CHAPTER 20

CoPP の設定

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

ここでは、次の内容を説明します。

- CoPP の概要（p.20-2）
- 注意事項および制限事項（p.20-6）
- CoPP の設定（p.20-7）
- CoPP 統計情報の表示（p.20-13）
- CoPP 設定の確認（p.20-14）
- CoPP の設定例（p.20-15）
- デフォルト設定（p.20-16）
- その他の参考資料（p.20-17）

CoPP の概要

NX-OS デバイスは、DoS 攻撃によるパフォーマンスへの影響を防ぐために CoPP を備えています。

スーパーバイザ モジュールは、管理する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。Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）や OSPF などのルーティング プロトコルは、装置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。
- マネージメント プレーン — CLI（コマンドライン インターフェイス）や 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、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。スーパーバイザ モジュールへの攻撃には、DoS 攻撃のようにコントロール プレーンを流れる IP トラフィック ストリームが非常に高いレートで発生するものなど、さまざまな種類があります。攻撃によってコントロール プレーンはこれらのパケットの処理に大量の時間を費やしてしまい、本来のトラフィック処理が不可能になります。

次に、DoS 攻撃の例を示します。

- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）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装置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。

- スーパーバイザの CPU 利用率が高くなります。
- キープアライブ メッセージおよびルーティング プロトコル アップデートが紛失します。これによりルート フラップおよび大規模なネットワークの停止につながります。
- 高い CPU 利用率により、CLI を使用する対話型セッションが遅くなったり、まったく応答がなくなったりします。
- メモリやバッファなどのリソースを正規の IP データ パケットに使用できなくなることがあります。
- パケット キューがいっぱいになり、種類を問わずパケットがドロップします。

注意　コントロール プレーンの保護策を適切に講じることで、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。

ここでは、次の内容について説明します。

- コントロール プレーンの保護（p.20-3）
- MQC（p.20-5）

- バーチャライゼーション サポート（p.20-5）

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、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、NX-OS デバイスはパケットをポリシングまたはマーク付けします。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らないようになります。

ここでは、次の内容について説明します。

- コントロール プレーンのパケット タイプ（p.20-3）
- 分類（p.20-3）
- レート制御メカニズム（p.20-4）
- デフォルトのポリシング ポリシー（p.20-4）

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。ほかには、IP オプションがセットし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。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）検査などの機能は、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。
- グリーニング 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、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。

分類

効果的に保護するために、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し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。パケットの分類に使用できるパラメータは、次のとおりです。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元 MAC アドレス
- 宛先 MAC アドレス
- VLAN

- 送信元ポート
- 宛先ポート
- 例外事由

レート制御メカニズム

パケットの分類が終わると、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 ポリシーを使用すると、トラフィックが所定の条件に一致する場合、超過する場合、または違反する場合のそれぞれ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。

- Committed information rate（CIR; 認定情報速度）
- PIR（Peak Information Rate; 最大情報レート）
- Committed burst（Bc; 認定バースト）サイズ
- Extended burst（Be; 拡張バースト）サイズ

さらに、一致トラフィック、超過トラフィック、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。

デフォルトのポリシング ポリシー

デフォルト ポリシーは、NX-OS デバイスを初回に起動したときに選択できます。NX-OS ソフトウェアには、コントロール プレーンの保護に使用できるデフォルト ポリシーがいくつか用意されています。最初のセットアップ スクリプトで、次のいずれかの CoPP ポリシー オプションを選択できます。

- strict
- moderate
- lenient
- none

オプションを選択しなかった場合や、セットアップ スクリプト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。CoPP ポリシーは、必要に応じてあとで変更できます。

注意　CoPP 保護を設定しないで none オプションを選択すると、NX-OS デバイスは DoS 攻撃対して脆弱なままになります。

MQC

CoPP は、Modular QoS（Quality of Service）CLI（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。

MQC の構造は、次の上位レベルの手順からなります。

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。

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。

バーチャライゼーション サポート

CoPP はデフォルト Virtual Device Context（VDC）でのみ設定できますが、その CoPP 設定は NX-OS デバイス上のすべての VDC に適用されます。VDC の詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』を参照してください。

CoPP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	CoPP に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、無償で提供されます。NX-OS のライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide, Release 4.0*』を参照してください。

注意事項および制限事項

CoPP には、次の構成に関する注意事項と制限事項があります。

- CoPP は、デフォルトの非 IP クラス以外の非 IP クラスをサポートしません。非 IP トラフィックをドロップする場合は、非 IP クラスの代わりに ACL を使用できます。また、スーパーバイザ モジュールに到達する非 IP トラフィックを制限する場合は、デフォルトの非 IP CoPP クラスを使用できます。
- CoPP ポリシー ACL ではロギングをイネーブルにできません。
- 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、またはシリーズ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、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となる場合があります。
- 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。サービス ポリシー出力 CoPP は、コントロール パネル インターフェイスには適用できません。
- ハードウェアの Access Control Entry（ACE; アクセス コントロール エントリ）ヒット カウンタは、ACL 論理にのみ使用できます。CPU のトラフィックを評価する場合は、ソフトウェアの ACE ヒット カウンタおよび **show access-lists** と **show policy-map type control-plane** コマンドを使用してください。
- 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。

（注）　Cisco IOS CLI の知識があるユーザは、この機能に関する Cisco NX-OS のコマンドが Cisco IOS のコマンドで使用されるものと異なる場合があることに注意してください。

CoPP の設定

ここでは、次の内容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（p.20-7）
- コントロール プレーン ポリシー マップの設定（p.20-9）
- コントロール プレーン サービス ポリシーの設定（p.20-12）

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。

作業を開始する前に

デフォルト VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

クラス マップ内に ACE ヒット カウンタを使用する場合は、IP ACL（第 10 章「IP ACL の設定」を参照）または MAC ACL（第 11 章「MAC ACL の設定」を参照）が設定してあることを確認します。

手順の概要

1. **config t**
2. **class-map type control-plane** [**match-all** | **match-any**] *class-map-name*
3. **match access-group name** *access-list-name*

   match exception ip icmp redirect

   match exception ip icmp unreachable

   match exception ip option

   match protocol arp

   match redirect arp-inspect

   match redirect dhcp-snoop
4. **exit**
5. **show class-map type control-plane** [*class-map-name*]
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	`config t`
	
	例：
	`switch# config t`
	`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	目的
ステップ 2	**class-map type control-plane** [**match-all** | **match-any**] *class-map-name* 例： switch(config)# class-may 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 マップ名に使用することはできません。
ステップ 3	**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。
	match exception ip icmp redirect 例： switch(config-cmap)# match exception ip icmp redirect	IP 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。
	match exception ip icmp unreachable 例： switch(config-cmap)# match exception ip icmp unreachable	IP ICMP 到達不能例外パケットのマッチングを指定します。
	match exception ip option 例： switch(config-cmap)# match exception ip option	IP オプション例外パケットのマッチングを指定します。
	match protocol arp 例： switch(config-cmap)# match protocol arp	IP ARP パケットのマッチングを指定します。
	match redirect arp-inspect 例： switch(config-cmap)# match redirect arp-inspect	ARP 検査リダイレクト パケットのマッチングを指定します。
	match redirect dhcp-snoop 例： switch(config-cmap)# match redirect dhcp-snoop	DHCP スヌーピング リダイレクト パケットのマッチングを指定します。
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	**show class-map type control-plane** [*class-map-name*] 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。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（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、デフォルトのポリサー一致アクションは、ドロップです。グリーニング パケットはデフォルト クラスを使用してポリシングされます。NX-OS ソフトウェアは、1 レート 2 カラー ポリシングと 2 レート 3 カラー ポリシングをサポートします。

作業を開始する前に

デフォルト VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

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（「コントロール プレーン クラス マップの設定」[p.20-7] を参照）。

手順の概要

1. **config t**
2. **policy-map type control-plane** *policy-map-name*
3. **class** {*class-map-name* [**insert-before** *class-map-name*] | **class-default**}
4. **police** [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]

   police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]

   police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
   conform {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]

   police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
   pir *pir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] [[**be**] *extended-burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]
5. （任意）**set cos** [**inner**] *cos-value*
6. （任意）**set dscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **sf** | **default**}
7. （任意）**set precedence** [**tunnel**] *prec-value*
8. **exit**
9. **exit**
10. **show policy-map type control-plane** [**expand**] [**name** *policy-map-name*]
11. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** 例： switch# config t 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	**policy-map type control-plane** *policy-map-name* 例： switch(config)# policy-may type control-plan 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**} 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。 （注） 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	目的
ステップ 4	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} **例：** `switch(config-pmap-c)# police cir 52000`	CIR を指定します。レートの有効な範囲は 0 ～ 80000000000 です。CIR のデフォルト単位は **bps** です。
	police [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] **例：** `switch(config-pmap-c)# police cir 52000 bc 1000`	CIR と Bc を指定します。CIR の有効な範囲は 0 ～ 80000000000 で、Bc の有効な範囲は 0 ～ 512000000 です。CIR のデフォルト単位は **bps** で、Bc サイズのデフォルト単位は **byte** です。
	police [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} **conform** {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}] **例：** `switch(config-pmap-c)# police cir 52000 conform transmit exceed drop`	CIR と一致アクションを指定します。CIR の有効な範囲は 0 ～ 80000000000 です。レートのデフォルト単位は **bps** です。*cos-value* と *prec-value* 引数の有効な範囲は 0 ～ 7 です。*dscp-value* 引数の有効な範囲は 0 ～ 63 です。 オプションは次のとおりです。 • **drop —** パケットをドロップします。 • **set-cos-transmit —** CoS 値を設定します。 • **set-dscp-transmit —** DSCP 値を設定します。 • **set-prec-transmit —** IP precedence 値を設定します。 • **transmit —** パケットを送信します。 • **set dscp dscp table cir-markdown-map —** 超過（exceed）アクションを CIR マークダウン マップに設定します。 • **set dscp dscp table pir-markdown-map —** 違反（violate）アクションを PIR マークダウン マップに設定します。 **（注）** 同じ CIR に Bc と一致（conform）アクションを指定できます。
	police [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} **pir** *pir-rate* [**bps** | **gbps** | **kbps**| **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]] **例：** `switch(config-pmap-c)# police cir 52000 pir 78000 be 2000`	CIR と PIR（Peak Information Rate; 最大情報レート）を指定します。CIR の有効な範囲は 0 ～ 80000000000 で、PIR の有効な範囲は 1 ～ 80000000000 です。任意で Be サイズを設定できます。Be の有効な範囲は 1 ～ 512000000 です。CIR のデフォルト単位は **bps**、PIR のデフォルト単位は **bps**、および Be サイズのデフォルト単位は **byte** です。 **（注）** 同じ CIR に Bc、一致（conform）アクション、および PIR を指定できます。
ステップ 5	**set cos** [**inner**] *cos-value* **例：** `switch(config-pmap-c)# set cos 1`	（任意）802.1Q CoS 値を指定します。Q-in-Q 環境には **inner** キーワードを使用します。有効な範囲は 0 ～ 7 であり、デフォルト値は 0 です。

	コマンド	目的
ステップ 6	**set dscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**} 例： switch(config-pmap-c)# set dscp 10	（任意）IPv4 と IPv6 パケットの DSCP 値を指定します。トンネル カプセル化を設定する場合は、**tunnel** キーワードを使用します。有効な範囲は 0 ～ 63 であり、デフォルト値は 0 です。
ステップ 7	**set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**} 例： switch(config-pmap-c)# set precedence 2	（任意）IPv4 と IPv6 パケットの IP precedence 値を指定します。トンネル カプセル化を設定する場合は、**tunnel** キーワードを使用します。有効な範囲は 0 ～ 7 であり、デフォルト値は 0 です。
ステップ 8	**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 9	**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 10	**show policy-map type control-plane** [**expand**] [**name** *class-map-name*] 例： switch(config)# show policy-map type control-plane	（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。
ステップ 11	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（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 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。

作業を開始する前に

デフォルト VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

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（「コントロール プレーン ポリシー マップの設定」[p.20-9] を参照）。

手順の概要

1. **config t**
2. **control-plane**
3. **service-policy input** *policy-map-name*
4. **exit**
5. **show running-config copp [all]**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** 例： switch# config t 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	**service-policy input** *policy-map-name* 例： switch(config-cp)# service-policy input PolicyMapA	入力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。
ステップ 4	**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 5	**show running-config copp** [**all**] 例： switch(config)# show running-config copp	（任意）CoPP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（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。

CoPP 統計情報の表示

CoPP 統計情報を表示できます。

作業を開始する前に

デフォルト VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

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

詳細な手順

	コマンド	目的
ステップ 1	**show policy-map interface control-plane** 例： switch# show policy-map interface control-plane	コントロール プレーン統計情報を表示します。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

CoPP 統計情報のクリア

CoPP 統計情報をクリアできます。

作業を開始する前に

デフォルト VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **show policy-map interface control-plane**
2. **clear copp statistics**

詳細な手順

	コマンド	目的
ステップ 1	**show policy-map interface control-plane** 例： switch# show policy-map interface control-plane	（任意）コントロール プレーン統計情報を表示します。
ステップ 2	**clear copp statistics** 例： switch# clear copp statistics	CoPP 統計情報をクリアします。

CoPP 設定の確認

CoPP の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show class-map type control-plane [*class-map-name*]	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 マップの設定を表示します。
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 startup-config copp	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。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

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。

```
config t
ip access-list copp-system-acl-igmp
permit igmp any 10.0.0.0/24

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

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

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

ip access-list copp-system-acl-gre
permit 47 any any

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

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

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

class-map type control-plane match-any copp-system-class-important
match access-group name copp-system-acl-tacas
match access-group name copp-system-acl-gre

class-map type control-plane match-any copp-system-class-normal
match access-group name copp-system-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option
match redirect dhcp-snoop
match redirect arp-inspect

policy-map type control-plane copp-system-policy
class copp-system-class-critical
police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
transmit violate drop

class copp-system-class-important
police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
transmit violate drop

class copp-system-class-normal
police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit exceed
transmit violate drop

class class-default
police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit exceed
transmit violate drop

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

デフォルト設定

表 20-1 に、CoPP パラメータのデフォルト設定を示します。

表 20-1　デフォルトの CoPP パラメータ

パラメータ	デフォルト

デフォルトポリシー	class-map type control-plane match-any copp-system-class-critical
	  match access-group name copp-system-acl-bgp
	  match access-group name copp-system-acl-eigrp
	  match access-group name copp-system-acl-igmp
	  match access-group name copp-system-acl-msdp
	  match access-group name copp-system-acl-ospf
	  match access-group name copp-system-acl-pim
	  match access-group name copp-system-acl-rip
	class-map type control-plane match-any copp-system-class-exception
	  match exception ip option
	  match exception ip icmp unreachable
	class-map type control-plane match-any copp-system-class-important
	  match access-group name copp-system-acl-glbp
	  match access-group name copp-system-acl-hsrp
	  match access-group name copp-system-acl-vrrp
	class-map type control-plane match-any copp-system-class-management
	  match access-group name copp-system-acl-ftp
	  match access-group name copp-system-acl-ntp
	  match access-group name copp-system-acl-radius
	  match access-group name copp-system-acl-snmp
	  match access-group name copp-system-acl-ssh
	  match access-group name copp-system-acl-tacacs
	  match access-group name copp-system-acl-telnet
	  match access-group name copp-system-acl-tftp
	class-map type control-plane match-any copp-system-class-monitoring
	  match access-group name copp-system-acl-icmp
	  match access-group name copp-system-acl-traceroute
	class-map type control-plane match-any copp-system-class-normal
	  match protocol arp
	class-map type control-plane match-any copp-system-class-redirect
	  match redirect dhcp-snoop
	  match redirect arp-inspect
	class-map type control-plane match-any copp-system-class-undesirable
	  match access-group name copp-system-acl-undesirable
	policy-map type control-plane copp-system-policy
	  class copp-system-class-critical
	  police cir 40900 kbps bc 250 ms conform transmit violate drop
	  class copp-system-class-important
	  police cir 1060 kbps bc 250 ms conform transmit violate drop
	  class copp-system-class-management
	  police cir 1580 kbps bc 250 ms conform transmit violate drop
	  class copp-system-class-normal
	  police cir 680 kbps bc 250 ms conform transmit violate drop
	  class copp-system-class-redirect
	  police cir 280 kbps bc 250 ms conform transmit violate drop
	  class copp-system-class-monitoring
	  police cir 100 kbps bc 250 ms conform transmit violate drop
	  class copp-system-class-exception
	  police cir 360 kbps bc 250 ms conform transmit violate drop
	  class copp-system-class-undesirable
	  police cir 32 kbps bc 250 ms conform drop violate drop
	  class class-default
	  police cir 100 kbps bc 250 ms conform transmit violate drop

その他の参考資料

CoPP の実装に関連する詳細情報については、次を参照してください。

- 関連資料（p.20-17）
- 規格（p.20-17）

関連資料

関連事項	タイトル
ライセンス	『*Cisco NX-OS Licensing Guide, Release 4.0*』
コマンド リファレンス	『*Cisco NX-OS Security Command Reference, Release 4.0*』
IP ACL	IP ACL の設定
MAC ACL	MAC ACL の設定

規格

規格	タイトル
RFC 2698	*A Two Rate Three Color Marker*