.

```
scale factor option configured within control-plane interface:
Scale-factor <scale factor value> module <module number>
<scale factor value>: from 0.10 to 2.00
Scale factor is recommended when a chassis is loaded with both F2 and M
Series modules.
SITE1-AGG1# conf t
```



```
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# scale-factor ?
<whole>.<decimal> Specify scale factor value from 0.10 to 2.00
```

```
SITE1-AGG1(config-cp)# scale-factor 1.0 ?
module Module
```

```
SITE1-AGG1(config-cp)# scale-factor 1.0 module ?
<1-10> Specify module number
```

```
SITE1-AGG1(config-cp)# scale-factor 1.0 module 4
SITE1-AGG1# show system internal copp info
<snip>
```

```
Linecard Configuration:
```

```
-----
```

```
Scale Factors
Module 1: 1.00
Module 2: 1.00
Module 3: 1.00
Module 4: 1.00
Module 5: 1.00
Module 6: 1.00
Module 7: 1.00
Module 8: 1.00
Module 9: 1.00
Module 10: 1.00
```

Surveillance et Gestion de CoPP

Avec la version 5.1 de Cisco NX-OS, il est possible de configurer un seuil de baisse par nom de classe de CoPP qui déclenche un message de Syslog dans l'événement que le seuil est dépassé. La commande **se connecte le level> <logging de niveau de count> d'octets <dropped par seuil de baisse.**

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# logging ?
drop Logging for dropped packets
```

```
SITE1-AGG1(config-pmap-c)# logging drop ?
threshold Threshold value for dropped packets
```

```
SITE1-AGG1(config-pmap-c)# logging drop threshold ?
<CR>
<1-80000000000> Dropped byte count
```

```
SITE1-AGG1(config-pmap-c)# logging drop threshold 100 ?
<CR>
level Syslog level
```

```
SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level ?
<1-7> Specify the logging level between 1-7
```

```
SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7
```

Voici un exemple d'un message de Syslog :

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
```

```

SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# logging ?
drop Logging for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop ?
threshold Threshold value for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop threshold ?
<CR>
<1-80000000000> Dropped byte count

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 ?
<CR>
level Syslog level

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level ?
<1-7> Specify the logging level between 1-7

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7

```

Compteurs de CoPP

CoPP prend en charge le même qos statistics que n'importe quelle autre interface. Il affiche les statistiques des classes qui forment la stratégie de service pour chaque module E/S qui prend en charge CoPP. Utilisez la commande de contrôle-avion de **show policy-map interface** de visualiser les statistiques pour CoPP.

Remarque: Toutes les classes devraient être surveillées en termes de paquets violés.

```

SITE1-AGG1# show policy-map interface control-plane
Control Plane

service-policy input: copp-policy-strict-CUSTOMIZED-COPP

class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
match access-group name copp-acl-bgp-CUSTOMIZED-COPP
match access-group name copp-acl-bgp6-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp-CUSTOMIZED-COPP
match access-group name copp-acl-igmp-CUSTOMIZED-COPP
match access-group name copp-acl-msdp-CUSTOMIZED-COPP
match access-group name copp-acl-ospf-CUSTOMIZED-COPP
match access-group name copp-acl-ospf6-CUSTOMIZED-COPP
match access-group name copp-acl-pim-CUSTOMIZED-COPP
match access-group name copp-acl-pim6-CUSTOMIZED-COPP
match access-group name copp-acl-rip-CUSTOMIZED-COPP
match access-group name copp-acl-rip6-CUSTOMIZED-COPP
match access-group name copp-acl-vpc-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp6-CUSTOMIZED-COPP
match access-group name copp-acl-mac-l2pt-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-ldp-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-oam-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-rsvp-CUSTOMIZED-COPP
match access-group name copp-acl-otv-as-CUSTOMIZED-COPP
match access-group name copp-acl-mac-otv-isis-CUSTOMIZED-COPP
match access-group name copp-acl-mac-fabricpath-isis-CUSTOMIZED-COPP
match protocol mpls router-alert
match protocol mpls exp 6
set cos 7
threshold: 100, level: 7
police cir 39600 kbps , bc 250 ms

```

```
module 1 :
conformed 22454 bytes; action: transmit
violated 0 bytes; action: drop
```

```
module 2 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

```
module 3 :
conformed 19319 bytes; action: transmit
violated 0 bytes; action: drop
```

```
module 4 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

Afin d'obtenir une vue d'agrégat des compteurs conformés et violés pour tout le class-map et modules E/S, utilisez le contrôle-avion de **show policy-map interface | « classe |conformez-vous| »** commande **violée**.

```
SITE1-AGG1# show policy-map interface control-plane | i "class|conform|violated"
class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
conformed 123126534 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 107272597 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
class-map copp-class-important-CUSTOMIZED-COPP (match-any)
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

La classe copp-class-l2-default et le classe-par défaut devraient être surveillés pour s'assurer qu'il n'y a aucune augmentation de haute, même pour les compteurs conformés. Dans le meilleur des cas, ces deux classes doivent avoir des faibles valeurs pour le compteur conformé et au moins aucune contre- augmentation violée.

Compteurs d'ACL

La commande de **statistics per-entry** n'est pas prise en charge pour l'ACL IP ou l'ACL de MAC utilisé dans le class-map de CoPP, et elle n'a aucun effet une fois appliquée à l'ACL IP de CoPP ou à l'ACL de MAC. (Il n'y a aucun contrôle CLI fait par le programme d'analyse syntaxique CLI). Afin de visualiser l'ACL de MAC de CoPP ou l'ACL IP frappe sur un module E/S, utilisent la commande **interne de détail d'entrées d'entrée de liste d'accès de show system**.

Voici un exemple :

```
!! 0180.c200.0041 is the destination MAC used for FabricPath IS-IS
```

```
SITE1-AGG1# show system internal access-list input entries det | grep 0180.c200.0041
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```


- La configuration de facteur d'échelle est recommandée quand un châssis est chargé avec la gamme F2 et les modules de gamme M.

Pratiques recommandées de surveillance de CoPP

Ce sont des recommandations de pratique recommandée pour la surveillance de CoPP :

- Configurez un seuil de message de Syslog pour CoPP (version 5.1 de Cisco NX-OS) afin de surveiller des baisses imposées par CoPP.
- Des messages de Syslog sont générés si les baisses dans une classe du trafic dépassent le seuil utilisateur-configuré.
- Le seuil et le niveau de connectants peuvent être personnalisés dans chaque classe du trafic avec l'utilisation de la commande **se connectante de <level> de niveau de <packet-count> de seuil de baisse**.
- Puisque l'option de « statistics per-entry » pour l'ACL de MAC de CoPP ou l'ACL IP n'est pas prise en charge, utilisez la commande **interne de det d'entrées d'entrée de liste d'accès de show system** de surveiller des hit d'entrées de contrôle d'accès (ACE).
- **La classe copp-class-l2-default et la commande de classe-par défaut** devraient être surveillées pour s'assurer qu'il n'y a aucune augmentation de haute, même pour les compteurs conformés.
- Toutes les classes devraient être surveillées en termes de paquets violés.
- Puisque **copp-classe-essentiel** est fortement essentiel mais a une stratégie de **baisse de violer**, moniteur d'il est conseillé de le débit de paquets conformés afin de recevoir une première indication quand la classe devient près au moment où elle commence la violation. Si le compteur violé augmente pour cette classe, il ne signifie pas nécessairement une alerte rouge. En revanche, il signifie que cette situation doit être étudiée dans à court terme.
- Utilisez la commande **stricte de profil de copp** après chaque mise à niveau du code de Cisco NX-OS, ou au moins après chaque principale mise à niveau du code de Cisco NX-OS ; si une modification de CoPP était précédemment terminée, elle doit être réappliquée.

Conclusions

- CoPP est une caractéristique réalisée par matériel qui protège le superviseur contre des attaques DoS.
- M1, F2, et support CoPP LCS de gamme M2. Les LCS de gamme F1 ne prennent en charge pas CoPP.
- La configuration de CoPP est semblable à MQC (QoS modulaire CLI).

- La configuration et la surveillance de CoPP est exécutée seulement dans un par défaut volts continu.
- CoPP par défaut BPP peut être utilisé avec des options strictes, modérées, clémentes, et denses.
- Copiez CoPP BPP CoPP personnalisé ordonne afin d'apparier des spécifications du réseau spécifiques.
- Des compteurs de CoPP (conformés et violés dans les octets par class-map) sont affichés avec la commande de contrôle-avion de **show policy-map interface**.
- Le trafic reçu par la CPU du module de superviseur égale le nombre total de FEs fois le débit laissé.
- Essayez d'éviter les ports partagés d'un technicien à travers VDCs différent.
- Suivez les pratiques recommandées de CoPP afin d'avec succès implémenter et surveiller les caractéristiques.

Fonctions non prises en charge

Ces caractéristiques ne sont pas prises en charge :

- Maintien de l'ordre distribué d'agrégat.
- Maintien de l'ordre de Microflow.
- Maintien de l'ordre d'exception de sortie.
- Soutien de CoPP du BPDU qui provient un port dot1q-tunnel (QinQ) : Protocole CDP (Cisco Discovery Protocol), dot1x, Protocole Spanning Tree (STP), et protocole VTP (VLAN Trunk Protocol).