コントロール プレーン ポリシングの設定

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、ルータまたはレイヤ 3 スイッチの任意の IP アドレスに宛てられた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。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、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、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。またたとえば、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。

次に、DoS 攻撃の例を示します。

- 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に、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。ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングやダイナミック アドレス解決プロトコル（ARP）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、クラスマップとポリシーマップを使用してパケット分類とレート制御ポリシーを設定し、厳格さを強めることが考えられます。

パケットの分類には、次のパラメータを使用できます。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- レイヤ 4 プロトコル

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。

ポリシング レートは 1 秒間あたりのパケット（PPS）という形式で指定されます。分類されたそれぞれのフローは、PPS で表すポリシング レート制限を指定することによって個別にポリシングできます。

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は、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 copp-system-policy が Cisco NX-OS ソフトウェアによって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。

- Default：レイヤ 2 およびレイヤ 3 ポリシー。CPU にバインドされているスイッチド トラフィックとルーテッド トラフィックの間で適切なポリシング バランスを提供します。
- Layer 2：レイヤ 2 ポリシー。CPU にバインドされているレイヤ 2 トラフィック（たとえば BPDU）により多くのプリファレンスを与えます。
- Layer 3：レイヤ 3 ポリシー。CPU にバインドされているレイヤ 3 トラフィック（たとえば、BGP、RIP、OSPF など）により多くのプリファレンスを与えます。

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。最初はこのデフォルト ポリシーを使用し、必要に応じて CoPP ポリシーを変更することを推奨します。

デフォルトの copp-system-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。

default、Layer 2 および Layer 3 テンプレートを切り替えるには、setup コマンドを使って設定ユーティリティを再び入力することができます。

デフォルト CoPP ポリシー

このポリシーは、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 テンプレートを変更することはできませんが、デバイスの CoPP 設定を変更できます。セットアップ ユーティリティを実行してデフォルトの CoPP ポリシー プロファイルをセットアップすると、CoPP ポリシーに対して既に行われたすべての変更が削除されます。

このポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1300
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
```

```
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 1000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 12000
  class copp-s-cdp
    police pps 400
  class copp-s-lacp
    police pps 400
  class copp-s-lldp
    police pps 200
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
  class copp-ftp
    police pps 100
  class copp-http
    police pps 100
```

レイヤ 2 CoPP ポリシー

このポリシーテンプレートを変更することはできませんが、デバイスの CoPP 設定を変更できます。セットアップ ユーティリティを実行してレイヤ 2 CoPP ポリシー プロファイルをセットアップすると、CoPP ポリシーに対して行われたすべての変更が削除されます。

このポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
```

```
  police pps 400
class copp-s-ipmc-g-hit
  police pps 400
class copp-s-ipmc-rpf-fail-g
  police pps 400
class copp-s-ipmc-rpf-fail-sg
  police pps 400
class copp-s-dhcpreq
  police pps 300
class copp-s-dhcpresp
  police pps 300
class copp-s-igmp
  police pps 400
class copp-s-routingProto2
  police pps 1200
class copp-s-eigrp
  police pps 200
class copp-s-pimreg
  police pps 200
class copp-s-pimautorp
  police pps 200
class copp-s-routingProto1
  police pps 900
class copp-s-arp
  police pps 200
class copp-s-ptp
  police pps 1000
class copp-s-bpdu
  police pps 12300
class copp-s-cdp
  police pps 400
class copp-s-lacp
  police pps 400
class copp-s-lldp
  police pps 200
class copp-icmp
  police pps 200
class copp-telnet
  police pps 500
class copp-ssh
  police pps 500
class copp-snmp
  police pps 500
class copp-ntp
  police pps 100
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
class copp-ftp
  police pps 100
class copp-http
  police pps 100
```

レイヤ 3 CoPP ポリシー

このポリシーテンプレートを変更することはできませんが、デバイスの CoPP 設定を変更できます。セットアップ ユーティリティを実行してレイヤ 3 CoPP ポリシー プロファイルをセットアップすると、CoPP ポリシーに対して行われたすべての変更が削除されます。

このポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 4000
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 4000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 6000
  class copp-s-cdp
    police pps 200
  class copp-s-lacp
    police pps 200
  class copp-s-lldp
    police pps 200
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
```

```
  police pps 100
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
class copp-ftp
  police pps 100
class copp-http
  police pps 100
```

CoPP クラス マップ

ポリシー内のクラスには、次の 2 つのタイプがあります。

- スタティック：これらのクラスは、各ポリシーテンプレートの一部であり、ポリシーまたは CoPP 設定から削除できません。スタティック クラスには、通常、デバイスの操作上重要と考えられ、ポリシーに必要なトラフィックが含まれます。
- ダイナミック：これらのクラスはポリシーから、作成、追加、または削除できます。ダイナミック クラスを使用して、要件に固有の CPU 行きトラフィック（ユニキャスト）用クラス/ポリシングを作成できます。

（注） copp-s-x という名前のクラスはスタティック クラスです。ACL は、スタティックとダイナミックの両方のクラスに関連付けることができます。

スイッチ宛ての Protocol-Independent Multicast（PIM）データ登録パケットと一致するように、新しい CoPP クラス「copp-s-pim-datareg」が追加されました。この CoPP クラスは、PIM データ登録パケットを 600 パケット/秒（pps）のポリサー レートで別個のキューに分類するために役立ちます。PIM プロトコルの 3 つの CoPP クラスを以下に示します。

- **copp-s-pimreg** - PIM hello や join-prune などの、マルチキャスト パケットである PIM プロトコル パケットに一致します。
- **copp-s-pimautorp** – PIM RP 選択プロトコル パケットに一致します。
- **copp-s-pim-datareg** - PIM データ登録パケットに一致します。

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。

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。

- 導入のシナリオに応じてデフォルト、L2、または L3 ポリシーを選択し、観察された動作に基づいて、CoPP ポリシーを後で変更することを推奨します。
- fast-reload を実行した後、トラフィックが完全に収束してから、トラフィックにおいて +/- 2 ～ 5 % の不規則性が約 30 ～ 40 秒間発生する場合は、ARP パケットに関する CoPP 値を大きくします。
- 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に加えて、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。
- **write erase** コマンドとリロードにより、**copp-s-bfd** コマンドに関して、ポリシングの 1 秒間あたりのパケット（PPS）のデフォルト値が 900 に変更されます。
- CoPP を継続的にモニター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済み 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。
- 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 は入力だけでサポートされます。**service-policy output copp** は、コントロール プレーン インターフェイスには適用できません。
- 新しい CoPP ポリシーの作成はサポートされていません。
- アップグレードする際には、デフォルト LLDP CoPP 値が 500 pps 未満であるかどうか確認してください。500 pps 未満である場合は、次のコマンドを使用して、手動で 500 pps に変更してください。

```
switch(config)# policy-map type control-plane policy-map-name
switch(config-pmap)# class copp-s-lldp
switch(config-pmap-c)# police pps 500
```

- glean（キャッシュ モードのクラス デフォルトのクラス マップ）に関するハードウェア カウンタはありません。
- MTU 障害クラス マップに関するカウンタはありません。
- NAT に関するハードウェア カウンタはありません。
- IPMCMISS に関するハードウェア カウンタはありません。
- スタティック クラス マップには match ACL ステートメントを追加できません。
- トンネルが設定されていない場合、Cisco Nexus 3500 シリーズ スイッチは、すべてのパケットをドロップします。また、トンネルが設定されている場合でも、トンネル インターフェイスが設定されていないか、トンネル インターフェイスがシャットダウン状態のときは、パケットがドロップされます。

  ポイントツーポイント トンネル（送信元と宛先）：Cisco Nexus 3500 シリーズ スイッチは、**feature tunnel** コマンドが設定されており、着信パケットの外部送信元および宛先アドレスと一致するトンネル送信元および宛先アドレスによって設定されている使用可能なトンネル インターフェイスが存在する場合に、そのスイッチを宛先とするすべての IP-in-IP パケットのカプセル化を解除します。送信元および宛先パケットが一致しない場合またはインターフェイスがシャットダウン状態の場合は、パケットがドロップされます。

  トンネルのカプセル化解除（送信元のみ）：Cisco Nexus 3500 シリーズ スイッチは、**feature tunnel** コマンドが設定されており、着信パケットの外部宛先アドレスと一致するトンネル送信元アドレスによって設定されている使用可能なトンネル インターフェイスが存在する場合に、そのスイッチを宛先とするすべての IP-in-IP パケットのカプセル化を解除します。送信元パケットが一致しない場合またはインターフェイスがシャットダウン状態の場合は、パケットがドロップされます。
- 前面パネル ポート経由で NXAPI を使用する場合は、パケットがドロップせず、出力が大きい CLI が予定時間内に戻るように、3000 PPS トラフィックを許可するように（http の）CoPP ポリシーを増やす必要があります。
- セットアップ スクリプトを実行すると、「*Enter to basic configuration (yes/no)?*」というプロンプトが表示されます。
  - *no* と応答すると、デフォルトの CoPP ポリシー テンプレートはシステムに適用されません。
  - *yes* と応答すると、稼働バージョンのデフォルトの CoPP ポリシー テンプレートがシステムに適用されます。この操作により、システム CoPP クラスに設定されているデフォルト以外のポリサー レートが上書きされます。

（注） スクリプトのセットアップ スクリプトの実行中に Ctrl+C を押すと、デフォルトの CoPP ポリシー テンプレートはシステムに適用されず、既存の CoPP ポリシーは変更されません

- セットアップ スクリプトを実行して基本設定を入力した後に Ctrl+C を押すと、残りのすべてのステップがスキップされ、「*Apply and save the config before exiting (yes/no)?*」というプロンプトが表示されます。
  - *no* と応答すると、デフォルトの CoPP ポリシーテンプレートはシステムに適用されません。
  - *yes* と応答すると、稼働バージョンのデフォルトの CoPP ポリシー テンプレートが適用されます。この操作により、システム CoPP クラスに設定されているデフォルト以外のポリサー レートが上書きされます。
- セットアップ スクリプトは、ユーザー定義の CoPP クラスを変更しません。
- セットアップ スクリプトが正常に実行され、その一環としてデフォルトの CoPP ポリシーテンプレートが適用されると、制御パケットが短時間ドロップされることがあります。この期間中に、コントロール プレーン プロトコルがフラップすることがあります。
- PPS のクレジットが使い果たされると、セットアップ スクリプトがデフォルトの CoPP ポリシーテンプレートの設定に失敗することがあります。これにより、PPS がゼロのシステム CoPP クラスが 1 つ以上生じることがあります。これにより、高い PPS 値を持つユーザー定義クラスがあるときに起こる可能性があります。デフォルトの CoPP ポリシーを適用するには、ユーザー定義の CoPP クラスの PPS 値を再設定して、セットアップ スクリプトを再度実行する必要があります。
- CDP（copp-s-cdp）、LLDP（copp-s-lldp）、LACP（copp-s-lacp）、BPDU（copp-s-bpdu）クラスのハードウェアおよびソフトウェア一致パケット カウンタが、Cisco Nexus 3548 プラットフォーム スイッチで集約されます。同様に、copp-s-dhcpreq および copp-s-dhcpresp クラスのハードウェアおよびソフトウェア一致パケット カウンタも集約されます。

CoPP のアップグレードに関する注意事項

CoPP には、アップグレードに関する次の注意事項があります。

- CoPP 機能をサポートしない Cisco NX-OS リリースから 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、スイッチの起動時にデフォルト ポリシーを使って CoPP が自動的にイネーブルにされます。別のポリシー（デフォルト、l3、l2）をイネーブルにするには、アップグレード後にセットアップ スクリプトを実行する必要があります。CoPP 保護を設定しない場合、NX-OS デバイスは DoS 攻撃に対して脆弱な状態のままになります。
- 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追加クラスを含む 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実行する必要があります。

- セットアップ スクリプトは、CPUに着信するさまざまなフローに対応するポリシング レートを変更するため、デバイスにトラフィックが発生する時間ではなく、スケジュールされたメンテナンス期間にセットアップ スクリプトを実行することを推奨します。
- Cisco NX-OS Release 6.0(2)A3(2) にアップグレードする際には、デフォルト LLDP CoPP 値が 500 pps 未満であるかどうか確認してください。500 より小さい場合は、次のコマンドを使用して、手動で 500 に変更してください。

```
switch(config)# policy-map type control-plane copp-system-policy
switch(config-pmap)# class copp-s-lldp
switch(config-pmap-c)# police pps 500
```

CoPP の設定

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 permit および deny は、マッチング時には無視されます。

始める前に

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。

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	**class-map type control-plane match-any** *class-map-name*
	例：
	`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。
		（注） 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。

	コマンドまたはアクション	目的
ステップ 3	（任意） **match access-group name** *access-list-name* 例： `switch(config-cmap)# match access-group name MyAccessList`	IP ACL のマッチングを指定します。複数の IP ACL のマッチングを行う場合は、このステップを繰り返します。 （注） 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	**exit**
	例：
	`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 5	（任意） **show class-map type control-plane** [*class-map-name*] 例： `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 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

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、そのクラスのデフォルトPPSは0になります。

IPv4 パケットのポリシーを設定できます。

始める前に

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。

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。

	コマンドまたはアクション	目的

ステップ 2	**policy-map type control-plane** *policy-map-name*
	例：
	`switch(config)# policy-map type control-plane copp-system-policy`
	`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 マップ名は大文字と小文字が区別されます。
		（注） ポリシー マップ名は変更できません。ポリシー マップの **copp-system-policy** 名のみを使用できます。単一の **type control-plane** ポリシー マップのみを設定できます。

ステップ 3	**class** {*class-map-name* | **class**}
	例：
	`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。

ステップ 4	**police** [**pps**] {*pps-value*} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] 例： `switch(config-pmap-c)# police pps 100 bc 10`	1 秒間あたりのパケット（PPS）およびコミット済みバースト（BC）に関するレート制限を指定します。PPS の範囲は 0 ～ 20,000 です。デフォルト PPS は 0 です。BC の範囲は 0 ～ 512000000 です。デフォルト BC サイズの単位はバイトです。

ステップ 5	**exit**
	例：
	`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 6	**exit**
	例：
	`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 7	（任意） **show policy-map type control-plane** [**expand**] [**name** *class-map-name*] 例： `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。

	コマンドまたはアクション	目的
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行設定を、スタートアップ設定にコピーします。

コントロール プレーン サービス ポリシーの設定

始める前に

コントロール プレーン ポリシー マップを設定します。

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	**control-plane**
	例：
	`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	**exit**
	例：
	`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 4	（任意） **show running-config copp** [**all**] 例： `switch(config)# show running-config copp`	CoPP 設定を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# 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、変更を継続的に保存します。

CoPP show コマンド

CoPP の設定情報を表示するには、次の show コマンドのいずれかを入力します。

コマンド	目的
show ip access-lists [*acl-name*]	CoPP の ACL を含め、システム内で設定されているすべての IPv4 ACL を表示します。
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。
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 PPS の値を表示します。
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。
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 startup-config copp [**all**]	スタートアップ 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。

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-policy

  class-map copp-s-default (match-any)
    police pps 400 , bc 0 packets
      HW Matched Packets    0
      SW Matched Packets   0
  class-map copp-s-ping (match-any)
    match access-group name copp-system-acl-ping
    police pps 100 , bc 0 packets
      HW Matched Packets    0
      SW Matched Packets   0
....
```

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

IP ACL の作成

```
ip access-list  copp-sample-acl
permit udp any any eq 3333
permit udp any any eq 4444
```

次に、着信パケットに適合する使用可能なトンネルが存在しない場合にすべての IP-in-IP（プロトコル 4）パケットを即座にドロップするように CoPP ポリシーを変更する例を示します。次の例に示すように、デフォルトの copp-s-selfip ポリシーの前に copp-s-ipinip を作成します。

```
ip access-list copp-s-ipinip
10 permit 4 any any
```

```
class-map type control-plane match-any copp-s-ipinip
match access-group name copp-s-ipinip
policy-map type control-plane copp-system-policy
class copp-s-ipinip
police pps 0
class copp-s-selfIp
police pps 500
class copp-s-default
police pps 400
```

関連する IP ACL を使用したサンプル CoPP クラスの作成

次に、CoPP の新規クラスおよび関連する ACL を作成する例を示します。

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

次に、CoPP ポリシーにクラスを追加する例を示します。

```
policy-map type control-plane copp-system-policy
Class copp-sample-class
 Police pps 100
```

次に、既存のクラス（copp-s-bpdu）の PPS を変更する例を示します。

```
policy-map type control-plane copp-system-policy
 Class copp-s-bpdu
 Police pps <new_pps_value>
```

既存または新規の CoPP のクラスと ACL を関連付ける

次に、ACL を既存または新規の CoPP クラスに関連付ける例を示します。

```
class-map type control-plane copp-s-eigrp
match access-grp name copp-system-acl-eigrp6
```

CoPP ポリシーにクラスを追加

次に、クラスがまだ追加されていない場合に、CoPP ポリシーにクラスを追加する例を示します。

```
policy-map type control-plane copp-system-policy
class copp-s-eigrp
police pps 100
```

ARP ACL ベースのダイナミック クラスの作成

ARP ACL では ARP TCAM を使用します。この TCAM のデフォルト サイズは 0 です。ARP ACL を CoPP で使用するには、その前に、この TCAM をゼロ以外のサイズに切り分ける必要があります。

```
hardware profile tcam region arpacl 128
copy running-config startup-config
reload
```

ARP ACL の作成

```
arp access-list copp-arp-acl
permit ip 20.1.1.1 255.255.255.0 mac any
```

ARP ACL をクラスに関連付けて、CoPP ポリシーにそのクラスを追加する手順は、IP ACL の場合の手順と同じです。

CoPP クラスの作成と ARP ACL の関連付け

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

CoPP ポリシーからのクラスの削除

```
policy-map type control-plane copp-system-policy
   no class-abc
```

システムからのクラスの削除

```
no class-map type control-plane copp-abc
```

コントロール プレーン クラス マップの設定の表示

```
show class-map type control-plane copp-s-pim-datareg
class-map type control-plane match-any copp-s-pim-datareg
```

次の例は、copp-s-pim-datareg クラスのインターフェイス コントロール プレーン情報を示しています。

```
switch# sh policy-map interface control-plane class copp-s-pim-datareg

       Control Plane

  service-policy  input: copp-system-policy

    class-map copp-s-pim-datareg (match-any)
      police pps 600 , bc 0 packets
        HW Matched Packets    55753
        SW Matched Packets   33931

switch#
```

insert-before オプションを使用して、パケットが複数のクラスと一致するかどうか、およびいずれか 1 つのクラスにプライオリティを割り当てる必要があるかどうかを確認

```
policy-map type control-plan copp-system-policy
class copp-ping insert-before copp-icmp
```

CoPP の設定例

次に、ACL、クラス、ポリシー、および個別のクラス ポリシングの CoPP の設定例を示します。

```
IP access list copp-system-acl-eigrp
        10 permit eigrp any 224.0.0.10/32
IP access list copp-system-acl-icmp
        10 permit icmp any any
IP access list copp-system-acl-igmp
        10 permit igmp any any
IP access list copp-system-acl-ntp
        10 permit udp any any eq ntp
```

```
        20 permit udp any eq ntp any
IP access list copp-system-acl-pimreg
        10 permit pim any any
IP access list copp-system-acl-ping
        10 permit icmp any any echo
        20 permit icmp any any echo-reply
IP access list copp-system-acl-routingproto1
        10 permit tcp any gt 1024 any eq bgp
        20 permit tcp any eq bgp any gt 1024
        30 permit udp any 224.0.0.0/24 eq rip
        40 permit tcp any gt 1024 any eq 639
        50 permit tcp any eq 639 any gt 1024
        70 permit ospf any any
        80 permit ospf any 224.0.0.5/32
        90 permit ospf any 224.0.0.6/32
IP access list copp-system-acl-routingproto2
        10 permit udp any 224.0.0.0/24 eq 1985
        20 permit 112 any 224.0.0.0/24
IP access list copp-system-acl-snmp
        10 permit udp any any eq snmp
        20 permit udp any any eq snmptrap
IP access list copp-system-acl-ssh
        10 permit tcp any any eq 22
        20 permit tcp any eq 22 any
IP access list copp-system-acl-stftp
        10 permit udp any any eq tftp
        20 permit udp any any eq 1758
        30 permit udp any eq tftp any
        40 permit udp any eq 1758 any
        50 permit tcp any any eq 115
        60 permit tcp any eq 115 any
IP access list copp-system-acl-tacacsradius
        10 permit tcp any any eq tacacs
        20 permit tcp any eq tacacs any
        30 permit udp any any eq 1812
        40 permit udp any any eq 1813
        50 permit udp any any eq 1645
        60 permit udp any any eq 1646
        70 permit udp any eq 1812 any
        80 permit udp any eq 1813 any
        90 permit udp any eq 1645 any
        100 permit udp any eq 1646 any
IP access list copp-system-acl-telnet
        10 permit tcp any any eq telnet
        20 permit tcp any any eq 107
        30 permit tcp any eq telnet any
        40 permit tcp any eq 107 any
IP access list copp-system-dhcp-relay
        10 permit udp any eq bootps any eq bootps
IP access list test
        statistics per-entry
        10 permit ip 1.2.3.4/32 5.6.7.8/32 [match=0]
        20 permit udp 11.22.33.44/32 any [match=0]
        30 deny udp 1.1.1.1/32 any [match=0]

class-map type control-plane match-any copp-icmp
  match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
  match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bfd
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-dai
class-map type control-plane match-any copp-s-default
```

```
class-map type control-plane match-any copp-s-dhcpreq
  match access-group name copp-system-acl-dhcps6
class-map type control-plane match-any copp-s-dhcpresp
  match access-group name copp-system-acl-dhcpc6
  match access-group name copp-system-dhcp-relay
class-map type control-plane match-any copp-s-eigrp
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-eigrp6
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-igmp
  match access-group name copp-system-acl-igmp
class-map type control-plane match-any copp-s-ipmcmiss
class-map type control-plane match-any copp-s-l2switched
class-map type control-plane match-any copp-s-l3destmiss
class-map type control-plane match-any copp-s-l3mtufail
class-map type control-plane match-any copp-s-l3slowpath
class-map type control-plane match-any copp-s-pimautorp
class-map type control-plane match-any copp-s-pimreg
  match access-group name copp-system-acl-pimreg
class-map type control-plane match-any copp-s-ping
  match access-group name copp-system-acl-ping
class-map type control-plane match-any copp-s-ptp
class-map type control-plane match-any copp-s-routingProto1
  match access-group name copp-system-acl-routingproto1
  match access-group name copp-system-acl-v6routingproto1
class-map type control-plane match-any copp-s-routingProto2
  match access-group name copp-system-acl-routingproto2
class-map type control-plane match-any copp-s-selfIp
class-map type control-plane match-any copp-s-ttl1
class-map type control-plane match-any copp-s-v6routingProto2
  match access-group name copp-system-acl-v6routingProto2
class-map type control-plane match-any copp-snmp
  match access-group name copp-system-acl-snmp
class-map type control-plane match-any copp-ssh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-stftp
  match access-group name copp-system-acl-stftp
class-map type control-plane match-any copp-tacacsradius
  match access-group name copp-system-acl-tacacsradius
class-map type control-plane match-any copp-telnet
  match access-group name copp-system-acl-telnet
policy-map type control-plane copp-system-policy
  class copp-s-selfIp
    police pps 500
  class copp-s-default
    police pps 400
  class copp-s-l2switched
    police pps 200
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-l3slowpath
    police pps 100
  class copp-s-dhcpreq
    police pps 300
```

```
  class copp-s-dhcpresp
    police pps 300
  class copp-s-dai
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1300
  class copp-s-v6routingProto2
    police pps 1300
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 1000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bfd
    police pps 350
  class copp-s-bpdu
    police pps 12000
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
control-plane
  service-policy input copp-system-policy
```

例：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、デフォルトCoPPポリシーを変更または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

  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 : switch

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

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

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

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

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

  Configure CoPP System Policy Profile ( default / l2 / l3 ) [default]: l2

The following configuration will be applied:
  switchname switch
  telnet server enable
  no ssh server enable
  policy-map type control-plane copp-system-policy ( l2 )

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

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

[########################################] 100%
```

例：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

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。