Nexusプラットフォームでのコントロールプレーンポリシング違反の確認

内容

はじめに

このドキュメントでは、Cisco Nexusスイッチのコントロールプレーンポリシング(CoPP)と、デフォルト以外のクラス違反に対するその影響について詳しく説明します。

前提条件

Control Plane Policing（CoPP；コントロールプレーンポリシング）、そのガイドラインと制限事項、および一般的な設定に関する基本的な情報、さらにQuality of Service(QoS)ポリシング(CIR)機能について理解しておくことをお勧めします。この機能の詳細については、該当するドキュメントを参照してください。

- Cisco Nexus 9000シリーズNX-OSセキュリティ設定ガイド、リリース10.2(x)
- Nexus 7000 シリーズ スイッチの CoPP
- Cisco Nexus 9000シリーズNX-OS Quality of Serviceコンフィギュレーションガイド、リリース10.2(x)

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアおよびハードウェアの要件に限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

コントロールプレーントラフィックは、リダイレクトアクセスコントロールリスト(ACL)によってスーパーバイザモジュールにリダイレクトされ、ハードウェアレートリミッタとCoPPの2つの保護レイヤを通過する一致したトラフィックをパントするようにプログラムされます。スーパーバイザモジュールの中断や攻撃を放置すると、深刻なネットワーク停止が発生する可能性があります。そのため、CoPPは保護メカニズムとして機能します。コントロールプレーンレベルで不安定な状態が存在する場合は、CoPPを確認することが重要です。これは、ループやフラッド、または不正なデバイスによって作成された異常なトラフィックパターンが原因で、スーパーバイザが正当なトラフィックを処理できなくなるためです。このような攻撃は、不正なデバイスによって不注意で実行されるか、攻撃者によって悪意をもって実行される可能性があり、通常はスーパーバイザモジュールまたはCPU宛てのトラフィックが高頻度で発生します。

Control Plan Policing（CoPP；コントロールプランポリシング）は、インバンド（前面パネル）ポートを介して受信された、ルータアドレス宛てのパケット、またはスーパーバイザの関与が必要なパケットをすべて分類し、ポリシングする機能です。この機能を使用すると、ポリシーマップをコントロールプレーンに適用できます。このポリシーマップは、通常のQuality of Service(QoS)ポリシーのように見え、非管理ポートからスイッチに着信するすべてのトラフィックに適用されます。ポリシングによるスーパーバイザモジュールの保護により、スイッチではパケットの廃棄による各クラスのCommitted Input Rate（CIR；認定入力レート）を超えるトラフィックのフラッドを緩和でき、スイッチへの過剰な負荷やパフォーマンスへの影響を回避できます。

CoPPカウンタを継続的に監視し、その正当性を説明することが重要です。これがこのドキュメントの目的です。CoPP違反がチェックされていないと、コントロールプレーンは関連する該当クラスで正規のトラフィックを処理できなくなります。CoPP設定は、ネットワークおよびインフラストラクチャの要件に対応する必要がある、流動的で継続的なプロセスです。CoPPのデフォルトのシステムポリシーは3つあります。デフォルトでは、最初の出発点とし strict てデフォルトポリシーを使用することを推奨し、このドキュメントの基盤として使用します。

CoPPは、前面パネルポートを介して受信されたインバンドトラフィックにのみ適用されます。アウトオブバンド管理ポート(mgmt0)はCoPPの対象ではありません。Cisco NX-OSデバイスハードウェアは、フォワーディングエンジンごとにCoPPを実行します。したがって、集約トラフィックによってスーパーバイザモジュールが過負荷状態にならないように、レートを選択します。

CIRはすべてのモジュールのCPUに送られるトラフィックの集約に適用されるため、これはエンドオブロー/モジュラスイッチにとって特に重要です。

該当ハードウェア

このドキュメントで説明するコンポーネントは、すべてのCisco Nexusデータセンタースイッチに適用されます。

コントロールプレーンポリシングの解釈

このドキュメントでは、Nexusスイッチで見られる最も一般的で重大なデフォルト以外のクラス違反に対処することを中心に説明します。

標準CoPPデフォルトプロファイル

CoPPの解釈方法を理解するには、最初にプロファイルが適用されていることを確認し、デフォルトプロファイルまたはカスタムプロファイルがスイッチに適用されているかどうかを理解する必要があります。

注：ベストプラクティスとして、すべてのNexusスイッチでCoPPを有効にする必要があります。この機能が有効になっていない場合、異なるプラットフォームがスーパーバイザ(SUP)に送られるトラフィックを制限する可能性があるため、すべてのコントロールプレーントラフィックが不安定になる可能性があります。たとえば、Nexus 9000でCoPPが有効になっていない場合、SUP宛てのトラフィックは50 ppsにレート制限されるため、スイッチはほとんど動作不能になります。CoPPは、Nexus 3000およびNexus 9000プラットフォームの要件と見なされます。

CoPPが有効になっていない場合は、 **setup** コマンドを使用するか、設定オプションの下にある標準デフォルトポリシーの1つを適用して、スイッチで再び有効にしたり、設定したりでき copp profile [dense|lenient|moderate|strict]ます。

保護されていないデバイスでは、トラフィックが適切にクラスに分類および分離されないため、特定の機能またはプロトコルに対するサービス拒否(DoS)の動作はその範囲に限定されず、コントロールプレーン全体に影響する可能性があります。

注:CoPPポリシーは、Ternary Content-Addressable Memory(TCAM)分類リダイレクトによって実装され、また **show system internal access-list input statistics module X | b CoPP** は **show hardware access-list input entries detail**で直接確認できます。

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

コントロールプレーンポリシングクラス

CoPPは、IPまたはMAC ACLに対応する一致に基づいてトラフィックを分類します。したがって、どのトラフィックがどのクラスに分類されるかを理解することが重要です。

これらのクラスはプラットフォームによって異なります。したがって、クラスの確認方法を理解することが重要です。

たとえば、Nexus 9000のトップオブラック(TOR)では次のようになります。

```
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
...
```

この例では、クラスマップはBorder Gateway Protocol(BGP)、Open Shortest Path First(OSPF)、Enhanced Interior Gateway Router Protocol(EIGRP)などのルーティングプロトコルに関連するトラフィックを copp-system-p-class-critical 含み、vPCなどの他のプロトコルを含みます。

IPまたはMAC ACLの命名規則は、関連するプロトコルまたは機能のプレフィックスを含めて、ほとんど説明を要しま copp-system-p-acl-[protocol|feature]せん。

特定のクラスを表示するには、**show**コマンドの実行中にクラスを直接指定できます。例：

```
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

通常、CoPPデフォルトプロファイルはデフォルト設定の一部として非表示になっていますが、 **show running-conf copp all**次のコマンドで設定を確認できます。

<#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)
...
```

前に示したクラスマップ copp-system-p-class-criticalは、デフォルトで非表示になっているシステムACLを呼び出す複数のmatchステートメントを参照し、一致する分類を参照します。たとえば、BGPの場合は次のようになります。

<#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)
```

これは、すべてのBGPトラフィックがこのクラスに一致し、その同じクラスの他のすべてのプロトコルとともに copp-system-p-class-criticalに分類されることを意味します。

Nexus 7000は、Nexus 9000と非常によく似たCoPP機能構造を使用します。

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

Nexus 7000ではモジュラスイッチであるため、クラスがモジュールで分割されますが、CIRはすべてのモジュールの集約に適用され、CoPPはシャーシ全体に適用されます。CoPPの検証と出力は、デフォルトまたは管理Virtual Device Context(VDC)からのみ確認できます。

コントロールプレーンの問題が発生した場合は、Nexus 7000でCoPPを確認することが特に重要です。これは、CoPP違反を引き起こす過剰なCPUバウンドトラフィックがあるVDCの不安定さが、他のVDCの安定性に影響を与える可能性があるためです。

Nexus 5600では、クラスが異なります。したがって、BGPの場合は独自の個別のクラスになります。

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)

Nexus 3100には3つのルーティングプロトコルクラスがあるため、BGPがどのクラスに属するかを確認するには、参照される4つのCoPP ACLを相互参照します。
EIGRPは、Nexus 3100上で独自のクラスによって処理されます。

<#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

この場合、BGPはACLによって照合されるため、 copp-system-acl-routingproto1CoPPクラスBGPはBGPに分類され copp-s-routingProto1ます。

コントロールプレーンポリシングの統計情報とカウンタ

CoPPはQoS統計情報をサポートし、すべてのモジュールについて、特定のクラスの認定入力レート(CIR)を確認または違反するトラフィックの集約カウンタを追跡します。

各クラスマップは、対応するクラスに基づいてCPUバウンドトラフィックを分類し、その分類に該当するすべてのパケットにCIRを付加します。例として、BGPトラフィックに関連するクラスを参照として使用します。

Nexus 9000トップオブラック(TOR)で次を実行し copp-system-p-class-criticalます。

<#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-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
```

クラスマップのセクションで、matchステートメントの後に、クラス内のすべてのトラフィックに関連するアクションが表示されます。内に分類されcopp-system-p-class-critical るすべてのトラフィックは、7のサービスクラス(CoS)で設定されます。これは、最も優先順位の高いトラフィックであり、このクラスは、36000 kbpsのCIRおよび1280000バイトのcommitted-burst-rate（CBR；認定バーストレート）でポリシングされます。

このポリシーに準拠するトラフィックはSUPに転送されて処理され、違反はドロップされます。

<#root>

set cos 7

police cir 36000 kbps , bc 1280000 bytes

次のセクションでは、モジュールに関する統計情報を示します。トップオブラック(TOR)スイッチでは、モジュール1はスイッチを指します。

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

出力に表示される統計情報は履歴であるため、コマンド実行時の現在の統計情報のスナップショットが提供されます。

ここでは、送信セクションと廃棄セクションの2つのセクションを解釈します。
送信されたデータポイントは、ポリシーに準拠するすべての送信パケットを追跡します。このセクションは、スーパーバイザが処理するトラフィックのタイプに関する情報を提供するため重要です。

提供レートの5分間の値から、現在のレートを把握できます。
適合したピークレートと日付は、ポリシー内およびポリシーが発生した時間に適合した、秒単位の最大ピークレートのスナップを提供します。
新しいピークが見られる場合は、この値と日付が置き換えられます。

統計情報の最も重要な部分は、ドロップされたデータポイントです。送信された統計情報と同様に、ドロップされたセクションは、ポリシングレートの違反によってドロップされた累積バイト数を追跡します。 また、過去5分間の違反率、違反したピーク、ピークがある場合はそのピーク違反のタイムスタンプも表示されます。繰り返しますが、新しいピークが見つかった場合は、この値と日付を置き換えます。他のプラットフォームでは、出力は異なりますが、ロジックは非常によく似ています。

Nexus 7000は同じ構造を使用し、検証は同じですが、参照されるACLによってクラスが若干異なる場合があります。

<#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
```

Nexus 5600の場合：

<#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;

レートやピークに関する情報は提供されませんが、適合および違反された集約バイトは提供されます。

Nexus 3100では、コントロールプレーン出力にOutPacketsとDropPacketsが表示されます。

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は適合パケットを参照し、DropPacketsはCIRの違反を参照します。このシナリオでは、関連付けられたクラスでドロップが発生していません。

Nexus 3500では、出力にHWとSWが一致したパケットが表示されます。

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は、HW内でACLによって照合されるパケットを示します。ソフトウェアが一致するパケットは、ポリシーに準拠するパケットです。HWとSWが一致するパケット間の違いは、違反を意味します。

この場合、値が一致するため、ルーティングプロトコル1クラスパケット（BGPを含む）でドロップは見られません。

アクティブドロップ違反のチェック

コントロールプレーンポリシングの統計情報は履歴であるため、アクティブな違反が増加しているかどうかを判断することが重要です。このタスクを実行する標準的な方法は、2つの完全な出力を比較し、違いを確認することです。

このタスクは手動で実行することも、Nexusスイッチが出力の比較を支援するdiffツールを提供することもできます。

出力全体を比較することはできますが、ドロップされた統計情報だけに焦点を当てるため、このコマンドは必要ありません。したがって、CoPP出力はフィルタリングして、違反だけに焦点を当てることができます。

コマンドは、次のとおりです。 show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y

---

注：現在の出力と前の出力を比較できるようにするには、このコマンドを2回実行する必要があります。

```
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;
```

前述のコマンドを使用すると、2つのクラス間のデルタを表示し、違反の増加を検出できます。

注:CoPP統計情報は履歴であるため、コマンドの実行後に統計情報をクリアして、アクティブな増加があるかどうかを確認するという方法も推奨されます。CoPP統計情報をクリアするには、コマンドを実行します。 **clear copp statistics**.

CoPPドロップのタイプ

CoPPは単純なポリシング構造であり、CIRに違反するCPUバウンドトラフィックはすべてドロップされます。それでも、この影響はドロップのタイプによって大きく異なります。

ロジックは同じですが、宛先が同じIPアドレスを持つトラフィックを 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

クラスマップ宛ての廃棄トラフィックと比較し copp-system-p-class-monitoringます。

```
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
```

最初のプロトコルは主にルーティングプロトコルを扱い、2番目のプロトコルは最も低い優先順位とCIRの1つを持つインターネット制御メッセージプロトコル(ICMP)を扱います。CIRの差は100倍です。したがって、クラス、影響、一般的なチェック/検証、および推奨事項を理解することが重要です。

CoPP のクラス

クラスモニタリング – copp-system-p-class-monitoring

このクラスには、IPv4、IPv6のICMP、および対象のスイッチ宛てのトラフィックのtracerouteが含まれます。


```
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

パケット損失または遅延のトラブルシューティングを行う際によく誤解されるのは、インバンドポートを介してスイッチにpingを実行することです。このポートはCoPPによってレート制限されています。CoPPはICMPに対して高度なポリシングを行うため、トラフィックや輻輳が少ない場合でも、インバンドインターフェイスに対するpingがCIRに違反すると、パケット損失を直接確認できます。

たとえば、パケットペイロードが500のルーテッドポートに直接接続されたインターフェイスに対してpingを実行すると、定期的に廃棄が発生する可能性があります。

<#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
```

ICMPパケットの宛先であるNexusで、違反が検出されてCPUが保護されると、CoPPによってそれらのパケットがドロップされたことがわかります。

<#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

遅延やパケット損失のトラブルシューティングを行うには、コントロールプレーントラフィックとなるスイッチ自体を宛先とするホストではなく、データプレーンによってスイッチ経由で到達可能なホストを使用することをお勧めします。データプレーントラフィックはスーパーバイザの介入なしでハードウェアレベルで転送/ルーティングされるため、CoPPによってポリシングされず、通常はドロップが発生しません。

推奨事項

- パケット損失の誤検出の結果を確認するには、スイッチではなくデータプレーンを介してスイッチにpingを送信します。
- Network Monitoring System（NMS；ネットワーク監視システム）またはICMPを積極的に使用するツールをスイッチに制限して、クラスのCommitted Input Rate（CIR；認定入力レート）のバーストを回避します。CoPPは、クラスに分類されるすべての集約トラフィックに適用されることに注意してください。

クラス管理 – copp-system-p-class-management

ここに示すように、このクラスには、IPv4およびIPv6通信用の通信(SSH、Telnet)、転送(SCP、FTP、HTTP、SFTP、TFTP)、クロック(NTP)、AAA(Radius/TACACS)、およびモニタリング(SNMP)に使用できるさまざまな管理プロトコルが含まれます。

```
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

このクラスに関連する最も一般的な動作またはドロップは次のとおりです。

- SSH/Telnetで接続するとCLIの速度が低下すると認識される。クラスにアクティブなドロップがある場合、通信セッションが遅くなり、ドロップに苦しむ可能性があります。
- スイッチ上でFTP、SCP、SFTP、TFTPプロトコルを使用してファイルを転送します。最も一般的な動作は、インバンド管理ポートによるsystem/kickstartブートイメージの転送です。これにより、転送時間が長くなり、クラスの集約帯域幅によって決定される送信セッションが閉じられたり終了したりする可能性があります。
- NTPの同期に問題がある場合、このクラスは不正なNTPエージェントや攻撃を軽減するため、重要です。
- AAA RadiusおよびTACACSサービスもこのクラスに属します。このクラスに影響が及ぶと、スイッチでのユーザアカウントの認可および認証サービスに影響が及ぶ可能性があります。これは、CLIコマンドの遅延の原因にもなります。
- SNMPもこのクラスでポリシングされます。SNMPクラスによるドロップが原因で見られる最も一般的な動作は、ウォーク、バルクコレクション、またはネットワークスキャンを実行するNMSサーバ上です。周期的な不安定性が発生した場合、通常はNMS収集スケジュールに関連付けられる。

推奨事項

- CLIの速度低下がこのクラスでのドロップとともに認識される場合は、コンソールアクセス(mgmt0)または管理アウト

オブバンドアクセス(mgmt0)を使用します。

- システムイメージをスイッチにアップロードする必要がある場合は、アウトオブバンド管理ポート(mgmt0)を使用するか、USBポートを使用して最も高速に転送します。

- NTPパケットが失われた場合は、show ntp peer-statusを確認し、到達可能性カラムを確認します。廃棄は377に変換されません。

- AAAサービスで問題が発生した場合、動作が軽減されるまで、ローカル専用ユーザを使用してトラブルシューティングを行います。

- SNMPの問題に対する緩和策には、攻撃性の低い動作、ターゲットを絞った収集、ネットワークスキャナの最小化などがあります。スキャナからCPUレベルで発生するイベントまでの定期的な時間を調べます。

クラスL3ユニキャストデータ – copp-system-p-class-l3uc-data

このクラスは、特に収集パケットを扱います。このタイプのパケットは、ハードウェアレートリミッタ(HWRL)でも処理されます。

着信IPパケットがラインカードで転送されるときにネクストホップのアドレス解決プロトコル(ARP)要求が解決されない場合、ラインカードはパケットをスーパーバイザモジュールに転送します。

スーパーバイザは、ネクストホップのMACアドレスを解決し、ハードウェアをプログラムします。

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

これは通常、スタティックルートが使用され、ネクストホップが到達不能または未解決の場合に発生します。

ARP要求が送信されると、ソフトウェアは/32ドロップ隣接関係をハードウェアに追加して、同じネクストホップIPアドレスへのパケットがスーパーバイザに転送されないようにします。ARPが解決されると、ハードウェアエントリが正しいMACアドレスで更新されます。ARPエントリがタイムアウト期間の前に解決されない場合、そのエントリはハードウェアから削除されます。

注:CoPPとHWRLは連携して動作し、CPUが確実に保護されます。これらは同様の機能を実行するように見えますが、HWRLが最初に発生します。実装は、ASICのフォワーディングエンジンで特定の機能が実装されている場所に基づきます。このシリアルアプローチにより、CPUに送られるすべてのパケットをレート化する細分性とマルチレイヤの保護が可能になります。

HWRLは、モジュール上のインスタンス/フォワーディングエンジンごとに実行され、コマンド**show hardware rate-limiter**で表示できます。HWRLは、このテクニカルドキュメントの範囲外です。

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

- データプレーントラフィックはハードウェアで処理できないため、違反としてスーパーバイザにパントされ、CPUに負荷がかかります。

推奨事項

- 収集ドロップを最小限に抑えるためのこの問題の一般的な解決策は、ネクストホップが到達可能であることを確認し、次の設定コマンドで収集スロットリングを有効にすることです。 **hardware ip glean throttle**.

Nexus 7000 8.4(2)では、M3およびF4モジュールのグリーニング隣接関係に対するブルーム型フィルタのサポートも導入されました。詳細については、『Cisco Nexus 7000シリーズNX-OSユニキャストルーティングコンフィギュレーションガイド』を参照してください。

到達不能なネクストホップアドレスを使用するスタティックルート設定を確認するか、RIBからそのようなルートを動的に削除するダイナミックルーティングプロトコルを使用します。

クラスCritical - class-map copp-system-p-class-critical

このクラスは、IPv4とIPv6、(RIP、OSPF、EIGRP、BGP)、auto-RP、仮想ポートチャネル(vPC)、l2pt、およびIS-ISのルーティングプロトコルを含む、L3の観点から最も重要なコントロールプレーンプロトコルを参照します。

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

ルーティングプロトコルへの転 copp-system-p-class-critical 送の不安定性によるドロップ。これには、隣接関係のドロップやコンバージェンス障害、アップデート/NLRI伝播などが含まれます。
このクラスでの最も一般的なポリシーのドロップは、ネットワーク上の不正なデバイスが（設定の誤りや障害により）異常な動作をしたり、拡張性に問題がある場合に発生する可能性があります。

推奨事項

- 上位層プロトコルの継続的な再コンバージェンスを引き起こす不正なデバイスやL2の不安定さなどの異常が検出されない場合は、スケールに対応するためにCoPPまたはより寛大なクラスのカスタム設定が必要になる場合があります。

- 既存のデフォルトプロファイルからカスタムCoPPプロファイルを設定する方法については、『CoPP設定ガイド』を参照してください。
CoPPベストプラクティスポリシーのコピー

クラスが重要 – copp-system-p-class-important

このクラスは、HSRP、VRRP、およびLLDPを含むファーストホップ冗長プロトコル(FHRP)に関連しています

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

ここで見られるドロップにつながる最も一般的な動作は、レイヤ2の不安定性に関する問題で、デバイスがアクティブ状態（スプリットブレイン）に移行するシナリオ、アグレッシブタイマー、設定の誤り、または拡張性につながります。

推奨事項：

- FHRPに対して、グループが適切に設定され、ロールがアクティブ/スタンバイまたはプライマリ/セカンダリのいずれかであり、適切にネゴシエートされていること、および状態にフラップがないことを確認します。
- L2でのコンバージェンスの問題またはL2ドメインのマルチキャスト伝播の問題を確認します。

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

L2 unpolicedクラスは、すべての上位層プロトコルの基盤となる重要なレイヤ2プロトコルすべてを指すため、最も高いCIRと優先度を持つほとんどポリシングされていないと見なされます。

このクラスは、実質的に、スパニングツリープロトコル(STP)、リンク集約コントロールプロトコル(LACP)、Cisco Fabric Service over Ethernet(CFSoE)を処理します

```
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
```

このクラスのポリシングCIRは50 Mbpsで、すべてのクラスの中で最高であり、バーストレートの吸収率も最高です。

影響

このクラスのドロップは、データ、コントロール、および管理プレーン上のすべての上位層プロトコルと通信が基盤となるレイヤ2の安定性に依存するため、グローバルな不安定につながります。

STP違反に関する問題は、TCNおよびSTPコンバージェンスの問題を引き起こす可能性があります。これには、STPのクレーム、MACのフラッシュ、移動、および無効な動作の学習などが含まれ、到達可能性の問題を引き起こし、トラフィックループを引き起こしてネットワークを不安定にする可能性があります。

このクラスはLACPも参照するため、0x8809に関連付けられたすべてのEtherTypeパケットを処理します。これには、ポートチャネルボンディングの状態を維持するために使用されるすべてのLACPDUが含まれます。このクラスが不安定になると、LACPDUがドロップされた場合にポートチャネルがタイムアウトする可能性があります。

Cisco Fabric Service over Ethernet(CSFoE)はこのクラスに属し、Nexusスイッチ間の重要なアプリケーション制御状態の通信に使用されます。そのため、安定性を確保することが不可欠です。

同じことが、CDP、UDLD、VTPなど、このクラス内の他のプロトコルにも当てはまります。

推奨事項

- 最も一般的な動作は、L2イーサネットの不安定性に関連しています。関連する機能拡張を利用してSTPが確定的な方法で適切に設計され、ネットワーク内の再コンバージェンスや不正なデバイスの影響が最小限に抑えられていることを確認します。L2拡張に参加しないすべてのエンドホストデバイスに対して適切なSTPポートタイプが設定され、TCNを最小限に抑えるためにエッジ/エッジトランクポートとして設定されていることを確認します。

- BPDUguard、Loopguard、BPDUfilter、RootGuardなどのSTP拡張機能を適宜使用して、障害の範囲、またはネットワーク上の誤設定や不正なデバイスに関する問題を制限します。

- 『Cisco Nexus 9000 NX-OSレイヤ2スイッチングコンフィギュレーションガイド、リリース10.2(x)』を参照してください。

- MACラーニングとフラッシュの無効化につながる可能性があるMAC移動動作を確認します。詳細：Nexus 9000 Mac移動のトラブルシューティングと防止方法

クラスマルチキャストルータ – class-map copp-system-p-class-multicast-router

このクラスは、データプレーンパス内のすべてのPIM対応デバイスを経由するルーテッドマルチキャスト共有ツリーの確立と制御に使用されるコントロールプレーンProtocol Independent Multicast(PIM)パケットを指します。このクラスには、First-Hop Router(FHR)、Last-Hop Router(LHR)、Intermediate-Hop Router(IHR)、およびRendezvous Point(RP)が含まれます。このクラスに分類されるパケットには、送信元に対するPIM登録、IPv4とIPv6の両方に対する受信者に対するPIM join、通常はPIM(224.0.0.13)宛てのトラフィック、およびMulticast Source Discovery Protocol(MSDP)が含まれます。追加のクラスがいくつかあることに注意してください。追加のクラスは、異なるクラスで処理されるマルチキャストまたはRP機能の非常に特殊な部分を扱います。

```
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

このクラスに関連するドロップに対する主な影響は、RPへのPIM登録によってマルチキャスト送信元に通信する問題、またはPIM joinが適切に処理されず、マルチキャストストリームの送信元またはRPへの共有パスツリーまたは最短パスツリーが不安定になる問題に関連しています。動作には、参加がないために正しく入力されていない発信インターフェイスリスト(OIL)、または環境全体で一貫して見られない(S、G)、(*、G)などがあります。また、相互接続にMSDPに依存するマルチキャストルーティングドメイ

ン間でも問題が発生する可能性があります。

推奨事項

- PIM制御関連の問題で最も一般的な動作は、スケールの問題、つまり不正な動作です。最も一般的な動作の1つは、UPnPでの実装が原因で発生し、メモリ枯渇の問題を引き起こす可能性があります。これは、フィルタと不正デバイスの範囲の縮小によって対処できます。デバイスのネットワーク役割に依存するマルチキャスト制御パケットを軽減およびフィルタリングする方法の詳細については、『Nexus 7K/N9Kでのマルチキャストフィルタリングの設定：シスコ

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

このクラスは、マルチキャストリスナー検出(MLD)、特にMLDクエリ、レポート、リダクション、およびMLDv2パケットタイプを参照します。MLDは、ホストが特定のグループのマルチキャストデータを要求するために使用するIPv6プロトコルです。MLDによって取得された情報を使用して、マルチキャストグループまたはチャネルメンバーシップのリストがインターフェイスごとに保持されます。MLDパケットを受信するデバイスは、要求されたグループまたはチャネルに対して受信したマルチキャストデータを、既知のレシーバのネットワークセグメントから送信します。MLDv1はIGMPv2から取得され、MLDv2はIGMPv3から取得されます。IGMPはIPプロトコル2メッセージタイプを使用し、MLDはICMPv6メッセージのサブセットであるIPプロトコル58メッセージタイプを使用します。

```
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

このクラスでのドロップは、リンクローカルIPv6マルチキャスト通信の問題に変換され、受信者からのリスナーレポートまたは一般的なクエリへの応答がドロップされる原因となり、ホストが受信するマルチキャストグループの検出を妨げる可能性があります。これはスヌーピングメカニズムに影響を与え、トラフィックを要求した予想されるインターフェイスを介してトラフィックを適切に転送しない可能性があります。

推奨事項

- MLDトラフィックはIPv6のリンクローカルレベルでは重要であるため、このクラスでドロップが発生した場合、最も一般的な原因はスケール、L2の不安定性、または不正なデバイスに関連しています。

クラスレイヤ3マルチキャストデータ – copp-system-p-class-l3mc-data およびクラスレイヤ3マルチキャストIPv6データ – copp-system-p-class-l3mcv6-data

これらのクラスは、SUPへのマルチキャスト例外リダイレクションに一致するトラフィックを参照します。この場合、これらのクラスで処理される条件は2つあります。1つ目はReverse Path Forwarding（RPF；リバースパス転送）の障害で、2つ目は宛先ミスです。宛先ミスとは、レイヤ3マルチキャスト転送テーブルに対するハードウェアでのルックアップが失敗し、データパケットがCPUにパントされるマルチキャストパケットのことです。これらのパケットは、マルチキャストコントロールプレーンをトリガー/インストールし、データプレーントラフィックに基づいてハードウェア転送テーブルエントリを追加するために使用されること

があります。RPFに違反するデータプレーンマルチキャストパケットもこの例外に一致し、違反として分類されます。

```
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障害と宛先ミスは、マルチキャストルータを通過するトラフィックフローに関連する設計または設定の問題を意味します。宛先ミスは状態の作成時に一般的に発生し、ドロップは(*, G)、(S, G)の障害のプログラミングと作成につながる可能性があります。

推奨事項

- RPF障害が発生した場合は、基本的なユニキャストRIB設計を変更するか、スタティックなmrouteを追加して、特定のインターフェイスを介してトラフィックを誘導します。
- 「RPF障害が原因でルータがマルチキャストパケットをホストに転送しない」を参照してください。

クラスIGMP: copp-system-p-class-igmp

このクラスは、特定のグループのマルチキャストデータを要求するために使用され、レイヤ2で目的の受信者にトラフィックを転送するグループおよび関連するOutgoing Interface List（OIL；発信インターフェイスリスト）を維持するためにIGMPスヌーピング機能によって使用される、すべてのバージョンのすべてのIGMPメッセージを参照します。IGMPメッセージは、RFC2236(Internet Group Management Protocol, Version 2)で文書化されているように、存続可能時間(TTL)が1である必要があるため、レイヤ3境界を通過しないため、ローカルで意味を持ちます。このクラスで処理されるIGMPパケットには、すべてのメンバーシップクエリ（一般クエリまたは送信元/グループ固有クエリ）と、メンバーシップが含まれ、レシーバーからのレポートが残されます。

```
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

このクラスでのドロップは、違反が原因でドロップされたIGMPメッセージのタイプに応じて、送信元と受信側の間のマルチキャスト通信のすべてのレベルで問題に変換されます。レシーバからのメンバーシップレポートが失われた場合、ルータはトラフィッ

クに関連するデバイスを認識しないため、関連する発信インターフェイスリストにインターフェイスまたはVLANが含まれません。このデバイスがクエリアまたは代表ルータでもある場合、送信元がローカルのレイヤ2ドメインを越えている場合、このデバイスはRPに向けて関連するPIM joinメッセージをトリガーしません。したがって、このデバイスは、受信側またはRPまでのマルチキャストツリー全体でデータプレーンを確立することはありません。脱退レポートが失われても、受信側は引き続き不要なトラフィックを受信する可能性があります。これは、ドメイン内のマルチキャストルータ間のクエリアおよび通信によってトリガーされるすべての関連IGMPクエリにも影響を与える可能性があります。

推奨事項

- IGMPドロップに関連する最も一般的な動作は、L2の不安定性、タイマーの問題、またはスケールに関連しています。

クラス標準 – copp-system-p-class-normalcopp-system-p-class-normal

このクラスは、標準ARPトラフィックに一致するトラフィックを参照し、ポートベースのネットワークアクセス制御に使用される802.1Xに関連するトラフィックも含みます。これは、ARP要求、Gratuitous ARP、リバースARPパケットがブロードキャストされ、レイヤ2ドメイン全体に伝搬されるため、違反が発生する最も一般的なクラスの1つです。ARPパケットはIPパケットではなく、L3ヘッダーを含まないため、L2ヘッダーの範囲だけで決定されることに注意してください。ルータが、スイッチ仮想インターフェイス(SVI)などそのサブネットに関連付けられたIPインターフェイスを使用して設定されている場合、ルータはARPパケットがハードウェアブロードキャストアドレス宛てであるために、SUPにARPパケットをパントして処理されるようにします。ブロードキャストストーム、レイヤ2ループ（STPまたはフラップによる）、またはネットワーク内の不正デバイスは、ARPストームを引き起こし、違反が大幅に増加する可能性があります。

```
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

このクラスでの違反の影響は、イベントの期間と環境でのスイッチの役割に大きく依存します。このクラスでのドロップは、ARPパケットが現在廃棄されているため、SUPエンジンによって処理されないことを意味し、不完全なARP解決によって引き起こされる2つの主な動作の原因となる可能性があります。

エンドホストの観点から見ると、ネットワーク内のデバイスはスイッチでアドレス解決を解決または完了できません。このデバイスがセグメントのデフォルトゲートウェイとして機能すると、デバイスがゲートウェイを解決できなくなり、L2イーサネットセグメント(VLAN)の外部にルーティングできなくなる可能性があります。ローカルセグメント上の他のエンドホストのARP解決を完了できるデバイスは、ローカルセグメント上で引き続き通信できます。

スイッチの観点から見ると、ストームと違反が蔓延している場合、スイッチが生成したARP要求のプロセスを完了できない原因にもなる可能性があります。これらの要求は、通常、ネクストホップまたは直接接続されたサブネットの解決のために生成されます。ARP応答は本質的にユニキャストですが、スイッチが所有するMACにアドレス指定されているため、ARPパケットであるため、この同じクラスに分類されます。これは、ネクストホップが解決されない場合にスイッチがトラフィックを適切に処理できず、隣接関係マネージャにホストのエントリがない場合にレイヤ2ヘッダーの書き換えに問題が発生する可能性があるため、到達可能

性の問題に変換されます。

この影響は、ARP違反を引き起こした基本的な問題の範囲によっても異なります。たとえば、ブロードキャストストームでは、ホストとスイッチは隣接関係を解決するためにARPを継続し、ネットワーク上で追加のブロードキャストトラフィックが発生する可能性があります。ARPパケットはレイヤ2であるため、レイヤ3の存続可能時間(TTL)が存在せずL2ループが切断されず、ループが継続して発生し、ループが切断されるまでネットワークが指数関数的に拡大します。

推奨事項

- STP、フラップ、不正デバイスなど、環境でARPストームを引き起こす可能性がある基本的なL2の不安定性を解決します。必要に応じて、リンクパスを開く任意の方法でループを切断します。
- ストーム制御は、ARPストームの緩和にも使用できます。ストーム制御が有効になっていない場合は、インターフェイスのカウンタ統計情報を調べて、インターフェイスを通過する合計トラフィックに対する、インターフェイス上のブロードキャストトラフィックの割合を確認します。
- ストームは発生していないが、環境で継続的なドロップが発生する場合は、SUPトラフィックを確認して、正当なトラフィックに影響を与える可能性がある不正なデバイス（ネットワーク上でARPパケットを絶えず送信しているデバイス）を特定します。
- 増加を確認できる状況は、ネットワーク上のホストの数と環境上のスイッチの役割によって異なります。ARPはエントリの再試行、解決、および更新を行うように設計されているため、ARPトラフィックが常に確認されると想定されています。散発的なドロップだけが見られる場合は、ネットワーク負荷が原因で一時的にドロップが発生している可能性があり、影響は認識されません。ただし、ネットワークを監視して把握し、予測される状況と異常な状況を適切に特定して区別することが重要です。

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

このクラスは、ICMPメッセージを使用してネイバーのローカルリンク層アドレスを決定するIPv6ネイバー探索/アドバタイズメントおよびルータ要請/アドバタイズメントパケットに関連するトラフィックを参照し、ネイバーデバイスの到達可能性と追跡に使用されます。

```
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

このクラスの違反は、ネイバーデバイス間のIPv6通信を妨げる可能性があります。これらのパケットは、ローカルリンク上のホストとルータ間のダイナミックな検出またはリンクレイヤ/ローカル情報を容易にするために使用されるためです。この通信が切断されると、関連するローカルリンクを越えた、またはローカルリンクを介した到達可能性に関する問題が発生する可能性があります。IPv6ネイバー間に通信の問題がある場合は、このクラスでドロップが発生していないことを確認します。

推奨事項

- ネイバーデバイスからの異常なICMP動作、特にネイバー探索やルータ探索に関連する異常なICMP動作を調べます。

- 定期的なメッセージに対して予想されるすべてのタイマー値とインターバル値が、環境全体で一致し、受け入れられることを確認します。たとえば、ルータアドバタイズメントメッセージ（RAメッセージ）の場合です。

クラス標準DHCP - copp-system-p-class-normal-dhcp

このクラスは、IPv4とIPv6の両方で同じローカルイーサネットセグメント上のブートストラッププロトコル（BOOTPクライアント/サーバ）、一般にDynamic Host Control Protocol(DHCP)パケットと呼ばれる関連トラフィックを参照します。これは、Discovery、Offer、Request、およびAcknowledge(DORA)パケット交換全体を通じて、任意のBOOTPクライアントから発信されるか、または任意のBOOTPサーバに宛てられたトラフィック通信にのみ特に関連し、UDPポート546/547を介したDHCPv6クライアント/サーバトランザクションも含まれます。

```
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

このクラスでの違反により、エンドホストがDHCPサーバからIPを適切に取得できなくなり、その結果、自動プライベートIPアドレス(APIPA)の範囲である169.254.0.0/16にフォールバックする可能性があります。このような違反は、デバイスが同時にブートを試行し、クラスに関連付けられたCIRを超える環境で発生する可能性があります。

推奨事項

- ホスト側とDHCPサーバ側のキャプチャで、DORAトランザクション全体が表示されることを確認します。スイッチがこの通信の一部である場合は、処理またはCPUにパントされたパケットを確認し、switch：および **show ip dhcp global statistics** びredirections：の統計情報を確認することも重要 **show system internal access-list sup-redirect-stats module 1 | grep -i dhcp**です。

クラス標準DHCPリレー応答 – copp-system-p-class-normal-dhcp-relay-response

このクラスは、IPv4とIPv6の両方のDHCPリレー機能に関連付けられたトラフィックを指し、リレーの下で設定された設定済みDHCPサーバに向けられます。これは特に、任意のBOOTPサーバから発信されるか、またはDORAパケット交換全体を介して任意のBOOTPクライアントに宛てられたトラフィック通信にのみ関連し、UDPポート546/547を介したDHCPv6クライアント/サーバトランザクションも含まれます。

```
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

このクラスに対する違反は、クラスcopp-system-p-class-normal-dhcpに対する違反と同じ影響を及ぼします。これは、両方とも同じトランザクションの一部であるためです。このクラスは、主にリレーエージェントサーバからの応答通信に重点を置いています。NexusはDHCPサーバとして機能せず、リレーエージェントとしてのみ機能するように設計されています。

推奨事項

- 通常のDHCPクラスと同じ推奨事項が適用されます。Nexusの機能はリレーエージェントとしてのみ動作するため、SUPではホストとスイッチ間のトランザクション全体がリレーとして動作し、スイッチとサーバが設定されます。

- スコープに応答する予期しないDHCPサーバがネットワーク上に存在したり、ループに留まってDHCP Discoverパケットでネットワークをフラッディングするような不正なデバイスがないことを確認します。コマンドshow ip dhcp relayと**show ip dhcp relay statistics**を使用して、追加のチェックを実行できます。

クラスNATフロー – copp-system-p-class-nat-flow

このクラスは、ソフトウェアスイッチのNATフロートラフィックを指します。新しいダイナミック変換が作成されると、変換がハードウェアにプログラムされるまでフローがソフトウェアで転送され、エントリがハードウェアにインストールされている間は、CoPPによってポリシングされてスーパーバイザにパントされるトラフィックが制限されます。

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

このクラスでのドロップは通常、新しいダイナミック変換とフローがハードウェアに高いレートでインストールされたときに発生します。この影響は、廃棄されてエンドホストに配信されないソフトウェアスイッチドパケットに関連し、損失や再送信につながる可能性があります。エントリがハードウェアにインストールされると、それ以上のトラフィックはスーパーバイザにパントされません。

推奨事項

- 該当するプラットフォームでダイナミックNATのガイドラインと制限事項を確認します。プラットフォームには、変換に数秒かかる可能性がある3548などの既知の制限事項があります。詳細については、「ダイナミックNATの制限事項」

クラス例外 – copp-system-p-class-exception

このクラスは、IPオプションおよびIP ICMP到達不能パケットに関連する例外パケットを参照します。宛先アドレスがForwarding

Information Base（FIB；転送情報ベース）になく、結果としてミスが発生する場合、SUPはICMP到達不能パケットを送信側に送り返します。IPオプションが有効になっているパケットも、このクラスに含まれます。IPオプションの詳細については、IANAのドキュメント「IPオプション番号」を参照してください。

```
 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

このクラスは厳重にポリシングされており、このクラスでのドロップは障害を示すものではなく、ICMP到達不能パケットとIPオプションパケットの範囲を制限する保護メカニズムを示しています。

推奨事項

- FIB上にない宛先に対してCPUで検出またはパントされるトラフィックフローがあるかどうかを確認します。

クラスのリダイレクト – copp-system-p-class-redirect

このクラスは、時刻の同期に使用されるPrecision Time Protocol(PTP)に関連付けられたトラフィックを参照します。これには、予約済み範囲224.0.1.129/32のマルチキャストトラフィック、UDPポート319/320のユニキャストトラフィック、およびEthetype 0X88F7が含まれます。

```
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

このクラスでのドロップは、適切に同期されていない、または適切な階層を確立していないデバイスでの問題につながる可能性があります。

推奨事項

- クロックの安定性を確認し、クロックが正しく設定されていることを確認します。PTPデバイスがマルチキャストまたはユニキャストPTPモードに設定され、両方が同時に設定されていないことを確認します。これはガイドラインおよび制限

に基づいて文書化されており、トラフィックが認定入力レートを超える可能性があります。

- 境界クロックと環境内のすべてのPTPデバイスの設計と設定を確認します。プラットフォームごとに異なるため、すべてのガイドラインと制限事項に従ってください。

クラスOpenFlow - copp-system-p-class-openflow

このクラスは、OpenFlowエージェントの動作と、コントローラとエージェント間の対応するTCP接続に関連するトラフィックを参照します。

```
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

このクラスでのドロップは、ネットワークのフォワーディングプレーンを管理するためにコントローラからの指示を適切に受信して処理しないエージェントの問題につながる可能性があります

推奨事項

- ネットワーク上で重複トラフィックが見られないこと、またはコントローラとエージェント間の通信を妨げるデバイスが見られないことを確認します。
- L2ネットワークに不安定な状態（STPまたはループ）がないことを確認します。

CoPPドロップのトラブルシューティング

CoPP違反をトラブルシューティングするための最初の手順は、次の項目を判別することです。

- 問題の影響と範囲。
- 環境内のトラフィックフローと、影響を受ける通信におけるスイッチの役割を理解します。
- 疑わしい関連クラスに違反があるかどうかを判断し、必要に応じて繰り返します。

たとえば、次の動作が検出されました。

- デバイスは、ネットワーク外の他のデバイスとは通信できませんが、ローカルでは通信できます。
- 影響はVLAN外部のルーティングされた通信に分離されており、スイッチはデフォルトゲートウェイとして機能します

。

- ホストをチェックすると、ゲートウェイにpingを実行できないことが示されます。ARPテーブルをチェックした後、ゲートウェイのエントリはIncompleteのままになります。

- ゲートウェイで解決される他のすべてのホストには、通信の問題はありません。ゲートウェイとして機能するスイッチのCoPPをチェックすると、違反が存在することが示され copp-system-p-class-normalます。

<#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;

- さらに、複数のコマンドチェックにより、ドロップが増加に対してアクティブであることが示されます。

- これらの違反は、正当なARPトラフィックのドロップを引き起こし、サービス拒否動作を引き起こす可能性があります。

CoPPが特定のクラス（この例ではARPおよびcopp-system-p-class-normal）に関連付けられたトラフィックへの影響を分離することを強調することが重要です。OSPF、BGPなど他のクラスに関連するトラフィックは、完全に異なるクラスに属するため、CoPPによってドロップされません。このチェックボックスをオフのままにすると、ARPの問題が他の問題にカスケードされ、最初から依存しているプロトコルに影響を与える可能性があります。たとえば、ARPキャッシュがタイムアウトし、過度の違反のために更新されない場合、BGPなどのTCPセッションは終了する可能性があります。

- 問題をさらに分離するために、Ethanalyzer、CPU-macインバンド統計情報、CPUプロセスなどのコントロールプレーンチェックを実行することを推奨します。

Ethanalyzer

CoPPによってポリシングされるトラフィックはCPUに送られるトラフィックのみに関連付けられるため、最も重要なツールの1つはEthanalyzerです。このツールはTSharkのNexus実装であり、スーパーバイザが送受信したトラフィックをキャプチャしてデコードできます。また、プロトコルやヘッダー情報などの異なる基準に基づくフィルタを使用することもできるため、CPUで送受信されるトラフィックを判別するための貴重なツールになります。

最初に、Ethanalyzerツールがターミナルセッションで直接実行されるとき、または分析用のファイルに送信されるときにスーパーバイザによって認識されるARPトラフィックを調べることが推奨されます。フィルタと制限を定義して、キャプチャを特定のパターンや動作に絞り込むことができます。これを行うには、柔軟な表示フィルタを追加します。

よくある誤解は、Ethanalyzerがスイッチを通過するすべてのトラフィックをキャプチャしてしまうことです。ホスト間のデータプレーントラフィックは、データポート間のハードウェアASICによってスイッチングまたはルーティングされるため、CPUの関与は不要です。そのため、Ethanalyzerキャプチャでは通常このトラフィックを確認できません。データプレーントラフィックをキャプチャするには、ELAMやSPANなどの他のツールを使用することをお勧めします。たとえば、ARPをフィルタリングするには、次のコマンドを使用します。

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

重要な設定可能フィールド：

- interface inband - SUP宛てのトラフィックを指します。
- display-filter arp – 適用されるtsharkフィルタを参照します。ほとんどのWiresharkフィルタが受け入れられます。
- limit-captured-frames 0 – 制限を参照します。0は無制限を表し、別のパラメータによって停止されるか、Ctrl+Cによって手動で停止されるまで続きます。
- autostop duration 60 - Ethanalyzerが60秒後に停止することを示します。これにより、CPUで確認されるARPトラフィックの60秒のスナップショットが作成されます。

Ethanalyzerの出力は、> arpcpuを使用してブートフラッシュ上のファイルにリダイレクトされ、手動で処理されます。60秒後にキャプチャが完了し、Ethanalyzerが動的に終了します。ファイルarpcpuはスイッチのブートフラッシュにあります。このブートフラッシュを処理してトップトーカーを抽出できます。例：

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

このフィルタは、ソース列とターゲット列に基づいて並べ替えられ、次に見つかった一意の一致（ただし、日付列は無視）に基づいてインスタンスをカウントし、表示された数を追加し、最後にカウントに基づいて上から下に並べ替え、最初の50件の結果を表示します。

このラボの例では、60秒以内に3台のデバイスから600を超えるARPパケットを受信しました。これらのデバイスは、攻撃を受けている可能性のあるデバイスとして特定されています。フィルタの最初の列には、指定した期間内にキャプチャファイルでこのイベントが発生したインスタンスの数が詳細に表示されます。

Ethanalyzerツールはインバンドドライバに対して動作しますが、これは本質的にASICへの通信であることを理解することが重要です。理論的には、パケットはカーネルを通過し、パケットマネージャは関連するプロセス自体に渡される必要があります。CoPPとHWRLは、トラフィックがEthanalyzerで確認される前に動作します。違反が増加している場合でも、一部のトラフィックは引き続き通過し、ポリシングレート内で適合されるため、CPUにパントされるトラフィックフローを把握するのに役立ちます。Ethanalyzerで確認されるトラフィックはCIRに違反してドロップされたトラフィックではないため、これは重要な違いです。

Ethanalyzerは、関連するすべてのSUPトラフィックをキャッチするために指定された表示フィルタまたはキャプチャフィルタなし

で、オープン形式で使用することもできます。これは、トラブルシューティングのアプローチの一部として、隔離手段として使用できます。

Ethanalyzerの詳細と使用方法については、テクニカルノート：

Nexus 7000 での Ethanalyzer トラブルシューティング ガイド

NexusプラットフォームでEthanalyzerを使用したコントロールプレーンおよびデータプレーンのトラフィック分析

注:Nexus 7000では、8.Xコードリリース以前は、admin VDCを介してのみEthanalyzerキャプチャを実行でき、すべてのVDCからのSUPバウンドトラフィックを取り込みます。VDC固有のEthanalyzerは、8.Xコードに含まれています。

CPU-MACインバンド統計情報

CPUに送られるトラフィックに関連するインバンド統計情報には、インバンドのTX/RX CPUトラフィックに関する関連する統計情報が保持されます。これらの統計情報は、コマンド：show hardware internal cpu-mac inband statsで確認できます。このコマンドは、現在のレートとピークレートの統計情報に関する情報を提供します。

```
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
```

ベストプラクティスとして、ベースラインを作成して追跡することをお勧めします。これは、スイッチとインフラストラクチャの役割によって、出力が大きく異 **show hardware internal cpu-mac inband stats** なるためです。このラボ環境では、通常の値と履歴のピークは通常、数百pps以下であるため、これは異常です。このコマンド **show hardware internal cpu-mac inband events** には、ピーク時の使用状況と検出時間に関するデータが含まれるため、履歴の参照としても役立ちます。

プロセスCPU

NexusスイッチはLinuxベースのシステムであり、Nexus Operating System(NXOS)はCPUプリエンプティブスケジューラ、マルチタスク、および各コアアーキテクチャのマルチスレッド化を利用して、すべてのプロセスへの公平なアクセスを提供します。したがって、スパイクは必ずしも問題を示しているわけではありません。ただし、継続的なトラフィック違反が見られる場合は、関連するプロセスも頻繁に使用され、CPU出力の下のトップリソースとして表示される可能性があります。CPUプロセスの複数のスナップショットを作成し、特定のプロセスの使用率が高いことを次のコマンドを使用して確認します。 **show processes cpu sort | exclude 0.0 or show processes cpu sort | grep <process>**.

プロセスCPU、インバンド統計情報、およびEthanalyzerの検証により、スーパバイザによって現在処理されているプロセスとトラフィックに関する洞察が得られ、データプレーンの問題に連鎖する可能性があるコントロールプレーントラフィックの継続的な不安定性を分離するのに役立ちます。CoPPは保護メカニズムであることを理解することが重要です。SUPにパントされたトラフィ

ックでのみ動作するため、反動的です。これは、予想される範囲を超えるトラフィックレートを廃棄することによって、スーパーバイザの完全性を保護するように設計されています。すべてのドロップが特定のCoPPクラスとインフラストラクチャおよびネットワーク設計に基づく検証済みの影響に重要性が関連するため、問題を示しているわけでも、介入が必要なドロップでもありません。プロトコルには、一時的なイベントを処理できるキープアライブや再試行などの組み込みメカニズムがあるため、散発的なバーストイベントによる廃棄は、影響に変換されません。確立されたベースラインを超えて、持続的なイベントまたは異常なイベントに焦点を当て続けます。CoPPは環境に固有のプロトコルと機能に従う必要があり、拡張の必要性に応じて、環境を調整するために監視し、継続的に繰り返す必要があることに注意してください。ドロップが発生した場合は、CoPPが意図せずにトラフィックをドロップしたか、または誤動作や攻撃に対応してトラフィックをドロップしたかを判断します。いずれの場合も、状況を分析し、スイッチ自体の範囲外となる可能性がある環境への影響と修正措置を分析することで介入の必要性を評価します。

追加情報

最近のプラットフォーム/コードでは、ポートのミラーとデータプレーントラフィックのCPUへのパントにより、SPANからCPUへの変換を実行できます。これは通常、ハードウェアレート制限とCoPPによって大幅にレート制限されます。CPUへのSPANの慎重な使用が推奨されますが、このドキュメントでは取り扱いません。

この機能の詳細については、次のテクニカルノートを参照してください。

Nexus 9000クラウドスケールASIC NX-OSのSPAN-to-CPU手順

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。