



## コントロールプレーンポリシングの設定

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

この章は、次の内容で構成されています。

- [CoPP の概要, 2 ページ](#)
- [コントロールプレーンの保護, 3 ページ](#)
- [CoPP ポリシー テンプレート, 5 ページ](#)
- [CoPP のクラス マップ, 8 ページ](#)
- [1 秒間あたりのパケットのクレジット制限, 9 ページ](#)
- [CoPP と管理インターフェイス, 9 ページ](#)
- [CoPP のライセンス要件, 9 ページ](#)
- [CoPP の注意事項と制約事項, 9 ページ](#)
- [CoPP のアップグレードの注意事項, 10 ページ](#)
- [CoPP の設定, 10 ページ](#)
- [CoPP show コマンド, 15 ページ](#)
- [CoPP 設定ステータスの表示, 16 ページ](#)
- [CoPP のモニタ, 16 ページ](#)
- [CoPP 統計情報のクリア, 17 ページ](#)
- [CoPP の設定例, 18 ページ](#)
- [CoPP の設定例, 19 ページ](#)
- [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, 22 ページ](#)
- [CoPP に関する追加情報, 23 ページ](#)

- [CoPP の機能の履歴, 23 ページ](#)

## 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拒絶 (DoS) 攻撃です。

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

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

### データ プレーン

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

### コントロールプレーン

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

### 管理プレーン

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

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

プレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

DoS 攻撃の例は次のとおりです。

- インターネット制御メッセージプロトコル (ICMP) エコー要求
- IP フラグメント
- TCP SYN フラッディング

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

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



注意

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

## コントロールプレーンの保護

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

## コントロールプレーンのパケットタイプ

コントロールプレーンには、次のような異なるタイプのパケットが到達します。

### 受信パケット

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

### 例外パケット

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

### リダイレクトパケット

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

### 収集パケット

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

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

## CoPP の分類

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

次のパラメータは、パケットの分類に使用できます。

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

- **Default** : スイッチドトラフィックとルーテッドトラフィック間の、CPU にバインドされているポリシングの適切なバランスを提供するレイヤ 2 およびレイヤ 3 のポリシー。
- **Layer 2** : 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るレイヤ 2 ポリシー
- **Layer 3** : 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るレイヤ 3 ポリシー

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。デフォルト ポリシーから開始して、必要に応じて後で 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 Access Control List (ACL; アクセス コントロール リスト) を追加する必要があります。

`setup` コマンドを使用して設定ユーティリティを再入力することで、**default**、**Layer 2** および **Layer 3** のテンプレートを切り替えることができます。

## 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、またはこれに関連付けられたクラス マップを変更することはできません。また、このポリシーのクラス マップ設定も変更できません。

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy
  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-ipmcmis
  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 300

```

## レイヤ 2 CoPP ポリシー

このポリシーには次の設定があります。

```

policy-map type control-plane copp-system-policy
  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-ipmcmis
  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 1200
class copp-s-v6routingProto2
  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-ntp
  police pps 1000
class copp-s-bfd
  police pps 350
class copp-s-bpdu
  police pps 12300
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
```

## レイヤ 3 CoPP ポリシー

このポリシーには次の設定があります。

```
policy-map type control-plane copp-system-policy
  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-ipmcmis
    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 4000
class copp-s-v6routingProto2
    police pps 1600
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-ntp
    police pps 1000
class copp-s-bfd
    police pps 350
class copp-s-bpdu
    police pps 6000
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

```

## CoPP のクラス 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行きトラフィック用クラス/ポリシーを作成できます。



(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。

## 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 のライセンス要件

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

## CoPP の注意事項と制約事項

CoPP 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。
- CoPP のカスタマイズは継続的なプロセスです。CoPP は、特定の環境で使用されているプロトコルや機能のほか、サーバ環境に必要なスーパーバイザ機能に従って設定する必要があります。これらのプロトコルや機能に変更されたら、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反応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、状況を分析して、別の CoPP ポリシーを使用するか、またはカスタマイズされた CoPP ポリシーを変更する必要があるかどうかを評価します。
- 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。
- IPv6 と IPv4 の CoPP ACL エントリには、別々の TCAM リージョンを使用します。IPv6 CoPP が動作するには、IPv6 ACL SUP TCAM リージョン (`ipv6-sup`) がゼロ以外のサイズに切り分けられている必要があります。詳細については、[ACL TCAM リージョン](#) および [ACL TCAM リージョン サイズの設定](#) のトピックを参照してください。

## CoPP のアップグレードの注意事項

CoPP 機能をサポートする Cisco NX-OS リリースに CoPP 機能をサポートしないリリースからアップグレードする場合は、アップグレード後にデバイスの CoPP をイネーブル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。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がある 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。

たとえば、Cisco NX-OS Release 5.0(3)U2(2) (CoPP 機能をサポートする) から Cisco NX-OS Release 5.0(3)U3(1) (IPv6 サポートの CoPP クラスを追加する) にアップグレードする場合、デバイス上の IPv6 CoPP 機能をイネーブルにするためにセットアップスクリプトを実行する必要があります。

セットアップスクリプトが 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。

## 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 キーワードの `permit` および `deny` は、照合時には無視されます。

IPv4 または IPv6 パケットのポリシーを設定できます。

### はじめる前に

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。

### 手順の概要

1. **configure terminal**
2. **class-map type control-plane match-any class-map-name**
3. (任意) **match access-group name access-list-name**
4. **exit**
5. (任意) **show class-map type control-plane [class-map-name]**
6. (任意) **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>class-map type control-plane match-any class-map-name</b>  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 <b>match-any</b> 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) <b>class-default</b> 、 <b>match-all</b> 、または <b>match-any</b> をクラスマップ名に使用できません。
ステップ 3	<b>match access-group name access-list-name</b>  例： switch(config-cmap)# match access-group name MyAccessList	(任意) 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 キーワードの <b>permit</b> および <b>deny</b> は、CoPP 照合時には無視されます。
ステップ 4	<b>exit</b>  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	<b>show class-map type control-plane [class-map-name]</b>  例： switch(config)# show class-map type control-plane	(任意) 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。

	コマンドまたはアクション	目的
ステップ 6	<b>copy running-config startup-config</b>  例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 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、デフォルトの PPS をサポートします。

IPv4 または IPv6 パケットのポリシーを設定できます。

はじめる前に

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。

### 手順の概要

1. **configure terminal**
2. **policy-map type control-plane *policy-map-name***
3. **class** {*class-map-name* [**insert-before** *class-map-name2*] | **class**}
4. **police** [**pps**] {*pps-value*}
5. **exit**
6. **exit**
7. (任意) **show policy-map type control-plane** [**expand**] [**name** *class-map-name*]
8. (任意) **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config)#</pre>	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	<b>policy-map type control-plane <i>policy-map-name</i></b>  例： <pre>switch(config)# policy-map type control-plane copp-system-policy switch(config-pmap)#</pre>	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。

	コマンドまたはアクション	目的
ステップ 3	<p><b>class</b> {<i>class-map-name</i> [<b>insert-before</b> <i>class-map-name2</i>]   <b>class</b>}</p> <p>例： switch(config-pmap)# class ClassMapA switch(config-pmap-c)#</p>	<p>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。</p>
ステップ 4	<p><b>police</b> [<b>pps</b>] {<i>pps-value</i>}</p> <p>例： switch(config-pmap-c)# police pps 100</p>	<p>パケット/秒 (PPS) の観点から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。</p>
ステップ 5	<p><b>exit</b></p> <p>例： switch(config-pmap-c)# exit switch(config-pmap)#</p>	<p>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。</p>
ステップ 6	<p><b>exit</b></p> <p>例： switch(config-pmap)# exit switch(config)#</p>	<p>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。</p>
ステップ 7	<p><b>show policy-map type control-plane</b> [<b>expand</b>] [<b>name</b> <i>class-map-name</i>]</p> <p>例： switch(config)# show policy-map type control-plane</p>	<p>(任意) 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。</p>
ステップ 8	<p><b>copy running-config startup-config</b></p> <p>例： switch(config)# copy running-config startup-config</p>	<p>(任意) 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。</p>

## コントロールプレーン サービス ポリシーの設定

はじめる前に

コントロールプレーン ポリシー マップを設定します。

手順の概要

1. **configure terminal**
2. **control-plane**
3. **[no] service-policy input *policy-map-name***
4. **exit**
5. (任意) **show running-config copp [all]**
6. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>control-plane</b>  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	<b>[no] service-policy input <i>policy-map-name</i></b>  例： switch(config-cp)# service-policy input copp-system-policy	入トラフィックのポリシー マップを指定します。
ステップ 4	<b>exit</b>  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 5	<b>show running-config copp [all]</b>  例： switch(config) # show running-config copp	(任意) CoPP 設定を表示します。
ステップ 6	<b>copy running-config startup-config</b>  例： switch(config) # copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を永続的に保存します。

# 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
<b>show ip access-lists</b> [ <i>acl-name</i> ]	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。
<b>show class-map type control-plane</b> [ <i>class-map-name</i> ]	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。
<b>show ipv6 access-lists</b>	CoPP IPv6 ACL を含め、デバイス上で設定されているすべての IPv6 ACL を表示します。
<b>show arp access-lists</b>	CoPP ARP ACL を含め、デバイス上で設定されているすべての ARP ACL を表示します。
<b>show policy-map type control-plane</b> [expand] [ <i>name</i> <i>policy-map-name</i> ]	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。
<b>show running-config copp</b> [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。
<b>show running-config aclmgr</b> [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。 <b>all</b> 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。
<b>show startup-config copp</b> [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
<code>show startup-config aclmgr [all]</code>	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。 <b>all</b> 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

### 手順の概要

1. `switch# show copp status`

### 手順の詳細

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

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

## CoPP のモニタ

### 手順の概要

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

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>switch# show policy-map interface control-plane</code>	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。



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

次に、CoPP をモニタする例を示します。

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

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

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

## CoPP 統計情報のクリア

### 手順の概要

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

### 手順の詳細

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

次に、インターフェース環境で、CoPP 統計情報をクリアする例を示します。

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

## CoPP 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
```

### 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>
```

### ダイナミック クラス (IPv6 ACL) の作成

次に、IPv6 ACL を作成する例を示します

```
ipv6 access-list copp-system-acl-eigrp6
10 permit 88 any ff02::a/128
```

次に、CoPP の既存または新規クラスと ACL を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
```

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 で使用できるようにする前に、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
```

**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、およびプライオリティをこれらのいずれかに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-routingprotol
  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]

IPv6 access list copp-system-acl-dhcpc6
10 permit udp any any eq 546
IPv6 access list copp-system-acl-dhcps6
10 permit udp any ff02::1:2/128 eq 547
20 permit udp any ff05::1:3/128 eq 547
IPv6 access list copp-system-acl-eigrp6
10 permit 88 any ff02::a/128
IPv6 access list copp-system-acl-v6routingProto2
10 permit udp any ff02::66/128 eq 2029
20 permit udp any ff02::fb/128 eq 5353
IPv6 access list copp-system-acl-v6routingproto1
10 permit 89 any ff02::5/128
20 permit 89 any ff02::6/128
30 permit udp any ff02::9/128 eq 521

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-dhcreq
match access-group name copp-system-acl-dhcps6
class-map type control-plane match-any copp-s-dhcreq
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-ipmcmis
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-ntp
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-snmpp
  match access-group name copp-system-acl-snmpp
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-stftpp
  match access-group name copp-system-acl-stftpp
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-ipmcmisss
    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-routingProtol
    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-snmpp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius

```

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

```

    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 / 12 / 13 ) [default]: 12

The following configuration will be applied:
  switchname switch
  telnet server enable
  no ssh server enable
  policy-map type control-plane copp-system-policy ( 12 )

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

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

[#####] 100%

```

## CoPPに関する追加情報

ここでは、CoPPの実装に関する追加情報について説明します。

### 関連資料

関連項目	参照先
ライセンス	Cisco NX-OS ライセンス ガイド
コマンドリファレンス	『Cisco Nexus 3000 Series Command Reference』

## CoPPの機能の履歴

表 1: CoPPの機能の履歴

機能名	機能情報
CoPP	5.0(3)U2(1)で導入
IPv6	5.0(3)U3(1)で導入
複数のACLをIPv4およびIPv6アクセスリストを含むCoPPクラスに関連付けることができます。	5.0(3)U3(1)で導入

