检验Nexus平台上的控制平面策略违规

目录

简介

本文档详细介绍Cisco Nexus交换机上的控制平面策略(CoPP)及其对非默认类违规的相关影响。

先决条件

思科建议您了解关于控制平面策略(CoPP)、其准则和限制、常规配置以及服务质量(QoS)策略(CIR)功能的基本信息。有关此功能的详细信息，请参阅适用的文档：

- Cisco Nexus 9000系列NX-OS安全配置指南，版本10.2(x)
- Nexus 7000系列交换机上的CoPP
- Cisco Nexus 9000系列NX-OS服务质量配置指南，版本10.2(x)

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件要求。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

通过重定向访问控制列表(ACL)，控制平面流量被重定向到管理引擎模块，该列表被编程为通过硬件速率限制器和CoPP这两层保护层的匹配流量。对管理引擎模块的任何中断或攻击（如果未选中）都可能导致严重的网络故障；因此CoPP作为一种保护机制存在。如果在控制平面级别存在不稳定性，则有必要检查CoPP，因为由环路或泛洪创建的异常流量模式，或者非法设备可能会对主管征税并阻止其处理合法流量。此类攻击可能无意中由欺诈设备实施，也可能由攻击者恶意实施，通常涉及高流量发往管理引擎模块或CPU。

控制计划策略(CoPP)功能可对通过带内（前面板）端口接收的所有数据包进行分类和策略，这些数据包的目的地是路由器地址或需要任何主管参与。此功能允许将策略映射应用于控制平面。此策略映射类似于正常的服务质量(QoS)策略，应用于从非管理端口进入交换机的所有流量。通过策略保护管理引擎模块，允许交换机通过丢弃数据包来缓解超出每个类别承诺输入速率(CIR)的流量泛洪，以防止交换机过载，从而影响性能。

持续监控CoPP计数器并证明其合理性非常重要，这正是本文档的目的。CoPP违规，如果保持未选中状态，可能会阻止控制平面进入相关受影响类上的真实流量进程。CoPP配置是一个不断变化的流程，必须响应网络和基础设施要求。CoPP有三种默认系统策略。默认情况下，思科建议使用默认 strict 策略作为初始起点，并用作本文档的基础。

CoPP仅适用于通过前面板端口接收的带内流量。带外管理端口(mgmt0)不受CoPP限制。Cisco NX-OS设备硬件基于每个转发引擎执行CoPP。因此，请选择速率，以使聚合流量不会压垮管理引擎模块。这对行尾式/模块化交换机尤为重要，因为CIR适用于所有模块的CPU绑定的总流量。

适用硬件

本文档涵盖的组件适用于所有Cisco Nexus数据中心交换机。

控制平面策略解释

本文档的重点在于解决Nexus交换机上最常见且最关键的非默认类违规。

标准CoPP默认配置文件

要了解如何解释CoPP，首先必须验证以确保应用了配置文件，并了解是否已在交换机上应用了默认配置文件或自定义配置文件。

注意：作为最佳实践，所有Nexus交换机都必须启用CoPP。如果未启用此功能，则可能导致所有控制平面流量不稳定，因为不同的平台可以限制受管理引擎(SUP)限制的流量。例如，如果Nexus 9000上未启用CoPP，则发往SUP的流量速率限制为50 pps，因此交换机几乎无法运行。CoPP被认为是Nexus 3000和Nexus 9000平台的一项要求。

如果CoPP未启用，可以使用命令或在交换机上重新启用或配置 **setup** CoPP，也可以使用配置选项：下的标准默认策略之一进行配置

copp profile [dense|lenient|moderate|strict]。

未受保护的设备不会正确地将流量分类并划分为不同的类别，因此特定功能或协议的任何拒绝服务行为都不会限制在该范围之内，并且可能会影响整个控制平面。

注意:CoPP策略通过三重内容可寻址存储器(TCAM)分类重定向实施，可以直接在或下方 **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

控制平面策略类

CoPP根据对应于IP或MAC ACL的匹配项对流量进行分类，因此，了解哪些流量分类在哪类下非常重要。

类取决于平台，可以有所不同。因此，了解如何验证类非常重要。

例如，在Nexus 9000架顶式(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
...
```

在本示例中，类映射包含与路由协议相关的流 copp-system-p-class-critical 量，例如边界网关协议(BGP)、开放最短路径优先(OSPF)、增强型内部网关路由器协议(EIGRP)，还包括其他协议，例如vPC。

IP或MAC ACL的名称约定大多对所涉及的协议或功能是自解释的，带有前 copp-system-p-acl-[protocol|feature]缀。

要查看特定类，可以在**show**命令运行时直接指定该类。例如：

```
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
```

虽然CoPP默认配置文件通常作为默认配置的一部分隐藏，但您可以看到具有以下内容的配 **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)
...
```

之前看到的类 copp-system-p-class-critical映射引用了调用系统ACL的多条match语句（默认情况下这些语句是隐藏的），并引用了匹配的分类。例如，对于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)
```

这意味着所有BGP流量都与此类匹配，并且与同一 copp-system-p-class-critical类上的所有其它协议一起被分类到下。

Nexus 7000使用与Nexus 9000非常类似的CoPP功能结构：

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

需要注意的是，在Nexus 7000上，由于这些是模块化交换机，您可以看到按模块划分的类；但是，CIR适用于所有模块的聚合，而CoPP适用于整个机箱。CoPP验证和输出只能从默认或管理虚拟设备环境(VDC)中看到。

如果发现控制平面问题，则在Nexus 7000上验证CoPP尤其重要，因为具有过多的CPU限制流量的VDC上的不稳定会导致CoPP违规，这会影响其他VDC的稳定性。

在Nexus 5600上，类有所不同。因此，对于BGP，它是自己的独立类：

```
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个路由协议类，因此，要验证BGP属于哪一类，请交叉引用所引用的4个CoPP ACL:
EIGRP在Nexus 3100上由其自己的类处理。

<#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
```

在这种情况下，BGP与ACL匹 copp-system-acl-routingproto1配，因此CoPP类BGP属于 copp-s-routingProto1is。

控制平面策略统计数据和计数器

CoPP支持QoS统计信息，以跟踪每个模块中确认或违反特定类的承诺输入速率(CIR)的流量的聚合计数器。

每个类映射根据其对应的类对CPU绑定的流量进行分类，并为属于该分类的所有数据包附加CIR。例如，与BGP流量相关的类用作参考：

在Nexus 9000架顶式(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语句之后，您将看到与该类中的所有流量相关的操作。分类在中的所有流量都使用服务类copp-system-p-class-critical 别(CoS)7进行设置，这是最高优先级流量，此类通过36000 kbps的CIR和1280000字节的承诺突发速率进行管制。

符合此策略的流量将转发到SUP进行处理并丢弃所有违规。

<#root>

set cos 7

police cir 36000 kbps , bc 1280000 bytes

下一节包含与具有单个模块的架顶式(TOR)交换机模块相关的统计信息，模块1是指交换机。

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

在输出中看到的统计信息是历史的，因此这提供了运行命令时当前统计信息的快照。

此处有两个部分要解释：传输部分和丢弃部分：
传输的数据点会跟踪所有符合策略传输的数据包。此部分很重要，因为它可以深入了解管理引擎处理的流量类型。

5分钟的offered rate值可深入了解当前速率。
一致的峰值速率和日期，提供策略内仍符合的最高每秒峰值速率及其发生时间的快照。
如果发现新的峰值，则会替换此值和日期。

统计信息最重要的部分是丢弃的数据点。与传输的统计信息一样，丢弃部分会跟踪由于违反策略速率而丢弃的累积字节。 它还提供过去5分钟的违规速率、违规峰值，如果存在峰值，则提供该峰值违规的时间戳。同样，如果发现新的峰值，则会替换此值和日期。
在其他平台上，输出各不相同，但逻辑非常相似。

Nexus 7000使用相同的结构，并且验证相同，尽管某些类在引用的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;

虽然它不提供有关速率或峰值的信息，但它仍提供一致和违反的聚合字节。

在Nexus 3100上，控制平面输出显示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是指一致的数据包，而DropPackets指违规CIR。在这种情况下，您不会看到关联类上的丢弃。

在Nexus 3500上，输出显示硬件和软件的匹配数据包：

```
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 Matched Packets（硬件匹配的数据包）是指由ACL在HW中匹配的数据包。与SW匹配的数据包符合策略。硬件与软件匹配的数据包之间的任何差异都意味着违规。

在这种情况下，当值匹配时，在路由协议–1类数据包（包括BGP）上不会出现丢包。

检查活动的丢弃违规

鉴于控制平面策略统计信息是历史性的，确定活动违规是否增加非常重要。执行此任务的标准方法是比较两个完整输出并检验所有差异。

此任务可以手动执行，或者Nexus交换机提供差异工具，以帮助比较输出。

虽然可以比较整个输出，但是由于焦点仅放在丢弃的统计信息上，因此不需要进行比较操作。因此，可以过滤CoPP输出以仅关注违规。

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

---

注：必须运行两次命令，差异才能将当前输出与上一输出进行比较。

```
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;
```

上一个命令可用于查看两个类之间的增量并查找违规增加。

注意：由于CoPP统计信息是历史性的，因此另一个建议是在运行命令后清除统计信息，以验证是否存在活动增加。要清除CoPP统计信息，请运行命令 **clear copp statistics**:。

CoPP丢弃的类型

CoPP是一种简单的策略结构，因为任何违反CIR的CPU绑定的流量都会被丢弃。然而，根据丢弃的类型，其影响差别很大。

尽管逻辑是相同的，但丢弃发往 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

与丢弃发往类映射的流量相 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

第一个协议主要涉及路由协议，第二个协议涉及优先级和CIR最低的Internet控制消息协议(ICMP)。CIR的差值是100倍。因此，了解类别、影响、通用检查/验证和建议非常重要。

CoPP类

类监控 — copp-system-p-class-monitoring

此类包括用于IPv4和IPv6的ICMP，以及定向到有问题的交换机的流量的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

影响

当出现丢包或延迟故障时，通常的误解是通过其带内端口（受CoPP速率限制）对交换机执行ping操作。由于CoPP严格控制ICMP，即使出现低流量或拥塞，如果带内接口违反CIR，也可以直接通过ping发现丢包。

例如，通过对路由端口上的直连接口执行ping操作（数据包负载为500），可以定期看到丢包情况。

<#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数据包发往的Nexus上，您会看到CoPP在检测到违规且CPU受到保护时丢弃了它们：

<#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

要解决延迟或丢包问题，建议使用数据平面通过交换机可访问的主机，而不是流向交换机本身的控制平面流量。数据平面流量在硬件级别转发/路由，无需管理引擎干预，因此不受CoPP监管，通常不会遇到丢包情况。

建议

- 通过数据层而不是交换机发送ping，检验数据包丢失的误报结果。
- 限制主动使用ICMP交换机的网络监控系统(NMS)或工具，从而避免通过类承诺输入速率进行突发。请记住，CoPP适用于属于该类别的所有汇聚流量。

班级管理 — copp-system-p-class-management

如图所示，此类包含不同的管理协议，可用于通信(SSH、Telnet)、传输(SCP、FTP、HTTP、SFTP、TFTP)、时钟(NTP)、AAA(Radius/TACACS)和监控(SNMP)，用于IPv4和IPv6通信。

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

影响

与该类关联的最常见行为或丢弃包括：

- 通过SSH/Telnet连接时感觉到CLI缓慢。如果类上有活动的丢弃，则通信会话可能较慢并遭受丢弃。
- 在交换机上使用FTP、SCP、SFTP、TFTP协议传输文件。最常见的行为是尝试通过带内管理端口传输系统/启动引导映像。这可能导致较高的传输时间和关闭/终止的传输会话由该类的聚合带宽决定。
- NTP同步问题，此类也很重要，因为它可以缓解非法NTP代理或攻击。
- AAA Radius和TACACS服务也属于此类。如果发现此类受到影响，则会影响交换机上针对用户帐户的授权和身份验证服务，这也可能导致CLI命令延迟。
- SNMP也在此类下受管制。由于SNMP类而导致丢弃的最常见行为发生在NMS服务器上，这些服务器执行漫游、批量收集或网络扫描。当周期性不稳定发生时，通常与NMS收集计划相关联。

建议

- 如果发现CLI缓慢以及此类中的丢弃，请使用控制台访问或管理带外访问(mgmt0)。
- 如果必须将系统映像上传到交换机，请使用带外管理端口(mgmt0)或使用USB端口实现最快传输。
- 如果NTP数据包丢失，请选中show ntp peer-status并验证reachability列，no drops会转换为377。
- 如果发现AAA服务存在问题，请使用仅本地用户进行故障排除，直到行为得到缓解。
- SNMP问题的缓解包括攻击性较弱的行为、目标收集或网络扫描程序的最小化。检查从scanners到CPU级别所发生事件的定期时间。

L3类单播数据 — copp-system-p-class-l3uc-data

此类专门处理收集数据包。这种类型的数据包也由硬件速率限制器(HWRL)处理。

如果在线路卡中转发传入IP数据包时无法解析下一跳的地址解析协议(ARP)请求，则线路卡会将数据包转发到Supervisor模块。

Supervisor解析下一跳的MAC地址并对硬件进行编程。

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

当使用静态路由且下一跳不可达或未解析时，通常会发生这种情况。

发送ARP请求时，软件会在硬件中添加/32丢弃邻接关系，以防止将数据包转发到同一下一跳IP地址以转发到管理引擎。解析ARP后，硬件条目将使用正确的MAC地址进行更新。如果在超时时间之前未解析ARP条目，则该条目将从硬件中删除。

注意:CoPP和HWRL协同工作以确保CPU受到保护。虽然它们似乎执行类似的功能，但HWRL首先发生。实施基于特定功能在ASIC上的转发引擎上的实施位置。此串行方法允许对所有CPU绑定的数据包进行分级的精细和多层保护。

HWRL在模块上按实例/转发引擎执行，并可使用命令进行查看**show hardware rate-limiter**。HWRL不在本技术文档范围内。

<#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
```

影响

- 数据平面流量会作为违规被传送至管理引擎，因为它无法在硬件中处理，因此会对CPU造成压力。

建议

- 此问题的通用解决方案是为了尽量减少收集丢弃，以确保下一跳可访问，并通过配置命令启用收集限制： **hardware ip glean throttle**.

在Nexus 7000 8.4(2)上，它还为M3和F4模块的聚集邻接引入了bloom filter支持。请参阅Cisco Nexus 7000系列NX-OS单播路由配置指南

查看使用不可达下一跳地址的所有静态路由配置，或使用动态路由协议从RIB中动态删除此类路由。

关键类别 — class-map copp-system-p-class-critical

此类引用了第3层最关键的控制层协议，包括IPv4和IPv6的路由协议(RIP、OSPF、EIGRP、BGP)、自动RP、虚拟端口通道(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
```

影响

路由协议 copp-system-p-class-critical 传输不稳定时丢弃，这可能包括丢弃的邻接关系或收敛失败，或者更新/NLRI传播。
此类中最常见的策略丢弃可能与网络上运行异常（由于配置错误或故障）或可扩展性的欺诈设备有关。

建议

- 如果没有检测到异常（例如导致上层协议连续重新收敛的流氓设备或L2不稳定），则可能需要使用CoPP或更宽松类的自定义配置来适应扩展。

- 有关如何从当前存在的默认配置文件配置自定义CoPP配置文件，请参阅CoPP配置指南。
[复制CoPP最佳实践策略]

班级重要 — copp-system-p-class-important

此类与第一跳冗余协议(FHRP)相关，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
```

影响

此处发现的最常见导致丢弃的行为是第2层不稳定问题，该问题导致设备转换到活动状态（大脑分割）场景、主动计时器、配置错误或可扩展性。

建议：

- 确保为FHRP正确配置组，并且角色为主用/备用或主用/辅助角色，并且已正确协商，并且状态上没有摆动。

- 检查L2的收敛问题或L2域的组播传播问题。

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

L2未管制类是指作为所有上层协议的基础的所有关键第2层协议，因此被视为具有最高CIR和优先级的几乎未管制。

此类可有效处理生成树协议(STP)、链路汇聚控制协议(LACP)、思科以太网交换矩阵服务(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

此类的警用CIR为50 Mbps，在所有类别中最高，突发速率吸收也最高。

影响

此类丢弃可能导致全局不稳定，因为数据、控制和管理平面上的所有上层协议及通信都依赖于底层第2层稳定性。

STP违规问题可能导致TCN和STP收敛问题，包括STP争议、MAC刷新、移动和学习禁用行为，这会导致可达性问题，并可能导致流量循环，从而破坏网络的稳定。

此类还引用LACP，并因此处理与0x8809关联的所有EtherType数据包，其中包括用于维护端口通道绑定状态的所有LACPDU。此类上的不稳定可能导致如果LACPDU被丢弃，端口通道超时。

Cisco Fabric Service over Ethernet(CSFoE)属于此类服务，用于在Nexus交换机之间传达关键的应用控制状态，因此对稳定性至关重要。

这同样适用于此类协议中的其他协议，包括CDP、UDLD和VTP。

建议

- 最常见的行为与L2以太网不稳定有关。确保STP采用确定性方式设计，同时发挥相关功能增强功能，以最大程度地降低网络重新融合或非法设备的影响。确保为未参与L2扩展的所有终端主机设备配置了正确的STP端口类型，并将其配置为边缘/边缘中继端口，以最小化TCN。
- 在适当情况下使用STP增强功能，如BPDUguard、Loopguard、BPDUfilter和RootGuard，以限制故障范围，或网络中配置错误或欺诈设备的问题。
- 请参阅Cisco Nexus 9000 NX-OS第2层交换配置指南，版本10.2(x)
- 检查可能导致MAC学习和刷新禁用的MAC移动行为。请参阅：Nexus 9000 Mac移动故障排除和预防方法

类组播路由器 — class-map copp-system-p-class-multicast-router

此类是指控制平面协议无关组播(PIM)数据包，用于通过数据平面路径中所有启用PIM的设备建立和控制路由组播共享树，包括第一跳路由器(FHR)、最后一跳路由器(LHR)、中间跳路由器(IHR)和交汇点(RP)。分类在此类中的数据包包括源的PIM注册、IPv4和IPv6接收器的PIM加入，通常包括任何发往PIM(224.0.0.13)的流量，以及组播源发现协议(MSDP)。请注意，还有几个额外的类，它们处理由不同类处理的非常具体的组播或RP功能部分。

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

影响

与此类相关的丢包的主要影响与通过PIM注册向RP或PIM加入未正确处理而与组播源通信的问题相关，这会使通往组播流源或RP的共享或最短路径树失去稳定性。行为可能包括由于缺少连接而未正确填充的传出接口列表(OIL)，或者(S， G)或(*, G)在整个环境中未一致看到。依赖MSDP进行互联的组播路由域之间也可能出现问题。

建议

- PIM控制相关问题最常见的行为是指扩展问题或欺诈行为。最常见的行为之一是由于UPnP上的实施，这也会导致内存耗尽问题。这可以通过过滤器和缩小非法设备范围来解决。有关如何缓解和过滤取决于设备网络角色的组播控制数据包的详细信息，请参阅：在Nexus 7K/N9K上配置组播过滤 — 思科

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

此类是指组播侦听程序发现(MLD)，尤其是MLD查询、报告、缩减和MLDv2数据包类型。MLD是主机用于请求特定组的组播数据的IPv6协议。利用通过MLD获取的信息，软件会逐个接口维护组播组或通道成员资格列表。接收MLD数据包的设备将所请求的组或信道的组播数据发送到已知接收器的网段之外。MLDv1源自IGMPv2,MLDv2源自IGMPv3。IGMP使用IP协议2消息类型，而MLD使用IP协议58消息类型，这是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

影响

此类上的丢弃会转换为本地链路IPv6组播通信问题，这会导致来自接收方的侦听程序报告或对常规查询的响应被丢弃，从而阻止主机要接收的组播组的发现。这可能会影响监听机制，并且无法通过请求流量的预期接口正确转发流量。

建议

- 由于MLD流量在IPv6的本地链路级别非常重要，如果此类上出现丢包，最常见的行为原因与扩展、L2不稳定或欺诈设备有关。

第3类组播数据 — copp-system-p-class-l3mc-data 和第3类组播IPv6数据 — copp-system-p-class-l3mcv6-data

这些类是指与指向SUP的组播异常重定向匹配的流量。在本例中，这两个类处理两个条件。第一个是反向路径转发(RPF)故障，第二个是目的地丢失。目标未命中是指在硬件中查找第3层组播转发表失败，因此数据包被传送到CPU的组播数据包。这些数据包有时用

于根据数据平面流量触发/安装组播控制平面和添加硬件转发表项。违反RPF的数据平面组播数据包也会与此例外匹配，并分类为违规。

```
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
```

影响

RPF故障和目的地未命中意味着与流量如何流经组播路由器相关的设计或配置问题。目标缺失在状态创建时很常见，丢弃可能导致编程和创建(*, G),(S， G)故障。

建议

- 在RPF发生故障时，对基础单播RIB设计执行更改，或添加静态mroute以引导流量通过特定接口。
- 请参阅由于RPF故障路由器不向主机转发组播数据包

IGMP类 — copp-system-p-class-igmp

此类是指所有IGMP消息，用于请求特定组的组播数据的所有版本，IGMP监听功能使用此类消息来维护组和相关传出接口列表(OIL)，将流量转发到第2层中的相关接收方。IGMP消息在本地具有重要意义，因为它们不经过第3层边界，因为它们的生存时间(TTL)必须为1，如RFC2236(Internet组管理协议，版本2)中所述。此类处理的IGMP数据包包括所有成员身份查询（常规或源/组特定的），以及接收方的成员身份和离开报告。

```
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
```

影响

此类上的丢弃将转换为源与接收器之间组播通信的所有级别的问题，具体取决于由于违规而丢弃的IGMP消息的类型。如果来自接收方的成员身份报告丢失，则路由器不知道流量中感兴趣的设备，因此它不会将接口/VLAN包含在其相关的传出接口列表中。如果此设备也是查询器或指定路由器，并且源超出本地第2层域时，它不会触发指向RP的相关PIM加入消息，因此它不会在整个组播树中建立到接收器或RP的数据平面。如果离开报告丢失，接收方可以继续接收不需要的流量。这也可能影响查询器触发的所有相关IGMP查询

以及域中组播路由器之间的通信。

建议

- 与IGMP丢弃相关的最常见行为与L2不稳定、计时器问题或扩展有关。

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

此类是指与标准ARP流量匹配的流量，还包括与802.1X关联的流量，用于基于端口的网络访问控制。这是遇到违规的最常见类之一，因为ARP请求、无偿ARP和逆向ARP数据包会广播并在整个第2层域中传播。请务必记住，ARP数据包不是IP数据包，这些数据包不包含L3报头，因此决策完全取决于L2报头的范围。如果路由器配置了与该子网关联的IP接口（例如交换机虚拟接口[SVI]），路由器会将ARP数据包传送到SUP进行处理，因为这些数据包的目的地是硬件广播地址。任何广播风暴、第2层环路（由于STP或摆动）或网络中的欺诈设备都可能导致ARP风暴，从而引起违规行为显着增加。

```
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
```

影响

此类违规的影响在很大程度上取决于事件的持续时间和交换机对环境的影响。此类丢弃意味着ARP数据包当前被丢弃，因此不会由SUP引擎处理，这会导致ARP解析不完整引起的两种主要行为。

从终端主机的角度来看，网络中的设备无法通过交换机解析或完成地址解析。如果此设备充当网段的默认网关，可能导致设备无法解析其网关，从而无法在其L2以太网网段(VLAN)之外路由。如果设备可以完成本地网段上其他终端主机的ARP解析，它们仍可以在本地网段上通信。

从交换机的角度来看，如果风暴和违规现象普遍存在，也可能导致交换机无法完成其生成的ARP请求过程。这些请求通常针对下一跳或直连子网分辨率生成。虽然ARP应答本质上是单播的，因为它们是发送到交换机所拥有的MAC地址，但是由于它们仍然是ARP数据包，因此它们被归入同一类。这会转换为可达性问题，因为如果下一跳未解决，交换机无法正确处理流量；如果邻接管理器没有主机的条目，则可能导致第2层报头重写问题。

影响还取决于触发ARP违规的基本问题的范围。例如，在广播风暴中，主机和交换机继续ARP以尝试解析邻接关系，这可能导致网络上的其他广播流量，并且由于ARP数据包是第2层，因此没有第3层生存时间(TTL)来中断L2环路，因此它们会继续环路，并在网络中呈指数增长，直到环路被破坏。

建议

- 解决可能在环境中引起ARP风暴（如STP、抖动或欺诈设备）的任何基础L2不稳定性。根据需要使用任意所需方法中断这些环路，以打开链路路径。

- 风暴控制也可用于缓解ARP风暴。如果未启用风暴控制，请验证接口上的计数器统计信息，以验证接口上显示的广播流量相对于通过该接口的总流量的百分比。

- 如果没有风暴，但环境中仍能看到持续丢弃，请验证SUP流量以识别任何非法设备，这些设备会持续在网络上发送ARP数据包，从而影响合法流量。

- 可以看到的增加取决于网络中的主机数量和交换机在环境中的角色，ARP设计为重试、解析和刷新条目，因此预期始终会看到ARP流量。如果只看到零星丢弃，则它们可能由于网络负载而成为瞬时，且不会察觉任何影响。但是，必须监控和了解网络，才能正确识别并区分预期和异常情况。

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

此类是指与IPv6邻居发现/通告以及路由器请求和通告数据包关联的流量，这些流量使用ICMP消息来确定邻居的本地链路层地址，用于邻居设备的连通性和跟踪。

```
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
```

影响

此类违规可能会阻碍邻居设备之间的IPv6通信，因为这些数据包用于促进本地链路上的主机和路由器之间的动态发现或链路层/本地信息。此通信中断也可能会导致连通性超出相关本地链路或通过相关本地链路出现问题。如果IPv6邻居之间存在通信问题，请确保此类上没有丢弃。

建议

- 检查来自邻居设备的任何异常ICMP行为，尤其是与邻居发现和/或路由器发现相关的行为。

- 确保整个环境中定期消息的所有预期计时器和间隔值一致且符合要求。例如，对于路由器通告消息（RA消息）。

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

此类是指与IPv4和IPv6的同一本地以太网网段上通常称为动态主机控制协议(DHCP)数据包的Bootstrap协议（BOOTP客户端/服务器）关联的流量。这仅与通过整个发现、提供、请求和确认(DORA)数据包交换从任何bootp客户端或发往任何BOOTP服务器的流量通信相关，还包括通过UDP端口546/547的DHCPv6客户端/服务器事务。

```
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
```

影响

此类违规可能会导致终端主机无法正确从DHCP服务器获取IP，从而回退到其自动私有IP地址(APIPA)范围169.254.0.0/16。此类违规情况可能发生在设备尝试同时启动从而超出与类关联的CIR的环境中。

建议

- 使用捕获验证，在主机和DHCP服务器端可以看到整个DORA事务。如果交换机是此通信的一部分，则还必须验证已处理或传送到CPU的数据包，并验证交换机：和重定向： **show ip dhcp global statistics** 的统计 **show system internal access-list sup-redirect-stats module 1 | grep -i dhcp**信息。

正常类DHCP中继响应 — copp-system-p-class-normal-dhcp-relay-response

此类是指与IPv4和IPv6的DHCP中继功能关联的流量，定向到在中继下配置的DHCP服务器。这仅与通过整个DORA数据包交换从任何BOOTP服务器或发往任何BOOTP客户端的流量通信相关，还包括通过UDP端口546/547的DHCPv6客户端/服务器事务。

```
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
```

影响

此类违规的影响与类copp-system-p-class-normal-dhcp的违规的影响相同，因为它们都是同一事务的一部分。本课程主要介绍来自中继代理服务器的响应通信。Nexus不充当DHCP服务器，它只用作中继代理。

建议

- 此处应用与类普通DHCP相同的建议。由于Nexus的功能仅仅是充当中继代理，因此在SUP上，您会看到主机和充当中继的交换机之间的整个事务，并且交换机和服务器会进行配置。

- 确保没有欺诈设备，例如网络上响应作用域的意外DHCP服务器，或者设备滞留在使用DHCP发现数据包泛洪网络的环路中。可通过命令：和执行其他检show ip dhcp relay **show ip dhcp relay statistics**查。

类NAT流 — copp-system-p-class-nat-flow

此类是指软件交换机NAT流流量。当创建新的动态转换时，软件会转发该流，直到在硬件中对该转换进行编程，然后由CoPP管制该流，以在硬件中安装条目时限制发送到管理引擎的流量。

```
class-map copp-system-p-class-nat-flow (match-any)
match exception nat-flow
set cos 7
police cir 800 kbps , bc 64000 bytes
```

影响

此类丢包通常发生在硬件中安装了高速率的新动态转换和流时。这种影响与被丢弃且未传输到终端主机的软件交换数据包有关，可能导致丢失和重传。条目在硬件中安装后，不会再有其它流量传送到Supervisor。

建议

- 检验相关平台上动态NAT的准则和限制。在平台上记录了一些已知限制，例如3548，在该版本中，转换可能需要几秒钟。请参阅：动态NAT的限制

类异常 — copp-system-p-class-exception

此类是指与IP选项和IP ICMP不可达数据包关联的异常数据包。如果转发信息库(FIB)中不存在目的地址并导致缺失，SUP会将ICMP不可达数据包发送回发送方。启用了IP选项的数据包也属于此类别。有关IP选项的详细信息，请参阅IANA文档：IP选项号

```
 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
```

影响

此类受到严格管制，此类上的丢弃不表示故障，而是表示一种保护机制，用于限制ICMP不可达和IP选项数据包的范围。

建议

- 验证是否发现任何流量流或流量被传送到CPU以寻找不在FIB上的目标。

类重定向 — copp-system-p-class-redirect

此类是指与用于时间同步的精确时间协议(PTP)关联的流量。这包括保留范围224.0.1.129/32的组播流量、UDP端口319/320和Ethetype 0X88F7上的单播流量。

```
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
```

影响

此类上的丢弃可能导致未正确同步或尚未建立正确层次结构的设备出现问题。

建议

- 确保时钟的稳定性，并确保时钟配置正确。确保PTP设备配置为组播或单播PTP模式，而不是同时配置这两种模式。这也记录在准则和限制中，可以将流量推至超过承诺输入速率。
- 查看环境中边界时钟和所有PTP设备的设计和配置。确保每个平台遵循所有准则和限制，因为它们各不相同。

类OpenFlow - copp-system-p-class-openflow

此类是指与OpenFlow代理操作以及控制器和代理之间的相应TCP连接关联的流量。

```
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
```

影响

此类丢弃可能导致代理出现问题，无法正确接收和处理来自控制器的指令以管理网络的转发平面

建议

- 确保网络中或任何阻碍控制器与代理之间通信的设备上没有发现重复的流量。
- 检验L2网络是否不不稳定（STP或环路）。

排除CoPP丢弃故障

对CoPP违规进行故障排除的第一步是确定：

- 问题的影响和范围。
- 了解环境中的流量以及交换机在受影响通信中的作用。
- 确定相关类上是否存在可疑的违规，然后根据需要进行迭代。

例如，已检测到列出的行为：

- 设备无法与其网络外部的其他设备通信，但可以在本地通信。
- 影响已隔离到VLAN外部的路由通信，且交换机充当默认网关。
- 检查主机表明他们无法ping通网关。检查其ARP表后，网关条目仍保留为Incomplete。
- 具有网关解决的所有其他主机没有通信问题。如果检查交换机上用作网关的CoPP，则表明存在违规行 copp-system-p-class-normal为。

<#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，多个命令检查显示丢弃正在增加。
- 这些违规可能会导致合法ARP流量被丢弃，从而导致拒绝服务行为。

需要重点强调的是，CoPP会隔离对特定类（在本例中为ARP和copp-system-p-class-normal）相关流量的影响。与其他类（例如OSPF、BGP）相关的流量不会被CoPP丢弃，因为它们完全属于不同的类。如果不选中该复选框，ARP问题可能会级联到其他问题，从而影响最初依赖它的协议。例如，如果ARP缓存超时，并且由于发生过多违规事件而没有刷新，TCP会话（如BGP）可以终止。

- 建议执行控制平面检查，例如Ethanalyzer、CPU-mac带内统计信息和CPU进程，以进一步隔离问题。

Ethanalyzer

由于CoPP管制的流量仅与CPU绑定的流量相关联，最重要的工具之一是Ethanalyzer。此工具是TShark的Nexus实施，允许捕获和解码管理引擎发送和接收的流量。它还可以使用基于不同条件的过滤器，例如协议或报头信息，因此成为确定CPU发送和接收的流量的宝贵工具。

建议首先检查Ethanalyzer工具在终端会话上直接运行或发送到文件以供分析时主管所看到的ARP流量。可以定义过滤器和限制，将捕获集中到特定模式或行为中。为此，请添加灵活的显示过滤器。

一个常见的误解是Ethanalyzer可捕获通过交换机的所有流量。主机之间的数据平面流量由硬件ASIC在数据端口之间交换或路由，不需要CPU参与，因此通常不会被Ethanalyzer捕获看到。要捕获数据平面流量，建议使用ELAM或SPAN等其他工具。例如，要过滤ARP，请使用命令：

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

重要的可配置字段：

- interface inband — 是指定向到SUP的流量
- display-filter arp — 指应用的鲨鱼过滤器，大多数Wireshark过滤器被接受
- limit-captured-frames 0 — 表示限制，0表示无限制，直到被另一个参数停止或由Ctrl+C手动停止
- autostop duration 60 — 表示Ethanalyzer在60秒后停止，因此创建在CPU上看到的60秒ARP流量的快照

Ethanalyzer输出重定向到带有> arpcpu的bootflash上的文件，以便手动处理。60秒后，捕获完成，Ethanalyzer动态终止，文件arpcpu位于交换机的bootflash上，然后对其进行处理以提取最大流量生成者。例如：

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

此筛选器的排序依据为：源列和目标列，然后找到的唯一匹配项（但忽略日期列），对实例进行计数并添加所看到的数量，最后根据计数对从上到下排序，并显示前50个结果。

在本实验示例中，在60秒内，从3台设备接收了超过600个ARP数据包，这些设备已被识别为可疑违规设备。过滤器上的第一列详细列出了在指定持续时间内捕获文件中发现此事件的实例数。

了解Ethanalyzer工具对带内驱动程序起作用非常重要，带内驱动程序实质上是与ASIC的通信。理论上，数据包需要通过内核和数据包管理器，才能传递到相关进程本身。CoPP和HWRL在Ethanalyzer上看到流量之前采取行动。即使违规活动在增加，某些流量仍然会通过并在警用速率内保持一致，这有助于深入了解传送到CPU的流量。这是一个重要的区别，因为Ethanalyzer上看到的流量不是违反CIR并被丢弃的流量。

Ethanalyzer也可以以开放方式使用，无需指定任何显示过滤器或捕获过滤器来捕获所有相关SUP流量。这可用作隔离措施，作为故障排除方法的一部分。

有关Ethanalyzer的更多详情和用法，请参阅TechNote:

Ethanalyzer on Nexus 7000故障排除指南

在Nexus平台上使用Ethanalyzer进行控制平面和数据平面流量分析

注意：在8.X代码发行版之前，Nexus 7000只能通过管理VDC执行Ethanalyzer捕获，其中包含来自所有VDC的SUP约束流量。特定于VDC的Ethanalyzer在8.X代码中存在。

CPU-MAC带内统计信息

与CPU绑定的流量关联的带内统计信息会保留带内TX/RX CPU流量的相关统计信息。可使用命令：检查这些统计信息show hardware internal cpu-mac inband stats，该命令提供对当前速率和峰值速率统计信息的深入了解。

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

作为一种最佳实践，建议创建和跟踪基线，因为由于交换机和基础架构的作用，的输出会大 **show hardware internal cpu-mac inband stats** 大变化。在此实验环境中，通常值和历史峰值通常不超过几百个pps，因此这是异常的。该命令 **show hardware internal cpu-mac inband events** 还可用作历史参考，因为它包含与峰值使用量和检测到该命令的时间相关的数据。

进程CPU

Nexus交换机是基于Linux的系统，Nexus操作系统(NXOS)利用CPU抢占式调度程序、多任务处理以及各自核心架构的多线程处理来提供对所有进程的公平访问，因此尖峰并不总是指示问题。但是，如果发现持续的流量违规，则相关进程可能也会大量使用并显示为排名靠前的资源（位于CPU输出下）。对CPU进程拍摄多个快照，以验证特定进程是否被大量使用，方法是使用 **show processes cpu sort | exclude 0.0 or show processes cpu sort | grep <process>**:。

进程CPU、带内统计信息和Ethanalyzer验证可深入了解管理引擎当前处理的进程和流量，并帮助隔离控制平面流量上可能级联到数据平面问题的持续不稳定性。了解CoPP是一种保护机制是非常重要的。它是反作用的，因为它只对传送到SUP的流量起作用。它旨在通过丢弃超出预期范围的流量速率来维护管理引擎的完整性。并非所有丢包都表示存在问题或需要干预，因为它们的重要性取决于具体的CoPP类别以及基于基础架构和网络设计的已验证的影响。由于偶发的突发事件造成的丢弃不会转化为影响，因为协议具有内置机制，例如keepalive和可以处理临时事件的重试。将焦点保持在已建立基线之外的持续事件或异常事件。请记住，CoPP必须遵守特定于环境的协议和功能，并且必须进行监控和不断迭代以根据扩展性需求进行优化。如果发生丢弃，请确定CoPP是无意丢弃流量，还是响应故障或攻击。无论发生哪种情况，都可以通过分析对环境的影响和采取纠正措施，来分析情况并评估干预的必要性，这些都可能超出交换机本身的范畴。

Additional Information

最新平台/代码可以通过端口镜像执行SPAN到CPU，并将数据平面流量传送到CPU。这通常受到硬件速率限制和CoPP的严重速率限制。建议谨慎使用SPAN到CPU，这不在本文档的讨论范围之内。

有关此功能的详细信息，请参阅列出的技术说明：

Nexus 9000云扩展ASIC NX-OS SPAN到CPU的过程

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。