コントロール プレーン ポリシングの設定

この章では、Cisco NX-OS デバイスでコントロール プレーン ポリシング（CoPP）を設定する手順を説明します。

この章は、次の内容で構成されています。

CoPP の概要

コントロール プレーン ポリシング（CoPP）はコントロール プレーンを保護し、それをデータ プレーンから分離することによって、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロール プレーンにポリシー マップを適用できるようになります。 このポリシー マップは通常の QoS ポリシーのように見え、非管理ポートからスイッチに入力されるすべてのトラフィックに適用されます。ネットワーク デバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイス インターフェイスに転送されるサービス拒絶（DoS）攻撃です。

Cisco NX-OS デバイスは、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。 このような攻撃は誤って、または悪意を持って実行される場合があり、通常は、スーパーバイザ モジュールまたは CPU 自体に宛てられた大量のトラフィックが含まれます。

スーパーバイザ モジュールは、管理対象のトラフィックを次の 3 つの機能コンポーネント（プレーン）に分類します。

データ プレーン

すべてのデータ トラフィックを処理します。 NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。 スイッチ自身に向けられたものでないパケットは、中継パケットと呼ばれます。 データ プレーンで処理されるのはこれらのパケットです。

コントロール プレーン

ルーティング プロトコルのすべての制御トラフィックを処理します。 ボーダー ゲートウェイ プロトコル（BGP）や Open Shortest Path First（OSPF）プロトコルなどのルーティング プロトコルは、デバイス間で制御パケットを送信します。 これらのパケットはルータのアドレスを宛先とし、コントロール プレーン パケットと呼ばれます。

管理プレーン

コマンドライン インターフェイス（CLI）や Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）など、NX-OS デバイスを管理する目的のコンポーネントを実行します。

スーパーバイザ モジュールには、マネージメント プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザモジュールの動作が途絶したり、スーパーバイザ モジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえばスーパーバイザに過剰なトラフィックが加わると、スーパーバイザモジュールが過負荷になり、NX-OS デバイス全体のパフォーマンスが低下する可能性があります。たとえば、スーパーバイザ モジュールに対する DoS 攻撃は、コントロール プレーンに対して非常に高速に IP トラフィック ストリームを生成することがあります。これにより、コントロール プレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

DoS 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 フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーション トラフィックの低下など）
- ルート プロセッサまたはスイッチ プロセッサの高い CPU 使用率
- ルーティング プロトコルのアップデートまたはキープアライブの消失によるルート フラップ
- 不安定なレイヤ 2 トポロジ
- CLI との低速な、または応答を返さない対話型セッション
- メモリやバッファなどのプロセッサ リソースの枯渇
- 着信パケットの無差別のドロップ

注意 コントロール プレーンの保護策を講じることで、スーパーバイザ モジュールを偶発的な攻撃や悪意ある攻撃から確実に保護することが重要です。

コントロール プレーンの保護

コントロール プレーンを保護するため、Cisco NX-OS デバイスはコントロール プレーンに向かうさまざまなパケットを異なるクラスに分離します。 クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザ モジュールに過剰な負担がかからないようになります。

コントロール プレーンのパケット タイプ

コントロール プレーンには、次のような異なるタイプのパケットが到達します。

受信パケット

ルータの宛先アドレスを持つパケット。 宛先アドレスには、レイヤ 2 アドレス（ルータ MAC アドレスなど）やレイヤ 3 アドレス（ルータ インターフェイスの IP アドレスなど）があります。 これらのパケットには、ルータ アップデートとキープアライブ メッセージも含まれます。 ルータが使用するマルチキャスト アドレス宛てに送信されるマルチキャスト パケットも、このカテゴリに入ります。

例外パケット

スーパーバイザ モジュールによる特殊な処理を必要とするパケット。 たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザ モジュールが送信側に到達不能パケットを返します。 他には、IP オプションがセットされたパケットもあります。

リダイレクト パケット

スーパーバイザ モジュールにリダイレクトされるパケット。 Dynamic Host Configuration Protocol（DHCP）スヌーピングやダイナミック Address Resolution Protocol（ARP; アドレス解決プロトコル）インスペクションなどの機能は、パケットをスーパーバイザ モジュールにリダイレクトします。

収集パケット

宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザ モジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットはすべて、コントロール プレーンへの悪意ある攻撃に利用され、Cisco NX-OS デバイスに過剰な負荷をかける可能性があります。 CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットをスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類

効果的に保護するために、Cisco NX-OS デバイスはスーパーバイザ モジュールに到達するパケットを分類して、パケット タイプに基づいた異なるレート制御ポリシーを適用できるようにします。 たとえば、Hello メッセージなどのプロトコル パケットには厳格さを緩め、IP オプションがセットされているためにスーパーバイザ モジュールに送信されるパケットには厳格さを強めることが考えられます。

レート制御メカニズム

パケットの分類が終わると、Cisco NX-OS デバイスにはスーパーバイザ モジュールに到達するパケットのレートを制御する 2 つの異なるメカニズム（ポリシングおよびレート制限）があります。

ハードウェア ポリサーを使用すると、トラフィックが所定の条件に一致する場合、または違反する場合について異なるアクションを定義できます。 このアクションには、パケットの送信、パケットのマーク付け、およびパケットのドロップがあります。

ポリシングには、次のパラメータを設定できます。

認定情報レート（CIR）

ビット レートとして指定する必要な帯域幅。

認定バースト（BC）

指定した時間枠内に CIR を超過する可能性があるが、スケジューリングには影響を与えないトラフィック バーストのサイズ。

CoPP クラス マップ

次の表に、使用可能なクラス マップとその設定を示します。

表 *1*：クラス マップの設定および説明

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-arp	match protocol arp match protocol nd	クラスは、すべての ARP パケットに一致します。 クラスは、すべての ARP パケットおよび ND（NA、NS、RA および RS）パケットに一致します。
class-map type control-plane match-any copp-system-class-bgp	match protocol bgp	クラスはすべての BGP パケットに一致します。
class-map type control-plane match-any copp-system-class-bridging	match protocol bridging	クラスはすべての STP および RSTP フレームに一致します。
class-map type control-plane match-any copp-system-class-cdp	match protocol cdp	クラスはすべての CDP フレームに一致します。
class-map type control-plane match-any copp-system-class-default	match protocol default	クラスはすべてのフレームに一致します。 デフォルト ポリサーに使用します。
class-map type control-plane match-any copp-system-class-dhcp	match protocol dhcp match protocol dhcp6	クラスは、すべての IPv4 DHCP パケットに一致します クラスは、すべての IPv4 DHCP パケットと IPv6 DHCP パケットの両方に一致します。
class-map type control-plane match-any copp-system-class-eigrp	match protocol eigrp match protocol eigrp6	クラスは、すべての IPv4 EIGRP パケットに一致します。 クラスは、IPv4 EIGRP パケットと IPv6 EIGRP パケットの両方に一致します。

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-exception	match protocol exception	Martian 宛先アドレスを持つパケットまたは MTU エラーが発生したパケットなど、クラスは IP ルーティングの目的で例外パケットとして扱われるすべての IP パケットに一致します（TTL 例外、IP フラグメント例外、および同一インターフェイス例外のパケットを除く）。
class-map type control-plane match-any copp-system-class-excp-ip-frag	match protocol ip_frag	クラスはフラグメント化したすべての IP パケットに一致します。（これらのパケットは、IP ルーティングの観点から例外パケットとして扱われます）。
class-map type control-plane match-any copp-system-class-excp-same-if	match protocol same-if	クラスは、IP ルーティングの例外パケットとして扱われるすべての IP パケットに一致します。パケットが一致するのは、宛先とすべきインターフェイスから受信したためです。
class-map type control-plane match-any copp-system-class-excp-ttl	match protocol ttl	クラスは、IP ルーティングの観点から TTL 例外パケットとして扱われる（TTL が 0 の場合）すべてのパケットに一致します。
class-map type control-plane match-any copp-system-class-fip	match protocol fip	クラスは FCoE Initialization Protocol に属するすべてのパケットに一致します。
class-map type control-plane match-any copp-system-class-glean	match protocol glean	クラスは、宛先の MAC 情報が使用不可能であるためにネクスト ホップにルーティングできないすべての IP パケットに一致します。

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-hsrp-vrrp	match protocol hsrp_vrrp match protocol hsrp6	クラスは、HSRP パケットおよび VRRP パケットに一致します。 クラスは、IPv4 HSRP、VRRP、および IPv6 HSRP パケットに一致します
class-map type control-plane match-any copp-system-class-icmp-echo	match protocol icmp_echo	クラスは、すべての ICMP エコー（ping）パケットに一致します。
class-map type control-plane match-any copp-system-class-igmp	match protocol igmp	クラスはすべての IGMP パケットに一致します。
class-map type control-plane match-any copp-system-class-isis	match protocol isis_dce	クラスはすべての ISIS プロトコル パケットに一致します。
class-map type control-plane match-any copp-system-class-l3dest-miss	match protocol unicast	クラスは FIB で宛先が見つからなかったすべてのユニキャスト ルーティングされたパケットに一致します。
class-map type control-plane match-any copp-system-class-lacp	match protocol lacp	クラスは、すべてのリンク アグリゲーション制御プロトコル（LACP）フレームに一致します。
class-map type control-plane match-any copp-system-class-lldp	match protocol lldp_dcx	クラスはすべての LLDP フレームに一致します。
class-map type control-plane match-any copp-system-class-mcast-miss	match protocol multicast	クラスは、FIB にエントリがないためにルーティングできなかったすべての IP マルチキャスト フレームに一致します。
class-map type control-plane match-any copp-system-class-mgmt	match protocol mgmt	クラスは、SNMP、HTTP、NTP、Telnet、SSH など、管理に関連するすべてのフレームに一致します。
class-map type control-plane match-any copp-system-class-msdp	match protocol msdp	クラスは MSDP パケットに一致します。

クラス マップ	設定	説明
class-map type control-plane match-any copp-system-class-ospf	match protocol ospf	クラスは OSPF プロトコル パケットに一致します。
class-map type control-plane match-any copp-system-class-pim-hello	match protocol pim	クラスはすべての PIM Hello パケットに一致します。
class-map type control-plane match-any copp-system-class-pim-register	match protocol reg	クラスはすべての PIM 登録パケットに一致します。
class-map type control-plane match-any copp-system-class-rip	match protocol rip	クラスはすべての RIP パケットに一致します。
class-map type control-plane match-any copp-system-class-udld	match protocol udld	クラスはすべての UDLD フレームに一致します。

CoPP ポリシー テンプレート

Cisco NX-OS デバイスの初回起動時に、DoS 攻撃からスーパーバイザ モジュールを保護するためのデフォルトの copp-system-policy が Cisco NX-OS ソフトウェアによりインストールされます。最初のセットアップ ユーティリティで、次のいずれかの CoPP ポリシー オプションを選択することにより、展開シナリオの CoPP ポリシー テンプレートを選択できます。

- デフォルト CoPP ポリシー（copp-system-policy-default）。
- 拡張レイヤ 2 CoPP ポリシー（copp-system-policy-scaled-l2）。
- 拡張レイヤ 3 CoPP ポリシー（copp-system-policy-scaled-l3）。
- カスタマイズされた CoPP ポリシー（copp-system-policy-customized）。

オプションを選択しなかった場合や、セットアップ ユーティリティを実行しなかった場合には、Cisco NX-OS ソフトウェアにより Default ポリシングが適用されます。 このデフォルト ポリシーから開始して、必要に応じて CoPP ポリシーを変更することを推奨します。

デフォルトの copp-system-policy-default ポリシーには、基本的なデバイス操作に最も適した値が設定されています。 使用する DoS に対する保護要件に適合するよう、特定のクラスや Access Control List（ACL; アクセス コントロール リスト）を追加する必要があります。

コントロール プレーン コンフィギュレーション モードで **service-policy input** *policy-name* コマンドを使用して、使用する CoPP ポリシーを変更できます。

デフォルト CoPP ポリシー

copp-system-policy-default ポリシーがスイッチにデフォルトで適用されます。 これには、ほとんどのネットワーク導入に適したポリサー レートを持つクラスが含まれています。 このポリシー、またはこれに関連付けられたクラスマップを変更することはできません。 また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-default
    class copp-system-class-igmp
      police cir 1024 kbps bc 65535 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-icmp-echo
      police cir 64 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-mcast-miss
      police cir 256 kbps bc 3200000 bytes
    class copp-system-class-excp-ip-frag
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-same-if
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-ttl
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-default
      police cir 2048 kbps bc 6400000 bytes
```

拡張レイヤ 2 CoPP ポリシー

copp-system-policy-scaled ポリシーには、デフォルト ポリシーと同じポリサー レートのほとんどのクラスがあります。 ただし、IGMP と ISIS に対しては、より高いポリサー レートが設定されています。 このポリシー、またはこれに関連付けられたクラスマップを変更することはできません。また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-scaled-l2
    class copp-system-class-igmp
      police cir 4096 kbps bc 264000 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-icmp-echo
      police cir 64 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-mcast-miss
      police cir 256 kbps bc 3200000 bytes
    class copp-system-class-excp-ip-frag
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-same-if
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-ttl
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-default
      police cir 2048 kbps bc 6400000 bytes
```

拡張レイヤ 3 CoPP ポリシー

copp-system-policy-scaled-l3 ポリシーには、デフォルト ポリシーと同じポリサー レートのほとんどのクラスがあります。 ただし、IGMP、ICMP エコー、ISIS、マルチキャスト欠落、および Glean に関連するクラスに対しては、より高いポリサー レートが設定されています。このポリシー、またはこれに関連付けられたクラスマップを変更することはできません。また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-scaled-l3
    class copp-system-class-igmp
      police cir 4096 kbps bc 264000 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 4000 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 4000 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-icmp-echo
      police cir 4000 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-mcast-miss
      police cir 4000 kbps bc 3200000 bytes
    class copp-system-class-excp-ip-frag
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-same-if
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-ttl
      police cir 64 kbps bc 3200000 bytes
```

```
    class copp-system-class-default
      police cir 2048 kbps bc 6400000 bytes
```

カスタマイズ可能な CoPP ポリシー

copp-system-policy-customized ポリシーは、デフォルト ポリシーと同様に設定され、別のクラス マップ情報のレートとバースト サイズ向けにカスタマイズできます。

このポリシーに設定されているクラス マップを追加または削除することはできません。

重要 このポリシーは上級ユーザ用です。 このポリシーを設定する場合は細心の注意を払い、実稼働ネットワークに導入する前に幅広いテストを行うことを推奨します。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy-customized
    class copp-system-class-igmp
      police cir 1024 kbps bc 65535 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-icmp-echo
      police cir 64 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-mcast-miss
```

```
  police cir 256 kbps bc 3200000 bytes
class copp-system-class-excp-ip-frag
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-same-if
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-ttl
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-default
  police cir 2048 kbps bc 6400000 bytes
```

CoPP と管理インターフェイス

Cisco NX-OS デバイスは、管理インターフェイス（mgmt0）をサポートしないハードウェア ベースの CoPP だけをサポートします。 アウトオブバンド mgmt0 インターフェイスは CPU に直接接続するため、CoPP が実装されているインバンド トラフィック ハードウェアは通過しません。

mgmt0 インターフェイスで、ACL を設定して、特定タイプのトラフィックへのアクセスを許可または拒否することができます。

CoPP のライセンス要件

この機能にはライセンスは不要です。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

CoPP の注意事項と制約事項

CoPP は、スイッチではデフォルトでイネーブルになっている機能です。 CoPP をイネーブルまたはディセーブルにすることはできません。

- 一度に 1 つのコントロール プレーン ポリシーだけを適用できます。
- CoPP ポリシーを削除すると、デフォルト CoPP ポリシーが適用されます。 このようにして、CoPP ポリシーが常に適用されます。
- クラスまたはポリシーの追加や削除はできません。
- クラスの順序の変更や、ポリシーのクラスの削除はできません。
- デフォルト、拡張レイヤ 2、または拡張レイヤ 3 ポリシーは変更できません。 ただし、カスタマイズされたポリシー内のクラスの情報レートやバースト サイズを変更することは可能です。
- カスタマイズされたポリシーが変更されていない限り、カスタマイズされたポリシー設定はデフォルトのポリシー設定と同じです。
- 以前のリリースからアップグレードしている場合は、デフォルト CoPP ポリシーがスイッチ上でデフォルトでイネーブルになります。

- カスタマイズされたポリシーを変更するか、または適用されたポリシーを変更すると、統計情報カウンタがリセットされます。
- ISSU を実行すると、統計情報カウンタがリセットされます。
- 最初にデフォルト CoPP ポリシーを使用した後、データセンターおよびアプリケーションの要件に基づいて、どの CoPP ポリシーを使用するかを後で決定することを推奨します。
- CoPP のカスタマイズは継続的なプロセスです。 CoPP は、特定の環境で使用されているプロトコルや機能のほか、サーバ環境に必要なスーパーバイザ機能に従って設定する必要があります。 これらのプロトコルや機能が変更されたら、CoPP を変更する必要があります。
- CoPP を継続的にモニタすることを推奨します。 ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。 どちらの場合も、状況を分析して、別の CoPP ポリシーを使用するか、またはカスタマイズされた CoPP ポリシーを変更する必要があるかどうかを評価します。
- 他のクラスマップで指定しないトラフィックはすべて、最後のクラス（デフォルト クラス）に配置されます。
- Cisco NX-OS ソフトウェアは、出力 CoPP とサイレント モードをサポートしません。 CoPP は、入力でのみサポートされます（コントロール プレーン インターフェイスに対して **service-policy output copp** コマンドは使用できません）。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

CoPP のデフォルト設定

次の表に、CoPP パラメータのデフォルト設定を示します。

表 *2*：*CoPP* パラメータのデフォルト設定

パラメータ	デフォルト
デフォルト ポリシー	copp-system-policy-default

CoPP の設定

スイッチへの CoPP ポリシーの適用

スイッチに次の CoPP ポリシーの 1 つを適用することができます。

- デフォルト CoPP ポリシー（copp-system-policy-default）。
- 拡張レイヤ 2 CoPP ポリシー（copp-system-policy-scaled-l2）。
- 拡張レイヤ 3 CoPP ポリシー（copp-system-policy-scaled-l3）。
- カスタマイズされた CoPP ポリシー（copp-system-policy-customized）。

手順の概要

1. switch# **configure terminal**
2. switch(config) # **control-plane**
3. switch(config-cp) # **service-policy input** *policy-map-name*
4. switch(config-cp) # **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **control-plane**	control-plane モードを開始します。
ステップ 3	switch(config-cp) # **service-policy input** *policy-map-name*	指定された CoPP ポリシー マップを適用します。*policy-map-name* には、copp-system-policy-default、copp-system-policy-scaled-l2、copp-system-policy-scaled-l3、または copp-system-policy-customized が適用可能です。
ステップ 4	switch(config-cp) # **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、デバイスに CoPP ポリシーを適用する例を示します。

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp) # service-policy input copp-system-policy-default
switch(config-cp) # copy running-config startup-config
```

カスタマイズされた CoPP ポリシーの変更

このポリシーに設定されたクラス マップの情報レートおよびバースト サイズだけを変更できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **policy-map type control-plane copp-system-policy-customized**
3. switch(config-pmap)# **class** *class-map-name*
4. switch(config-pmap-c)# **police cir** *rate-value* **kbps bc** *buffer-size* **bytes**
5. switch(config-pmap-c) # **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **policy-map type control-plane copp-system-policy-customized**	カスタマイズされた CoPP ポリシーのコンフィギュレーション モードを開始します。
ステップ 3	switch(config-pmap)# **class** *class-map-name*	定義済みポリシーの任意の CoPP にリスト表示された 28 の定義済みクラス マップのうちの 1 つを指定します。
ステップ 4	switch(config-pmap-c)# **police cir** *rate-value* **kbps bc** *buffer-size* **bytes**	認定情報レート（CIR）および認定バースト サイズ（BC）を設定します。 cir に指定できる範囲は 1 ～ 20480 です。bc に指定できる範囲は 1500 ～ 6400000 です。
ステップ 5	switch(config-pmap-c) # **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

次に、カスタマイズされた CoPP ポリシーを変更する例を示します。

```
switch(config)# policy-map type control-plane copp-system-policy-customized
switch(config-pmap)# class copp-system-class-bridging
switch(config-pmap-c)# police cir 10000 kbps bc 2400000 bytes
```

CoPP の設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	関連するクラス マップのあるコントロール プレーン ポリシー マップを表示します。

コマンド	目的
show policy-map interface control-plane	ポリシーの値と関連するクラスマップ、およびポリシーごとまたはクラスマップごとのドロップが表示されます。
show class-map type control-plane [*class-map-name*]	このクラス マップにバインドされている ACL を含め、コントロール プレーン クラス マップの設定を表示します。

CoPP 設定ステータスの表示

手順の概要

1. switch# **show copp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show copp status**	CoPP 機能の設定ステータスを表示します。

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

CoPP のモニタ

手順の概要

1. switch# **show policy-map interface control-plane**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show policy-map interface control-plane**	適用された CoPP ポリシーの一部であるすべてのクラスに関して、パケット レベルの統計情報を表示します。 一致した、および違反したパケット カウンタなど。

	コマンドまたはアクション	目的
		統計情報は、OutPackets（コントロール プレーンに対して許可されたパケット）と DropPackets（レート制限によってドロップされたパケット）に関して指定します。

次に、CoPP をモニタする例を示します。

```
switch# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy-default

class-map copp-system-class-igmp (match-any)
match protocol igmp
police cir 1024 kbps , bc 65535 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
class-map copp-system-class-pim-hello (match-any)
match protocol pim
police cir 1024 kbps , bc 4800000 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
....
```

CoPP 統計情報のクリア

手順の概要

1. （任意） switch#**show policy-map interface control-plane**
2. switch# **clear copp statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch#**show policy-map interface control-plane**	（任意） 現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。
ステップ 2	switch# **clear copp statistics**	CoPP 統計情報をクリアします。

次に、インターフェース環境で、CoPP 統計情報をクリアする例を示します。

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

CoPP に関する追加情報

ここでは、CoPP の実装に関する追加情報について説明します。

関連資料

関連項目	参照先
ライセンス	*Cisco NX-OS* ライセンス ガイド
コマンド リファレンス	『*Cisco Nexus 5000 Series NX-OS Security Command Reference*』

CoPP の機能の履歴

表 *3* : ***CoPP*** の機能の履歴

機能名	機能情報
CoPP	5.1(3)N1(1) で導入
CoPP	5.2(1)N1(1) での追加の IPv6 サポート