CHAPTER 47

コントロール プレーン ポリシングの設定

この章では、Cisco IOS Release 12.2SX 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。

（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 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

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

この章で説明する内容は、次のとおりです。

- 「CoPP の概要」（P.47-1）
- 「CoPP のデフォルト設定」（P.47-2）
- 「CoPP 設定時の注意事項および制約事項」（P.47-2）
- 「CoPP の設定」（P.47-3）
- 「CoPP のモニタ」（P.47-4）
- 「トラフィック分類の定義」（P.47-5）

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
- マネジメント プレーン
- コントロール 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 は、CoPP のハードウェア サポートを行います。CoPP は、PFC3 のレート リミッタと連携して動作します。

PFC3 は、組み込みの「特殊ケース用」レート リミッタをサポートします。このレート リミッタは、IP オプション、TTL および MTU の失敗、エラーの生じたパケット、マルチキャスト パケットといった ACL の分類に該当しない、特定のシナリオで使用できます。特殊ケース用レート リミッタをイネーブルにすると、このレート リミッタは基準に適合するパケットに対し、CoPP ポリシーを優先します。

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 を使用してコントロール プレーンおよびマネジメント プレーンを保護することで、ルーティングの安定性、到達可能性、および確実なパケット配信を維持できます。CoPP では、Modular QoS CLI（MQC; モジュラ QoS コマンドライン インターフェイス）から専用のコントロール プレーン設定を使用して、コントロール プレーン パケットに対するフィルタリングおよびレート制限機能を提供します。

CoPP のデフォルト設定

CoPP はデフォルトでディセーブルにされています。

CoPP 設定時の注意事項および制約事項

CoPP を設定する場合は、次の注意事項および制約事項に従ってください。

- **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。
  - 他のインターフェイスに対する大規模な QoS 設定があると、領域が足りなくなる可能性があります。この場合は、CoPP がソフトウェア内で完全に実行され、パフォーマンス低下や CPU サイクル消費につながる可能性があります。TCAM の利用率を確認するには、**show tcam utilization** コマンドを入力します。
  - **match protocol arp** コマンドで設定した CoPP ポリシー。
  - Release 12.2(33)SXI4 以降のリリースでは、**match access-group** *arp_acl* コマンドで設定した CoPP ポリシーがサポートされます。
  - CoPP は ARP ポリシーをサポートしません。ARP ポリシング メカニズムは、ARP ストームからの保護を実現します。
- CoPP は転送エンジン単位で実行され、ソフトウェア CoPP は集約的に実行されます。
- CoPP は MAC ACL をサポートしません。
- 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には、非 IP クラスの代わりに ACL を使用できます。また、RP CPU に到達する非 IP トラフィックを制限するには、デフォルトの非 IP CoPP クラスを使用できます。

- PFC3A では、出力 QoS と CoPP を同時に設定できません。この状況では、CoPP はソフトウェア内で実行されます。出力 QoS と CoPP を同時に設定できないことを示す警告メッセージが表示されます。
- 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、またはスイッチ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、スイッチへのリモート 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。
- PFC3 は、組み込みの特殊ケース用レート 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。特殊ケース用レート リミッタをイネーブルにする場合は、このレート リミッタが基準に適合するパケットに対し、CoPP ポリシーを優先することに注意してください。
- 出力 CoPP、およびサイレント モードは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、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。
- ハードウェア内の ACE ヒット カウンタは、ACL 論理だけに対応します。CPU トラフィックのトラブルシューティングおよび評価には、ソフトウェア ACL のヒット カウンタ、および **show access-list**、**show policy-map control-plane**、**show mls ip qos** コマンドが役立ちます。

CoPP の設定

CoPP では MQC を使用することで、トラフィックの分類基準を定義し、分類したトラフィックに対して設定可能なポリシー アクションを指定します。最初にクラス マップを定義して、分類の対象となるトラフィックを識別する必要があります。クラス マップは、特定のトラフィック クラスに対するパケットを定義します。トラフィックを分類したあとは、識別したトラフィックにポリシー アクションを適用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 コマンドを使用すると、CoPP サービス ポリシーをコントロール 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」（P.47-5）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化します。
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**]	トラフィックと一致する ACL を定義します。 • **permit** は、名前付き IP アクセス リストにパケットが適合する条件を設定します。 • **deny** は、名前付き IP アクセス リストがパケットを拒否す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とそうでないトラフィックの識別には ACL を設定する必要があります。

	コマンド	目的
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。**match** ステートメントを使用して、クラスに関連付けるトラフィックを指定します。
	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。**class** *traffic-class-name* コマンドを使用して、サービス ポリシー マップにクラスを関連付けます。**police** ステートメントを使用して、サービス ポリシー マップにアクションを関連付けます。
ステップ 4	Router(config)# **control-plane** Router(config-cp)#	コントロールプレーンのコンフィギュレーション モードを有効にします。
ステップ 5	Router(config-cp)# **service-policy input** *service-policy-name*	QoS サービス ポリシーをコントロール プレーンに適用します。

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

- 以降のクラスで設定されたフィルタリングおよびポリシングと一致することを避けるため、ポリシングは各クラスで設定します。CoPP では、police コマンドを含まないクラスにはフィルタリングを適用しません。police コマンドのないクラスは、どのトラフィックとも一致しません。
- 分類に使用する 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。
- 次の一致タイプだけがサポートされます。
  - **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行われます。
- 1 つの **match** コマンドを、1 つのクラス マップだけに入力できます。

サービス ポリシーを定義する場合は、**police** ポリシー マップ アクションだけがサポートされます。

サービス ポリシーをコントロール プレーンに適用する場合は、**input** 方向だけがサポートされます。

CoPP のモニタ

サイト固有のポリシーを作成するには、**show policy-map control-plane** コマンドを入力することで、コントロール プレーン ポリシーの統計情報をモニタでき、CoPP のトラブルシューティングを行うことが可能です。このコマンドを使用すると、実際に適用されたポリシーについてのダイナミックな情報を表示できます。たとえば、ハードウェアおよびソフトウェア内において、設定されたポリシーに適合する、またはこれを超過するバイト数およびパケット数を表示できます。

show policy-map control-plane コマンドの出力結果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#
```

ハードウェア カウンタを表示して、ポリシーによってドロップおよび転送されたバイト数を確認するには、**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

ここでは、CoPP トラフィックを分類する方法について説明します。

- 「トラフィック分類の概要」（P.47-6）
- 「トラフィック分類の注意事項」（P.47-7）
- 「CoPP トラフィック分類の基本的な ACL の例」（P.47-7）

トラフィック分類の概要

定義できるクラスの数に制限はありませんが、一般的にトラフィックは、相対的な重要度に基づくクラスに分類されます。次に、グループ分けの例を示します。

- Border Gateway Protocol（BGP）：BGP ルーティング プロトコルにおいて、ネイバー関係を維持するために重要なトラフィック。BGP キープ アライブ、ルーティング更新などです。BGP ルーティング プロトコルの維持は、ネットワーク内での接続、またはサービス プロバイダーとの接続を維持するうえで重要です。BGP を実行しないサイトでは、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）：IGP ルーティング プロトコルを維持するうえで重要なトラフィック。たとえば Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）などです。IGP ルーティング プロトコルの維持は、ネットワーク内の接続を維持するうえで重要です。
- 管理：日常業務で必要とされ、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）、Network Time Protocol（NTP）、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、Terminal Access Controller Access Control System（TACACS）、HTTP、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、File Transfer Protocol（FTP; ファイル転送プロトコル）などがあります。
- レポート：レポート目的で、ネットワーク パフォーマンスに関する統計情報の生成に使用されるトラフィック。たとえば、Cisco IOS IP サービス レベル契約を使用して、異なる DSCP 設定で ICMP を生成し、さまざまな QoS データ クラス内の応答時間をレポートできます。
- モニタ：スイッチのモニタに使用するトラフィック。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）、traceroute などです。
- クリティカルなアプリケーション：特定のお客様の環境に固有の、クリティカルなアプリケーション 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 Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用するお客様もいます。このトラフィックの例としては、GRE、Hot Standby Router Protocol（HSRP）、Virtual Router Redundancy Protocol（VRRP）、Session Initiation Protocol（SIP）、データ リンク スイッチング、Dynamic Host Configuration Protocol（DHCP）、Multicast Source Discovery Protocol（MSDP）、IGMP、Protocol Independent Multicast（PIM）、マルチキャスト トラフィック、IPsec などが挙げられます。
- レイヤ 2 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。現時点では、一致プロトコル分類基準を使用して明示的に分類可能な唯一のレイヤ 2 プロトコルが、ARP となります。
- 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した場合は、**show** コマンドを使用すると、拒否したトラフィックの概算統計情報を収集し、その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 クラスを備えているため、他のユーザ定義クラスでは明示的に識別されないトラフィックに適用する処理を指定できます。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。デフォルト分類を設定しておくと、統計情報をモニタして、通常であれば識別されないコントロール プレーン宛てトラフィックのレートを決定できます。このトラフィックを識別したあとは、追加の分析を行うことで該当カテゴリに分類できます。必要であれば、このトラフィックにも対応するように、他の CoPP ポリシー エントリを更新することもできます。

トラフィックの分類が完了すると、ACL は、ポリシーの定義に使用するトラフィック クラスを作成します。CoPP 分類に使用する基本的な ACL の例については、「CoPP トラフィック分類の基本的な ACL の例」（P.47-7）を参照してください。

トラフィック分類の注意事項

トラフィック分類を定義する場合は、次の注意事項および制約事項に従ってください。

- 実際の CoPP ポリシーを作成する前に、どのトラフィックをどのクラスに分類するかを識別しておく必要があります。トラフィックは相対的な重要度に基づき、9 つのクラスに分類されます。実際に必要となるクラス数はこれとは異なる可能性があり、各自のローカルな要件、およびセキュリティ ポリシーに基づき選択する必要があります。
- 双方向的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的な ACL の例

ここでは、CoPP 分類の基本的な ACL の例を示します。各例では、一般的に必要とされるトラフィックを、以下の ACL によって識別します。

- ACL 120：クリティカルなトラフィック
- ACL 121：重要なトラフィック
- ACL 122：通常のトラフィック
- 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

次の例では、クリティカルなトラフィックに対する ACL 120 を定義します。

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

次の例では、既知のピアからスイッチの BGP TCP ポートへの、BGP トラフィックを許可します。

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

次の例では、ピアの BGP ポートからこのスイッチへの BGP トラフィックを許可します。

```
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
```

次の例では、重要なクラスに対する ACL 121 を定義します。

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

次の例では、TACACS ホストからのリターン トラフィックを許可します。

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

次の例では、サブネットからスイッチへの SSH アクセスを許可します。

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

次の例では、指定のサブネット内のホストからスイッチへの Telnet フル アクセスを許可し、残りのサブネットをポリシングします。

```
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
```

次の例では、NMS ホストからスイッチへの SNMP アクセスを許可します。

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

次の例では、既知のクロック ソースからの NTP パケットの受信をスイッチに許可します。

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

次の例では、通常のトラフィック クラスに対する ACL 122 を定義します。

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

次の例では、スイッチから送信される traceroute トラフィックを許可します。

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

次の例では、ping を発行したスイッチへの応答を受信することを許可します。

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

次の例では、スイッチへの ping の送信を許可します。

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

次の例では、不要なクラスに対する ACL 123 を定義します。

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

（注） 次の例では、ACL 123 は分類およびモニタのための許可エントリであり、トラフィックは CoPP ポリシーの結果に基づいてドロップされます。

この例では、UDP 1434 宛てに送信され、ポリシングの対象となるすべてのトラフィックを許可します。

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

次の例では、他のすべてのトラフィックに対する ACL 124 を定義します。

```
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

ヒント