



## コントロールプレーンポリシング (CoPP)

- 「CoPP の前提条件」 (P.77-1)
- 「CoPP の制約事項」 (P.77-2)
- 「CoPP の概要」 (P.77-3)
- 「CoPP のデフォルト設定」 (P.77-3)
- 「CoPP の設定方法」 (P.77-5)
- 「CoPP のモニタ」 (P.77-9)



(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、次の資料を参照してください。

[http://www.cisco.com/en/US/products/ps11846/prod\\_command\\_reference\\_list.html](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](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](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

- PFC および DFC では、マルチキャスト トラフィックと一致するクラスがハードウェアでサポートされます。
- ブロードキャスト パケットについては、ハードウェアでは CoPP がサポートされません。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。
- 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 トラフィックをドロップでき、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 ACL では **log** キーワードを使用しないでください。
- 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。この場合は、CoPP がソフトウェアで実行される場合があります。
- 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。
- 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。
- PFC および DFC は、組み込みの **special-case** 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 platform 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。
- CoPP はフォワーディング 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 では、**log** キーワードを使用した ACE がサポートされません。
- CoPP では、ハードウェア QoS TCAM リソースが使用されます。**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。
- 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 の概要

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

コントロール プレーン ポリシング (CoPP) 機能は、不要なトラフィックまたは 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によりスイッチのセキュリティを向上させます。PFC および DFC では、CoPP がハードウェアでサポートされます。CoPP はハードウェア レート リミッタと連携して動作します。

PFC および DFC では、組み込みの「特殊ケース」レート リミッタがサポートされます。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は、これを使用できます。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。

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。

## CoPP のデフォルト設定

CoPP はデフォルトで有効になっています。デフォルトの CoPP 設定をディセーブルにするには、**no service-policy input policy-default-autocopp** コントロールプレーン コンフィギュレーション モード コマンドを入力します。

これらは、デフォルトの CoPP クラス マップです。

```
class-map match-any class-copp-icmp-redirect-unreachable
class-map match-all class-copp-glean
class-map match-all class-copp-receive
class-map match-all class-copp-options
class-map match-all class-copp-broadcast
class-map match-all class-copp-mcast-acl-bridged
class-map match-all class-copp-slb
class-map match-all class-copp-mtu-fail
class-map match-all class-copp-ttl-fail
class-map match-all class-copp-arp-snooping
```

```

class-map match-any class-copp-mcast-copy
class-map match-any class-copp-ip-connected
class-map match-any class-copp-match-igmp
  match access-group name acl-copp-match-igmp
class-map match-all class-copp-unknown-protocol
class-map match-any class-copp-vacl-log
class-map match-all class-copp-mcast-ipv6-control
class-map match-any class-copp-match-pimv6-data
  match access-group name acl-copp-match-pimv6-data
class-map match-any class-copp-mcast-punt
class-map match-all class-copp-unsupp-rewrite
class-map match-all class-copp-ucast-egress-acl-bridged
class-map match-all class-copp-ip-admission
class-map match-all class-copp-service-insertion
class-map match-all class-copp-mac-pbf
class-map match-any class-copp-match-mld
  match access-group name acl-copp-match-mld
class-map match-all class-copp-ucast-ingress-acl-bridged
class-map match-all class-copp-dhcp-snooping
class-map match-all class-copp-wccp
class-map match-all class-copp-nd
class-map match-any class-copp-ipv6-connected
class-map match-all class-copp-mcast-rpf-fail
class-map match-any class-copp-ucast-rpf-fail
class-map match-all class-copp-mcast-ip-control
class-map match-any class-copp-match-pim-data
  match access-group name acl-copp-match-pim-data
class-map match-any class-copp-match-ndv6
  match access-group name acl-copp-match-ndv6
class-map match-any class-copp-mcast-v4-data-on-routedPort
class-map match-any class-copp-mcast-v6-data-on-routedPort

```

これは、デフォルトの CoPP ポリシー マップです。

```

policy-map policy-default-autocopp
  class class-copp-mcast-v4-data-on-routedPort
    police rate 10 pps burst 1 packets
    conform-action drop
    exceed-action drop
  class class-copp-mcast-v6-data-on-routedPort
    police rate 10 pps burst 1 packets
    conform-action drop
    exceed-action drop
  class class-copp-icmp-redirect-unreachable
    police rate 100 pps burst 10 packets
    conform-action transmit
    exceed-action drop
  class class-copp-ucast-rpf-fail
    police rate 100 pps burst 10 packets
    conform-action transmit
    exceed-action drop
  class class-copp-vacl-log
    police rate 2000 pps burst 1 packets
    conform-action transmit
    exceed-action drop
  class class-copp-mcast-punt
    police rate 1000 pps burst 256 packets
    conform-action transmit
    exceed-action drop
  class class-copp-mcast-copy
    police rate 1000 pps burst 256 packets
    conform-action transmit
    exceed-action drop
  class class-copp-ip-connected

```

```

police rate 1000 pps burst 256 packets
  conform-action transmit
  exceed-action drop
class class-copp-ipv6-connected
  police rate 1000 pps burst 256 packets
  conform-action transmit
  exceed-action drop
class class-copp-match-pim-data
  police rate 1000 pps burst 1000 packets
  conform-action transmit
  exceed-action drop
class class-copp-match-pimv6-data
  police rate 1000 pps burst 1000 packets
  conform-action transmit
  exceed-action drop
class class-copp-match-mld
  police rate 10000 pps burst 10000 packets
  conform-action set-discard-class-transmit 48
  exceed-action transmit
class class-copp-match-igmp
  police rate 10000 pps burst 10000 packets
  conform-action set-discard-class-transmit 48
  exceed-action transmit
class class-copp-match-ndv6
  police rate 1000 pps burst 1000 packets
  conform-action set-discard-class-transmit 48
  exceed-action drop

```

## CoPP の設定方法

- 「CoPP の設定」 (P.77-5)
- 「CoPP トラフィック分類の定義」 (P.77-6)

## CoPP の設定

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)# <b>ip access-list extended</b> <i>access_list_name</i>	拡張 ACL を作成します。 <b>(注)</b> 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2	Router(config-ext-nacl)# <b>{permit   deny} protocol</b> <b>source source_wildcard destination</b> <i>destination_wildcard</i> [ <b>precedence precedence</b> ] [ <b>tos tos</b> ] [ <b>established</b> ] [ <b>log   log-input</b> ] [ <b>time-range time_range_name</b> ] [ <b>fragments</b> ]	ACL のフィルタリングを設定します。 <ul style="list-style-type: none"> <li>• <b>permit</b> 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。</li> <li>• <b>deny</b> 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。</li> </ul>
ステップ3	Router(config)# <b>class-map</b> <i>traffic_class_name</i>	クラス マップを作成します。
ステップ4	Router(config-cmap)# <b>match</b> { <b>ip precedence</b>   <b>ip dscp</b>   <b>access_group</b> }	クラス マップでの一致を設定します。
ステップ5	Router(config)# <b>policy-map</b> <i>service-policy-name</i>	サービス ポリシー マップを定義します。

## ■ CoPP の設定方法

	コマンド	目的
ステップ 6	Router(config-pmap)# <b>class</b> <i>traffic_class_name</i>	ポリシー マップ クラスを作成します。
ステップ 7	Router(config-pmap-c)# <b>police</b> <i>bits_per_second</i> [ <i>normal_burst_bytes</i> [ <i>maximum_burst_bytes</i> ]] [ <i>pir_peak_rate_bps</i> ] [[ <b>conform-action</b> <i>selected_action</i> ] <b>exceed-action</b> <i>selected_action</i> ] <b>violate-action</b> <i>selected_action</i> ]  Router(config-pmap-c)# <b>police rate units bps</b> [ <b>burst</b> <i>burst_bytes bytes</i> ] [ <i>peak-rate</i> <i>peak_rate_bps bps</i> ] [ <i>peak-burst peak_burst_bytes</i> <i>bytes</i> ] [ <b>conform-action</b> <i>selected_action</i> ] [ <b>exceed-action</b> <i>selected_action</i> ] [ <b>violate-action</b> <i>selected_action</i> ]  Router(config-pmap-c)# <b>police rate units pps</b> [ <b>burst</b> <i>burst_packets packets</i> ] [ <b>peak-rate</b> <i>peak_rate_pps pps</i> ] [ <b>peak-burst</b> <i>peak_burst_packets packets</i> ] [ <b>conform-action</b> <i>selected_action</i> ] [ <b>exceed-action</b> <i>selected_action</i> ] [ <b>violate-action</b> <i>selected_action</i> ]  Router(config-pmap-c)# <b>police flow</b> [ <b>mask</b> { <i>src-only</i>   <i>dest-only</i>   <i>full-flow</i> }] <i>bits_per_second normal_burst_bytes</i> [[ <b>conform-action</b> { <i>drop</i>	サービス ポリシー マップでのポリシングを設定します。 次のいずれかを設定できます。 <ul style="list-style-type: none"> <li>• バイト ベースのポリシング。</li> <li>• パケット ベースのポリシング。</li> <li>• フロー ベースのポリシング。</li> </ul> 「ポリシー マップ クラスのポリシングの設定」(P.63-12)を参照してください。
ステップ 8	Router(config)# <b>control-plane</b>	制御プレーン コンフィギュレーション モードを開始します。
ステップ 9	Router(config-cp)# <b>service-policy</b> <i>input</i> <i>service-policy-name</i>	QoS サービス ポリシーを制御プレーンに適用します。

## CoPP トラフィック分類の定義

- 「トラフィック分類の概要」(P.77-6)
- 「トラフィック分類の制約事項」(P.77-8)
- 「CoPP トラフィック分類の基本 ACL 例」(P.77-8)

### 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。

- Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル) : 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 : 日常業務に必要な、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、Secure Shell (SSH; セキュア シェル)、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)、Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル)、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 : 特定顧客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。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がある、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收容。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.77-8) を参照してください。

## トラフィック分類の制約事項

- 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（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 : クリティカルなトラフィック
- 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、クリティカルなトラフィック用に 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ーする例を示します。

```
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
```

## CoPP のモニタ

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#

```

ポリシーによってドロップ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 platform qos ip** コマンドを入力します。

```

Router# show platform 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

```



**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](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