Nexus 7000系列交換機上的CoPP

目錄

簡介

本檔案介紹在Nexus 7000系列交換器(包括F1、F2、M1和M2系列模組和線路卡(LC))上使用控制平面管制(CoPP)的方式、方式及原因。 還包括最佳做法策略，以及如何自定義CoPP策略。

必要條件

需求

思科建議您瞭解Nexus作業系統CLI。

採用元件

本檔案中的資訊是根據搭載Supervisor 1模組的Nexus 7000系列交換器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

Nexus 7000系列交換機上的CoPP概述

CoPP對網路運行至關重要。對控制/管理平面的拒絕服務(DoS)攻擊（可能無意或惡意實施）通常涉及高流量率，從而導致CPU使用率過高。Supervisor模組處理資料包的時間過長。

此類攻擊的示例包括：

- 網際網路控制訊息通訊協定(ICMP)回應要求。
- 使用**ip-options set傳送的**資料包。

這可能導致：

- 保活消息和路由協定更新丟失。
- 填充資料包隊列，導致任意丟棄。
- 緩慢或無響應的互動式會話。

攻擊會破壞網路的穩定性和可用性，並導致影響業務的網路故障。

CoPP是一種基於硬體的功能，可保護Supervisor免受DoS攻擊。它控制允許資料包到達Supervisor的速率。CoPP功能類似於連線到稱為控制平面的特殊介面的輸入**QoS策略**。但是，CoPP是一個安全功能，而不是QoS的一部分。為了保護Supervisor，CoPP將資料平面資料包與控制平面資料包分離（異常邏輯）。 它標識來自有效資料包的DoS攻擊資料包（分類）。 CoPP允許對這些資料包進行分類：

- 接收資料包
- 組播資料包
- 異常資料包
- 重定向資料包
- 廣播MAC +非IP資料包
- 廣播MAC + IP封包(請參閱思科錯誤ID CSCub47533 -命中CoPP的第2層Vlan（無SVI）中的封包)
- 廣播MAC + IP資料包
- 路由器MAC +非IP資料包
- ARP資料包

在對資料包分類後，還可以對資料包進行標籤，並根據資料包型別分配不同的優先順序。可以設定conform、exceed和violate操作(transmit、drop、mark-down)。如果沒有將監察器附加到類，則新增其符合操作為drop的預設監察器。收集資料包使用default-class進行管制。支援一個速率、兩種顏色和兩個速率、三種顏色策略。

到達Supervisor模組上CPU的流量可通過以下四個路徑進入：

1. 用於線卡傳送的流量的帶內介面（前面板埠）。
2. 用於管理流量的管理介面(mgmt0)。

3. 控制檯使用的控制和監控處理器(CMP)介面。

4. 交換式乙太網路輸出頻段(EOBC)，用於控制Supervisor模組的線卡並交換狀態訊息。

只有通過帶內介面傳送的流量會受到CoPP的制約，因為這是通過線卡上的轉發引擎(FE)到達Supervisor模組的唯一流量。CoPP的Nexus 7000系列交換機實施僅基於硬體，這意味著Supervisor模組不會在軟體中執行CoPP。CoPP功能（管制）在每個FE上獨立實施。為CoPP策略對映配置各種速率時，必須考慮系統中的線卡數量。

Supervisor接收的總流量是N倍X，其中N是Nexus 7000系統上的FE數，X是特定類允許的速率。配置的管制器值按每個FE應用，容易命中CPU的聚合流量是所有FE上一致和傳輸的流量的總和。換句話說，到達CPU的流量等於配置的符合率乘以FE的數量。

- N7K-M148GT-11/L LC有1 FE
- N7K-M148GS-11/L LC有1 FE
- N7K-M132XP-12/L LC有1 FE
- N7K-M108X2-12L LC有2個FE
- N7K-F248XP-15 LC有12 FE(SOC)
- N7K-M235XP-23L LC有2個FE
- N7K-M206FQ-23L LC有2個FE
- N7K-M202CF-23L LC有2個FE

CoPP配置僅在預設虛擬裝置環境(VDC)中實施；但是，CoPP策略適用於所有VDC。所有線卡都應用相同的全域性策略。如果相同FE的埠屬於不同的VDC（M1系列或M2系列LC），則CoPP在VDC之間應用資源共用。 例如，一個FE的埠（即使在不同的VDC中）會根據CoPP的相同閾值計數。

如果同一FE在不同的VDC之間共用，並且給定類別的控制平面流量超過閾值，這將影響同一FE上的所有VDC。如果可能，建議每個VDC專用一個FE，以便隔離CoPP實施。

當交換機首次啟動時，必須對預設策略進行程式設計以保護**控制平面**。CoPP提供預設策略，這些策略作為初始啟動序列**的一部分**應用於控制平面。

為什麼在Nexus 7000系列交換機上使用CoPP

Nexus 7000系列交換機部署為聚合或核心交換機。因此，它是網路的耳朵和大腦。處理網路中的最大負載。它必須處理頻繁和突發請求。一些請求包括：

- **生成樹橋接通訊協定資料單元(BPDU)處**理 — 預設為每兩秒一次。
- **第一躍點備**援 — 這包括熱待命路由器通訊協定(HSRP)、虛擬路由器備援通訊協定(VRRP)和閘道負載平衡通訊協定(GLBP) — 預設值每三秒一次。
- **地址解析** — 包括地址解析協定/鄰居發現(ARP/ND)、轉發資訊庫(FIB)收集 — 每台主機(例如網路介面控制器(NIC)分組)每秒最多一個請求。
- **動態主機控制協定(DHCP**)- DHCP請求，中繼 — 每台主機每秒最多一個請求。
- **第3**層(L3)的路由協定。

- **資料中心**互連 — 重疊傳輸虛擬化(OTV)、多重協定標籤交換(MPLS)和虛擬私人LAN服務(VPLS)。

CoPP對於保護CPU免受伺服器配置錯誤或潛在的DoS攻擊至關重要，這些攻擊使CPU具有足夠的週期來處理關鍵控制平面消息。

Nexus 7000系列交換機上的控制平面處理

Nexus 7000系列交換機採用分散式控制平面方法。它在每個I/O模組上都有一個多核，在Supervisor模組上還有一個用於交換機控制平面的多核。它將大量任務解除安裝到I/O模組CPU，用於訪問控制清單(ACL)和FIB程式設計。它根據線卡的數量擴展控制平面容量。這避免了管理引擎CPU瓶頸，這在集中式方法中可見。硬體速率限制器和基於硬體的CoPP可保護控制平面免受惡意活動的影響。

CoPP最佳實踐策略

CoPP最佳實踐策略(BPP)是在Cisco NX-OS版本5.2中引入的。**show running-config**命令輸出不顯示CoPP BPP的內容。**show run all** 命令顯示CoPP BPP的內容。

```
-----------------------------------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為使用者提供了四個預設策略選項：

- 嚴格
- 中等
- 寬大
- 密集(6.0(1)版中引入)

如果未選擇任何選項或跳過設定，則應用嚴格管制。所有這些選項使用相同的類對映和類，但用於策略控制的承諾資訊速率(CIR)和突發計數(BC)值不同。在低於5.2.1的Cisco NX-OS版本中，使用**setup**命令更改選項。Cisco NX-OS版本5.2.1對CoPP BPP進行了增強，因此無需使用**setup**命令即可更改選項；使用**copp profile**命令。

```
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
```

使用**show copp profile <profile-type>**命令檢視預設CoPP BPP配置。使用**show copp status**命令驗證CoPP策略已正確應用。

```
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
```

要檢視兩個CoPP BPP之間的差異，請使用**show copp diff profile <profile-type 1> profile <profile-type 2>** 命令：

```
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----------------------------------------
```

如何自定義CoPP策略

使用者可以建立自定義CoPP策略。克隆預設CoPP BPP，並將其連線到**控制平面介面**，因為CoPP BPP是只讀的。

```
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.
```

copp copy profile <profile-type> <prefix> [suffix]命令建立CoPP BPP的克隆。此指令用於修改預設設定。**copp copy profile**命令是**exec mode**命令。使用者可以選擇訪問清單、類對映和策略對映名稱的字首或字尾。例如，**copp-system-p-policy-strict**更改為**[prefix]copp-policy-strict[suffix]**。克隆的配置被視為使用者配置，並包含在**show run**輸出中。

```
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#
```

可以使用以下命令來標籤超出和違反指定允許資訊速率(PIR)的流量：

```
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)#
```

將自定義CoPP策略應用於全域性介面**控制平面**。使用**show copp status**命令以驗證CoPP策略是否已正確應用。

```
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
```

自定義CoPP策略案例研究

本節介紹客戶需要多個監控裝置才能頻繁ping本地介面的真實示例。當客戶想要修改CoPP策略以達成以下目的時，在此場景中遇到困難：

- 增加CIR，以便這些特定地址可以ping本地裝置而不會違反策略。
- 允許其他IP地址保持對本地裝置執行ping的能力，但出於故障排除目的，CIR較低。

解決方案如下面的示例所示，該示例使用單獨的類對映建立自定義策略。單獨的類對映包含監控裝置的指定IP地址，類對映具有更高的CIR。這還保留了原始類對映*監控*，它以較低的CIR捕獲所有其他IP地址的ICMP流量。

```
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
F340.13.19-Nexus7000-1(config)# copp copy profile strict prefix TAC_CHANGE
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# ip access-list TAC_CHANGE-copp-acl-specific-icmp
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo-reply
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# exit
F340.13.19-Nexus7000-1(config)# sho ip access-lists TAC_CHANGE-copp-acl-specific-
icmp IP access list TAC_CHANGE-copp-acl-specific-icmp
10 permit icmp 1.1.1.1/32 2.2.2.2/32 echo
20 permit icmp 1.1.1.1/32 2.2.2.2/32 echo-reply
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# class-map type control-plane match-any
TAC_CHANGE-copp-class-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)# match access-group name TAC_CHANGE-copp
-acl-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)#exit
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#policy-map type control-plane TAC_CHANGE-copp-
policy-strict
F340.13.19-Nexus7000-1(config-pmap)# class TAC_CHANGE-copp-class-specific-icmp
insert-before
TAC_CHANGE-copp-class-monitoring
F340.13.19-Nexus7000-1(config-pmap-c)# set cos 7
F340.13.19-Nexus7000-1(config-pmap-c)# police cir 5000 kbps bc 250 ms conform transmit
violate drop
F340.13.19-Nexus7000-1(config-pmap-c)# exit
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)# exit
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# control-plane
F340.13.19-Nexus7000-1(config-cp)# service-policy input TAC_CHANGE-copp-policy-strict
F340.13.19-Nexus7000-1(config-cp)# end
F340.13.19-Nexus7000-1#
```

```
F340.13.19-Nexus7000-1# sho policy-map interface control-plane
Control Plane
service-policy input TAC_CHANGE-copp-policy-strict
<abbreviated output>
class-map TAC_CHANGE-copp-class-specific-icmp (match-any)
match access-group name TAC_CHANGE-copp-acl-specific-icmp
set cos 7
police cir 5000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/secclass-map TAC_CHANGE-copp-class-monitoring (match-any)
match access-group name TAC_CHANGE-copp-acl-icmp
match access-group name TAC_CHANGE-copp-acl-icmp6
match access-group name TAC_CHANGE-copp-acl-mpls-oam
match access-group name TAC_CHANGE-copp-acl-traceroute
match access-group name TAC_CHANGE-copp-acl-http-response
match access-group name TAC_CHANGE-copp-acl-smtp-response
match access-group name TAC_CHANGE-copp-acl-http6-response
match access-group name TAC_CHANGE-copp-acl-smtp6-response
set cos 1
police cir 130 kbps bc 1000 ms
conform action: transmit
violate action: drop
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
<abbreviated output>
```

CoPP資料結構

CoPP BPP資料結構構造為：

- **ACL配置**:IP ACL和MAC ACL。
- **分類器配置**:類對映匹配IP ACL或MAC ACL。

- **管制器配**置：設定CIR、BC、符合操作和違反操作。監察器具有兩種速率（CIR和BC）和兩種顏色（符合和違反）。

```
mac access-list copp-system-p-acl-mac-fabricpath-isis
permit any 0180.c200.0015 0000.0000.0000
permit any 0180.c200.0014 0000.0000.0000

ip access-list copp-system-p-acl-bgp
permit tcp any gt 1024 any eq bgp
permit tcp any eq bgp any gt 1024

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-pim
<snip>
match access-group name copp-system-p-acl-mac-fabricpath-isis
policy-map type control-plane copp-system-p-policy-dense
class copp-system-p-class-critical
set cos 7
police cir 5000 kbps bc 250 ms conform transmit violate drop
```

CoPP比例因子

Cisco NX-OS版本6.0中引入的縮放因子配置用於縮放特定線卡所應用CoPP策略的管制器速率。這會增加或減少特定線卡的監察器速率，但不會改變目前的CoPP策略。更改立即生效，無需重新應用CoPP策略。

```
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
```

CoPP監控和管理

在Cisco NX-OS版本5.1中，可以根據CoPP類名稱配置丟棄閾值，以便在超出閾值時觸發系統日誌消息。命令是**logging drop threshold <dropped bytes count> level <logging level>**。

```
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
```

以下是系統日誌消息的示例：

```
%COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class:
copp-system-class-critical,
check show policy-map interface control-plane for more info.
```

CoPP計數器

CoPP支援與任何其他介面相同的QoS統計資訊。它顯示構成每個支援CoPP的I/O模組的服務策略的類的統計資訊。使用**show policy-map interface control-plane**命令檢視CoPP的統計資訊。

附註：所有類別都應根據遭到破壞的資料包進行監控。

```
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
```

若要獲取所有類對映和I/O模組的已一致和違規計數器的聚合檢視，請使用**show policy-map interface control-plane | i "class|conform|violated"**命令。

```
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
```

應監控**class copp-class-l2-default**和**class-default**，以確保即使對於一致計數器也沒有出現大幅增加。理想情況下，這兩個類必須具有一致計數器的低值，並且至少沒有違反計數器的增加。

ACL計數器

CoPP類對映中使用的IP ACL或MAC ACL不支援**statistics per-entry**命令，且應用於CoPP IP ACL或MAC ACL時不起作用。（CLI分析器不執行CLI檢查）。 若要檢視I/O模組上的CoPP MAC ACL或IP ACL命中，請使用**show system internal access-list input entries detail**命令。

以下是範例：

```
!! 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]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [30042]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [29975]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8965]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8935]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [58233]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [27689]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

CoPP配置最佳實踐

以下是CoPP配置的最佳實踐建議：

- 預設使用嚴格CoPP模式。
- 建議當機箱完全裝載F2系列模組或比任何其他I/O模組裝載F2系列模組更多時，使用密集型CoPP配置檔案。
- 建議不要禁用CoPP。根據需要調整預設CoPP。
- 監控意外丟棄，並根據預期流量新增或修改預設CoPP策略。
- 根據機箱中的FE數量，可以增加或減少CoPP的CIR和BC設定。這還取決於網路上裝置的角色、運行的協定等。

- 由於資料中心中的流量模式**不斷變**化，因此對CoPP的自定義是一個持續的過程。
- CoPP和VDC:同一FE的所有埠應屬於同一VDC，這對於F2系列LC來說很容易，但對於一個M2系列或M108 LC來說則不是那麼容易。這是因為，如果相同FE的埠屬於不同的VDC（M1系列或M2系列LC），則在VDC之間共用CoPP資源。 一個FE的埠（即使在不同的VDC中）會根據CoPP的相同閾值計數。
- 當機箱同時裝有F2系列和M系列模組時，建議使用比例因子配置。

CoPP監控最佳實踐

以下是CoPP監控的最佳實踐建議：

- 為CoPP（Cisco NX-OS版本5.1）配置系統日誌消息閾值，以監控CoPP實施的丟包。
- 如果流量類中的丟棄超過使用者配置的閾值，將生成系統日誌消息。
- 可以使用**logging drop threshold <packet-count> level <level>**命令在每個流量類內自定義日誌記錄閾值和級別。
- 由於不支援CoPP MAC ACL或IP ACL的「每條目的統計資訊」選項，請使用**show system internal access-list input entries det**命令監控訪問控制條目(ACE)命中。
- 應監控**class copp-class-l2-default和class-default**命令，以確保即使對於一致的計數器，也不會出現高增長。
- 所有類別都應根據遭到破壞的資料包進行監控。
- 由於**copp-class-critical**至關重要，但具有**violate drop**策略，因此最好監控已一致資料包的速率，以便在類接近開始發生違規時接收早期指示。如果違規計數器增加此類，則不一定表示紅色警報。相反、這意味著必須在短期內調查這種情況。
- 在每次Cisco NX-OS代碼升級後或至少每次主要Cisco NX-OS代碼升級後使用**copp profile strict**命令；如果CoPP修改之前已經完成，則必須重新應用。

結論

- CoPP是一種基於硬體的功能，可保護Supervisor免受DoS攻擊。
- M1、F2和M2系列LC支援CoPP。F1系列LC不支援CoPP。
- CoPP配置類似於MQC（模組化QoS CLI）。
- CoPP配置和監控僅在預設VDC中執行。
- 預設CoPP BPP可以與嚴格、中等、寬度和密集選項一起使用。

- 將CoPP BPP克隆到自定義CoPP規則，以便匹配特定網路要求。
- 使用**show policy-map interface control-plane**命令顯示CoPP計數器（按照每個類對映的位元組數一致和違規）。
- Supervisor模組的CPU接收的流量等於FE的總數乘以允許的速率。
- 嘗試避免一個FE的共用埠跨不同的VDC。
- 遵循CoPP最佳實踐，以成功實施和監控功能。

不支援的功能

不支援以下功能：

- 分散式聚合管制。
- 微流管制。
- 出口異常管制。
- 對來自dot1q通道連線埠(QinQ)的BPDU的CoPP支援：Cisco Discovery Protocol(CDP)、DOT1x、生成樹協定(STP)和VLAN中繼線協定(VTP)。