コントロール プレーン ポリシングの設定

この章は、次の項で構成されています。

- CoPP について, on page 1
- CoPP の注意事項と制約事項 （19 ページ）
- CoPP のデフォルト設定, on page 24
- CoPP の設定, on page 24
- 出力 CoPP のプロトコル ACL フィルタリング （33 ページ）
- CoPP の設定の確認, on page 37
- CoPP 設定ステータスの表示, on page 40
- CoPP のモニタリング, on page 40
- SNMP での CoPP のモニタリング （41 ページ）
- CoPP 統計情報のクリア, on page 42
- CoPP の設定例, on page 42
- CoPP に関する追加情報, on page 45

CoPP について

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 ポリシーに似ており、非管理ポートからスイッチに入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妨害（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。Cisco 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）や簡易ネットワーク管理プロトコル（SNMP）など、Cisco 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、管理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、Cisco 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

Caution 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。

次の例外は、ラインカードからのみ発生する可能性があります。

- match exception ip option
- match exception ipv6 option
- match exception ttl-failure

次の例外は、ファブリック モジュールからのみ発生する可能性があります。

- match exception ipv6 icmp unreachable
- match exception ip icmp unreachable

次の例外は、ラインカードとファブリック モジュールから発生する可能性があります。

- match exception mtu-failure

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。

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、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。クラス マップとポリシー マップを使用して、パケットの分類およびレート制御ポリシーを設定します。

出力 CoPP

Cisco NX-OS リリース 10.2(3)F 以降、出力 CoPP は Nexus 93180YC-EX、Nexus 93180YC-FX、Nexus 93240YC-FX2、Nexus 93360YC-FX2、Nexus 9336C-FX2、Nexus 9336C-FX2-E、Nexus 93180YC-FX3、N9K-C9316D-GX、N9K-C93600CD-GX、Nexus 9364C-GX、N9K-C9332D-GX2B、Nexus 9364C および Nexus 9332C クラウドスケール スイッチでサポートされます。

出力 CoPP は、カスタム/デフォルトの CoPP ポリシーに加えて適用できます。

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メカニズムがあります。スーパーバイザ モジュールへのトラフィックのレート制御には 2 つのメカニズムを使用します。1 つはポリシング、もう 1 つはレート制限と呼ばれるものです。

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）
望ましい帯域幅を、ビット レート、またはリンク レートの割合として指定します。

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。

さらに、一致トラフィックおよび違反トラフィックに対して、送信またはドロップなどの異なるアクションを設定できます。

ポリシング パラメータの詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

ダイナミックおよびスタティック CoPP ACL

CoPP アクセス コントロール リスト（ACL）は、ダイナミックまたはスタティックに分類されます。Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチは、ダイナミック CoPP ACL のみを使用します。Cisco Nexus 9200 シリーズ スイッチは、ダイナミック CoPP ACL とスタティック CoPP ACL の両方を使用します。

ダイナミック CoPP ACL は、転送情報ベース（FIB）ベースのスーパーバイザ リダイレクト パケットに対してのみ機能し、スタティック CoPP ACL は ACL ベースのスーパーバイザ リダイレクト パケットに対してのみ機能します。ダイナミック CoPP ACL は myIP およびリンク ローカル マルチキャスト トラフィックでサポートされ、スタティック CoPP ACL は他のすべてのタイプのトラフィックでサポートされます。

スタティック CoPP ACL は、サブストリングによって識別されます。これらのサブストリングのいずれかを持つ ACL は、スタティック CoPP ACL として分類されます。

- MAC ベースのスタティック CoPP ACL サブストリング：
  - acl-mac-cdp-udld-vtp
  - acl-mac-cfsoe
  - acl-mac-dot1x
  - acl-mac-l2-tunnel
  - acl-mac-l3-isis
  - acl-mac-lacp
  - acl-mac-lldp
  - acl-mac-sdp-srp
  - acl-mac-stp
  - acl-mac-undesirable
- プロトコルベースのスタティックCoPP ACLサブストリング：
  - acl-dhcp
  - acl-dhcp-relay-response
  - acl-dhcp6
  - acl-dhcp6-relay-response
  - acl-ptp
- マルチキャストベースのスタティックCoPP ACLサブストリング：
  - acl-igmp

スタティックCoPP ACLの詳細については、を参照してください。CoPP の注意事項と制約事項（19 ページ）

デフォルトのポリシング ポリシー

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-p-policy-strict ポリシーが 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、保護レベルを設定できます。

- Strict：このポリシーは 1 レート、2 カラーです。
- Moderate：このポリシーは 1 レート、2 カラーです。重要クラスのバースト サイズは strict ポリシーより大きく、lenient ポリシーより小さくなります。
- Lenient：このポリシーは 1 レート、2 カラーです。重要クラスのバースト サイズは moderate ポリシーより大きく、dense ポリシーより小さくなります。
- Dense：このポリシーは 1 レート、2 カラーです。ポリサーの CIR 値は、strict ポリシーよりも低くなります。
- Skip：コントロール プレーン ポリシーは適用されません。（ネットワークのコントロール プレーンに影響するため、Skip オプションの使用は推奨されません）。

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、strict ポリシングが適用されます。strict ポリシーから開始し、必要に応じて、CoPP ポリシーを変更することを推奨します。

Note POAP を使用する場合、デフォルトでは厳格なポリシングは適用されないため、CoPP ポリシーを設定する必要があります。

copp-system-p-policy 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、特定のクラスやアクセス コントロール リスト（ACL）を追加する必要があります。デフォルト CoPP ポリシーは、ソフトウェアをアップグレードしても変更されません。

Caution skip オプションを選択し、その後に CoPP 保護を設定していない場合、Cisco NX-OS デバイスは DoS 攻撃対して脆弱な状態になります。

CLI プロンプトから **setup** コマンドを実行して再度セットアップ ユーティリティを起動するか、または **copp profile** コマンドを使用して、CoPP のデフォルト ポリシーを再割り当てできます。

Related Topics

デフォルトの CoPP ポリシーの変更または再適用 （31 ページ）

デフォルト クラス マップ

copp-system-class-critical クラスの設定は次のとおりです。

```
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
```

copp-system-class-exception クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-exception
      match exception ip option
      match exception ip icmp unreachable
      match exception ipv6 option
      match exception ipv6 icmp unreachable
```

copp-system-class-exception-diag クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-exception-diag
      match exception ttl-failure
      match exception mtu-failure
```

copp-system-class-important クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-important
      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
```

copp-system-class-l2-default クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l2-default
      match access-group name copp-system-p-acl-mac-undesirable
```

copp-system-class-l2-unpoliced クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l2-unpoliced
      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
```

copp-system-class-l3mc-data クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l3mc-data
      match exception multicast rpf-failure
      match exception multicast dest-miss
```

copp-system-class-l3uc-data クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-l3uc-data
      match exception glean
```

copp-system-class-management クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-management
      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
```

copp-system-class-monitoring クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-monitoring
      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
```

copp-system-class-multicast-host クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-multicast-host
      match access-group name copp-system-p-acl-mld
```

copp-system-class-multicast-router クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-multicast-router
      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
```

copp-system-class-nat-flow クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-nat-flow
      match exception nat-flow
```

copp-system-class-ndp クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-ndp
      match access-group name copp-system-p-acl-ndp
```

copp-system-class-normal クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal
      match access-group name copp-system-p-acl-mac-dot1x
      match protocol arp
```

copp-system-class-normal-dhcp クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal-dhcp
      match access-group name copp-system-p-acl-dhcp
      match access-group name copp-system-p-acl-dhcp6
```

copp-system-class-normal-dhcp-relay-response クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-response
      match access-group name copp-system-p-acl-dhcp-relay-response
      match access-group name copp-system-p-acl-dhcp6-relay-response
```

copp-system-class-normal-igmp クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-normal-igmp
      match access-group name copp-system-p-acl-igmp
```

copp-system-class-redirect クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-redirect
      match access-group name copp-system-p-acl-ptp
```

copp-system-class-undesirable クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-undesirable
      match access-group name copp-system-p-acl-undesirable
      match exception multicast sg-rpf-failure
```

copp-system-class-fcoe クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-fcoe
      match access-group name copp-system-p-acl-mac-fcoe
```

（注） copp-system-class-fcoe クラスは Cisco Nexus 9200 シリーズ スイッチではサポートされていません。

strict デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、strict CoPP ポリシーの設定は次のとおりです。

（注） 新しいイメージにアップグレードする前の既存のコピーまたはカスタム CoPP プロファイルの CIR 値は、以前と同じ CIR 値になります。新しいイメージのデフォルト プロファイルからコピーされた新しい CoPP プロファイルでは、新しい CIR 値になります。

```
policy-map type control-plane copp-system-p-policy-strict
  class copp-system-p-class-l3uc-data
```

```
  set cos 1
  police cir 800 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-critical
  set cos 7
  police cir 36000 kbps bc 1280000 bytes conform transmit violate drop
class copp-system-p-class-important
  set cos 6
  police cir 2500 kbps bc 1280000 bytes conform transmit violate drop
class copp-system-p-class-multicast-router
  set cos 6
  police cir 2600 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-management
  set cos 2
  police cir 10000 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-multicast-host
  set cos 1
  police cir 1000 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 2400 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 2200 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1400 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 1300 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 1500 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 3000 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 280 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 150 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 800 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 400 kbps bc 32000 bytes conform transmit violate drop
class class-default
  set cos 0
  police cir 400 kbps bc 32000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、strict CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-strict
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 400 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 300 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 100 pps bc 64 packets conform transmit violate drop
```

```
  class copp-system-p-class-l2-default
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate drop
  class class-default
    set cos 0
    police cir 50 pps bc 32 packets conform transmit violate drop
```

moderate デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、moderate CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-moderate
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 1920000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 1920000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 192000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 192000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1300 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1500 kbps bc 96000 bytes conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 3000 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 150 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 150 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 192000 bytes conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate drop
```

```
  class copp-system-p-class-undesirable
    set cos 0
    police cir 200 kbps bc 48000 bytes conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 800 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 400 kbps bc 48000 bytes conform transmit violate drop
  class class-default
    set cos 0
    police cir 400 kbps bc 48000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、moderate CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-moderate
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1500 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 400 pps bc 96 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-monitoring
```

```
    set cos 1
    police cir 300 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 100 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 50 pps bc 48 packets conform transmit violate drop
  class class-default
    set cos 0
    police cir 50 pps bc 48 packets conform transmit violate drop
```

lenient デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、lenient CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-lenient
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 2560000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 2560000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1300 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1500 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 3000 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-redirect
```

```
    set cos 1
    police cir 280 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 200 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 800 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 400 kbps bc 64000 bytes conform transmit violate drop
  class class-default
    set cos 0
    police cir 400 kbps bc 64000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、lenient CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-lenient
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
```

```
    police cir 400 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 300 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 100 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 50 pps bc 64 packets conform transmit violate drop
  class class-default
    set cos 0
    police cir 50 pps bc 64 packets conform transmit violate drop
```

デンス デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、dense CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 4500 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 370 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 2500 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 2
    police cir 300 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 600 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
```

```
    police cir 1400 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 1
    police cir 350 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 750 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 750 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 1400 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 100 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
  class class-default
    set cos 0
    police cir 200 kbps bc 32000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、dense CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 2
    police cir 1000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 1200 pps bc 32 packets conform transmit violate drop
```

```
class copp-system-p-class-normal
  set cos 1
  police cir 750 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-ndp
  set cos 1
  police cir 750 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 150 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 200 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 2500 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 50 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 750 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop
```

1 秒間あたりのパケットのクレジット制限

特定のポリシーの 1 秒間あたりのパケット（PPS）の合計（ポリシーの各クラス部分の PPS の合計）の上限は、PPS のクレジット制限（PCL）の上限になります。特定のクラスの PPS が増加して PCL 超過すると、設定が拒否されます。目的の PPS を増やすには、PCL を超える PPS の分を他のクラスから減少させる必要があります。

モジュラ QoS コマンドライン インターフェイス

CoPP は、モジュラ QoS コマンドライン インターフェイス（MQC）を使用します。MQC は CLI の構造を持っています。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー（ポリシー マップ）の作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。トラフィック ポリシーには、トラフィック クラスに適用する CoPP 機能を含めます。

Procedure

ステップ 1 **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。

次に、copp-sample-class と呼ばれる新しいマップを作成する例を示します。

```
class-map type control-plane copp-sample-class
```

ステップ 2 **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィックの処理方法が決まります。

ステップ 3 **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロール プレーンに適用します。

次に、コントロール プレーンにポリシー マップを適用する例を示します。

```
control-plane
service-policy input copp-system-policy
```

Note
copp-system-policy は常に設定され、適用されます。このコマンドを明示的に使用する必要はありません。

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。

Related Topics

IP ACL の設定
MAC ACL の設定

CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- 最初に strict デフォルト CoPP ポリシーを使用し、後で、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 CoPP ポリシーを変更することを推奨します。

- 第 1 世代の Cisco Nexus 9000 シリーズ スイッチ（非 EX/FX/FX2）は、送信元ベースの CoPP をサポートしていません。この制限は、クラウド スケールの ASIC ベースの Cisco Nexus スイッチには存在しません。
- **match-all** オプションは CoPP クラスマップではサポートされず、常に **match-any** オプションにはデフォルトになります。
- CoPP のカスタマイズは継続的なプロセスです。CoPP を設定するときには、特定の環境で使用されるプロトコルや機能のみならず、サーバ環境に必要なスーパーバイザ機能を考慮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。いずれの場合も、状況を分析し、CoPP ポリシーを変更する必要を評価します。
- 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。このクラス内のドロップをモニタし、これらのドロップが必要のないトラフィックに基づいているのか、または設定されていないために追加が必要な機能の結果であるかどうかを調査します。
- アクセス コントロール リスト（ACL）を通してルータ プロセッサにリダイレクトする必要のあるパケット（たとえば、ARP および DHCP）を判定するために、すべてのブロードキャスト トラフィックが CoPP ロジックを通して送信されます。リダイレクトする必要のないブロードキャスト トラフィックは CoPP ロジックに対して照合され、準拠したパケットと違反したパケットの両方がハードウェア内でカウントされますが、CPU には送信されません。CPU に送信しなければならないブロードキャスト トラフィックと、CPU に送信する必要のないブロードキャスト トラフィックを異なるクラスに分離する必要があります。
- CoPP を設定した後、古いクラス マップや未使用のルーティング プロトコルなど、使用されていないものはすべて削除してください。
- CoPP ポリシーによって、ルーティング プロトコルなどのクリティカルなトラフィック、またはデバイスへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、Cisco NX-OS デバイスへのリモート アクセスが禁止され、コンソール接続が必要になる場合があります。
- 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）。
- ハードウェアのアクセス コントロール エントリ（ACE）ヒット カウンタは、ACL 論理だけで使用できます。CPU のトラフィックを評価するには、ソフトウェアの ACE ヒット カウンタと **show access-lists** および **show policy-map type control-plane** コマンドを使用します。
- Cisco NX-OS デバイスのハードウェアは、フォワーディング エンジン単位で CoPP を実行します。CoPP は分散ポリシーをサポートしていません。したがって、レートを選択する

場合は、集約トラフィックでスーパーバイザ モジュールに過剰な負荷をかけることのない値にしてください。

- 複数のフローが同じクラスにマッピングされる場合、個々のフローの統計情報は使用できません。
- CoPP 機能をサポートする Cisco NX-OS リリースから、新しいプロトコルのその他のクラスを含む CoPP 機能をサポートする Cisco NX-OS リリースにアップグレードする場合は、CoPP の新しいクラスを使用可能にするためにセットアップ ユーティリティを **setup** コマンドで実行するか **copp profile** コマンドを実行する必要があります。
- コントロール プレーン ポリシング（CoPP）機能をサポートしている Cisco NX-OS リリースから CoPP 機能をサポートしていない以前の Cisco NX-OS リリースへのダウングレードを実行する前に、**show incompatibility nxos bootflash:***filename* コマンドを使用して互換性を確認しておく必要があります。非互換な部分が存在する場合は、ソフトウェアをダウングレードする前に、ダウングレードイメージと互換性がない機能をすべて無効化してください。
- CoPP は無効にできません。これを無効にしようとすると、パケットは 50 パケット/秒。
- スキップ CoPP ポリシー オプションは、ネットワークのコントロール プレーンに影響を与える可能性があるため、Cisco NX-OS 初期設定ユーティリティから削除されました。
- Cisco Nexus 9200シリーズスイッチは、10 kbpsの倍数でのみCoPPポリサーレートをサポートします。10 kbpsの倍数でないレートが設定されている場合、そのレートは切り捨てられます。たとえば、55 Kbps のレートを設定しても、スイッチは 50 kbps を使用します。（**show policy-map type control-plane** コマンドで表示されるのはユーザ設定のレートです。詳細については、「CoPP の設定の確認 （37 ページ）」を参照してください）。
- Cisco Nexus 9200 シリーズ スイッチでは、ip icmp redirect、IPv6 icmp redirect、ip ICMP unreachable、ipv6 icmp unreachable、および mtu-failure は同じ TCAM エントリを使用し、これらがすべて分類されるクラスマップではポリシー中に最初の例外が存在します。CoPP 厳密プロファイルでは、クラス例外クラスマップに分類されます。別の CoP Pポリシーでは、最初の例外が異なるクラスマップ（たとえば、class-exception-diag）にある場合、残りの例外は同じクラスマップに分類されます。
- copp-system-class-fcoe クラスは Cisco Nexus 9200 シリーズ スイッチではサポートされていません。
- スタティック アCoPP ACL には、次のガイドラインと制限事項が適用されます。
  - Cisco Nexus 9200 シリーズ スイッチのみがスタティック CoPP ACL を使用します。
  - スタティック CoPP ACL は、別の CoPP クラスに再マッピングできます。
  - スタティック CoPP ACL のアクセス コントロール エントリ（ACE）は変更または削除できません。
  - CoPP ACL にスタティック ACL のサブストリングがある場合、このタイプのトラフィックに対してマッピングされます。たとえば、ACL に acl-mac-stp サブストリングが含まれている場合、STP トラフィックはこの ACL のクラス マップに分類されます。

- スタティック CoPP ACL は、CoPP ポリシー内での位置、設定される順序、および **show policy-map type control-plane** コマンドの出力での表示に関係なく、ダイナミック CoPP ACL よりも優先されます。
- CoPP ポリシーにスタティック CoPP ACL が必要です。これを行わないと、CoPP ポリシーは拒否されます。

- Cisco Nexus リリース 9.2(2) 以降、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX シリーズ スイッチ、および Cisco Nexus 9500 プラットフォーム スイッチは、プロトコル ACL フィルタリングをサポートしています。このリリースでは、IPv6 ACL はサポートされていません。
- Cisco NX-OS リリース 9.2(3) 以降では、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX シリーズ スイッチ、および Cisco Nexus 9500 プラットフォーム スイッチのダイナミック CoPP で IPv6 ACL がサポートされています。
- 出力 CoPP 用のプロトコル ACL フィルタリングには、次の制限があります。
  - 出力 CoPP ACL を定義すると、既存のルールを追加または削除できなくなります。これは、出力 CoPP ACL に付加されたすべてのクラスマップとポリシーマップに適用されます。
  - 既存の出力 CoPP を新しいポリシーで上書きすることはできません。新しいポリシーを追加する前に、既存の出力 CoPP を削除する必要があります。
  - 拒否アクションは適用されません。
  - すべてのエントリは TCAM でプログラムされ、同じエントリを持つ 2 つの MAC または IP ACL が作成され、同じまたは異なるクラスマップにバインドされている場合、異なる TCAM スペースを使用します。
  - 出力 CoPP でサポートされる TCAM カービングの最大数は 128 エントリです。24 エントリは予約済みで、残りの 104 エントリは出力 CoPP 用で、すべて倍幅です。これは、52（Ipv4、mac、Ipv6）エントリのいずれかになります。
  - ポリサーを使用すると、cir と burst を 0 にして、トラフィックを完全にドロップできます。
  - SNMP MIB は、サポートされません。
- パケットが複数の例外条件を満たしている場合、CoPP は CoPP ACL が設定されている順序に基づいてパケットを照合し、単一のクラスに対してのみ照合します。これは予期された CoPP 動作です。

  Cisco NX-OS リリース 9.3 (4) 以降では、UC FIB MISS 例外は CoPP クラス（copp-system-p-class-exception）に対してカウントされます。したがって、パケットに TTL（accounted user class copp-system-p-class-exception-diag）と UC FIM MISS 例外の両方がある場合、UC FIB MISS 例外と見なされます。この動作は、copp-system-p-class-exception クラスの順序が copp-system-p-class-exception-diag クラスよりも高い CoPP クラスの順位のた

めに発生します。NX-OS リリース 9.3(4) より前の NX-OS リリースでは、UC FIB MISS 例外は CoPP ルールによって明示的に処理されませんでした。

- CoPP 処理は 2 つの段階で構成されます。最初の段階では、各クラスポリシーで実際のパケット サイズが再利用されますが、パケットが 2 番目の段階に入ると、44 バイトの内部ヘッダーが追加されます。これにより、すべての CoPP クラスの適合ポリシーまたは違反ポリシーが変更されます。この制限は、Cisco Nexus 9300-FX、Nexus 9300-FX2、Nexus 9364C、Nexus 9332C、および 9300-GX プラットフォーム スイッチに適用されます。
- Cisco NX-OS リリース 10.1(2) 以降、CoPP は Cisco Nexus X9624D-R2 ライン カードおよび 9508-FM-R2 スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(2) 以降、CoPP は 9364D-GX2A および 9332D-GX2B スイッチでサポートされます。
- Cloudscale IPv6 リンクローカル BGP のサポートには、512 を超える ing-sup TCAM リージョンを切り分ける必要があります (これを有効にするには、リロードが必要です)。
- Cisco NX-OS リリース 10.3(1)F 以降、CoPP ACL は Cisco Nexus 9808 スイッチでサポートされます。
  - Cisco NX-OS リリース 10.4(1)F 以降、CoPP ACL は、Cisco Nexus X98900CD-A および X9836DM-A ライン カードを搭載した Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、CoPP ACL は、Cisco Nexus 9804 スイッチ、および Cisco Nexus X98900CD-A と X9836DM-A ライン カードでサポートされます。
- Cisco Nexus 9808/9804 スイッチには、SUP CoPP ACL サポートに関する次の制限があります。
  - ポリサー レートは、ステージ 1 で 161 PPS の倍数です。
  - ステージ 0 にはシェーパーがありません。
  - ステージ 2 の出力は LC/モジュール レベルで、ステージ 3 の出力は SUP/CPU レベルです。
  - ファブリック/FM は、インバンド パスに関与しません。
  - ステージ 1、ステージ 2、およびステージ 3 の CoPP ポリシーは PPS です。
  - CoPP ステージ 3 の統計情報は、システムのスイッチオーバー後にゼロにリセットされます。
  - カスタム CoPP では、ポリサー レートの変更のみがサポートされます。
- トラフィックの影響時にトラフィック損失を回避するには、Cisco Nexus 9300 GX/FX/FX2/FX3、9504-FM-G および 9508-FM-G スイッチと X9716D-GX ライン カードで CoPP クラスの通常の CIR 値を 2200 kbps に構成します。

- Cisco NX-OS リリース 10.3(2)F 以降、R/RX ラインカードを備えた Cisco Nexus 9504 および 9508 モジュラ シャーシで、CoPP の ソース IP ベースのフィルタリングのサポートが追加されました。

（注） IPv6 の場合、ソース IP ベースのフィルタリングは、24b MSB までサポートされます。

- Cisco NX-OS リリース 10.4(1)F 以降、CoPP ACL は Cisco Nexus 9332D-H2R スイッチでサポートされます。

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。

***Table 1: 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	strict
デフォルト ポリシー	9 ポリシー エントリ **Note** 関連するクラス マップでサポートされるポリシーの最大数は 128 です。
スケール ファクタ値	1.00

CoPP の設定

ここでは、CoPP の設定方法について説明します。

コントロール プレーン クラス マップの設定

コントロール プレーン ポリシーのコントロール プレーン クラス マップを設定する必要があります。

トラフィックを分類するには、既存の ACL に基づいてパケットを照合します。ACL キーワードの permit および deny は、照合時には無視されます。

IP バージョン 4（IPv4）および IP バージョン 6（IPv6）のパケットに対してポリシーを設定できます。

Before you begin

クラス マップ内で ACE ヒット カウンタを使用する場合は、IP ACL が設定してあることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	**class-map type control-plane** [**match-all** | **match-any**] *class-map-name*
	Example:
	`switch(config)# class-map type control-plane ClassMapA`
	`switch(config-cmap)#`
		コントロール プレーン クラス マップを指定し、クラスマップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。
		Note
		class-default、match-all、または match-any をクラス マップ名に使用できません。

ステップ 3	(Optional) **match access-group name** *access-list-name* **Example:** `switch(config-cmap)# match access-group name MyAccessList`	IP ACL のマッチングを指定します。 **Note** ACL キーワード permit および deny は、CoPP マッチング時には無視されます。
ステップ 4	(Optional) **match exception** {**ip** | **ipv6**} **icmp redirect** **Example:** `switch(config-cmap)# match exception ip icmp redirect`	IPv4 または IPv6 ICMP リダイレクト例外パケットのマッチングを指定します。
ステップ 5	(Optional) **match exception** {**ip** | **ipv6**} **icmp unreachable** **Example:** `switch(config-cmap)# match exception ip icmp unreachable`	IPv4 または IPv6 ICMP 到達不能例外パケットのマッチングを指定します。
ステップ 6	(Optional) **match exception** {**ip** | **ipv6**} **option** **Example:**	IPv4 または IPv6 ICMP オプション例外パケットのマッチングを指定します。

	Command or Action	Purpose
	`switch(config-cmap)# match exception ip option`	
ステップ 7	**match protocol arp** **Example:** `switch(config-cmap)# match protocol arp`	IP アドレス解決プロトコル（ARP）および逆アドレス解決プロトコル（RARP）パケットのマッチングを指定します。
ステップ 8	**exit** **Example:** `switch(config-cmap)# exit switch(config)#`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 9	(Optional) **show class-map type control-plane** [*class-map-name*] **Example:** `switch(config)# show class-map type control-plane`	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。
ステップ 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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ます。

コントロール プレーン ポリシー マップの設定

CoPP のポリシーマップを設定する必要があります。ポリシーマップにはポリシングパラメータを含めます。クラスのポリサーを設定しなかった場合、次のデフォルトが設定されます。

- 50 パケット/秒（pps）、32 パケットのバースト（Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチの場合）
- 150 キロビット/秒（kbps）、32,000 バイトのバースト（Cisco Nexus 9200 シリーズ スイッチの場合）

Before you begin

コントロール プレーン クラス マップが設定してあることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:**	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。

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**policy-map type control-plane** *policy-map-name*
	Example:
	`switch(config)# policy-map type control-plane ClassMapA`
	`switch(config-pmap)#`
		コントロール プレーン ポリシー マップを指定し、ポリシーマップ コンフィギュレーション モードを開始します。ポリシー マップ名は最大 64 文字で、大文字と小文字は区別されます。

ステップ 3	**class** {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}
	Example:
	`switch(config-pmap)# class ClassMapA`
	`switch(config-pmap-c)#`
		コントロール プレーン クラス マップ名またはクラスデフォルトを指定し、コントロールプレーン クラス コンフィギュレーション モードを開始します。
		class-default クラス マップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。

ステップ 4	次のいずれかのコマンドを入力します。
	• **police** [**cir**] {*cir-rate* [*rate-type*]}
	• **police** [**cir**] {*cir-rate* [*rate-type*]} [**bc**] *burst-size* [*burst-size-type*]
	• **police** [**cir**] {*cir-rate* [*rate-type*]]} **conform transmit** [**violate drop**]
	Example:
	`switch(config-pmap-c)# police cir 52000 bc 1000 packets`
	Example:
	`switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes`
		認定情報レート（CIR）を指定します。レート範囲を次に示します。
		• 01 ー 268435456 pps（Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチの場合）
		• 0 ー 80000000000 bps / gbps / kbps / mbps（Cisco Nexus 9200 シリーズ スイッチの場合）
		Note
		CIR レートの範囲は 0 から始まります。以前のリリースでは、CIR レートの範囲は 1 から始まります。0 の値ではパケットがドロップします。
		committed burst (BC) 範囲は次のようになります。
		• 1 ー 1073741パケット（Cisco Nexus 9300 および 9500 シリーズ、3164Q、31128PQ、3232C、および 3264Q スイッチの場合）
		• 1ー 512000000 バイト / kbytes / mbytes（Cisco Nexus 9200 シリーズ スイッチの場合）

	Command or Action	Purpose
		適合送信アクションは、パケットを送信します。 **Note** 同じ CIR に BC と一致（conform）アクションを指定できます。
ステップ 5	(Optional) **logging drop threshold** [*drop-count* [**level** *syslog-level*]] **Example:** `switch(config-pmap-c)# logging drop threshold 100`	ドロップされたパケットのしきい値を指定し、ドロップ数が設定したしきい値を超えた場合、Syslog を生成します。*drop-count* 引数の範囲は 1 ～ 8000000000 バイトです。*syslog-level* 引数の範囲は 1 ～ 7 であり、デフォルトレベルは 4 です。
ステップ 6	(Optional) **set cos** *cos-value* **Example:** `switch(config-pmap-c)# set cos 1`	802.1Q CoS 値を指定します。範囲は 0 ～ 7 です。デフォルト値は 0 です。

ステップ 7	**exit**
	Example:
	`switch(config-pmap-c)# exit`
	`switch(config-pmap)#`
		ポリシー マップ クラス コンフィギュレーション モードを終了します。

ステップ 8	**exit**
	Example:
	`switch(config-pmap)# exit`
	`switch(config)#`
		ポリシーマップ コンフィギュレーション モードを終了します。

ステップ 9	(Optional) **show policy-map type control-plane** [**expand**] [**name** *class-map-name*] **Example:** `switch(config)# show policy-map type control-plane`	コントロール プレーン ポリシー マップの設定を表示します。
ステップ 10	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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ます。

Related Topics

コントロール プレーン クラス マップの設定 （24 ページ）

コントロール プレーン サービス ポリシーの設定

CoPP サービス ポリシーに対して 1 つまたは複数のポリシー マップを設定できます。

Note CoPP ポリシーを変更し CoPP のカスタム ポリシーを適用しようとした場合、ハードウェア内では非アトミックとして設定され、次のメッセージが表示されます。

```
This operation can cause disruption of control traffic. Proceed (y/n)?  [no] y
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT24-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
 update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT23-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
 update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT21-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
 update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT25-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
 update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT26-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
 update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT22-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
 update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT4-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
 update done for CoPP
```

Before you begin

コントロール プレーン ポリシー マップが設定してあることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	**control-plane**
	Example:
	`switch(config)# control-plane`
	`switch(config-cp)#`
		コントロール プレーン 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	[**no**] **service-policy input** *policy-map-name* **Example:** `switch(config-cp)# service-policy input PolicyMapA`	入トラフィックのポリシー マップを指定します。ポリシー マップが複数ある場合は、このステップを繰り返します。 CoPPはディセーブルにできません。このコマンドの **no** 形式を入力すると、パケットは 50 パケット/秒。

	Command or Action	Purpose

ステップ 4	**exit**
	Example:
	`switch(config-cp)# exit`
	`switch(config)#`
		コントロール プレーン コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show running-config copp** [**all**] **Example:** `switch(config)# show running-config copp`	CoPP 設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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ます。

Related Topics

コントロール プレーン ポリシー マップの設定 （26 ページ）

ラインカードごとの CoPP のスケール ファクタの設定

ラインカードごとの CoPP のスケール ファクタを設定できます。

スケール ファクタの設定は、特定のラインカードに適用された CoPP のポリシーのポリサー レートのスケーリングに使用されます。受け入れ値は 0.10 ～ 2.00 です。特定のラインカードに対して現在の CoPP ポリシーを変更せずに、ポリサー レートを増加または削減できます。変更はすぐに有効となるため、CoPP ポリシーを再適用する必要はありません。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	**control-plane**
	Example:
	`switch(config)# control-plane`
	`switch(config-cp)#`
		コントロール プレーン 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	**scale-factor** *value* **module** *multiple-module-range* **Example:**	ライン カードごとにポリサー レートを設定します。許可されたスケール ファクタ値は 0.10 ～ 2.00 です。スケール ファクタ値が設定されている場合、ポリ

	Command or Action	Purpose
	`switch(config-cp)# scale-factor 1.10 module 1-2`	シング値にはモジュールの対応するスケール ファクタ値が乗算され、特定のモジュールにプログラミングされます。 デフォルトのスケール ファクタ値 1.00 に戻すには、**no scale-factor** *value* **module** *multiple-module-range* コマンドを使用するか、**scale-factor 1 module** *multiple-module-range* コマンドを使用して明示的にデフォルトのスケール ファクタである値 1.00 に設定します。
ステップ 4	(Optional) **show policy-map interface control-plane** **Example:** `switch(config-cp)# show policy-map interface control-plane`	CoPP ポリシーが適用される場合に適用されるスケール ファクタ値を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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ます。

デフォルトの CoPP ポリシーの変更または再適用

別のデフォルト CoPP ポリシーに変更したり、同じデフォルト CoPP ポリシーを再適用したりすることができます。

Procedure

	Command or Action	Purpose
ステップ 1	[] [| |] **nocopp profilestrictmoderatelenient dense** **Example:** `switch(config)# copp profile moderate`	CoPPベストプラクティスポリシーを適用します。 CoPPはディセーブルにできません。このコマンドに **no** フォームを入力する場合、パケットは 1 秒あたり 50 パケットににレート制限されます.
ステップ 2	(Optional) **show copp status** **Example:** `switch(config)# show copp status`	最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、CoPP ベスト プラクティス ポリシーがコントロー

	Command or Action	Purpose
		ル プレーンにアタッチされていることを確認することもできます。
ステップ 3	(Optional) **show running-config copp** **Example:** `switch(config)# show running-config copp`	実行コンフィギュレーション内の CoPP 設定を表示します。

Related Topics

セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用 （43 ページ）

CoPP ベスト プラクティス ポリシーのコピー

CoPP ベスト プラクティス ポリシーは読み取り専用です。その設定を変更する場合は、それをコピーする必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	**copp copy profile** {**strict** | **moderate** | **lenient** | **dense**} {**prefix** | **suffix**} *string* **Example:** `switch# copp copy profile strict prefix abc`	CoPP ベスト プラクティス ポリシーのコピーを作成します。 CoPP は、指定したプレフィックスまたはサフィックスのすべてのクラス マップおよびポリシー マップの名前を変更します。
ステップ 2	(Optional) **show copp status** **Example:** `switch# show copp status`	最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、コピーされたポリシーがコントロール プレーンにアタッチされていないことを確認することもできます。
ステップ 3	(Optional) **show running-config copp** **Example:** `switch# show running-config copp`	コピーされたポリシー設定を含む、実行コンフィギュレーション内の CoPP 設定を表示します。

出力 CoPP のプロトコル ACL フィルタリング

出力CoPPのプロトコルACLフィルタリングにより、NX-OSスイッチは、ホストMAC、IPv4、およびIPv6アドレスに基づいてコントロール プレーンへのすべてのトラフィックをフィルタリングできます。

出力 CoPP の ARP ACL フィルタリングの構成

出力 CoPP で、MAC ACL フィルタリングを構成できます。

Before you begin

コントロール プレーン ポリシー マップが設定してあることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **hardware access-list tcam region erg-copp** *size* **Example:** `switch(config)# hardware access-list tcam region erg-copp 128`	CoPP TCAM リージョン サイズを設定します。
ステップ 3	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	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ます。
ステップ 4	**reload** **Example:** `switch(config)# reload`	デバイスがリロードされます。 **Note** 新しいサイズの値は、**copy running-config startup-config** + **reload** を入力するか、すべてのラインカード モジュールをリロードした後にのみ有効になります。

ステップ 5	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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

	Command or Action	Purpose

ステップ 6	**mac access-list mac-foo-1**
	Example:
	`switch# mac access-list mac-foo-1`
	`switch(config-mac-acl)#`	

ステップ 7	**class-map type control-plane** [**match-all** | **match-any**] *class-map-name*
	Example:
	`switch(config)# class-map type control-plane match-any c-map2`
	`switch(config-cmap)#`
		コントロール プレーン クラス マップを指定し、クラスマップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。

ステップ 8	(Optional) **match access-group name** *access-list-name* **Example:** `switch(config-cmap)# match access-group name IP-foo-1`	

ステップ 9	**policy-map type control-plane** *policy-map-name*
	Example:
	`switch(config)# policy-map type control-plane ClassMapA`
	`switch(config-pmap)#`
		コントロール プレーン ポリシー マップを指定し、ポリシーマップ コンフィギュレーションモードを開始します。ポリシー マップ名は最大 64 文字で、大文字と小文字は区別されます。

ステップ 10	**class** {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}
	Example:
	`switch(config-pmap)# class ClassMap2`
	`switch(config-pmap-c)#`
		コントロール プレーン クラス マップ名またはクラスデフォルトを指定し、コントロールプレーン クラス コンフィギュレーションモードを開始します。
		class-default クラス マップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。

ステップ 11	次のいずれかのコマンドを入力します。 • **police** [**cir**] {*cir-rate* [*rate-type*]} • **police** [**cir**] {*cir-rate* [*rate-type*]} [**bc**] *burst-size* [*burst-size-type*] • **police** [**cir**] {*cir-rate* [*rate-type*]]} **conform transmit** [**violate drop**] **Example:** `switch(config-pmap-c)# police cir 52000 bc 1000 packets`	認定情報レート（CIR）を指定します。レート範囲を次に示します。 認定バースト（BC）の範囲は次のとおりです。

	Command or Action	Purpose

ステップ 12	**control-plane Dynamic mode**
	Example:
	`switch(config)# control-plane dynamic`
	`switch(config-cp-dyn)#`
		制御プレーン動的コンフィギュレーション モードに入ります。

ステップ 13	**service-policy-dynamic input** *policy-map-name* **Example:** `switch(config-cp-dyn)# service-policy-dynamic input PolicyMap1`	入トラフィックのポリシーマップを指定します。

出力 CoPP の IP ACL フィルタリングの構成

出力 CoPP で IP ACL フィルタリングを設定できます。

始める前に

コントロール プレーン ポリシー マップが設定してあることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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	[**no**] **hardware access-list tcam region erg-copp** *size* 例： `switch(config)# hardware access-list tcam region erg-copp 128`	CoPP TCAM リージョンの出力サイズを設定します。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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ます。
ステップ 4	**reload** 例： `switch(config)# reload`	デバイスがリロードされます。 （注） 新しいサイズの値は、**copy running-config startup-config** + **reload** を入力するか、すべてのラインカード

	コマンドまたはアクション	目的
		モジュールをリロードした後にのみ有効になります。

ステップ 5	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 6	**ip access-list IP-foo-1**
	例：
	`switch# ip access-list mac-foo-1`
	`switch(config-acl)#`	

ステップ 7	**permit tcp access-list IP-foo-1** *eq bgp* 例： `switch(config-acl)# 10 permit tcp 10.1.1.1/32 10.1.1.2/32 eq bgp`	

ステップ 8	**class-map type control-plane** [**match-all** | **match-any**] *class-map-name*
	例：
	`switch(config)# class-map type control-plane match-any c-map2`
	`switch(config-cmap)#`
		コントロール プレーン クラス マップを指定し、クラスマップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。

ステップ 9	**match access-group name** *access-list-name* 例： `switch(config-cmap)# match access-group name IP-foo-1`	

ステップ 10	**policy-map type control-plane** *policy-map-name*
	例：
	`switch(config)# policy-map type control-plane ClassMapA`
	`switch(config-pmap)#`
		コントロール プレーン ポリシー マップを指定し、ポリシーマップ コンフィギュレーションモードを開始します。ポリシー マップ名は最大 64 文字で、大文字と小文字は区別されます。

ステップ 11	**class** {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}
	例：
	`switch(config-pmap)# class ClassMap2`
	`switch(config-pmap-c)#`
		コントロール プレーン クラス マップ名またはクラスデフォルトを指定し、コントロールプレーン クラス コンフィギュレーションモードを開始します。
		class-default クラス マップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。

	コマンドまたはアクション	目的

ステップ 12	次のいずれかのコマンドを入力します。
	• **police** [**cir**] {*cir-rate* [*rate-type*]}
	• **police** [**cir**] {*cir-rate* [*rate-type*]} [**bc**] *burst-size* [*burst-size-type*]
	• **police** [**cir**] {*cir-rate* [*rate-type*]]} **conform transmit** [**violate drop**]
	例：
	`switch(config-pmap-c)# police cir 52000 bc 1000 packets`
	例：
	`switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes`
		認定情報レート（CIR）を指定します。レート範囲を次に示します。
		認定バースト（BC）の範囲は次のとおりです。

ステップ 13	**control-plane Dynamic mode**
	例：
	`switch(config)# control-plane dynamic`
	`switch(config-cp-dyn)#`
		制御プレーン動的コンフィギュレーション モードに入ります。

ステップ 14	**service-policy-dynamic input** *policy-map-name* 例： `switch(config-cp-dyn)# service-policy-dynamic input PolicyMap1`	入トラフィックのポリシーマップを指定します。終了

CoPP の設定の確認

CoPP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	コントロール プレーン ポリシー マップと関連するクラスマップ、および CIR と BC の値を表示します。

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。また、CoPP ポリシーが適用されている場合は、スケール ファクタ値も表示されます。スケール ファクタ値がデフォルト（1.00）の場合は表示されません。 **Note** スケール ファクタは、CIR と BC の値を各モジュールで内部的に変更しますが、ディスプレイに表示されるのは、設定された CIR と BC の値のみです。モジュールに実際に適用される値は、スケール ファクタに設定値を掛けた値です。
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。

コマンド	目的
show copp diff profile {**strict** | **moderate** | **lenient** | **dense**} [**prior-ver**] **profile** {**strict** | **moderate** | **lenient** | **dense**} **show copp diff profile**	2 つの CoPP ベスト プラクティス ポリシーの違いを表示します。 prior-ver オプションを指定しない場合、このコマンドは、現在適用されている 2 つのデフォルトの CoPP のベスト プラクティス ポリシー（現在適用されている厳密なポリシーと現在適用されている中程度のポリシーなど）の差異を表示します。 prior-ver オプションを指定した場合、このコマンドは、現在適用されているデフォルトの CoPP ベスト プラクティス ポリシーと以前に適用したデフォルトの CoPP ベスト プラクティス ポリシーの違いを表示します（現在適用されている厳密なポリシーと以前適用した緩いポリシーなど）。
show copp profile {**strict** | **moderate** | **lenient** | **dense**}	クラスおよびポリサー値とともに、CoPP ベスト プラクティス ポリシーの詳細を表示します。
show running-config aclmgr [**all**]	実行コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show running-config copp [**all**]	実行コンフィギュレーション内の CoPP 設定を表示します。

コマンド	目的
show startup-config aclmgr [**all**]	スタートアップ コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

CoPP 設定ステータスの表示

Procedure

	Command or Action	Purpose
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。

Example

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 のモニタリング

Procedure

	Command or Action	Purpose
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。 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。

Example

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-p-policy-strict

    class-map copp-system-p-class-critical (match-any)
      set cos 7
      police cir 19000 pps , bc 128 packets
      module 4 :
        transmitted 373977 packets;
        dropped 0 packets;
```

SNMP での CoPP のモニタリング

Cisco Nexus リリース 9.2(3) 以降、CoPP は Cisco クラスベース QoS MIB（cbQoSMIB）をサポートします。CoPP 要素はすべて、SNMP を使用してモニタできるようになりました（ただし変更は不可）。この機能は、コントロールプレーンにアタッチされたポリシーとサブ要素（クラス、一致ルール、セット アクションなど）にのみ適用されます。コントロール プレーンで使用されていないポリシーの要素は、SNMP では見えません。

次の cbQoSMIB テーブルがサポートされます。

- ccbQosServicePolicy
- cbQosInterfacePolicy
- cbQosObjects
- cbQosPolicyMapCfg
- cbQosClassMapCfg
- cbQosMatchStmtCfg
- cbQosPoliceCfg
- cbQosSetCfg

（注） SNMP MIB は、ダイナミック CoPP ではサポートされていません。

CoPP 統計情報のクリア

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) switch# **show policy-map interface control-plane**	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。

Example

次に、インターフェイス環境で、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 の設定例

ここでは、CoPP の設定例を示します。

CoPP の設定例

次に、IP ACL と MAC ACL を使用する CoPP を設定する例を示します。

```
configure terminal
ip access-list copp-system-p-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-p-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-p-acl-arp
permit any any 0x0806

ip access-list copp-system-p-acl-tacas
permit udp any any eq 49

ip access-list copp-system-p-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-p-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-igmp
match access-group name copp-system-p-acl-msdp
```

```
class-map type control-plane match-any copp-system-p-class-normal
match access-group name copp-system-p-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option

policy-map type control-plane copp-system-p-policy

class copp-system-p-class-critical
police cir 19000 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-important
police cir 500 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-normal
police cir 300 pps bc 32 packets conform transmit violate drop

class class-default
police cir 50 pps bc 32 packets conform transmit violate drop

control-plane
service-policy input copp-system-p-policy
```

CoPP クラスを作成し、ACL を関連付けるには、次のようにします。

```
class-map type control-plane copp-arp-class
match access-group name copp-arp-acl
```

CoPP ポリシーにクラスを追加するには、次のようにします。

```
policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500
```

次に、COPP 制限をカスタマイズする例を示します。

```
copp copy profile strict suffix CUSTOMIZED-COPP
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
class copp-class-redirect-CUSTOMIZED-COPP
police cir 1500 mbps bc 125 mbytes conform transmit violate drop
control-plane
service-policy input copp-policy-strict-CUSTOMIZED-COPP
```

セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用

セットアップ ユーティリティを使用して CoPP のデフォルト ポリシーを再適用する例を次に示します。

```
switch# setup

         ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
```

```
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.


Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no)[y]: <CR>

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : <CR>

  Enable license grace period? (yes/no) [n]: n

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

  Configure the default gateway? (yes/no) [y]: n

  Configure advanced IP options? (yes/no) [n]: <CR>

  Enable the telnet service? (yes/no) [n]: y

  Enable the ssh service? (yes/no) [y]: <CR>

    Type of ssh key you would like to generate (dsa/rsa) : <CR>

  Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L3]: <CR>

  Configure default switchport interface state (shut/noshut) [shut]: <CR>

  Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict


The following configuration will be applied:
  password strength-check
  no license grace-period
  no telnet server enable
  no system default switchport
  system default switchport shutdown
  policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#
```

CoPP ポリシー制限の変更

次の例では、CoPP 制限を変更して、PTP インターフェイス全体で PTP 状態を安定させます。

```
copp copy profile strict suffix CUSTOMIZED-COPP
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
class copp-class-redirect-CUSTOMIZED-COPP
police cir 1500 mbps bc 125 mbytes conform transmit violate drop
control-plane
service-policy input copp-policy-strict-CUSTOMIZED-COPP
```

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	マニュアル タイトル
ライセンス	*Cisco NX-OS* ライセンス ガイド

標準

標準	タイトル
RFC 2698	『A Two Rate Three Color Marker』

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。