コントロール プレーン ポリシング（CoPP）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の URL の『Cisco IOS Master Command List, Release 15.1SY』を参照してください。
  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- CoPP の詳細については、次のドキュメントを参照してください。
  http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-663623.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
技術マニュアルのアイデア フォーラムに参加する

CoPP の前提条件

なし。

CoPP の制約事項

- **mls qos** コマンドによって PFC QoS をグローバルにイネーブルにしないかぎり、CoPP はハードウェアでイネーブルにされません。**mls qos** コマンドを入力しない場合は、CoPP ではハードウェア アクセラレーションが使用されません。
- CoPP は次の場合にソフトウェアでサポートされます。
  - マルチキャスト トラフィック。
  - ブロードキャスト トラフィック。

  （注）　ブロードキャスト DoS 攻撃からの保護を実現するには、ACL、トラフィック ストーム制御、および CoPP ソフトウェア保護を組み合わせて使用します。

  - **log** キーワードを設定した CoPP ポリシー ACL。ソフトウェアでサポートされる CoPP 処理を回避するには、CoPP ポリシー ACL で **log** キーワードを使用しないようにします。
  - その他のインターフェイスで QoS 設定が大きい場合は、TCAM スペースが不足することがあります。この状況が発生した場合は、CoPP が全体的にソフトウェアで実行され、パフォーマンスの低下および CPU サイクルの消費という結果になることがあります。**show tcam utilization** コマンドを入力し、TCAM の使用状況を確認してください。
  - **match protocol arp** コマンドで設定した CoPP ポリシー。
  - CoPP は、**match access-group** *arp_acl* コマンドで設定したポリシーをサポートします。
- CoPP は転送エンジンごとに実行され、ソフトウェア CoPP は一括で実行されます。
- CoPP は MAC ACL をサポートしません。
- CoPP では、デフォルトの非 IP クラスを除いて、非 IP クラスがサポートされません。非 IP クラスの代わりに ACL を使用して非 IP トラフィックを廃棄でき、デフォルトの非 IP CoPP クラスを使用して、RP CPU に到達する非 IP トラフィックに制限できます。
- CoPP ポリシーによって、ルーティング プロトコルまたはスイッチへの対話型アクセスなどの重要なトラフィックがフィルタリングされないことを確認してください。このトラフィックをフィルタリングすると、スイッチへのリモート アクセスが妨害され、コンソール接続が必要になることがあります。
- PFC3 は、組み込みの特殊ケース レート リミッタをサポートします。これは、ACL を使用できない状況（TTL、MTU、IP オプションなど）で便利です。特殊ケース レート リミッタをイネーブルにする場合は、この特殊ケース レート リミッタにより、レート リミッタの基準に一致するパケットの CoPP ポリシーが上書きされることに注意してください。
- 出力 CoPP もサイレント モードもサポートされません。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、制御プレーン インターフェイスに適用できません）。
- ハードウェアの ACE ヒット カウンタは ACL ロジック専用です。ソフトウェア ACE ヒット カウンタ、および **show access-list** コマンド、**show policy-map control-plane** コマンド、**show mls ip qos** コマンドを使用して、CPU トラフィックのトラブルシューティングと評価ができます。

コントロール プレーン ポリシングに関する情報

RP によって管理されるトラフィックは、次の 3 つの機能コンポーネント（*プレーン*）に分類されます。

- データ プレーン
- 管理プレーン
- 制御プレーン

CoPP 機能を使用すると、不要なトラフィックや DoS トラフィックから RP を保護し、重要なコントロール プレーンおよび管理トラフィックを優先させることができるので、スイッチのセキュリティを強化できます。PFC3 および DFC3 では、CoPP がハードウェアでサポートされます。CoPP は PFC3 レート リミッタと連携して動作します。

PFC3 は、組み込みの「特殊ケース」レート リミッタをサポートします。IP オプション ケース、TTL および MTU のエラー ケース、エラーを含むパケット、マルチキャスト パケットなどの特定シナリオを ACL が分類できない場合に使用できます。特殊ケース レート リミッタをイネーブルにすると、この特殊ケース レート リミッタにより、レート リミッタの基準に一致するパケットの CoPP ポリシーが上書きされます。

RP の管理するトラフィックのほとんどは、コントロール プレーンおよびマネジメント プレーンによって処理されます。CoPP を使用すると、制御プレーンおよび管理プレーンを保護でき、ルーティングの安定性、到達可能性、パケット配信を確保できます。CoPP では、Modular QoS CLI（MQC）で専用制御プレーン設定が使用され、フィルタ機能およびレート制限機能が制御プレーン パケットに提供されます。

CoPP のデフォルト設定

CoPP はデフォルトでディセーブルです。

CoPP の設定方法

CoPP は MQC を使用してトラフィック分類基準を定義し、分類されたトラフィックの設定可能ポリシー アクションを指定します。最初にクラス マップを定義し、分類するトラフィックを識別する必要があります。クラス マップでは、特定トラフィック クラスのパケットが定義されます。トラフィックを分類したら、識別されたトラフィックにポリシー アクションを実行するための、ポリシー マップを作成できます。**control-plane** グローバル コンフィギュレーション コマンドでは、CoPP サービス ポリシーを制御プレーンに直接付加できます。

トラフィック分類基準を定義する方法については、「トラフィック分類の定義方法」（P.70-6）を参照してください。

CoPP を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	MLS QoS をグローバルにイネーブルにします。
ステップ 2	`Router(config)# ip access-list extended access-list-name` `Router(config-ext-nacl)# {permit | deny} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [established] [log | log-input] [time-range time-range-name] [fragments]`	次のように、トラフィックと照合する ACL を定義します。 • **permit** では、パケットが名前付き IP アクセス リストで合格する条件を設定します。 • **deny** では、パケットが名前付き IP アクセス リストで不合格になる条件を設定します。 **（注）** ほとんどの場合は、重要なトラフィックまたは重要でないトラフィックを識別する ACL を設定する必要があります。
ステップ 3	`Router(config)# class-map traffic-class-name` `Router(config-cmap)# match {ip precedence} |{ip dscp} | access-group`	パケット分類基準を定義します。クラスに関連するトラフィックを識別するには、**match** ステートメントを使用します。

	`Router(config)# policy-map service-policy-name`
	`Router(config-pmap)# class traffic-class-name`
	`Router(config-pmap-c)# police {bits-per-second [normal-burst-bytes] [maximum-burst-bytes] [pir peak-rate-bps]} | [conform-action action] [exceed-action action] [violate-action action]`
		サービス ポリシー マップを定義します。クラスをサービス ポリシー マップに関連付けるには、**class** *traffic-class-name* コマンドを使用します。サービス ポリシー マップにアクションを関連付けるには、**police** ステートメントを使用します。

ステップ 4	`Router(config)# control-plane` `Router(config-cp)#`	制御プレーン コンフィギュレーション モードに入ります。
ステップ 5	`Router(config-cp)# service-policy input service-policy-name`	QoS サービス ポリシーを制御プレーンに適用します。

パケット分類基準を定義するときは、次の注意事項および制約事項に従ってください。

- 後続クラスで設定されるフィルタリングとポリシングに一致しないようにするには、クラスごとにポリシングを設定します。CoPP は、police コマンドを含まないクラスでフィルタリングを適用しません。police コマンドを含まないクラスはどのトラフィックとも一致しません。
- 分類に使用される ACL は QoS ACL です。サポートされる QoS ACL は、IP 標準 ACL、拡張 ACL、および名前付き ACL です。
- サポートされる一致タイプは以下だけです。
  - **ip precedence**
  - **ip dscp**
  - **access-group**
- ハードウェアでは IP ACL だけがサポートされます。
- MAC ベースの照合はソフトウェアだけで実行されます。
- 単一クラス マップで入力できる **match** コマンドは 1 つだけです。

サービス ポリシーを定義する場合、サポートされているアクションは **police** ポリシー マップ アクションだけです。

制御プレーンにサービス ポリシーを適用する場合は、**input** 方向だけがサポートされます。

CoPP のモニタリング方法

サイト固有ポリシーを開発して制御プレーン ポリシーの統計をモニタし、CoPP をトラブルシューティングするには、**show policy-map control-plane** コマンドを入力できます。このコマンドでは、レート情報、およびハードウェアとソフトウェアの両方で設定されたポリシーに適合するバイト数（およびパケット数）と適合しないバイト数（およびパケット数）など、実際に適用されたポリシーに関するダイナミックな情報が表示されます。

show policy-map control-plane コマンドの出力は次のようになります。

```
Router# show policy-map control-plane
Control Plane Interface
  Service policy CoPP-normal
Hardware Counters:
class-map: CoPP-normal (match-all)
      Match: access-group 130
      police :
        96000 bps 3000 limit 3000 extended limit
      Earl in slot 3 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps

Software Counters:
    Class-map: CoPP-normal (match-all) 0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      police:
        96000 bps, 3125 limit, 3125 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Router#
```

ポリシーによって廃棄されたり転送されたりしたバイトのハードウェア カウンタを表示するには、**show mls qos ip** コマンドを入力します。

```
Router# show mls qos ip
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                           Id         Id
------------------------------------------------------------------------------
CPP  5  In CoPP-normal    0    1   dscp  0         505408       83822272
CPP  9  In CoPP-normal    0    4   dscp  0              0              0
Router#
```

CoPP アクセス リストの情報を表示するには、**show access-lists coppacl-bgp** コマンドを入力します。

```
Router# show access-lists coppacl-bgp
Extended IP access list coppacl-bgp
```

```
10 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp (4 matches)
20 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
30 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp (1 match)
40 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

トラフィック分類の定義方法

トラフィック分類の概要

任意の数のクラスを定義できますが、一般的にトラフィックは、相対的な重要性に基づいたクラスにグループ化されます。グループ化の例を以下に示します。

- ボーダー ゲートウェイ プロトコル（BGP）：BGP キープアライブおよびルーティング アップデートなどの BGP ルーティング プロトコルのネイバー関係の維持で重要となるトラフィック。BGP ルーティング プロトコルを維持することは、ネットワーク内の接続を維持するために、またはサービス プロバイダーにとって重要です。BGP を実行しないサイトでこのクラスを使用する必要はありません。
- 内部ゲートウェイ プロトコル（IGP）：Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）などの IGP ルーティング プロトコルの維持で重要になるトラフィック。IGP ルーティング プロトコルを維持することは、ネットワーク内の接続を維持するために重要となります。
- 管理：日常業務で必要な、頻繁に使用される必須トラフィック。たとえば、リモート ネットワーク アクセスに使用するトラフィックや、Cisco IOS イメージの更新および管理トラフィックです。これには、Telnet、セキュア シェル（SSH）、ネットワーク タイム プロトコル（NTP）、簡易ネットワーク管理プロトコル（SNMP）、Terminal Access Controller Access Control System（TACACS）、ハイパーテキスト転送プロトコル（HTTP）、簡易ファイル転送プロトコル（TFTP）、ファイル転送プロトコル（FTP）などがあります。
- レポート：レポートする目的でネットワーク パフォーマンス統計を生成するために使用されるトラフィック。たとえば、さまざまな QoS データ クラス内の応答時間でレポートするために、Cisco IOS IP サービス レベル契約（SLA）を使用して、さまざまな DSCP 設定で ICMP を生成することなど。
- モニタ：スイッチのモニタに使用されるトラフィック。このトラフィックは許可する必要がありますが、スイッチを危険にさらすことがあってはなりません。CoPP を使用すると、このトラフィックは許可されますが、低いレートに制限できます。たとえば、ICMP エコー要求（ping）および traceroute など。
- クリティカル アプリケーション：特定カスタマーの環境に固有で重要なクリティカル アプリケーション トラフィック。このクラスに分類するトラフィックは、ユーザに必要なアプリケーションの要件に合わせて、特別に調整する必要があります。マルチキャストを使用するお客様もいれば、IP セキュリティまたは総称ルーティング カプセル化（GRE）を使用するお客様もいます。たとえば、GRE、ホットスタンバイ ルータ プロトコル（HSRP）、仮想ルータ冗長プロトコル（VRRP）、Session Initiation Protocol（SIP）、データ リンク スイッチング（DLSw）、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）、Multicast Source Discovery Protocol（MSDP）、インターネット グループ管理プロトコル（IGMP）、Protocol Independent Multicast（PIM）、マルチキャスト トラフィック、IPSec など。

- レイヤ 2 プロトコル：アドレス解決プロトコル（ARP）に使用されるトラフィック。ARP パケットが過剰に発生すると、RP リソースが独占され、他の重要なプロセスがリソース不足になってしまう可能性があります。CoPP を使用して ARP パケットをレート制限すると、このような状況を回避できます。現在、一致プロトコル分類基準を使用して明確に分類できるレイヤ 2 プロトコルは、ARP だけです。
- 不要：RP へのアクセスを無条件でドロップおよび拒否する必要のある、不正な、または悪意あるトラフィックを明示的に指定します。この分類は、スイッチ宛ての既知のトラフィックを常に拒否する必要があり、デフォルト カテゴリに含まれないようにする場合に特に便利です。トラフィックを明示的に拒否する場合は、**show** コマンドを入力して拒否トラフィックに関する概算統計を収集してレートを見積もることができます。
- デフォルト：他に分類されない、RP 宛ての残りのトラフィックすべてを収容。MQC はデフォルト クラスを提供するので、ユーザは、その他のユーザ定義クラスで明示的に識別されないトラフィックに適用する処置を指定できます。このトラフィックの RP へのアクセス レートは、大幅に制限されます。デフォルト分類を適切に使用すると、統計をモニタし、これを使用しない場合は識別されないコントロール プレーンを宛先とするトラフィックのレートを判断できます。このトラフィックが識別されたあとは、さらに分析を実行して分類し、必要な場合は、その他の CoPP ポリシー エントリを更新してこのトラフィックに対応できます。

トラフィックの分類が完了したら、ポリシーの定義に使用される、トラフィックのクラスを ACL が構築します。CoPP 分類の基本的な ACL の例については、「CoPP トラフィック分類の基本 ACL 例」（P.70-7）を参照してください。

トラフィック分類のガイドライン

トラフィック分類を定義するときは、次のガイドラインおよび制約事項に従ってください。

- 実際の CoPP ポリシーを開発する前に、必要なトラフィックを識別してさまざまなクラスに分類する必要があります。トラフィックは、相対的な重要性に基づく 9 個のクラスにグループ化されます。実際に必要となるクラスの数は異なることがあり、ローカルの要件とセキュリティ ポリシーに基づいて選択する必要があります。
- 双方向に一致するポリシーを定義する必要はありません。ポリシーは入力だけに適用されるため、トラフィックは一方向（ネットワークから RP へ）だけで識別します。

CoPP トラフィック分類の基本 ACL 例

ここでは、CoPP 分類の基本的な ACL 例を示します。この例では、一般的に必要なトラフィックが、次の ACL で識別されます。

- ACL 120：クリティカル トラフィック
- ACL 121：重要トラフィック
- ACL 122：通常トラフィック
- ACL 123：不要なトラフィックを明示的に拒否
- ACL 124：その他すべてのトラフィック

次に、クリティカル トラフィック用に ACL 120 を定義する例を示します。

```
Router(config)# access-list 120 remark CoPP ACL for critical traffic
```

次に、既知のピアからこのスイッチの BGP TCP ポートへの BGP を許可する例を示します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp
```

次に、ピアの BGP ポートからこのスイッチへの BGP を許可する例を示します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
Router(config)# access-list 120 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp
Router(config)# access-list 120 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

次に、重要クラス用に ACL 121 を定義する例を示します。

```
Router(config)# access-list 121 remark CoPP Important traffic
```

次に、TACACS ホストからのリターン トラフィックを許可する例を示します。

```
Router(config)# access-list 121 permit tcp host 1.1.1.1 host 10.9.9.9 established
```

次に、サブネットからスイッチへの SSH アクセスを許可する例を示します。

```
Router(config)# access-list 121 permit tcp 10.0.0.0 0.0.0.255 host 10.9.9.9 eq 22
```

次に、特定サブネットのホストからスイッチへの Telnet の完全アクセスを許可し、残りのサブネットをポリシングする例を示します。

```
Router(config)# access-list 121 deny tcp host 10.86.183.3 any eq telnet
Router(config)# access-list 121 permit tcp 10.86.183.0 0.0.0.255 any eq telnet
```

次に、NMS ホストからスイッチへの SNMP アクセスを許可する例を示します。

```
Router(config)# access-list 121 permit udp host 1.1.1.2 host 10.9.9.9 eq snmp
```

次に、スイッチが既知のクロック ソースから NTP パケットを受信できるようにする例を示します。

```
Router(config)# access-list 121 permit udp host 1.1.1.3 host 10.9.9.9 eq ntp
```

次に、通常トラフィック クラス用に ACL 122 を定義する例を示します。

```
Router(config)# access-list 122 remark CoPP normal traffic
```

次に、スイッチからの traceroute トラフィックを許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any ttl-exceeded
Router(config)# access-list 122 permit icmp any any port-unreachable
```

次に、ping を発信したスイッチに応答の受信を許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any echo-reply
```

次に、スイッチへの ping を許可する例を示します。

```
Router(config)# access-list 122 permit icmp any any echo
```

次に、不要クラス用に ACL 123 を定義する例を示します。

```
Router(config)# access-list 123 remark explicitly defined "undesirable" traffic
```

（注） 次の例において、ACL 123 は分類とモニタを目的とした許可エントリであり、トラフィックは CoPP ポリシーの結果としてドロップされます。

次に、UDP 1434 を宛先とするすべてのトラフィックをポリシング用に許可する例を示します。

```
Router(config)# access-list 123 permit udp any any eq 1434
```

次に、その他すべてのトラフィック用に ACL 124 を定義する例を示します。

```
Router(config)# access-list 124 remark rest of the IP traffic for CoPP
Router(config)# access-list 124 permit ip any any
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する