驗證Nexus平台上的控制平面策略違規

目錄

簡介

本檔案將詳細介紹Cisco Nexus交換器上的控制平面管制(CoPP)及其對非預設類別違規的相關影響。

必要條件

思科建議您瞭解有關控制階段管制(CoPP)、其准則和限制、一般組態以及服務品質(QoS)管制(CIR)功能的基本資訊。有關此功能的詳細資訊，請參閱適用的文檔：

- Cisco Nexus 9000系列NX-OS安全配置指南10.2(x)版
- Nexus 7000系列交換機上的CoPP
- Cisco Nexus 9000系列NX-OS服務品質配置指南，版本10.2(x)

需求

本文件沒有特定需求。

採用元件

本檔案所述內容不限於特定軟體和硬體需求。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

通過重定向訪問控制清單(ACL)，控制平面流量被重定向到管理引擎模組。重定向訪問控制清單(ACL)被程式設計為對經過硬體速率限制器和CoPP兩個保護層的匹配流量進行推送。如果對Supervisor模組進行任何中斷或攻擊，如果不加以檢查，可能會導致嚴重的網路故障；因此CoPP作為一種保護機制存在。如果在控制平面級別存在不穩定性，請務必檢查CoPP，因為由環路或泛洪建立的異常流量模式，或者流氓裝置可能會對主管徵稅並阻止其處理合法流量。此類攻擊可能無意中由流氓裝置實施，也可能由攻擊者惡意實施，通常涉及目的地為Supervisor模組或CPU的高流量率。

控制計畫管制(CoPP)是一項功能，可對透過頻內（前面板）連線埠接收的所有封包進行分類和管制，這些封包目的地為路由器位址，或是需要任何主管人員參與。此功能允許將策略對映應用於控制平面。此策略對映類似於正常的服務品質(QoS)策略，應用於從非管理埠進入交換機的所有流量。通過策略保護管理引擎模組允許交換機通過丟棄資料包來緩解超出每個類別的承諾輸入速率(CIR)的流量泛洪，以防止交換機被淹沒，從而影響效能。

連續監控CoPP計數器並證明其合理性非常重要，這就是本文的目的。CoPP違規，如果保持未選中狀態，可以阻止控制平面在相關受影響類上處理真正的流量。CoPP配置是一個流動且持續的過程，必須響應網路和基礎設施要求。CoPP有三種預設系統策略。預設情況下，思科建議使用默 strict 認策略作為初始起點，並用作本文檔的基礎。

CoPP僅適用於通過前面板埠接收的帶內流量。帶外管理埠(mgmt0)不受CoPP制約。Cisco NX-OS裝置硬體在轉發引擎的基礎上執行CoPP。因此，請選擇速率，以使聚合流量不會壓垮管理引擎模組。這對行尾/模組化交換機尤為重要，因為CIR適用於所有模組的CPU繫結流量的聚合流量。

適用硬體

本文檔中涉及的元件適用於所有Cisco Nexus資料中心交換機。

控制平面策略解釋

本文檔的重點是解決在Nexus交換機上出現的最常見和最關鍵的非預設類違規。

標準CoPP預設配置檔案

要瞭解如何解釋CoPP，首先必須驗證以確保應用了配置檔案，並瞭解是否對交換機應用了預設配置檔案或自定義配置檔案。

注意：作為最佳實踐，所有Nexus交換機都必須啟用CoPP。如果未啟用此功能，則可能會導致所有控制平面流量不穩定，因為不同的平台可以限制與Supervisor(SUP)繫結的流量。例如，如果在Nexus 9000上未啟用CoPP，則目的地為SUP的流量速率限製為50 pps，因此交換機幾乎無法運行。CoPP被認為是Nexus 3000和Nexus 9000平台的一項要求。

如果CoPP未啟用，則可以使用命令或在交換機上重新啟用或配置 **setup** 它，也可以應用配置選項：下的一個標準預設策略 copp profile [dense|lenient|moderate|strict]。

未受保護的裝置不會正確地將流量分類並劃分為多個類別，因此特定功能或協定的任何拒絕服務行為都不會限制在該範圍內，並且會影響整個控制平面。

注意:CoPP策略通過三重內容可定址儲存器(TCAM)分類重定向實施，可以直接在或下 **show system internal access-list input statistics module X | b CoPP** 看 **show hardware access-list input entries detail**到。

N9K1# show copp status Last Config Operation: None Last Config Operation Timestamp: None Last Config Operation Status: None Policy-map attached t

控制階段策略類

CoPP根據對應於IP或MAC ACL的匹配項對流量進行分類，因此，瞭解哪個流量分類在哪個類別下非常重要。

與平台相關的類可能有所不同。因此，瞭解如何驗證類非常重要。

例如，在Nexus 9000架頂式(TOR)上：

```
N9K1# show policy-map interface control-plane
Control Plane

Service-policy input: copp-system-p-policy-strict
...
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
```

5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
...

在本例中，類別對映包含與路由協定(例如邊界網關協定(BGP)、開放最短路徑優先(OSPF)、增強型內部網關路由器協定(EIGRP))相關的流 copp-system-p-class-critical 量，並包含其他協定（例如vPC）。

IP或MAC ACL的名稱約定大多對所涉及的協定或功能進行解釋，字首為 copp-system-p-acl-[protocol|feature]前。

要檢視特定類，可以在**show**命令運行時直接指定該類。舉例來說：

N9K-4# show policy-map interface control-plane class copp-system-p-class-management
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
module 1 :
transmitted 0 bytes;
5-minute offered rate 0 bytes/sec
conformed 0 peak-rate bytes/sec

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

雖然CoPP預設配置檔案通常作為預設配置的一部分隱藏，但您可以看到以下配 **show running-conf copp all**置：

<#root>

N9K1# show running-config copp all

!Command: show running-config copp all
!Running configuration last done at: Tue Apr 26 16:34:10 2022
!Time: Sun May 1 16:41:55 2022

version 10.2(1) Bios:version 05.45
control-plane
scale-factor 1.00 module 1
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-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
(snip)
...
```

類別對映(copp-system-p-class-critical以前看到)引用多個呼叫系統ACL的match語句（預設情況下是隱藏的），並引用匹配的分類。例如，對於BGP:

<#root>

N9K1# show running-config aclmgr all | b

copp-system-p-acl-bgp

```
ip access-list
```

copp-system-p-acl-bgp

```
10 permit tcp any gt 1023 any eq bgp
20 permit tcp any eq bgp any gt 1023
(snip)
```

這表示任何BGP流量都與此類匹配，並且與同一 copp-system-p-class-critical類上的所有其它協定一起被分類到。

Nexus 7000使用與Nexus 9000非常類似的CoPP功能結構：

```
N77-A-Admin# show policy-map interface control-plane
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
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
```

必須注意的是，在Nexus 7000上，由於這些是模組化交換機，您可以看到按模組劃分的類；但是，CIR應用於所有模組的聚合，而CoPP應用於整個機箱。CoPP驗證和輸出只能從預設或管理虛擬裝置環境(VDC)中看到。

如果發現控制平面問題，則在Nexus 7000上驗證CoPP特別重要，因為如果過多的CPU流量導致CoPP違規，VDC上的不穩定可能會影響其他VDC的穩定性。

在Nexus 5600上，類會有所不同。因此，對於BGP，它是其自己的單獨類：

N5K# show policy-map interface control-plane
Control Plane
(snip)
class-map copp-system-class-bgp (match-any)
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
(snip)

在Nexus 3100上，有3個路由協定類，因此要驗證BGP屬於哪一個類，請交叉引用所引用的4個CoPP ACL:
EIGRP在Nexus 3100上由自己的類處理。

<#root>

N3K-C3172# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy

class-map copp-s-routingProto2 (match-any)
match access-group name copp-system-acl-routingproto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-v6routingProto2 (match-any)
match access-group name copp-system-acl-v6routingProto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-eigrp (match-any)
match access-group name copp-system-acl-eigrp
match access-group name copp-system-acl-eigrp6
police pps 200
OutPackets 0
DropPackets 0
class-map copp-s-routingProto1 (match-any)
match access-group name

copp-system-acl-routingproto1

match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 0
DropPackets 0

```
N3K-C3172# show running-config aclmgr

!Command: show running-config aclmgr
!No configuration change since last restart
!Time: Sun May 1 18:14:16 2022

version 9.3(9) Bios:version 5.3.1
ip access-list copp-system-acl-eigrp
10 permit eigrp any 224.0.0.10/32
ipv6 access-list copp-system-acl-eigrp6
10 permit eigrp any ff02::a/128
ip access-list
```

copp-system-acl-routingproto1

10 permit tcp any gt 1024 any eq bgp

20 permit tcp any eq bgp any gt 1024

```
30 permit udp any 224.0.0.0/24 eq rip
40 permit tcp any gt 1024 any eq 639
50 permit tcp any eq 639 any gt 1024
70 permit ospf any any
80 permit ospf any 224.0.0.5/32
90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
10 permit udp any 224.0.0.0/24 eq 1985
20 permit 112 any 224.0.0.0/24
ipv6 access-list copp-system-acl-v6routingProto2
10 permit udp any ff02::66/128 eq 2029
20 permit udp any ff02::fb/128 eq 5353
30 permit 112 any ff02::12/128
ipv6 access-list copp-system-acl-v6routingproto1
10 permit 89 any ff02::5/128
20 permit 89 any ff02::6/128
30 permit udp any ff02::9/128 eq 521
```

在這種情況下，BGP會與ACL相 copp-system-acl-routingproto1匹配，因此CoPP類BGP屬於 copp-s-routingProto1is。

控制平面策略統計資料和計數器

CoPP支援QoS統計資訊以跟蹤每個模組中確認或違反特定類的承諾輸入速率(CIR)的流量聚合計數器。

每個類對映根據與CPU繫結的類對CPU流量進行分類，並為屬於該分類的所有資料包附加CIR。例如，與BGP流量相關的類用作參考：

在Nexus 9000架頂式(TOR)上，可 copp-system-p-class-critical以：

class-map copp-system-p-class-critical (match-any)
match access-group name

copp-system-p-acl-bgp

```
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

在class-map部分的match語句之後，您會看到與該類中的所有流量相關的操作。分類在內的所有流量都使用服務類copp-system-p-class-critical 別(CoS)為7來設定，這是最高優先順序的流量，此類別使用36000 kbps的CIR和1280000位元組的承諾突發速率來進行管制。

符合此策略的流量將轉發到SUP進行處理並丟棄任何違規。

<#root>

set cos 7

police cir 36000 kbps , bc 1280000 bytes

下一節包含與具有單個模組的架頂式(TOR)交換機模組相關的統計資訊，模組1是指交換機。

module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec

在輸出中看到的統計資訊是歷史的，因此這樣可以在命令運行時提供當前統計資訊的快照。

此處有兩個部分要解釋：傳輸部分和丟棄部分：
所傳輸的資料點跟蹤所傳輸的所有符合策略的資料包。本節很重要，因為它提供了對Supervisor處理的流量型別的深入分析。

5分鐘的offered rate值可讓您深入瞭解當前速率。
一致的峰值速率和日期，提供策略內仍保持一致的每秒最高峰值速率的快照，以及發生該快照的時間。
如果出現新的峰值，則會替換此值和日期。

統計資訊最重要的部分是丟棄的資料點。與傳輸的統計資訊一樣， dropped部分會跟蹤由於違反管制速率而丟棄的累積位元組。 它還提供過去5分鐘的違規速率、違規的峰值，如果有峰值，則提供該峰值違規的時間戳。再一次，如果出現新的峰值，就會取代這個值和日期。在其他平台上，輸出各不相同，但邏輯非常相似。

Nexus 7000使用相同的結構，驗證也相同，儘管某些類在引用的ACL上略有不同：

<#root>

class-map

copp-system-p-class-critical

(match-any)
match access-group name

copp-system-p-acl-bgp

match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert

set cos 7

police cir 36000 kbps bc 250 ms

conform action: transmit

violate action: drop

```
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
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
```

在Nexus 5600上：

<#root>

class-map copp-system-class-bgp

(match-any)

match protocol bgp

police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;

雖然它不提供有關速率或峰值的資訊，但它仍提供已一致和違規的聚合位元組。

在Nexus 3100上，控制平面輸出顯示OutPackets和DropPackets。

class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 8732060
DropPackets 0

OutPackets指格式化的資料包，而DropPackets指違反CIR的行為。在此情況中，您不會在關聯的類上看到任何丟棄。

在Nexus 3500上，輸出顯示硬體和軟體的匹配資料包：

```
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
police pps 900
HW Matched Packets 471425
SW Matched Packets 471425
```

HW匹配資料包是指由ACL在HW中匹配的資料包。與SW匹配的資料包符合策略。與HW和SW匹配的資料包之間的任何差異都意味著違規。

在這種情況下，由於值相符，路由通訊協定–1類別封包（包括BGP）上沒有看到捨棄。

檢查活動丟棄違規

由於控制平面策略統計資訊是歷史性的，因此確定活動違規是否增加非常重要。執行此任務的標準方法是比較兩個完整輸出並驗證所有差異。

此任務可以手動執行，或者Nexus交換機提供差異工具，以幫助比較輸出。

雖然可以比較整個輸出，但是由於焦點僅放在丟棄的統計資訊上，因此不需要進行比較。因此，可以過濾CoPP輸出以只關注違規。

命令如下： show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y

---

註：必須運行兩次命令，才能將當前輸出與上一輸出進行比較。

```
N9K-3# show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y
    class-map copp-system-p-class-l3uc-data (match-any)             class-map copp-system-p-class-l3uc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-critical (match-any)              class-map copp-system-p-class-critical (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-important (match-any)             class-map copp-system-p-class-important (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-openflow (match-any)              class-map copp-system-p-class-openflow (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-router (match-any       class-map copp-system-p-class-multicast-router (match-any
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-host (match-any)        class-map copp-system-p-class-multicast-host (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-l3mc-data (match-any)             class-map copp-system-p-class-l3mc-data (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal (match-any)                class-map copp-system-p-class-normal (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-ndp (match-any)                   class-map copp-system-p-class-ndp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp (match-any)           class-map copp-system-p-class-normal-dhcp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp-relay-response        class-map copp-system-p-class-normal-dhcp-relay-response
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
        violated 0 peak-rate byte/sec                                   violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-igmp (match-any)           class-map copp-system-p-class-normal-igmp (match-any)
      module 1 :                                                      module 1 :
        dropped 0 bytes;                                                dropped 0 bytes;
```

使用上面的命令可以檢視兩個類之間的增量並查詢違規增加。

注意：由於CoPP統計資訊是歷史性的，因此另一項建議是在運行命令後清除統計資訊，以驗證是否存在活動增加。要清除CoPP統計資訊，請運行命令： **clear copp statistics**。

CoPP丟棄的型別

CoPP是一種簡單的策略結構，因為任何違反CIR的CPU繫結流量都會被丟棄。然而，其影響因液滴的型別而大相逕庭。

雖然邏輯是相同的，但丟棄目的地為 copp-system-p-class-critical.

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes

與丟棄目的地為類對映的流量相 copp-system-p-class-monitoring比。

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes

第一種協定主要處理路由協定，第二種協定處理優先順序和CIR最低的網際網路控制消息協定(ICMP)。CIR的差值為百倍。因此，瞭解類別、影響、常規檢查/驗證以及建議非常重要。

CoPP類

類監控 — copp-system-p-class-monitoring

此類包括適用於IPv4和IPv6的ICMP，以及定向到相關交換機的流量的traceroute。

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes

影響

在出現資料包丟失或延遲故障時，通常的誤解是通過其帶內埠（受CoPP速率限制）對交換機執行ping。由於CoPP嚴格控制ICMP，即使存在低流量或擁塞，如果帶內介面違反CIR，也可以通過ping直接看到資料包丟失。

例如，對路由埠上的直連介面執行ping操作時（資料包負載為500），可以定期看到丟包情況。

<#root>

N9K-3# ping 192.168.1.1 count 1000 packet-size 500
...
--- 192.168.1.1 ping statistics ---
1000 packets transmitted, 995 packets received,

0.50% packet loss

round-trip min/avg/max = 0.597/0.693/2.056 ms

在ICMP封包目的地的Nexus上，您會看到CoPP已將其捨棄，因為系統偵測到違規行為且已保護CPU:

<#root>

N9K-4# show policy-map interface control-plane class copp-system-p-class-monitoring
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
module 1 :
transmitted 750902 bytes;
5-minute offered rate 13606 bytes/sec
conformed 13606 peak-rate bytes/sec
at Sun May 01 22:49:24 2022

dropped 2950 bytes;

5-min violate rate 53 byte/sec

violated 53 peak-rate byte/sec at Sun May 01 22:49:24 2022

若要排解延遲或封包遺失的疑難問題，建議使用資料平面透過交換器可連線的主機，而不是目的地為交換器本身（控制平面流量）。資料平面流量在硬體級別進行轉發/路由，而不需要SUP干預，因此不受CoPP監管，並且通常不會遇到丟包情況。

行動

- 透過資料層在交換器上傳送ping，而不是傳送至交換器，以驗證封包遺失的誤報結果。
- 限制主動使用ICMP的網路監控系統(NMS)或工具，以避免通過類的承諾輸入速率突發流量。請記住，CoPP適用於屬於類的所有聚合流量。

班級管理 — copp-system-p-class-management

如此處所示，此類包含不同的管理通訊協定，可用於通訊(SSH、Telnet)、傳輸(SCP、FTP、HTTP、SFTP、TFTP)、時鐘(NTP)、AAA(Radius/TACACS)和監控(SNMP)，以進行IPv4和IPv6通訊。

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh

match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes

影響

與該類關聯的最常見行為或丟棄包括：

- 通過SSH/Telnet連線時感覺到CLI緩慢。如果類上有活動的丟包，則通訊會話可能很慢，並且會發生丟包。
- 使用交換器上的FTP、SCP、SFTP、TFTP通訊協定傳輸檔案。最常見的行為是嘗試通過帶內管理埠傳輸系統/啟動引導映像。這會導致較高的傳輸時間和關閉/終止的傳輸會話（由類的聚合頻寬決定）。
- NTP同步問題，此類也很重要，因為它可以緩解非法NTP代理或攻擊。
- AAA Radius和TACACS服務也屬於此類別。如果認為此類受到影響，則可能影響交換機上使用者帳戶授權和身份驗證服務，這也可能導致CLI命令延遲。
- SNMP也在此類下管制。由於SNMP類而丟棄引起的最常見行為發生在NMS伺服器上，這些伺服器執行漫遊、批次收集或網路掃描。當週期性不穩定發生時，通常與NMS收集計畫相關。

行動

- 如果感覺到CLI速度慢以及此類中的丟棄情況，請使用控制檯訪問或管理帶外訪問(mgmt0)。
- 如果必須將系統映像上傳到交換機，請使用帶外管理埠(mgmt0)或使用USB埠實現最快傳輸。
- 如果NTP資料包丟失，請檢查show ntp peer-status並驗證可達性列，no drops會轉換為377。
- 如果AAA服務出現問題，請使用僅本地使用者進行故障排除，直到行為得到緩解。
- 針對SNMP問題的緩解包括不太積極的行為、目標收集或最小化網路掃描程式。檢查從scanners到CPU級別可見事件的定期時間。

L3類單播資料 — copp-system-p-class-l3uc-data

此類專門處理收集的資料包。硬體速率限制器(HWRL)也會處理此類封包。

如果線上卡中轉發傳入IP資料包時未解析下一跳的地址解析協定(ARP)請求，線卡會將資料包轉發到管理引擎模組。

Supervisor解析下一跳的MAC地址並對硬體程式設計。

class-map copp-system-p-class-l3uc-data (match-any)
match exception glean
set cos 1

這通常發生在使用靜態路由且下一跳無法到達或未解析時。

在傳送ARP請求時，軟體會在硬體中新增/32丟棄鄰接關係，以防止將資料包轉發到同一下一跳IP地址以轉發到Supervisor。解析ARP後，硬體條目將使用正確的MAC地址更新。如果在超時時間之前未解析ARP條目，則該條目將從硬體中刪除。

注意:CoPP和HWRL協同工作，確保CPU受到保護。雖然它們似乎執行類似的功能，HWRL首先發生。實施基於在ASIC上的轉發引擎上實施特定功能的位置。此串列方法允許精細度和多層保護為所有CPU繫結的資料包評級。

HWRL在模組上按例項/轉發引擎執行，並且可以使用命令進行查**show hardware rate-limiter**看。HWRL不在本技術文檔的範圍之內。

<#root>

show hardware rate-limiter

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters

Module: 1
R-L Class Config Allowed Dropped Total
+----------------+----------+--------------------+--------------------+--------------------+

L3 glean 100 0 0 0

L3 mcast loc-grp 3000 0 0 0
access-list-log 100 0 0 0
bfd 10000 0 0 0
fex 12000 0 0 0
span 50 0 0 0
sflow 40000 0 0 0
vxlan-oam 1000 0 0 0
100M-ethports 10000 0 0 0
span-egress disabled 0 0 0
dot1x 3000 0 0 0
mpls-oam 300 0 0 0
netflow 120000 0 0 0

```
ucs-mgmt 12000 0 0 0
```

影響

- 由於無法在硬體中處理資料平面流量，因此資料平面流量會作為違規流向Supervisor，從而對CPU造成壓力。

行動

- 此問題的常見解決方案是最小化清除丟棄，以確保下一跳可訪問，並通過配置命令啟用清除限制： **hardware ip glean throttle**.

在Nexus 7000 8.4(2)上，它還為M3和F4模組引入了Bloom過濾器支援，以實現聚合鄰接。請參閱：Cisco Nexus 7000系列NX-OS單播路由配置指南

檢視使用無法到達的下一跳地址的任何靜態路由配置，或使用動態路由協定動態地從RIB中刪除此類路由。

關鍵類別 — class-map copp-system-p-class-critical

此類從第3層角度引用了最關鍵的控制層協定，其中包括IPv4和IPv6的路由協定(RIP、OSPF、EIGRP、BGP)、自動RP、虛擬埠通道(vPC)以及l2pt和IS-IS。

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

影響

路由協定 copp-system-p-class-critical 傳輸不穩定性時丟棄（可能包括鄰接關係被丟棄或收斂失敗），或者更新/NLRI傳播。
此類中最常見的策略丟棄可能與網路上行為異常（由於配置錯誤或故障）或可擴充性的欺詐裝置有關。

行動

- 如果沒有檢測到異常情況（如導致上層協定連續重新收斂的流氓裝置或L2不穩定性），則可能需要自定義配置CoPP或更寬鬆的類來適應擴展。

- 請參閱CoPP配置指南，瞭解如何根據當前存在的預設配置檔案配置自定義CoPP配置檔案。
[複製CoPP最佳實踐策略]

重要類 — copp-system-p-class-important

此類與第一躍點備援通訊協定(FHRP)相關，包括HSRP、VRRP和LLDP

```
class-map copp-system-p-class-important (match-any)
match access-group name copp-system-p-acl-hsrp
match access-group name copp-system-p-acl-vrrp
match access-group name copp-system-p-acl-hsrp6
match access-group name copp-system-p-acl-vrrp6
match access-group name copp-system-p-acl-mac-lldp
set cos 6
police cir 2500 kbps , bc 1280000 bytes
```

影響

此處發現的最常見的導致丟棄的行為是第2層不穩定問題，該問題導致裝置轉換到活動狀態（拆分大腦）場景、主動計時器、配置錯誤或可擴充性。

建議：

- 確保為FHRP正確配置了組，且角色處於主用/備用或主/輔助狀態，且已正確協商，並且狀態中沒有擺動。

- 檢查L2的收斂問題或L2域的組播傳播問題。

Class L2 Unpoliced - copp-system-p-class-l2-unpoliced

L2未管制類是指作為所有上層協定的基礎的所有關鍵第2層協定，因此幾乎被視為具有最高CIR和優先順序的未管制協定。

此類可有效處理跨距樹狀目錄通訊協定(STP)、連結彙總控制通訊協定(LACP)、思科乙太網路光纖服務(CFSoE)

```
class-map copp-system-p-class-l2-unpoliced (match-any)
match access-group name copp-system-p-acl-mac-stp
```

match access-group name copp-system-p-acl-mac-lacp
match access-group name copp-system-p-acl-mac-cfsoe
match access-group name copp-system-p-acl-mac-sdp-srp
match access-group name copp-system-p-acl-mac-l2-tunnel
match access-group name copp-system-p-acl-mac-cdp-udld-vtp
set cos 7
police cir 50 mbps , bc 8192000 bytes

此類的管制CIR為50 Mbps，是所有類中最高的，突發速率吸收也最高。

影響

此類上的丟棄可能導致全域性不穩定，因為所有上層協定以及資料、控制和管理平面上的通訊都依賴於底層第2層穩定性。

STP違規問題可能導致TCN和STP收斂問題，包括STP爭議、MAC刷新、移動和學習禁用行為，這將導致可達性問題，並可能導致流量循環，從而破壞網路的穩定。

此類還引用LACP，並因此處理與0x8809關聯的所有EtherType資料包，其中包括用於維護埠通道繫結狀態的所有LACPDU。如果丟棄了LACPDU，此類上的不穩定可能導致埠通道超時。

Cisco Fabric Service over Ethernet(CSFoE)屬於此類，用於在Nexus交換機之間傳達重要的應用控制狀態，因此對穩定性至關重要。

這同樣適用於此類別中的其他通訊協定，包括CDP、UDLD和VTP。

行動

- 最常見的行為與L2乙太網不穩定有關。確保STP採用確定性方式設計，同時利用相關的功能增強功能來最大程度地減少網路中重新融合或欺詐裝置的影響。確保為未參與L2擴展的所有終端主機裝置配置了正確的STP埠型別，並將其配置為邊緣/邊緣中繼埠，以最小化TCN。
- 在適當情況下使用STP增強功能，如BPDUguard、Loopguard、BPDUfilter和RootGuard，以限制故障範圍，或網路中的配置錯誤或欺詐裝置問題。
- 請參閱：Cisco Nexus 9000 NX-OS第2層交換配置指南10.2(x)版
- 檢查可能導致MAC學習和刷新停止的MAC移動行為。請參閱：Nexus 9000 Mac移動故障排除和預防方法

類別多點傳送路由器 — class-map copp-system-p-class-multicast-router

此類是指控制平面協定無關組播(PIM)資料包，用於通過資料平面路徑中所有啟用了PIM的裝置建立和控制路由組播共用樹，包括第一跳路由器(FHR)、最後一跳路由器(LHR)、中間跳路由器(IHR)和匯聚點(RP)。分類在此類別中的封包包括來源的PIM註冊、IPv4和IPv6的接收者的PIM加入(通常為任何目的地為PIM(224.0.0.13)的流量)以及多點傳送來源探索通訊協定(MSDP)。請注意，還有幾個額外的類，這些類處理由不同類處理的組播或RP功能的特定部分。

class-map copp-system-p-class-multicast-router (match-any)
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
match access-group name copp-system-p-acl-pim6

match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
match exception mvpn
set cos 6
police cir 2600 kbps , bc 128000 bytes

影響

與此類相關的丟包的主要影響與通過PIM註冊向RP或PIM加入未正確處理而與組播源通訊的問題相關，這會導致通向組播流源或RP的共用或最短路徑樹不穩定。行為可能包括由於缺少連線而未正確填充的傳出介面清單(OIL)，或者(S， G)或(*, G)（在環境中未一致看到）。依賴MSDP進行互連的組播路由域之間也可能出現問題。

行動

- PIM控制相關問題最常見的行為是指規模問題或欺詐行為。由於UPnP上的實施而發現最常見的行為之一，這也會導致記憶體耗盡問題。這可以通過過濾器和減少流氓裝置的範圍來解決。有關如何緩解和過濾取決於裝置網路角色的組播控制資料包的詳細資訊，請參閱：在Nexus 7K/N9K上配置組播過濾 — 思科

Class Multicast Host - copp-system-p-class-multicast-host

此類是指組播偵聽器發現(MLD)，具體來說，是MLD查詢、報告、縮減和MLDv2資料包型別。MLD是主機用於請求特定組的組播資料的IPv6協定。利用通過MLD獲取的資訊，軟體會維護每個介面的多播組或通道成員清單。接收MLD資料包的裝置將所請求的組或通道所接收的組播資料傳送到已知接收器的網段之外。MLDv1從IGMPv2匯出，MLDv2從IGMPv3匯出。IGMP使用IP協定2消息型別，而MLD使用IP協定58消息型別，這是ICMPv6消息的子集。

class-map copp-system-p-class-multicast-host (match-any)
match access-group name copp-system-p-acl-mld
set cos 1
police cir 1000 kbps , bc 128000 bytes

影響

此類上的丟棄會轉換為本地鏈路IPv6組播通訊問題，這可能導致來自接收方的偵聽程式報告或對常規查詢的響應被丟棄，從而阻止發現主機要接收的組播組。這可能會影響窺探機制，而且無法透過要求流量的預期介面正確轉送流量。

行動

- 由於MLD流量在IPv6的本地鏈路級別非常重要，如果此類上出現丟包，則最常見的行為原因與擴展、L2不穩定或欺詐裝置有關。

第3類組播資料 — copp-system-p-class-l3mc-data 和第3類組播IPv6資料 — copp-system-p-class-l3mcv6-data

這些類別是指與指向SUP的組播異常重定向匹配的流量。在這種情況下，這兩個類處理兩個條件。第一個是反向路徑轉發(RPF)故障

，第二個是目的地丟失。目的地未命中是指第3層組播轉發表在硬體中查詢失敗，因此資料包被推到CPU的組播資料包。這些資料包有時用於根據資料平面流量觸發/安裝組播控制平面和新增硬體轉發表項。違反RPF的資料平面組播資料包也會與此例外匹配，並分類為違規。

```
class-map copp-system-p-class-l3mc-data (match-any)
match exception multicast rpf-failure
match exception multicast dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes

class-map copp-system-p-class-l3mcv6-data (match-any)
match exception multicast ipv6-rpf-failure
match exception multicast ipv6-dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes
```

影響

RPF失敗和目的地未命中意味著存在與流量如何流經組播路由器相關的設計或配置問題。目標缺失在建立狀態時很常見，丟棄可能導致程式設計和建立(*, G),(S， G)故障。

行動

- 在RPF出現故障的情況下，對基本單播RIB設計執行更改，或新增靜態mroute以引導流量通過特定介面。
- 請參閱由於RPF故障路由器不將組播資料包轉發到主機

IGMP類 — copp-system-p-class-igmp

此類是指所有IGMP消息，用於請求特定組的組播資料的所有版本，並由IGMP監聽功能用來維護組和相關傳出介面清單(OIL)，這些清單將流量轉發到第2層感興趣的接收器。IGMP消息在本地有意義，因為它們沒有經過第3層邊界，因為它們的生存時間(TTL)必須為1，如RFC2236(Internet組管理協定版本2)中所述。此類處理的IGMP資料包包括所有成員查詢（常規或源/組特定的），以及接收者的成員資格和離開報告。

```
class-map copp-system-p-class-normal-igmp (match-any)
match access-group name copp-system-p-acl-igmp
set cos 3
police cir 3000 kbps , bc 64000 bytes
```

影響

此類上的丟棄將轉換為源與接收方之間組播通訊的所有級別的問題，具體取決於由於違規而丟棄的IGMP消息的型別。如果來自接收者的成員身份報告丟失，則路由器不會感知對流量感興趣的裝置，因此它不會將介面/VLAN包含在其相關的傳出介面清單中。如果此裝置也是查詢器或指定路由器，則在源超出本地第2層域時，它不會觸發指向RP的相關PIM加入消息，因此它始終不會建立通過組播

樹到達接收器或RP的資料平面。如果離開報告丟失，接收方可以繼續接收不需要的流量。這也可能影響查詢器觸發的所有相關IGMP查詢以及域中組播路由器之間的通訊。

行動

- 與IGMP丟棄相關的最常見行為與L2不穩定、計時器問題或擴展有關。

Class Normal - copp-system-p-class-normalcopp-system-p-class-normal

此類是指與標準ARP流量匹配的流量，還包括與802.1X（用於基於埠的網路訪問控制）關聯的流量。這是最常見的類之一，當ARP請求、無償ARP、反向ARP資料包在整個第2層域中廣播和傳播時，會遇到衝突。請務必記住，ARP資料包不是IP資料包，這些資料包不包含L3報頭，因此決策完全取決於L2報頭的範圍。如果路由器配置了與該子網關聯的IP介面（如交換機虛擬介面[SVI]），則路由器會將ARP資料包轉發到SUP進行處理，因為這些資料包的目的地是硬體廣播地址。任何廣播風暴、第2層環路（由於STP或擺動）或網路中的假冒裝置都會導致ARP風暴，從而導致違規行為顯著增加。

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
```

影響

此類違規的影響在很大程度上取決於事件的持續時間以及交換機對環境的影響。此類丟棄意味著ARP資料包當前被丟棄，因此不會由SUP引擎處理，這會導致ARP解析不完整引起的兩個主要行為。

從終端主機的角度來看，網路中的裝置無法通過交換機解析或完成地址解析。如果此裝置充當網段的預設網關，可能會導致裝置無法解析其網關，從而無法在其L2乙太網網段(VLAN)之外路由。如果裝置可以完成本地網段上其他終端主機的ARP解析，則它們仍可以在本地網段上通訊。

從交換機的角度來看，如果風暴和違規情況普遍存在，也可能導致交換機無法完成其生成的ARP請求過程。這些請求通常針對下一跳或直連子網的解析度生成。雖然ARP應答實際上是單播的，因為它們是傳送到交換機所擁有的MAC地址，但它們仍歸入同一類，因為它們是ARP資料包。這會轉化為可達性問題，因為如果下一跳未解決，交換機無法正確處理流量；如果鄰接管理器沒有主機的條目，則可能會導致第2層報頭重寫問題。

影響還取決於觸發ARP違規的基本問題的範圍。例如，在廣播風暴中，主機和交換機繼續ARP嘗試解析鄰接關係，這可能會導致網路上的額外廣播流量，並且由於ARP資料包是第2層，因此沒有第3層生存時間(TTL)來中斷L2環路，因此它們會繼續回圈，並在整個網路中呈指數增長，直到環路斷開。

行動

- 解決可能在環境中引起ARP風暴（如STP、襟翼或欺詐裝置）的任何基礎L2不穩定性。根據需要使用任何所需的方法中斷這些環路，以開啟鏈路路徑。
-

風暴控制也可用於緩解ARP風暴。如果未啟用風暴控制，請驗證介面上的計數器統計資訊，以驗證介面上顯示的廣播流量相對於通過該介面的總流量的百分比。

- 如果沒有風暴，但環境中仍出現持續丟棄的情況，請驗證SUP流量以識別任何惡意裝置，這些裝置在網路上持續傳送ARP資料包，從而影響合法流量。

- ARP的增加量取決於網路中的主機數量和交換機在環境中的角色，ARP設計為重試、解析和刷新條目，因此預期始終會看到ARP流量。如果只看到零星的丟包，則它們可能由於網路負載而成為瞬時，且不會察覺到影響。但是，監控和瞭解網路以正確識別並區分預期和異常情況非常重要。

Class NDP - copp-system-p-acl-ndp

此類是指與IPv6鄰居發現/通告以及路由器請求和通告資料包關聯的流量，這些流量使用ICMP消息來確定鄰居的本地鏈路層地址，並且用於鄰居裝置的連通性和跟蹤。

```
class-map copp-system-p-class-ndp (match-any)
match access-group name copp-system-p-acl-ndp
set cos 6
police cir 1400 kbps , bc 32000 bytes
```

影響

此類上的違規可能會阻礙相鄰裝置之間的IPv6通訊，因為這些資料包用於促進本地鏈路上的主機和路由器之間的動態發現或鏈路層/本地資訊。此通訊中斷也可能會引起超越或通過相關本地鏈路的可達性問題。如果IPv6鄰居之間存在通訊問題，請確保此類上沒有丟包。

行動

- 檢查來自鄰居裝置的任何異常ICMP行為，尤其是與鄰居發現和/或路由器發現相關的行為。

- 確保定期消息的所有預期計時器和間隔值在整個環境中都一致並符合要求。例如，對於路由器通告消息（RA消息）。

Class Normal DHCP - copp-system-p-class-normal-dhcp

此類是指與IPv4和IPv6的本地乙太網段上的引導協定（BOOTP客戶端/伺服器）(通常稱為動態主機控制協定(DHCP)資料包)關聯的流量。這僅與通過整個發現、提供、請求和確認(DORA)資料包交換從任何bootp客戶端或發往任何BOOTP伺服器的流量通訊相關，還包括通過UDP埠546/547的DHCPv6客戶端/伺服器事務。

```
class-map copp-system-p-class-normal-dhcp (match-any)
match access-group name copp-system-p-acl-dhcp
match access-group name copp-system-p-acl-dhcp6
set cos 1
police cir 1300 kbps , bc 32000 bytes
```

影響

此類上的違規可能導致終端主機無法正確從DHCP伺服器獲取IP，從而回退到其自動私有IP地址(APIPA)範圍169.254.0.0/16。此類違規可能會發生在裝置試圖同時啟動並因此超出與類關聯的CIR的環境中。

行動

- 使用captures驗證在主機和DHCP伺服器端上是否看到整個DORA事務。如果交換器是此通訊的一部分，則還必須驗證已處理或傳送到CPU的封包，並驗證switch：和redirection：上的統 **show ip dhcp global statistics** 計資料 **show system internal access-list sup-redirect-stats module 1 | grep -i dhcp**。

類正常DHCP中繼響應 — copp-system-p-class-normal-dhcp-relay-response

此類是指與IPv4和IPv6的DHCP中繼功能關聯的流量，這些流量定向到在中繼下配置的DHCP伺服器。這僅與通過整個DORA資料包交換從任何BOOTP伺服器發起、或發往任何BOOTP客戶端的流量通訊相關，還包括通過UDP埠546/547的DHCPv6客戶端/伺服器事務。

```
class-map copp-system-p-class-normal-dhcp-relay-response (match-any)
match access-group name copp-system-p-acl-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp6-relay-response
set cos 1
police cir 1500 kbps , bc 64000 bytes
```

影響

此類違規的影響與類copp-system-p-class-normal-dhcp的違規的影響相同，因為它們都是同一事務的一部分。本課程主要介紹來自中繼代理伺服器的響應通訊。Nexus不充當DHCP伺服器，它僅用作中繼代理。

行動

- 此處應用與類普通DHCP相同的建議。由於Nexus的功能僅僅是充當中繼代理，因此在SUP上，您期望看到主機和交換機之間的整個事務充當中繼，並且交換機和伺服器進行配置。

- 確保沒有欺詐裝置，例如網路中響應作用域的意外DHCP伺服器，或者裝置陷入使用DHCP發現資料包淹沒網路的環路中。可通過命令show ip dhcp relay **show ip dhcp relay statistics** 和執行其他檢查。

NAT流類 — copp-system-p-class-nat-flow

此類是指軟體交換機NAT流流量。當建立新的動態轉換時，軟體將轉發該流，直到在硬體中程式設計該轉換，然後由CoPP管制該流，以限制當條目安裝在硬體中時流向Supervisor的流量。

```
class-map copp-system-p-class-nat-flow (match-any)
match exception nat-flow
set cos 7
```

police cir 800 kbps , bc 64000 bytes

影響

當硬體中安裝了高速率的新動態轉換和流時，通常會發生此類丟棄。其影響與被丟棄但未傳送到終端主機的軟體交換資料包有關，這可能導致丟失和重新傳輸。一旦條目安裝在硬體中，便不會再有流量被傳送到Supervisor。

行動

- 檢驗相關平台上動態NAT的准則和限制。平台上有一些已知的限制，例如3548，轉換可能需要幾秒鐘。請參閱：動態NAT的限制

類異常 — copp-system-p-class-exception

此類是指與IP選項和IP ICMP無法到達資料包關聯的異常資料包。如果目的地位址在轉送資訊庫(FIB)上不存在並導致遺漏，SUP會將ICMP無法到達的封包傳送回傳送者。已啟用IP選項的資料包也屬於此類別。有關IP選項：IP選項編號的詳細資訊，請參閱IANA文檔

```
 class-map copp-system-p-class-exception (match-any)
match exception ip option
match exception ip icmp unreachable
match exception ipv6 option
match exception ipv6 icmp unreachable
set cos 1
police cir 150 kbps , bc 32000 bytes
```

影響

此類會受到嚴格管制，此類上的捨棄並不表示失敗，而是表示了一種保護機制，以限制ICMP不可達和IP選項資料包的範圍。

行動

- 驗證對於不在FIB上的目標，是否存在發現或轉發到CPU的任何流量流。

類重定向 — copp-system-p-class-redirect

此類是指與用於時間同步的精確時間協定(PTP)關聯的流量。這包括保留範圍224.0.1.129/32的多播流量、UDP埠319/320和Ethetype 0X88F7上的單播流量。

```
class-map copp-system-p-class-redirect (match-any)
match access-group name copp-system-p-acl-ptp
match access-group name copp-system-p-acl-ptp-l2
match access-group name copp-system-p-acl-ptp-uc
set cos 1
```

police cir 280 kbps , bc 32000 bytes

影響

此類上的丟棄可能導致未正確同步或尚未建立正確層次的裝置出現問題。

行動

- 確保時鐘的穩定性，並確保其配置正確。確保PTP裝置配置為組播或單播PTP模式，而不是同時配置兩者。這也記錄在「准則和限制」中，可以將流量推至超過承諾輸入速率。
- 檢視環境中邊界時鐘和所有PTP裝置的設計和配置。確保每個平台都遵循所有准則和限制，因為這些准則和限制各不相同。

OpenFlow類 — copp-system-p-class-openflow

此類是指與OpenFlow代理操作和控制器與代理之間的相應TCP連線相關聯的流量。

class-map copp-system-p-class-openflow (match-any)
match access-group name copp-system-p-acl-openflow
set cos 5
police cir 1000 kbps , bc 32000 bytes

影響

此類上的丟棄可能導致代理出現問題，無法正確接收和處理來自控制器的指令以管理網路的轉發平面

行動

- 確保網路上或任何妨礙控制器與代理之間通訊的裝置都沒有出現重複的流量。
- 檢驗L2網路是否不穩定（STP或環路）。

排除CoPP丟棄故障

對CoPP違規進行故障排除的第一步是確定：

- 問題的影響和範圍。
- 瞭解環境中的流量以及交換機在受影響通訊中的作用。
- 確定相關類上是否存在可疑的違規，然後根據需要進行迭代。

例如，已檢測到列出的行為：

- 裝置無法與其網路之外的其他裝置通訊，但可以在本地通訊。
- 影響已隔離到VLAN外部的路由通訊，且交換機充當預設網關。
- 檢查主機表明它們無法ping通網關。檢查其ARP表後，網關條目仍保留為Incomplete。
- 具有網關解決的所有其他主機沒有通訊問題。如果檢查交換機上用作網關的CoPP，則表明存在違規行 copp-system-p-class-normal為。

<#root>

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
module 1 :
transmitted 3292445628 bytes;

dropped 522023852 bytes;

- 此外，多個命令檢查顯示丟棄數在增加。
- 這些違例可能會導致合法ARP流量被丟棄，從而導致拒絕服務行為。

必須強調的是，CoPP隔離對特定類相關流量的影響，在本例中為ARP和copp-system-p-class-normal。與其他類（例如OSPF、BGP）相關的流量不會被CoPP丟棄，因為它們完全屬於不同的類。如果不進行檢查，ARP問題可能會級聯到其他問題，這可能會影響最初依賴它的協定。例如，如果ARP快取超時，並且由於發生過度違規而沒有刷新，TCP會話（如BGP）可以終止。

- 建議執行控制平面檢查，例如Ethanalyzer、CPU-mac帶內狀態和CPU進程，以進一步隔離問題。

Ethanalyzer

由於CoPP控制的流量僅與CPU流量相關聯，因此最重要的工具之一是Ethanalyzer。此工具是Nexus的TShark實現，允許捕獲和解碼管理引擎傳送和接收的流量。它還可以使用基於不同標準的過濾器（例如協定或報頭資訊），因此成為確定CPU傳送和接收的流量的寶貴工具。

建議首先檢查Ethanalyzer工具在終端作業階段直接執行或傳送到檔案以供分析時主管所看到的ARP流量。可以定義過濾器和限制，以將捕獲聚焦到特定模式或行為。為此，請新增靈活的顯示過濾器。

一個常見的誤解是Ethanalyzer會捕獲通過交換機的所有流量。主機之間的資料平面流量由資料埠之間的硬體ASIC交換或路由，不需要CPU參與，因此通常不會被Ethanalyzer捕獲看到。若要擷取資料平面流量，建議使用其他工具，例如ELAM或SPAN。例如，要過濾ARP，請使用命令：

ethanalyzer local interface inband display-filter arp limit-captured-frames 0 autostop duration 60 > arpcpu

重要可配置欄位：

- interface inband — 是指導向到SUP的流量
- display-filter arp — 表示應用的tshark過濾器，接受大多數Wireshark過濾器
- limit-captured-frames 0 — 表示限制，0表示無限制，直到被另一個引數停止或由Ctrl+C手動停止
- autostop duration 60 — 指Ethanalyzer在60秒後停止，因此它會建立CPU上看到的60秒ARP流量的快照

Ethanalyzer輸出將重新導向至使用> arpcpu的bootflash上的檔案，以便手動處理。60秒後，捕獲完成，Ethanalyzer動態終止，檔案arpcpu位於交換機的bootflash上，然後對其進行處理以提取最大流量生成者。舉例來說：

show file bootflash:arpcpu | sort -k 3,5 | uniq -f 2 -c | sort -r -n | head lines 50

669 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:47 -> ff:ff:ff:ff:ff:ff ARP Who has 10.1.1.1? Tell 10.1.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:43 -> ff:ff:ff:ff:ff:ff ARP Who has 10.2.1.1? Tell 10.2.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:41 -> ff:ff:ff:ff:ff:ff ARP Who has 10.3.1.1? Tell 10.3.1.2

此篩選器的排序依據為：源列和目標列，然後找到唯一匹配項（但忽略日期列），對例項進行計數並新增顯示的數量，最後根據計數從上到下排序，並顯示前50個結果。

在本實驗示例中，在60秒內，從三台裝置接收了超過600個ARP資料包，這些裝置已被確定為可疑犯罪裝置。過濾器上的第一列詳細列出了在指定持續時間內，捕獲檔案中出現此事件的例項數。

瞭解Ethanalyzer工具對帶內驅動程式的作用十分重要，它實質上是與ASIC的通訊。理論上，資料包需要通過核心和資料包管理器傳遞給關聯進程本身。CoPP和HWRL在Ethanalyzer上看到流量之前採取行動。即使違規行為在增加，某些流量仍然會通過並符合警方的速率，這有助於深入瞭解流向CPU的流量。這是一個重要的區別，因為Ethanalyzer上顯示的流量不是違反CIR並被丟棄的流量。

Ethanalyzer也可以以開放方式使用，而無需指定任何顯示過濾器或捕獲過濾器來捕獲所有相關SUP流量。這可以用作隔離措施，作為故障排除方法的一部分。

有關Ethanalyzer的其他詳細資訊和用法，請參閱TechNote:

Nexus 7000上的Ethanalyzer故障排除指南

在Nexus平台上使用Ethanalyzer進行控制平面和資料平面流量分析

注意：在8.X代碼發佈之前，Nexus 7000隻能通過管理VDC執行Ethanalyzer捕獲，其中包含來自所有VDC的SUP繫結流量。特

定於VDC的Ethanalyzer以8.X代碼提供。

CPU-MAC帶內統計資訊

與CPU繫結的流量關聯的帶內統計資訊會保留帶內TX/RX CPU流量的相關統計資訊。可以使用命令：檢查這些統計資訊show hardware internal cpu-mac inband stats，該命令提供對當前速率和峰值速率統計資訊的深入分析。

```
show hardware internal cpu-mac inband stats`
================ Packet Statistics =====================
Packets received: 363598837
Bytes received: 74156192058
Packets sent: 389466025
Bytes sent: 42501379591
Rx packet rate (current/peak): 35095 / 47577 pps
Peak rx rate time: 2022-05-10 12:56:18
Tx packet rate (current/peak): 949 / 2106 pps
Peak tx rate time: 2022-05-10 12:57:00
```

作為最佳實踐，建議建立和跟蹤基線，因為由於交換機和基礎結構的作用，的輸出會顯 **show hardware internal cpu-mac inband stats** 著變化。在此實驗環境中，通常值和歷史峰值通常不大於幾百個pps，因此這是異常的。此命令 **show hardware internal cpu-mac inband events** 還可用作歷史參考，因為它包含與峰值使用量和檢測到該值的時間相關的資料。

進程CPU

Nexus交換機是基於Linux的系統，而Nexus作業系統(NXOS)利用CPU搶先排程程式、多工處理以及各自核心架構的多執行緒處理來提供對所有進程的公平訪問，因此尖峰並不總是指示問題。但是，如果出現持續的流量違規，則相關進程可能也會被大量使用，並且會作為CPU輸出下的頂級資源出現。對CPU進程拍攝多個快照，以驗證特定進程是否被大量使用 **show processes cpu sort | exclude 0.0 or show processes cpu sort | grep <process>**:。

進程CPU、帶內統計和Ethanalyzer驗證提供對主管當前處理的進程和流量的見解，並幫助隔離控制平面流量上可能串接到資料平面問題的持續不穩定性。瞭解CoPP是一種保護機制非常重要。這是反作用的，因為它只對傳送到SUP的流量起作用。它旨在通過丟棄流量速率（超過預期範圍）來維護主管的完整性。並非所有丟棄都表明存在問題或需要干預，因為它們的重要性取決於具體的CoPP類別以及基於基礎架構和網路設計的已驗證的影響。由於偶發的突發事件導致的丟棄不會轉化為影響，因為協定具有內建機制，例如keepalive和可以處理瞬態事件的重試。將焦點保持在已建立基線之外的持續事件或異常事件。請記住，CoPP必須遵守特定於環境的協定和功能，並且必須進行監控和持續迭代以根據擴展性需求隨其發展對其進行微調。如果發生丟包，請確定CoPP是否無意中或響應故障或攻擊而丟棄流量。無論發生哪種情況，都可以通過分析對環境的影響和採取適當的糾正措施，來分析情況並評估干預的必要性，而這種影響和措施可能不在交換機本身的範圍內。

其他資訊

最新平台/代碼可以通過埠映象和資料平面流量傳送到CPU執行SPAN到CPU的功能。這通常受到硬體速率限制和CoPP的嚴重速率限制。建議謹慎使用SPAN到CPU，這不在本檔案的範圍之內。

有關此功能的詳細資訊，請參閱列出的技術說明：

Nexus 9000雲擴展ASIC NX-OS SPAN到CPU過程

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。