Nexus 7000系列交换机上的CoPP

目录

简介
先决条件
要求
使用的组件
Nexus 7000系列交换机上的CoPP概述
为什么Nexus 7000系列交换机上使用CoPP
Nexus 7000系列交换机的控制平面处理
CoPP最佳实践政策
如何自定义CoPP策略
定制CoPP策略案例研究
CoPP数据结构
CoPP比例因子
CoPP监控和管理
CoPP计数器
ACL计数器
CoPP配置最佳实践
CoPP监控最佳实践
结论
不支持的功能

简介

本文档介绍在Nexus 7000系列交换机(包括F1、F2、M1和M2系列模块和线卡(LC))上使用控制平面管制(CoPP)的内容、方式和原因。 它还包括最佳实践策略以及如何自定义 CoPP 策略。

先决条件

要求

思科建议您了解Nexus操作系统CLI。

使用的组件

本文档中的信息基于带Supervisor 1模块的Nexus 7000系列交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

Nexus 7000系列交换机上的CoPP概述

CoPP对网络运行至关重要。对控制/管理平面的拒绝服务(DoS)攻击通常涉及导致CPU使用率过高的高流量。管理引擎模块花费大量时间处理数据包。

此类攻击的示例包括：

- 互联网控制消息协议(ICMP)回应请求。
- 使用ip-options集**发送的数**据包。

这可能导致：

- 丢失保持连接消息和路由协议更新。
- 填充数据包队列，导致不加区分地丢弃。
- 交互式会话速度缓慢或无响应。

攻击会压垮网络稳定性和可用性，并导致影响业务的网络中断。

CoPP是基于硬件的功能，可保护Supervisor免受DoS攻击。它控制允许数据包到达管理引擎的速率。CoPP功能的建模方式与连接到特殊接口（称为控制平面）的输入QoS**策略类似**。但是，CoPP是安全功能，不是QoS的一部分。为了保护Supervisor，CoPP将数据平面数据包与控制平面数据包（异常逻辑）分离。 它识别来自有效数据包（分类）的DoS攻击数据包。 CoPP允许对以下数据包进行分类：

- 接收数据包
- 组播数据包
- 异常数据包
- 重定向数据包
- 广播MAC +非IP数据包
- 广播MAC + IP数据包(请参阅Cisco Bug ID CSCub47533 - Packets in L2 Vlan(No SVI)命中CoPP)
- 组播MAC + IP数据包
- 路由器MAC +非IP数据包
- ARP数据包

在对数据包进行分类后，还可以标记该数据包并根据数据包的类型分配不同的优先级。可以设置Conform、Exceed和Ivolate操作（传输、丢弃、标记关闭）。如果没有监察器附加到类，则添加符合操作为drop的默认监察器。glean数据包使用default-class进行管制。支持一个速率、两个颜色和两个速率、三个颜色策略。

到达Supervisor模块上CPU的流量可通过四条路径进入：

1. 线卡发送的流量的带内接口（前面板端口）。
2. 用于管理流量的管理接口(mgmt0)。

3. 用于控制台的控制和监控处理器(CMP)接口。

4. 交换以太网带外通道(EOBC)，用于控制Supervisor模块的线卡并交换状态消息。

只有通过带内接口发送的流量受CoPP限制，因为这是通过线卡上的转发引擎(FE)到达Supervisor模块的唯一流量。CoPP的Nexus 7000系列交换机实施仅基于硬件，这意味着CoPP不由管理引擎模块在软件中执行。CoPP功能（策略）在每个FE上独立实施。当为CoPP策略映射配置了各种速率时，必须考虑系统中线卡的数量。

管理引擎接收的总流量是N次X，其中N是Nexus 7000系统上的FE数，X是特定类允许的速率。配置的监察器值基于每个FE应用，并且容易到达CPU的聚合流量是所有FE上一致和传输的流量的总和。换句话说，到达CPU的流量等于配置的符合率乘以FE的数量。

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

CoPP配置仅在默认虚拟设备环境(VDC)中实施；但是，CoPP策略适用于所有VDC。所有线卡都应用相同的全局策略。如果同一FE的端口属于不同VDC（M1系列或M2系列LC），CoPP将应用VDC之间的资源共享。 例如，一个FE的端口（即使在不同的VDC中）根据CoPP的相同阈值计数。

如果同一FE在不同VDC之间共享，且给定的控制平面流量类超过阈值，则会影响同一FE上的所有VDC。建议为每个VDC指定一个FE，以便尽可能隔离CoPP实施。

当交换机首次启动时，必须对默认策略进行编程以保护**控制平面**。CoPP提供默认策略，这些策略作为初始**启动序**列的一部分应用于控制平面。

为什么Nexus 7000系列交换机上使用CoPP

Nexus 7000系列交换机部署为聚合或核心交换机。因此，它是网络的耳朵和大脑。它处理网络中的最大负载。它必须处理频繁和突发请求。一些请求包括：

- **生成树桥接协议数据单元(BPDU)处理** — 默认值为每两秒一次。
- **第一跳冗余** — 包括热备份路由器协议(HSRP)、虚拟路由器冗余协议(VRRP)和网关负载均衡协议(GLBP) — 默认为每三秒一次。
- **地址解析** — 这包括地址解析协议/邻居发现(ARP/ND)、转发信息库(FIB)Glean — 每台主机每秒最多一个请求，例如网络接口控制器(NIC)组合。
- **动态主机控制协议(DHCP)** - DHCP请求，中继 — 每台主机每秒最多一个请求。
- **第3**层(L3)的路由协议。

- **数据中心互**联 — 重叠传输虚拟化(OTV)、多协议标签交换(MPLS)和虚拟专用局域网服务(VPLS)。

CoPP对于保护CPU免受误配置服务器或潜在DoS攻击至关重要，这使CPU有足够的周期来处理关键控制平面消息。

Nexus 7000系列交换机的控制平面处理

Nexus 7000系列交换机采用分布式控制平面方法。它在每个I/O模块上都有一个多核，在Supervisor模块上有一个用于交换机控制平面的多核。它将大量任务卸载到I/O模块CPU，以便访问控制列表(ACL)和FIB编程。它根据线卡的数量调整控制平面容量。这可避免集中式方法中出现的Supervisor CPU瓶颈。硬件速率限制器和基于硬件的CoPP可保护控制平面免受恶意或恶意活动的影响。

CoPP最佳实践政策

CoPP最佳实践策略(BPP)在Cisco NX-OS版本5.2中引入。**show running-config**命令输出不显示CoPP BPP的内容。show run **all命令**显示CoPP BPP的内容。

```
-----------------------------------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为用户提供四个默认策略选项：

- 严格
- Moderate（一般）
- 宽大
- 密集(版本6.0(1)中引入)

如果未选择任何选项或跳过设置，则应用严格管制。所有这些选项使用相同的类映射和类，但策略使用不同的承诺信息速率(CIR)和突发计数(BC)值。在5.2.1之前的Cisco NX-OS版本中，**setup**命令用于更改选项。Cisco NX-OS版本5.2.1对CoPP BPP进行了增强，以便在不使用setup命令的情况下更改**选项**;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>**命令查看默认CoPP BPP配置。使用**show copp status**命令验证CoPP策略是否已正确应用。

```
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
```

要查看两个CoPP BPP之间的差异，请使用**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----------------------------------------
```

如何自定义CoPP策略

用户可以创建自定义的CoPP策略。克隆默认CoPP BPP，并将其连接到**控制平**面接口，因为CoPP BPP是只读的。

```
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**令创建CoPP BPP的克隆。这用于修改默认配置。copp copy profile**命令**是执行模式**命令**。用户可以为访问列表、类映射和策略映射名称选择前缀或后缀。例如，**copp-system-p-policy-strict被更**改为**[prefix]copp-policy-strict[suffix]**。克隆的配置被视为用户配置，并包含在**show run输**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#
```

可以使用以下命令来标记超过并违反指定允许信息速率(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)#
```

将自定义的CoPP策略应用到全局接口控制平面。使用show copp status命令验证CoPP策略是否已正确应用。

```
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
```

定制CoPP策略案例研究

本节介绍客户需要多个监控设备才能频繁ping本地接口的真实示例。当客户要修改CoPP策略以：

- 增加CIR，以便这些特定地址能够ping通本地设备，而不违反策略。
- 允许其他IP地址保持ping本地设备的能力，但CIR较低，以便进行故障排除。

解决方案在下一个示例中显示，即使用单独的类映射创建自定义策略。单独的类映射包含监控设备的指定IP地址，且类映射具有更高的CIR。这也会保留原始类映射监控,它捕获CIR较低的所有其他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数据结构

CoPP BPP数据结构构造为：

- **ACL 配置:**IP ACL和MAC ACL。
- **分类器配置**:与IP ACL或MAC ACL匹配的类映射。
- **监察器配置**:设置CIR、BC、遵循操作和违反操作。监察器有两种速率（CIR和BC）和两种颜色（符合和违规）。

```
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中引入的缩放因子配置用于缩放特定线卡所应用CoPP策略的监察器速率。这会增加或降低特定线卡的监察器速率，但不会更改当前CoPP策略。更改会立即生效，无需重新应用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监控和管理

使用Cisco NX-OS版本5.1，可以根据CoPP类名称配置丢弃阈值，在超出阈值时触发系统日志消息。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
```

以下是系统日志消息的示例：

```
%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计数器

CoPP支持与任何其他接口相同的QoS统计信息。它显示构成每个支持CoPP的I/O模块服务策略的类的统计信息。使用**show policy-map interface control-plane**命令查看CoPP的统计信息。

> **注意**：所有类都应根据违反的数据包进行监控。

```
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
```

要获取所有类映射和I/O模块的一致和违规计数器的聚合视图，请使用**show policy-map interface control-plane | i "class|conform|iffied"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
```

应**监控copp-class-l2-default和class-default类，**以确保即使对于符合的计数器也不会出现高增长。理想情况下，这两个类对于符合的计数器必须具有低值，并且至少没有违反的计数器增加。

ACL计数器

CoPP类映射中使用的IP ACL或MAC ACL不支持**statistics per-entry**命令，并且该命令在应用于

CoPP IP ACL或MAC ACL时无效。（CLI解析器不执行CLI检查）。 要查看I/O模块上的CoPP MAC ACL或IP ACL命中，请使用**show system internal access-list input entries detail命**令。

示例如下：

```
!! 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配置最佳实践

以下是CoPP配置的最佳实践建议：

- 默认情况下使用严格CoPP模式。
- 当机箱满载F2系列模块或装载的F2系列模块比任何其他I/O模块多时，建议使用密集CoPP配置文件。
- 不建议禁用CoPP。根据需要调整默认CoPP。
- 监控意外丢弃，并根据预期流量添加或修改默认CoPP策略。
- 根据机箱中的FE数量，可以增加或减少CoPP的CIR和BC设置。这还取决于网络中设备的角色、运行的协议等。
- 由于数据中心中的流量模**式不断**变化，因此CoPP的定制是一个持续的过程。
- CoPP和VDC:同一FE的所有端口应属于同一VDC，F2系列LC比较容易，但M2系列或M108

LC不那么容易。这是因为，如果同一FE的端口属于不同VDC（M1系列或M2系列LC），则VDC之间的CoPP资源共享。 一个FE的端口（即使在不同VDC中）计数到CoPP的相同阈值。

- 当机箱同时装有F2系列和M系列模块时，建议进行比例因子配置。

CoPP监控最佳实践

以下是CoPP监控的最佳实践建议：

- 为CoPP（Cisco NX-OS版本5.1）配置系统日志消息阈值，以监控CoPP实施的丢包。
- 如果流量类内的丢弃超过用户配置的阈值，将生成系统日志消息。
- 使用logging drop threshold <packet-count> level <level>命令，可在每个流量类**别中自定义日志记录阈值和级别**。
- 由于不支持CoPP MAC ACL或IP ACL的“统计每条目”选项，请使用**show system internal access-list input entries det**命令监控访问控制条目(ACE)命中。
- 应**监控class copp-class-l2-default和class-default命令，以确保即使对于符合的计数器也不会出现高增量。**
- 所有类都应根据违反的数据包进行监控。
- 由**于copp类关键型**非常重要，但有违**反丢包策略**，因此最好监控符合的数据包的速率，以便在类接近其开始违规的时刻时收到早期指示。如果违反的计数器增加此类，则不一定表示红色警报。相反，这意味着必须在短期内调查这种情况。
- 在每次Cisco NX-OS代码升级后或至少在每次主要Cisco NX-OS代码升级后使用**copp profile strict命令；**如果之前已完成CoPP修改，则必须重新应用。

结论

- CoPP是基于硬件的功能，可保护Supervisor免受DoS攻击。
- M1、F2和M2系列LC支持CoPP。F1系列LC不支持CoPP。
- CoPP配置类似于MQC（模块化QoS CLI）。
- CoPP配置和监控仅在默认VDC中执行。
- 默认CoPP BPP可与严格、中度、宽大和密集的选项一起使用。
- 将CoPP BPP克隆到自定义CoPP规则，以匹配特定网络要求。
- CoPP计数器（符合和违反的字节单位为每个类映射）使用**show policy-map interface control-plane命令显**示。

- 管理引擎模块的CPU接收的流量等于FE总数乘以允许的速率。
- 尝试避免跨不同VDC的一个FE的共享端口。
- 遵循CoPP最佳实践以成功实施和监控功能。

不支持的功能

不支持以下功能：

- 分布式聚合策略。
- 微流策略。
- 出口异常管制。
- 对来自dot1q隧道端口(QinQ)的BPDU的CoPP支持：思科发现协议(CDP)、DOT1x、生成树协议(STP)和VLAN中继协议(VTP)。