

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[在连结7000系列交换机概述的CoPP](#)

[为什么在连结7000系列交换机的CoPP](#)

[处理在连结7000系列交换机的控制层面](#)

[CoPP最佳实践策略](#)

[如何定制CoPP策略](#)

[定制的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](#)

[监控最佳实践的CoPP](#)

[结论](#)

[不支持的功能](#)

简介

本文描述什么，和控制平面策略(CoPP)如何为什么在连结7000系列交换机使用，包括F1， F2， M1和M2系列模块与卡(LCs)。它也包括最佳实践策略，以及如何定制CoPP策略。

[先决条件](#)

[要求](#)

思科建议您有连结操作系统CLI知识。

[使用的组件](#)

本文档中的信息根据连结7000系列交换机用Supervisor 1模块。

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。

在连结7000系列交换机概述的CoPP

CoPP对网络操作至关重要。对控制/管理层面的一次服务拒绝(DoS)攻击，可以疏忽地或有恶意被犯罪，典型地介入导致CPU过度利用的高速率流量。Supervisor模块花费处理数据包的过量的时刻。

示例的这样攻击包括：

- 互联网控制消息协议(ICMP) ECHO请求。
- 与设置的ip options的发送的数据包。

这可以导致：

- keep-alive消息和路由协议更新损耗。
- 信息包队列填充，导致不加区别的丢包。
- 缓慢或无答复的交互式会话。

攻击可能淹没网络稳定性和可用性和导致事务影响网络中断。

CoPP是保护从DOS攻击的Supervisor的一个基于硬件的功能。它控制数据包允许到达Supervisor的速率。CoPP功能被模拟类似输入QoS策略附加对呼叫**控制面板**的特殊接口。然而，CoPP是QoS的而不是安全功能部分。为了保护Supervisor，CoPP从控制层面数据包(例外逻辑)分离数据层面数据包。它识别从有效信息包(分类)的DOS攻击数据包。CoPP允许这些数据包的分类：

- 接收数据包
- 组播数据包
- 例外数据包
- 重定向数据包
- 广播MAC +非IP信息包
- 广播MAC + IP信息包(请参阅Cisco Bug ID [CSCub47533](#) -在L2点击CoPP)的VLAN (没有SVI)的数据包
- Mcast MAC + IP信息包
- 路由器MAC +非IP信息包
- ARP数据包

在数据包分类后，数据包可能被标记，并且使用的分配不同的优先级根据数据包种类也。一致，超出，并且违反操作(传输、丢弃，减价)可以设置。如果策略器没有附加对类，则默认策略器被添加一致操作是丢弃。汇集数据包管辖与默认组。两种颜色的，并且两请对估计，三颜色管制支持一速率。

点击在Supervisor模块的CPU的流量能通过四个路径进来：

1. 带内接口(前面板端口)流量的由线卡发送。
2. 用于管理数据流(mgmt0)的管理接口。
3. 用于控制台的控制和监控处理器(CMP)接口。
4. 交换以太网结合信道(EoBC)控制从Supervisor模块的线卡和交换状态消息。

通过带内接口发送的仅流量是受CoPP支配，因为这是到达Supervisor模块到转发引擎的唯一的流量(FEs)在线卡。CoPP的连结7000系列交换机实施只基于硬件的，因此意味着CoPP在软件方面没有执行由Supervisor模块。CoPP功能(管制)在每个FE独立地实现。当多种速率为CoPP策略映射时配置，必须关于线卡数量在系统的采取考虑事项。

Supervisor接收的总流量是N时间x，其中N是FEs编号在连结7000系统的，并且X是为特定类允许的速率。已配置的策略器值在a应用每个FE基本类型，并且倾向的总流量点击CPU是一致的和传送的流量的总和在所有的FEs。换句话说，点击CPU的流量等于已配置的一致FEs编号乘的速率。

- N7K-M148GT-11/L LC有1个FE
- N7K-M148GS-11/L LC有1个FE
- N7K-M132XP-12/L LC有1个FE
- N7K-M108X2-12L LC有2个FE
- N7K-F248XP-15 LC有12个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配置在默认虚拟设备上下文(VDC)只实现;然而，CoPP策略为所有VDCs是可适用的。同一项全局策略为所有线卡应用。CoPP应用在VDCs之间的资源共享，如果同样FEs的港属于另外VDCs (M1系列或M2系列LC)。例如，一个FE端口，在另外VDCs，计数CoPP的同样阈值。

如果同样FE共享区别VDCs和控制层面流量之间一给的类超出阈值，这影响在同样FE的所有VDCs。推荐若可能投入每个VDC一个FE为了隔离CoPP实施。

当交换机出来第一次时，必须编程默认策略保护**控制面板**。CoPP提供默认策略，作为初始启动顺序一部分，应用到**控制面板**。

为什么在连结7000系列交换机的CoPP

连结7000系列交换机配置作为聚合或核心交换机。因此，它是网络的耳朵和智慧。它处理在网络的**最大载荷**。它必须处理**常见和突发流量请求**。一些请求包括：

- **生成树网桥协议数据单元(BPDU)处理**-默认是每两秒。
- **第一个跳跃冗余**-这包括热备份路由协议(HSRP)、虚拟路由冗余协议(VRRP)和网关负载均衡协议(GLBP) -默认是每三秒。
- **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)汇集-一请求每秒，每台主机，例如网络接口控制器(NIC)合作。
- **动态主机控制协议(DHCP)** - DHCP请求，中继-一请求每秒，每台主机。
- **第3层的(L3)路由协议。**
- **数据中心互连-重叠传输虚拟化(OTV)**，多协议标签交换(MPLS)和虚拟专用LAN服务(VPLS)。

CoPP是重要为了保护CPU以防止误配置的服务器或可能性DOS攻击，允许CPU有处理足够的周期**关键控制层面消息**。

处理在连结7000系列交换机的控制层面

连结7000系列交换机采取一分布式控制层面方法。它有一多芯在每输入输出模块，以及一多芯在 Supervisor 模块的交换机控制层面的。它卸载密集任务对访问控制列表(ACL)和FIB编程的输入输出模块CPU。它扩展控制层面产能用线卡数量。这避免Supervisor CPU瓶颈，在一集中化方法被看到。硬件速率防幅器和基于硬件的CoPP保护从坏或恶意活动的控制层面。

CoPP最佳实践策略

CoPP最佳实践策略(BPP)在Cisco NX-OS版本5.2介绍。**show running-config**命令输出不显示CoPP BPP的内容。**all**命令的**show run**显示CoPP BPP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提供四个选项给用户为默认策略：

- 严格
- 一般
- 宽大
- 密集(介绍在版本6.0(1))

如果选项没有选择或，如果设置被跳过，然后严格管制应用。所有这些选项使用同样类映射和类，但是不同的承诺信息速率(CIR)和突发流量计数(BC)修正的值。在Cisco NX-OS版本中早于5.2.1，**setup**命令用于更改选项。Cisco NX-OS版本5.2.1介绍增强对CoPP BPP，以便选项可以更改，不用**setup**命令;请使用**profile**命令的**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
```

请使用**show copp**配置文件<profile-type>命令查看默认CoPP BPP配置。请使用**status**命令显示的**copp**验证CoPP策略正确地应用。

```

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

```

为了查看两CoPP BPPs之间的差异，使用显示copp diff配置文件<profile类型1>配置文件<profile类型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-----

```

如何定制CoPP策略

用户能创建一项定制的CoPP策略。因为CoPP BPP只读，请克隆默认CoPP BPP，并且附加它对控制面板接口。

```

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复制配置文件<profile-type> <prefix> [suffix]命令创建CoPP BPP的克隆。这用于为了修改默认配置。**profile**命令copp的复制是EXEC模式命令。用户能选择前缀或后缀access-list，类映射和策略映射名称的。例如，CoPP系统p策略严格更改对[**prefix**] CoPP策略严格[**suffix**]。被克隆的配置在**show run**输出中对待用户配置和包括。

```

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#

```

是可能的标记在超出并且违犯指定的允许的信息速率的流量下(PIR)用这些命令：

```

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)#

```

适用于定制的CoPP策略全局接口控制面板。请使用status命令显示的copp为了验证CoPP策略正确地应用。

```

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

```

定制的CoPP策略案例研究

此部分描述客户要求多个监听设备为了频繁地ping本地接口的一实时示例。当客户要修改CoPP策略为了时，困难在此方案遇到：

- 增加CIR，以便这些具体地址能ping本地设备和不违犯策略。
- 允许其他IP地址维护能力ping本地设备，但是在为了实现故障排除目的更低CIR。

解决方案在下一个示例显示，是创建与分开的类映射的一个客户化策略。分开的类映射包含监听设备的指定的IP地址，并且类映射有更加高的CIR。这也离开原始类映射监听，捕获所有的ICMP流量其他IP地址在更低CIR。

```

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
```

CoPP数据结构

CoPP BPP数据结构被修建如下：

- **ACL配置**：IP ACL和MAC ACL。
- **分类器配置**：匹配IP ACL或MAC ACL的类映射。
- **策略器配置**：设置CIR，BC，一致操作，并且违反操作。策略器有两速率(CIR和BC)和两个颜色(一致和违反)。

```
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
```

CoPP比例因子

在Cisco NX-OS版本介绍的比例因子配置6.0用于扩展已应用CoPP策略的策略器速率特定的线路卡的。这增加或减少特定的线路卡的策略器速率，但是不更改当前CoPP策略。更改立即有效，并且没有需要重新应用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，配置一丢弃阈值每触发在事件的一系统消息阈值被超出的CoPP类名称是可能的。命令记录丢弃阈值<dropped字节count>级别<logging的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
这是系统消息的示例：
```

```
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 Logged 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
```

CoPP计数器

CoPP支持QoS统计信息和其他接口一样。它显示形成每输入输出模块的服务策略该支持CoPP类的统计信息。请使用**show policy-map interface**控制面板命令查看CoPP的统计信息。

注意：应该监控所有类根据被违犯的数据包。

```
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
```



```
[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

这些是CoPP配置的最佳实践推荐：

- 默认情况下请使用严格CoPP模式。
- 密集的CoPP配置文件，当机箱用F2系列模块比所有其他输入输出模块时，充分地装载或用F2系列模块装载推荐。
- 没有推荐禁用CoPP。调整默认CoPP，当必要时。
- 监控不愿意的丢包，并且添加或者修改在符合的默认CoPP策略成预计流量。
- 基于FEs编号在机箱的，CoPP的CIR和BC设置可以增加或减小。这根据设备的角色在网络的也，运行的协议，等等。
- 由于流量模式在**数据中心**经常更改，CoPP的自定义是一不变进程。
- CoPP和VDC：同样FE的所有端口应该属于同样VDC，为F2系列LC是容易，但是没有如容易为M2系列或M108 LC。这是因为在VDCs之间的CoPP资源共享，如果同样FE的端口属于另外VDCs (M1系列或M2系列LC)。一个FE端口，在另外VDCs，计数CoPP的同样阈值。
- 比例因子配置，当机箱用F2系列和M系列模块时，装载推荐。

监控最佳实践的CoPP

这些是CoPP监控的最佳实践推荐：

- 配置CoPP的(Cisco NX-OS版本5.1)一系统消息阈值为了监控CoPP强制执行的丢包。
- 如果在数据流类别内的丢包超出用户配置的阈值，系统消息生成。
- 记录日志阈值和级别可以在与使用的每数据流类别内定制**记录日志丢弃阈值<packet-count>级别<level>**命令。
- 由于不支持CoPP MAC ACL或IP ACL的“统计信息每条目”选项，请使用**show system内部access-list输入条目det**命令监控访问控制条目(ACE)命中数。
- 应该监控类**copp-class-l2-default**和**class-default**命令保证没有高增加，为一致的计数器。
- 应该监控所有类根据被违犯的数据包。
- 由于CoPP中集**集团**关键是高度重要的，但是有**违反丢弃策略**，它是良好的做法监控速率一致的

数据包为了接收一个早期的征兆，当类变为近对开始侵害的瞬间时。如果被违犯的计数器为此类增加，不一定含义一种红色警戒。相反，含义在短期必须调查此情况。

- 请使用copp配置文件严格命令在每次Cisco NX-OS代码升级以后或者至少在每次主要Cisco NX-OS代码升级以后;如果CoPP修改以前完成，必须重新应用。

结论

- CoPP是保护从DOS攻击的Supervisor的一个基于硬件的功能。
- M1、F2和M2系列LCs支持CoPP。F1系列LCs不支持CoPP。
- CoPP配置类似于MQC (模块化QoS CLI)。
- CoPP配置和监视在默认VDC仅被执行。
- 默认CoPP BPP可以与严格，一般，宽大和密集选项一起使用。
- 克隆CoPP BPP对定制的CoPP规则为了匹配特定网络要求。
- CoPP计数器(一致和违犯在字节每类映射)用show policy-map interface控制面板命令显示。
- Supervisor模块的CPU接收的流量等于FEs总数乘允许速率。
- 设法避免一个FE共享端口在另外VDCs间的。
- 跟随CoPP最佳实践为了顺利地实现和监控功能。

不支持的功能

不支持这些功能：

- 分布式聚集管制。
- 微流策略管理。
- 出口例外管制。
- 来自dot1q-tunnel端口BPDU的CoPP支持(QinQ)：思科设备发现协议(CDP)、Dot1x，生成树协议和VLAN中继协议(VTP)。