Nexus 7000 シリーズ スイッチの CoPP

目次

概要

このドキュメントでは、Nexus 7000 シリーズ スイッチでどのコントロール プレーン ポリシング（CoPP）がどのように、なぜ使用されているかについて説明します。これには、F1、F2、M1、および M2 シリーズ モジュールとライン カード（LC）が含まれます。 また、ベスト プラクティスのポリシーと、CoPP ポリシーをカスタマイズする方法についても説明します。

前提条件

要件

次の Nexus オペレーティング システム CLI に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、スーパーバイザー 1 モジュールを搭載した Nexus 7000 シリーズ NX-OS デバイスに基づくものです。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

Nexus 7000 シリーズ スイッチの CoPP の概要

CoPP は、ネットワーク動作に不可欠です。 コントロール プレーンまたは管理プレーンへのサービス拒絶（DoS）攻撃は不注意または悪意をもって実行され、通常は、過度な CPU 使用率を発生させる高レートのトラフィックを含みます。 スーパーバイザ モジュールはパケットの処理に、とてつもなく多くの時間を使用します。

このような攻撃の例は、次のとおりです。

- インターネット制御メッセージ プロトコル（ICMP）エコー要求。
- [ip-options] が設定された送信パケット。

この結果、次が起きる可能性があります。

- キープアライブ メッセージおよびルーティング プロトコルのアップデートが失われる。
- 無差別なドロップの原因となるパケット キューの輻輳。
- 低速または応答しないインタラクティブなセッション。

攻撃はネットワークの安定性とアベイラビリティを圧倒し、ビジネスに影響するネットワークの停止につながる可能性があります。

CoPP は、DoS 攻撃からスーパーバイザを保護するハードウェア ベースの機能です。 パケットがスーパーバイザに到達することができるレートを制御します。 CoPP 機能は、[control-plane] と呼ばれる特別なインターフェイスに接続されている入力 QoS ポリシーのようにモデル化されます。 ただし、CoPP は QoS の一部ではなく、セキュリティ機能です。 スーパーバイザを保護するため、CoPP はコントロール プレーン パケットからデータ プレーン パケットを分離します（例外ロジック）。 これは、有効なパケットと DoS 攻撃パケットを区別します（分類）。 CoPP は、次のパケットの分類を可能にします。

- 受信パケット
- マルチキャスト パケット
- 例外パケット
- リダイレクト パケット
- ブロードキャスト MAC + 非 IP パケット
- ブロードキャスト MAC + IP パケット（詳細については、Cisco Bug ID CSCub47533：CoPP をヒットする L2 VLAN（SVI なし）のパケットを参照してください）。
- マルチキャスト MAC + IP パケット
- ルータ MAC + 非 IP パケット
- ARP パケット

パケットが分類されたら、パケットをマーキングし、パケットの種類に基づいて異なるプライオ

リティを割り当てるために使用できます。 適合、超過、違反のアクション（送信、ドロップ、マークダウン）を設定できます。 クラスにポリサーが接続されていない場合、適合のアクションがドロップにあるデフォルトのポリサーが追加されます。 収集パケットは、デフォルトクラスでポリシングされます。 1 つのレートで 2 色、および 2 つのレートで 3 色のポリシングがサポートされています。

スーパーバイザ モジュールで CPU をヒットするトラフィックは、次の 4 つのパスを経由して受信されます。

1. ライン カードによって送信されたトラフィックのインバンド インターフェイス（前面パネルのポート）。

2. 管理トラフィックに使用する管理インターフェイス（mgmt0）。

3. コンソールに使用する Control and Monitoring Processor（CMP）インターフェイス。

4. スーパーバイザ モジュールのラインカードを制御し、ステータス メッセージを交換する Switched Ethernet Out Band Channel（EOBC）。

インバンド インターフェイスを介して送信されたトラフィックのみが CoPP の対象になります。これは、このトラフィックがライン カードのフォワーディング エンジン（FE）を通してスーパーバイザ モジュールに到達する唯一のトラフィックであるためです。 Nexus 7000 シリーズ スイッチの CoPP の実装はハードウェア ベースのみです。これは、CoPP はスーパーバイザ モジュールによってソフトウェアで実行されないことを意味します。 CoPP 機能（ポリシング）は、各 FE で個別に実行されます。 さまざまなレートが CoPP のポリシーマップ用に設定されている場合、システム内のライン カードの数に応じて考慮する必要があります。

スーパーバイザが受信するトラフィックの総量は、N 掛ける X です。ここで、N は Nexus 7000 システム上の FE の数、X は特定のクラスに許可されているレートです。 設定されたポリサーの値は FE 単位で適用され、CPU をヒットする傾向がある集約トラフィックはすべての FE 上で適合および送信されたトラフィックの合計です。 つまり、CPU をヒットするトラフィックは設定された適合レートに、FE の数を乗算した値と等しくなります。

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

CoPP 設定は、デフォルトの仮想デバイス コンテキスト（VDC）のみで実行されます。 ただし、CoPP のポリシーはすべての VDC に適用できます。 同じグローバル ポリシーは、すべてのライン カードに適用されます。 CoPP は同じ FE のポートが異なる VDC（M1 シリーズまたは M2 シリーズ LC）に属している場合、VDC 間にリソース共有を適用します。 たとえば、異なる VDC 上にあっても 1 つの FE のポートは、CoPP の同じしきい値に対してカウントされます。

同じ FE が異なる VDC 間で共有されている場合に、コントロール プレーン トラフィックの特定のクラスがしきい値を超えると、これは同じ FE のすべての VDC に影響します。 可能であれば、CoPP の適用を分離するために、VDC ごとに 1 つの専用の FE を提供することが推奨されます。

スイッチを初めて起動したときは、[control-plane] を保護するために、デフォルト ポリシーをプログラムする必要があります。 CoPP は初期起動シーケンスの一部として [control-plane] に適用されるデフォルト ポリシーを提供します。

Nexus 7000 シリーズ スイッチで CoPP を実行する理由

Nexus 7000 シリーズ スイッチは、集約スイッチまたはコア スイッチとして配置されます。 したがって、このスイッチはネットワークの耳と頭脳になります。 このスイッチは、ネットワーク内の最大負荷を処理します。 頻繁かつ大量に発生する要求を処理する必要があります。 要求の一部には、次が含まれます。

- **スパニング ツリー ブリッジ プロトコル データ ユニット（BPDU）の処理**：デフォルトは 2 秒ごとです。
- **ファースト ホップ冗長性**：これには、ホットスタンバイ ルータ プロトコル（HSRP）、仮想ルータ冗長プロトコル（VRRP）、およびゲートウェイ ロード バランシング プロトコル（GLBP）が含まれます。デフォルトは 3 秒ごとです。
- **アドレス解決**：これには、アドレス解決プロトコル/ネイバー探索（ARP/ND）、転送情報ベース（FIB）収集が含まれます。1 秒ごと、ネットワーク インターフェイス コントローラ（NIC）チーム化のようなホストごとに最大 1 要求です。
- **動的ホスト制御プロトコル（DHCP）**：DHCP 要求、リレー。1 秒ごと、ホストごとに最大 1 要求です。
- レイヤ 3（L3）用の**ルーティング プロトコル**。
- **データセンターの相互接続**：Overlay Transport Virtualization（OTV）、マルチプロトコル ラベル スイッチング（MPLS）、および仮想プライベート LAN サービス（VPLS）。

CoPP は、CPU が重要なコントロール プレーン メッセージを処理するのに十分なサイクルを持てるように、誤って設定されたサーバや潜在的な DoS 攻撃から CPU を保護するために必要です。

Nexus 7000 シリーズ スイッチでのコントロール プレーン処理

Nexus 7000 シリーズ スイッチは、分散されたコントロール プレーンの方法を使用します。 各 I/O モジュールのマルチコアに加えて、スーパーバイザ モジュールのスイッチ コントロール プレーンのマルチコアがあります。 これは、アクセス コントロール リスト（ACL）や FIB プログラミング用の I/O モジュール CPU に集中的なタスクをオフロードします。 ライン カードの数でコントロール プレーンのキャパシティを拡大します。 これによって、集中化されたアプローチで発生するスーパーバイザの CPU ボトルネックを回避します。 ハードウェア レート リミッタとハードウェアベースの CoPP は、不正または悪意のあるアクティビティからコントロール プレーンを保護します。

CoPP の Best Practices Policy

CoPP の Best Practices Policy（BPP）は、Cisco NX-OS リリース 5.2 で導入されました。 **show running-config** コマンドの出力は、CoPP BPP の内容を表示しません。 **show run all** コマンドは、CoPP BPP の内容を表示します。

```
-----------------------------------SNIP----------------------------------------
SITE1-AGG1# show run copp

!! Command: show running-config copp
!! Time: Mon Nov 5 22:21:04 2012

version 5.2(7)
copp profile strict


SITE1-AGG1# show run copp all

!! Command: show running-config copp all
!! Time: Mon Nov 5 22:21:15 2012

version 5.2(7)
-----------------------------SNIP--------------------
control-plane
service-policy input copp-system-p-policy-strict
copp profile strict
```

CoPP はデフォルト ポリシーに、次の 4 つのオプションをユーザに提供します。

- Strict
- 警告
- Lenient
- Dense（リリース 6.0(1) で導入）

オプションが選択されていない、または設定をスキップした場合、Strict ポリシングが適用されます。 これらのオプションはすべて同じクラス マップとクラスを使用しますが、ポリシングに異なる認定情報レート（CIR）と Burst Count（BC）値を使用します。 Cisco NX-OS リリース 5.2.1 よりも前では、オプションを変更するために **setup** コマンドを使用します。 Cisco NX-OS リリース 5.2.1 では、**setup** コマンドを使用せずにオプションを変更できるようにする CoPP BPP の拡張機能が導入されました。 代わりに **copp profile** コマンドを使用します。

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# copp profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1(config)# copp profile strict
SITE1-AGG1(config)# exit
```

次のように、**show copp profile <profile-type>** コマンドを使用してデフォルトの CoPP BPP 設定を表示します。 **show copp status** コマンドを使用して、CoPP ポリシーが正しく適用されたことを確認します。

```
SITE1-AGG1# show copp status
Last Config Operation: copp profile strict
Last Config Operation Timestamp: 20:40:27 PST Nov 5 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-system-p-policy-strict
```

2 つの CoPP BPP の違いを確認するには、**show copp diff profile <profile-type 1> profile <profile-type 2>** コマンドを使用します。

```
SITE1-AGG1# show copp diff profile strict profile moderate
A '+' represents a line that has been added and
a '-' represents a line that has been removed.
-policy-map type control-plane copp-system-p-policy-strict
- class copp-system-p-class-critical
- set cos 7
- police cir 39600 kbps bc 250 ms conform transmit violate drop
- class copp-system-p-class-important
- set cos 6
- police cir 1060 kbps bc 1000 ms conform transmit violate drop
----------------------SNIP----------------------------------------
+policy-map type control-plane copp-system-p-policy-moderate
+ class copp-system-p-class-critical
+ set cos 7
+ police cir 39600 kbps bc 310 ms conform transmit violate drop
+ class copp-system-p-class-important
+ set cos 6
+ police cir 1060 kbps bc 1250 ms conform transmit violate drop
----------------------SNIP----------------------------------------
```

CoPP ポリシーをカスタマイズする方法

ユーザは、カスタマイズされた CoPP ポリシーを作成できます。 CoPP BPP は読み取り専用であるため、デフォルトの CoPP BPP をクローニングして [control-plane] インターフェイスに接続します。

```
SITE2-AGG1(config)# policy-map type control-plane copp-system-p-policy-strict
^
% String is invalid, 'copp-system-p-policy-strict' is not an allowed string at
'^' marker.
```

copp copy profile <profile-type> <prefix> [suffix] コマンドは、CoPP BPP のクローンを作成します。 これは、デフォルトの設定を変更するために使用されます。 **copp copy profile** コマンドは **exec mode** コマンドです。 ユーザはアクセスリスト、クラスマップ、およびポリシーマップ名のプレフィックスまたはサフィックスを選択できます。 たとえば、**copp-system-p-policy-strict** は、**[prefix]copp-policy-strict[suffix]** に変更されます。 クローニングされた設定は、ユーザの設定として扱われ、**show run** の出力に含まれます。

```
SITE1-AGG1# copp copy profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1# copp copy profile strict ?
prefix Prefix for the copied policy
suffix Suffix for the copied policy
SITE1-AGG1# copp copy profile strict suffix ?
WORD Enter prefix/suffix for the copied policy (Max Size 20)
SITE1-AGG1# copp copy profile strict suffix CUSTOMIZED-COPP
SITE1-AGG1# show run copp | grep policy-map
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1#
```

これらのコマンドを使用して、指定された Permitted Information Rate（PIR）を超過し、違反するトラフィックをマークダウンすることができます。

```
SITE1-AGG1(config)# policy-map type
control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms ?
<CR>
```

```
conform Specify a conform action
pir Specify peak information rate

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir ?
<1-80000000000> Peak Information Rate in bps/kbps/mbps/gbps

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps ?
<CR>
<1-512000000> Peak Burst Size in bytes/kbytes/mbytes/packets/ms/us
be Specify extended burst
conform Specify a conform action

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform ?
drop Drop the packet
set-cos-transmit Set conform action cos val
set-dscp-transmit Set conform action dscp val
set-prec-transmit Set conform action precedence val
transmit Transmit the packet

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform
set-dscp-transmit ef exceed set dscp1 dscp2 table cir-markdown-map violate
set1 dscp3 dscp4 table1 pir-markdown-map
SITE1-AGG1(config-pmap-c)#
```

カスタマイズされた CoPP ポリシーをグローバル インターフェイス [control-plane] に適用します。 **show copp status** コマンドを使用して、CoPP ポリシーが正しく適用されたことを確認します。

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

カスタマイズされた CoPP ポリシー ケーススタディ

このセクションは頻繁にローカルインターフェイスを ping するように顧客は複数のモニタリング デバイスが要求する実質例を記述します。 問題はこのシナリオで顧客が CoPP ポリシーを修正したいと思うとき見つけられます:

- これらの特定 の アドレスがローカルデバイスを ping し、ポリシーに違反なできるように CIR を増加して下さい。
- 他の IP アドレスがトラブルシューティングを行うのに下部の CIR でローカルデバイスを、ping する機能を維持できるようにして下さい。

ソリューションは別途の class-map でカスタマイズされた ポリシーを作成することである次 の例で示されています。 別途の class-map はモニタリング デバイスの規定 された IP アドレスが含まれ、class-map により高い CIR があります。 下部の CIR で他の IP アドレスすべてのための ICMP トラフィックをキャプチャ するこれはまた*監察*するオリジナル class-map を去ります。

```
SITE1-AGG1# conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

CoPP のデータ構造

CoPP BPP のデータ構造は、次のように構成されています。

- **ACL の設定**： IP ACL および MAC ACL。
- **分類子の設定**： クラス マップと一致する IP ACL または MAC ACL。
- **ポリサーの設定**： CIR、BC、適合アクション、および違反アクションを設定します。 ポリサーには 2 つのレート（CIR と BC）、および 2 つの色（適合と違反）があります。

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

CoPP のスケール ファクタ

Cisco NX-OS リリース 6.0 で導入されたスケール ファクタ設定は、特定のラインカードに適用された CoPP ポリシーのポリサー レートをスケーリングするために使用されます。 この設定は特定のライン カードのポリサー レートを増減しますが、現在の CoPP ポリシーは変更されません。 変更はただちに有効になり、CoPP ポリシーを再適用する必要はありません。

```
scale factor option configured within control-plane interface:
Scale-factor <scale factor value> module <module number>
<scale factor value>: from 0.10 to 2.00
Scale factor is recommended when a chassis is loaded with both F2 and M
Series modules.
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# scale-factor ?
<whole>.<decimal> Specify scale factor value from 0.10 to 2.00

SITE1-AGG1(config-cp)# scale-factor 1.0 ?
```

```
module Module

SITE1-AGG1(config-cp)# scale-factor 1.0 module ?
<1-10> Specify module number

SITE1-AGG1(config-cp)# scale-factor 1.0 module 4
SITE1-AGG1# show system internal copp info
<snip>
Linecard Configuration:
-----------------------
Scale Factors
Module 1: 1.00
Module 2: 1.00
Module 3: 1.00
Module 4: 1.00
Module 5: 1.00
Module 6: 1.00
Module 7: 1.00
Module 8: 1.00
Module 9: 1.00
Module 10: 1.00
```

CoPP のモニタリングと管理

Cisco NX-OS リリース 5.1 では、しきい値を超過した場合に Syslog メッセージをトリガーする CoPP クラス名ごとのドロップしきい値を設定することができます。 コマンドは **logging drop threshold <dropped bytes count> level <logging level>** です。

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# logging ?
drop Logging for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop ?
threshold Threshold value for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop threshold ?
<CR>
<1-80000000000> Dropped byte count

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 ?
<CR>
level Syslog level

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level ?
<1-7> Specify the logging level between 1-7

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7
```

次に Syslog メッセージの例を示します。

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# logging ?
drop Logging for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop ?
threshold Threshold value for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop threshold ?
```

```
<CR>
<1-80000000000> Dropped byte count

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 ?
<CR>
level Syslog level

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level ?
<1-7> Specify the logging level between 1-7

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7
```

CoPP カウンタ

CoPP は、他のインターフェイスと同じ QoS 統計情報をサポートします。 CoPP をサポートするすべての I/O モジュールのサービス ポリシーを形成するクラスの統計情報が表示されます。 CoPP の統計情報を表示するには、**show policy-map interface control-plane** コマンドを使用します。

> **注:** すべてのクラスは違反するパケットによって監視する必要があります。

```
SITE1-AGG1# show policy-map interface control-plane
Control Plane

service-policy input: copp-policy-strict-CUSTOMIZED-COPP

class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
match access-group name copp-acl-bgp-CUSTOMIZED-COPP
match access-group name copp-acl-bgp6-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp-CUSTOMIZED-COPP
match access-group name copp-acl-igmp-CUSTOMIZED-COPP
match access-group name copp-acl-msdp-CUSTOMIZED-COPP
match access-group name copp-acl-ospf-CUSTOMIZED-COPP
match access-group name copp-acl-ospf6-CUSTOMIZED-COPP
match access-group name copp-acl-pim-CUSTOMIZED-COPP
match access-group name copp-acl-pim6-CUSTOMIZED-COPP
match access-group name copp-acl-rip-CUSTOMIZED-COPP
match access-group name copp-acl-rip6-CUSTOMIZED-COPP
match access-group name copp-acl-vpc-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp6-CUSTOMIZED-COPP
match access-group name copp-acl-mac-l2pt-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-ldp-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-oam-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-rsvp-CUSTOMIZED-COPP
match access-group name copp-acl-otv-as-CUSTOMIZED-COPP
match access-group name copp-acl-mac-otv-isis-CUSTOMIZED-COPP
match access-group name copp-acl-mac-fabricpath-isis-CUSTOMIZED-COPP
match protocol mpls router-alert
match protocol mpls exp 6
set cos 7
threshold: 100, level: 7
police cir 39600 kbps , bc 250 ms
module 1 :
conformed 22454 bytes; action: transmit
violated 0 bytes; action: drop

module 2 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

```
module 3 :
conformed 19319 bytes; action: transmit
violated 0 bytes; action: drop

module 4 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

すべてのクラスマップと I/O モジュールの適合および違反カウンタの集約されたビューを取得するには、**show policy-map interface control-plane | i "class|conform|violated"** コマンドを使用します。

```
SITE1-AGG1# show policy-map interface control-plane | i "class|conform|violated"
class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
conformed 123126534 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 107272597 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
class-map copp-class-important-CUSTOMIZED-COPP (match-any)
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

適合カウンタの場合であっても、高い増加がないことを確認するために、**class copp-class-l2-default and class-default** を監視する必要があります。 理想的には、これら 2 つのクラスの適合カウンタは低い値で、少なくとも違反カウントが増加していない必要があります。

ACL カウンタ

statistics per-entry コマンドは、CoPP クラスマップで使用される IP ACL または MAC ACL ではサポートされておらず、CoPP IP ACL または MAC ACL に適用しても効果がありません。（CLI パーサーによって実行される CLI チェックはありません）。 I/O モジュールに対する CoPP MAC ACL または IP ACL のヒットを表示するには、**show system internal access-list input entries detail** コマンドを使用します。

次に例を示します。

```
!! 0180.c200.0041 is the destination MAC used for FabricPath IS-IS

SITE1-AGG1# show system internal access-list input entries det | grep 0180.c200.0041
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [30042]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [29975]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8965]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8935]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [58233]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [27689]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

```
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

CoPP 設定のベスト プラクティス

CoPP 設定に推奨される次のベスト プラクティスがあります。

- CoPP の Strict モードをデフォルトで使用します。
- CoPP の Dense プロファイルは、シャーシに F2 シリーズ モジュールが完全に搭載されているか、他の I/O のモジュールよりも多くの F2 シリーズ モジュールが搭載されいている場合に推奨されます。
- CoPP を無効にすることは推奨されません。 必要に応じてデフォルトの CoPP を調整します。
- 意図しないドロップを監視し、予想されるトラフィックに応じてデフォルトの CoPP ポリシーを追加または変更します。
- シャーシ内の FE の数に基づいて、CoPP の CIR と BC の設定を増減できます。 これは、ネットワーク上のデバイスの役割、実行するプロトコルなどにも基づいています。
- 「データセンター」ではトラフィック パターンがに常に変化するため、CoPP のカスタマイゼーションは絶え間なく続くプロセスです。
- CoPP と VDC： 同じ FE のすべてのポートは同じ VDC に属する必要があります。これは、F2 シリーズ LC では容易ですが、M2 シリーズまたは M108 LC では容易ではありません。 これは、CoPP は同じ FE のポートが異なる VDC（M1 シリーズまたは M2 シリーズ LC）に属している場合、VDC 間でリソース共有されるためです。 異なる VDC 上にあっても 1 つの FE のポートは、CoPP の同じしきい値に対してカウントされます。
- スケール ファクタ設定は、シャーシに F2 シリーズおよび M シリーズ モジュールの両方が搭載されている場合に推奨されます。

CoPP モニタリングのベスト プラクティス

CoPP モニタリングに推奨される次のベスト プラクティスがあります。

- CoPP によるドロップを監視するために CoPP（Cisco NX-OS リリース 5.1）の Syslog メッセージのしきい値を設定します。

- Syslog メッセージは、トラフィック クラス内のドロップがユーザ設定のしきい値を超過した場合に生成されます。

- ロギングのしきい値とレベルは、**logging drop threshold <packet-count> level <level>** コマンドを使用して各トラフィック クラス内でカスタマイズできます。

- CoPP MAC ACL または IP ACL の [statistics per-entry] オプションはサポートされていないため、**show system internal access-list input entries det** コマンドを使用してアクセス コントロール エントリ（ACE）のヒット数を監視します。

- 適合カウンタの場合であっても、高い増加がないことを確認するために、**class copp-class-l2-default and class-default** コマンドを監視する必要があります。

- すべてのクラスは違反するパケットによって監視する必要があります。

- **copp-class-critical** はきわめて重要ですが、**violate drop** ポリシーが設定されているため、クラスが違反を開始する時点に近くなったら早期指摘を受け取るために、適合パケットのレートを監視することをお勧めします。 このクラスの違反カウンタが増加しても、非常アラートを意味するとは限りません。 むしろ、この状況を短時間で調査する必要があることを意味します。

- Cisco NX-OS コードのアップグレードごとに、または少なくとも主要な Cisco NX-OS コードのアップグレード後に、**copp profile strict** コマンドを使用します。 前に CoPP の変更を完了した場合は、再度適用する必要があります。

結論

- CoPP は、DoS 攻撃からスーパーバイザを保護するハードウェア ベースの機能です。

- M1、F2、および M2 シリーズ LC は CoPP をサポートしています。 F1 シリーズ LC は CoPP をサポートしていません。

- CoPP 設定は MQC（Modular QoS CLI）に似ています。

- CoPP の設定とモニタリングはデフォルトの VDC のみで実行されます。

- デフォルト CoPP BPP は Strict、Moderate、Lenient、および Dense オプションで使用できます。

- CoPP BPP カスタマイズされた CoPP を特定のネットワーク要求を一致するために支配しますクローンとして作って下さい。

- CoPP カウンタ（クラスマップごとのバイト単位での適合と違反）は、**show policy-map interface control-plane** コマンドで表示されます。

- スーパーバイザ モジュールの CPU で受信されたトラフィックは、FE の合計数に許可されたレートを乗算した値と等しくなります。
- 異なる VDC 間での 1 つの FE の共有ポートは回避してください。
- 正常に機能を実行およびモニタリングするには、CoPP のベスト プラクティスに従ってください。

サポートされていない機能

次の機能はサポートされていません。

- 分散型の集約ポリシング。
- マイクロフロー ポリシング。
- 出力の例外ポリシング。
- dot1q トンネル ポート（QinQ）からの BPDU の CoPP サポート： Cisco Discovery Protocol（CDP）、DOT1x、スパニング ツリー プロトコル（STP）、および VLAN トランク プロトコル（VTP）。