分類、マーキング、およびポリシング

（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
- 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

分類、マーキング、およびポリシング ポリシーに関する情報

分類、マーキング、およびポリシング ポリシーの概要

分類、マーキング、およびポリシング設定は、インターフェイスに対応付けられポリシーによって定義されます。分類、マーキング、およびポリシングは、入力インターフェイスに設定されている QoS コマンドや、キューイング ポリシーの影響を受けません。

Traffic Classification

トラフィック分類により、設定したクラスに分類されるときに、ネットワークでそのトラフィックを認識できるようになります。特定の QoS を適用するためには、ネットワーク トラフィックを分類する必要があります。

分類は、包括的にすることもできれば（レイヤ 2 VLAN のすべてのトラフィック、あるインターフェイスを通るすべてのトラフィックなど）、極端に具体的にすることもできます（たとえば、トラフィックの特定の側面を認識する **match** コマンドによるクラス マップを使用可能）。

QoS を分類および適用してから（マーキングなど）、別のインターフェイスまたはネットワーク デバイスで、マークした値に基づいて分類し、別の QoS を適用することができます。

PFC および任意の DFC は、**class-map match-all** クラス マップで単一の **match** コマンドをサポートします。ただし、**match protocol** コマンドは、**match dscp** または **match precedence** コマンドによってクラス マップに設定できます。

PFC および任意の DFC は、**class-map match-any** クラス マップで複数の **match** コマンドをサポートします。

クラス マップでは、表 63-1 に記載されている **match** コマンドを使用して、一致基準に基づくトラフィック クラスを設定できます。

表 63-1　トラフィック分類のクラス マップの match コマンドと一致基準

match コマンド	方向	一致基準
match access-group {*access_list_number* | **name** *access_list_name*}	両方	アクセス コントロール リスト（ACL）。 **（注）** ACL は、次の要素の照合に使用します。 - CoS 値 - VLAN ID - パケット長
match any	両方	任意の一致基準
match cos	入力	CoS 値
match discard-class	両方	廃棄クラスの値。
match dscp **（注）** **match protocol** コマンドは、**match dscp** コマンドでクラス マップに設定できます。	両方	DSCP 値。
match l2 miss	入力	現在学習されていない MAC レイヤの宛先アドレスにアドレス指定されているため、VLAN でフラッディングしたレイヤ 2 トラフィック。
match mpls experimental topmost	両方	最上位ラベルの MPLS EXP 値。
match precedence **（注）** **match protocol** コマンドは、**match precedence** コマンドでクラス マップに設定できます。	両方	IP precedence 値。
match protocol {**arp** | **ip** | **ipv6**} **（注）** **match protocol** コマンドは、**match dscp** コマンドまたは **match precedence** コマンドでクラス マップに設定できます。	両方	プロトコル。
match qos-group	両方	QoS グループ ID。

PFC および任意の DFC は、**match access group** コマンドで使用するために、次の ACL タイプをサポートしています。

プロトコル	番号付き ACL の有無	拡張 ACL の有無	名前付き ACL の有無
IPv4	Yes： 1 ～ 99 1300 ～ 1999	Yes： 100 ～ 199 2000 ～ 2699	Yes
IPv6	N/A	Yes（名前付き）	Yes
MAC レイヤ	N/A	N/A	Yes
ARP	N/A	N/A	Yes

トラフィック マーキング

（注）　ポリシングでもトラフィックをマーキングできます。

ネットワーク トラフィックをマーキングすると、特定のトラフィック クラスの属性を設定または変更できます。これにより、クラス ベースの QoS 機能で、マーキングに基づいてトラフィック クラスを認識できるようになります。

次の 2 種類のトラフィック マーキング方法があります。

- ポリシーマップ **set** コマンドで設定値を適用できます。表 63-2 に、使用可能なポリシーマップ **set** コマンドと対応する属性を示します。

表 63-2　Configured-Value Policy-Map コマンド

set コマンド	トラフィック属性	入力	出力
set cos *cos_value*	レイヤ 2 CoS 値	Y	Y
set dscp *dscp_value*	レイヤ 3 DSCP 値	Y	Y
set precedence *precedence_value*	レイヤ 3 IP precedence 値	Y	Y
set dscp tunnel *dscp_value*	総称ルーティング カプセル化（GRE）トンネリングされたパケットのトンネル ヘッダーにあるレイヤ 3 DSCP 値	Y	Y
set discard-class *discard_value*	discard-class 値	Y	Y
set qos-group *group_id*	QoS グループ ID	Y	Y
set mpls experimental imposition *exp_value*	すべての割り当て済みラベル エントリの MPLS 実験（EXP）フィールド	Y	Y
set mpls experimental topmost *exp_value*	すべての最上位ラベル エントリの MPLS 実験（EXP）フィールド	Y	Y

- ポリシーマップ **set** コマンドで、受信した値にマップを適用できます。表 63-3 に、使用可能なポリシーマップ **set** コマンドと対応する属性を示します。

表 63-3　Mapped-Value Policy-Map コマンド

set コマンド	マップ名	トラフィック属性	入力	出力
set dscp cos	**dscp-cos-map**	レイヤ 3 DSCP 値	Y	N
set dscp precedence	**dscp-precedence-map**	レイヤ 3 DSCP 値	Y	N

ポリシングについて

ポリシングの概要

次の処理を行うポリサーを設定できます。

- トラフィックのマーキング
- 帯域利用率の制限およびトラフィックのマーキング

ポリサーは、入力および出力インターフェイスに適用できます。入力ポリシングが最初に適用され、続いて出力ポリシングが適用されます。

ポリシングを使用すると、QoS 設定で定義されたトラフィック転送ルールに適合するように、着信および発信トラフィックをレート制限できます。システムにおいてトラフィックが転送される方法を定義した設定済みルールは、契約と呼ばれます。この契約に適合しないトラフィックは、低い DSCP 値にマーク ダウンされるか、またはドロップされます。

ポリシングでは、アウトオブプロファイル パケットがバッファに保存されません。したがって、ポリシングが伝搬遅延に影響することはありません。逆に、トラフィック シェーピングではアウトオブプロファイル トラフィックをバッファに保存することで、トラフィック バーストを緩和します （PFC QoS はシェーピングをサポートしません）。

PFC および DFC は、入力および出力 PFC QoS をサポートしています。これには、入力および出力ポリシングが含まれます。ポリサーは、ポート単位または VLAN 単位で入力トラフィックに適用されます。出力トラフィックに対するポリシングは、VLAN 単位だけで行われます。

ポリシングでは、レイヤ 2 フレーム サイズを使用します。帯域利用率限度は、認定情報レート（CIR）で指定します。より高い最大情報レート（Peak Information Rate）も指定できます。レートを超過するパケットは、「アウト オブ プロファイル」または「不適合」です。

ポリサーごとに、アウトオブプロファイル パケットをドロップするか、新しい DSCP 値を適用するかを指定します（新しい DSCP 値を適用することを「マークダウン」といいます）。アウトオブプロファイル パケットは、元のプライオリティを維持しないため、インプロファイル パケットが消費した帯域幅の一部としてカウントされません。

PIR を設定する場合は、PIR アウトオブプロファイル アクションを CIR アウトオブプロファイル アクションよりも厳密なものする必要があります。たとえば、CIR アウトオブプロファイル アクションがトラフィックをマークダウンするアクションの場合、PIR アウトオブプロファイル アクションはトラフィックを送信するアクションにできません。

PFC QoS はあらゆるポリサーで、設定変更可能なグローバル テーブルを使用して、内部 DSCP 値をマークダウンされた DSCP 値にマッピングします。マークダウンが発生すると、PFC QoS はこのテーブルからマークダウンされた DSCP 値を取得します。ユーザが個々のポリサーでマークダウン後の DSCP 値を指定できません。

（注）

- デフォルトでは、マークダウン テーブルは、マークダウンが起こらないように設定されています。つまり、マークダウンされた DSCP 値は、元の DSCP 値と同じです。マークダウンをイネーブルにするには、ネットワークに合わせてテーブルを適切に設定します。
- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。

Per-Interface ポリサー

PFC QoS は、インターフェイス別のポリサーで指定された帯域幅制限を、一致したトラフィックに適用します。たとえば、一致するすべての TFTP トラフィックに 1 Mbps を許可するようインターフェイス別のポリサーを設定すると、TFTP トラフィックが 1 Mbps に制限されます。

ポリシー マップ クラスのインターフェイス別ポリサーは、**police** コマンドを使用して定義します。インターフェイス別ポリサーを複数の入力ポートに対応付けると、各ポリサーによって、各入力ポート上の一致するトラフィックが個別にポリシングされます。

集約ポリサー

集約ポリサーの概要

PFC QoS は、1 つの集約ポリサーで指定される帯域幅限度を、一致するトラフィックのすべてのフローに対して累積方式で適用します。たとえば、VLAN 1 および VLAN 3 上のすべての TFTP トラフィック フローの帯域幅として、1 Mbps を許可するように集約ポリサーを設定すると、VLAN 1 および VLAN 3 上のすべての TFTP トラフィック フローは、合計 1 Mbps となるように制限されます。

名前付き集約ポリサーは、**platform qos aggregate-policer** コマンドを使用して作成します。名前付き集約ポリサーを複数の入力ポートに対応付けると、そのポリサーが付加された全入力ポートからの一致するトラフィックがポリシングされます。

最大 1,023 個の集約ポリサーを設定できます。設定されている集約ポリサーをインターフェイスに適用して、最大 16,384 個のポリサー インスタンスを設定できます。

分散型の集約ポリサー

分散型の集約ポリシングがイネーブルの場合、集約ポリサーは、DFC を搭載したさまざまなスイッチング モジュールまたは PFC によってサポートされているインターフェイスで、ポリシングを同期します。分散型の集約ポリシングは、次のタイプに分類される最初の 4,096 個の集約ポリサー インスタンスに適用されます。

- VLAN、トンネル、ポート チャネル インターフェイスに適用された集約ポリサー。

- 共有集約ポリサー。
- 出力ポリシー内の集約ポリサー。

分散型の集約ポリシングがイネーブルの場合、ハードウェアでサポートされている機能を超える部分の集約ポリサーは、非分散型の集約ポリサーとして機能します。

非分散型の集約ポリサー

非分散型の集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。

個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。

- ポート チャネル インターフェイスに適用されたポリサー。
- スイッチ仮想インターフェイスに適用されたポリサー。
- レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。

この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

マイクロフロー ポリサー

PFC QoS は、マイクロフロー ポリサーで指定される帯域幅限度を、一致するトラフィックの各フローに対して個別に適用します。たとえば、VLAN 1 および VLAN 3 で TFTP トラフィックを 1 Mbps に制限するようにマイクロフロー ポリサーを設定すると、VLAN 1 の各フローに 1 Mbps が、VLAN 3 の各フローに 1 Mbps がそれぞれ許可されます。つまり、VLAN 1 上に 3 つのフロー、VLAN 3 上に 4 つのフローが存在する場合、microflow ポリサーは、これらの各フローに対して 1 Mbps を許可します。

マイクロフロー ポリサーの帯域幅限度を適用するように、PFC QoS を次のように設定できます。

- マイクロフロー ポリサーは、最大 127 通りのレートとバースト パラメータの組み合わせを使用して作成できます。
- ポリシー マップ クラスのマイクロフロー ポリサーは、**police flow** コマンドを使用して作成します。
- 送信元アドレスだけを使用するようにマイクロフロー ポリサーを設定できます。これにより宛先アドレスに関係なく、特定の送信元アドレスからのすべてのトラフィックにマイクロフロー ポリサーを適用します。
- 宛先アドレスだけを使用するようにマイクロフロー ポリサーを設定できます。これにより、送信元アドレスに関係なく、特定の宛先アドレスへのすべてのトラフィックにマイクロフロー ポリサーが適用されます。

- MAC レイヤ microflow ポリシングの場合、PFC QoS はプロトコルおよび送信元と宛先の MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、EtherType が異なるトラフィックでも、同じフローの一部であると見なします。IPX トラフィックをフィルタリングするように MAC ACL を設定できます。
- ARP トラフィックには、マイクロフロー ポリシングを適用できません。
- リリース 15.1(1) SY1 以降のリリースでは、出力マイクロフロー宛先専用ポリシングをサポートしています。出力ポリシングは VLAN ごとで、レイヤ 3 インターフェイスまたは SVI に適用されます。リリース 15.1(1) SY1 よりも前のリリースでは、**output** キーワードで対応付けられたポリシーはマイクロフロー ポリシングをサポートしません。

各ポリシー マップ クラスに集約ポリサーおよびマイクロフロー ポリサーの両方を含めると、単独の帯域利用率と、他のフローと合算された帯域利用率に基づいて、フローのポリシングを行うことができます。

（注）　トラフィックに集約ポリシングとマイクロフロー ポリシングを実行する場合、集約ポリサーおよびマイクロフロー ポリサーを同じポリシー マップ クラスに組み込み、各ポリサーで同じ **conform-action** および **exceed-action** キーワード オプションを使用する必要があります（**drop**、**set-dscp-transmit**、**set-prec-transmit**、または **transmit**）。

たとえば、グループの個々のメンバーに適した帯域幅限度を設定してマイクロフロー ポリサーを作成し、さらに、グループ全体として適切な帯域幅限度を設定して名前付き集約ポリサーを作成できます。グループのトラフィックと一致するポリシー マップ クラスに、この両方のポリサーを含めます。この組み合わせは、個々のフローには別々に作用し、グループには集約的に作用します。

ポリシー マップ クラスに集約ポリサーおよびマイクロフロー ポリサーの両方が含まれている場合、PFC QoS はいずれかのポリサーに基づいてアウトオブプロファイル ステータスに対応し、そのポリサーの指定に従って、新しい DSCP 値を適用するか、またはパケットをドロップします。両方のポリサーからアウトオブプロファイル ステータスが戻された場合には、いずれかのポリサーでパケットのドロップが指定されていれば、パケットはドロップされます。指定されていない場合は、マークダウンされた DSCP 値が適用されます。

分類、マーキング、およびポリシング ポリシーの設定方法

分散型の集約ポリシングのイネーブル化

分散型の集約ポリシングイネーブルにするには、次の作業を行います。

コマンド	目的
Router(config)# **platform qos police distributed** {**strict** | **loose**}	分散型の集約ポリシングをイネーブルにします。 • **strict** キーワードを使用すると、使用可能なハードウェア リソースを超えるインターフェイスに対して集約ポリサーが適用されません。 • **loose** キーワードを使用すると、使用可能なハードウェア リソースを超えるインターフェイスに、非分散型として集約ポリサーを適用できます。

次に、厳密な分散型集約ポリシングをグローバルにイネーブルにする例を示します。

```
Router(config)# platform qos police distributed strict
Router(config)#
```

次に、分散型集約ポリシングをグローバルにディセーブルにする例を示します。

```
Router(config)# no platform qos police distributed
Router(config)#
```

クラス マップの設定

クラス マップの作成

クラス マップを作成するには、次の作業を行います。

コマンド	目的
Router(config)# **class-map** [**match-all** | **match-any**] *class_name*	クラス マップを作成します。 （注）　**match** キーワードを入力しない場合、デフォルトは **match-all** です。

クラス マップでのフィルタリングの設定

クラス マップにフィルタリングを設定するには、表 63-1、「トラフィック分類のクラス マップの match コマンドと一致基準」を参照して、match コマンドを入力します。

クラス マップの設定の確認

クラス マップの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router (config-cmap)# end`	コンフィギュレーション モードを終了します。
ステップ 2	`Router# show class-map class_name`	設定を確認します。

次に、**ipp5** という名前のクラス マップを作成し、IP precedence 5 のトラフィックと一致するようにフィルタリングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# end
```

次に、設定を確認する例を示します。

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

ポリシー マップ コンフィギュレーション

ポリシー マップの概要

ポリシー マップには、ポリシー マップ コマンドがそれぞれ異なる 1 つまたは複数のポリシー マップ クラスを含めることができます。

インターフェイスで受信するトラフィック タイプごとに、個別のポリシー マップ クラスをポリシー マップ内に設定します。各トラフィック タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。PFC QoS は、一致したトラフィックに複数のポリシー マップ クラスのコマンドを適用することはありません。

ポリシー マップの作成

ポリシー マップを作成するには、次の作業を行います。

コマンド	目的
Router(config)# **policy-map** *policy_name*	ポリシー マップを作成します。

ポリシー マップ クラスの設定に関する注意事項および制約事項

- PFC QoS は、**class** *class_name* **destination-address**、**class** *class_name* **input-interface**、**class** *class_name* **qos-group**、および **class** *class_name* **source-address** ポリシー マップ コマンドをサポートしていません。
- PFC QoS は、**class default** ポリシー マップ コマンドをサポートします。
- PFC QoS は、インターフェイスにポリシー マップが付加されないかぎり、サポート対象外のコマンドが使用されているかどうかを検出しません。
- PFC QoS は、クラスごとに複数の ACL の一致をサポートしません。

ポリシー マップ クラスの作成およびフィルタリングの設定

ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリングするように設定するには、次の作業を行います。

コマンド	目的
Router(config-pmap)# **class** *class_name*	ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリングするように設定します。 **（注）** PFC QoS は、**match** コマンドが 1 つだけ指定されているクラス マップをサポートします。

ポリシー マップ クラス アクションの設定

- 「ポリシー マップ クラス アクションの制約事項」（P.63-10）
- 「ポリシー マップ クラス マーキングの設定」（P.63-11）
- 「ポリシー マップ クラスの信頼状態の設定」（P.63-12）
- 「ポリシー マップ クラスのポリシングの設定」（P.63-12）

ポリシー マップ クラス アクションの制約事項

- ポリシー マップには、1 つ以上のポリシー マップ クラスを含めることができます。
- 各トラフィック タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。
- PFC QoS は、1 つのポリシー マップ クラスのコマンドだけをトラフィックに適用します。QoS で、1 つのポリシー マップ クラスのフィルタリングに一致したトラフィックには、他のポリシー マップ クラスで設定したフィルタリングは適用されません。

- ハードウェアでスイッチングされるトラフィックの場合、PFC QoS は **bandwidth**、**priority**、**queue-limit**、または **random-detect** ポリシー マップ クラス コマンドをサポートしません。これらのコマンドはソフトウェアでスイッチングされるトラフィックに使用できるので、設定が可能です。
- PFC QoS では、**set qos-group** ポリシー マップ クラス コマンドはサポートされません。
- PFC QoS は、IPv4 トラフィックに対して **set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドをサポートします。
  - 非 IP トラフィック上で **set ip dscp** および **set ip precedence** コマンドを使用して、出力レイヤ 2 CoS 値の基準である内部 DSCP 値をマーキングできます。
  - **set ip dscp** および **set ip precedence** コマンドは、**set dscp** および **set precedence** コマンドとしてコンフィギュレーション ファイルに保存されます。
- PFC QoS では、IPv4 および IPv6 トラフィック用の **setdscp** および **set precedence** ポリシー マップ クラス コマンドがサポートされます。
- ポリシー マップ クラスで、次の 3 つすべてを実行することができません。
  - **set** コマンドによるトラフィックのマーキング
  - 信頼状態の設定
  - ポリシングの設定

  ポリシー マップ クラスでは、トラフィックを **set** コマンドによってマーキングするか、次のいずれか、あるいは両方を実行できます。
  - 信頼状態の設定
  - ポリシングの設定

（注） ポリシングを設定する場合は、ポリシング キーワードでトラフィックをマーキングできます。

ポリシー マップ クラス マーキングの設定

PFC QoS は、すべてのトラフィックに対し、**set** ポリシー マップ クラス コマンドを使用したポリシー マップ クラス マーキングをサポートします。ポリシー マップ クラス マーキングを設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# set {dscp dscp_value | precedence ip_precedence_value}`	ポリシー マップ クラスを設定して、設定されている DSCP 値または IP precedence 値と一致するトラフィックをマーキングするようにします。

ポリシー マップ クラスの信頼状態の設定

（注）　**service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを対応付けることができません。

ポリシー マップ クラスの信頼状態を設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# trust {cos | dscp | ip-precedence}`	ポリシー マップ クラスの信頼状態を設定します。この設定によって、PFC QoS が初期内部 DSCP 値の作成元として使用する値が選択されます。

ポリシー マップ クラスの信頼状態を設定する場合、次の点に注意してください。

- 入力ポート上に設定されている信頼状態を使用するには、**no trust** コマンド（これがデフォルトです）を使用します。
- **cos** キーワードを使用すると、PFC QoS は受信した CoS または入力ポートの CoS に基づいて、内部 DSCP 値を設定します。
- **dscp** キーワードを使用すると、PFC QoS は受信した DSCP を使用します。
- **ip-precedence** キーワードを使用すると、PFC QoS は受信した IP precedence に基づいて DSCP を設定します。

ポリシー マップ クラスのポリシングの設定

- 「ポリシー マップ クラスのポリシングの制約事項」（P.63-12）
- 「名前付き集約ポリサーの使用」（P.63-12）
- 「インターフェイス別ポリサーの設定」（P.63-13）
- 「インターフェイス別マイクロフロー ポリサーの設定」（P.63-15）

ポリシー マップ クラスのポリシングの制約事項

- PFC QoS は **set-qos-transmit** ポリサー キーワードをサポートしません。
- PFC QoS は、**exceed-action** キーワードの引数として **set-dscp-transmit** キーワードまたは **set-prec-transmit** キーワードをサポートしません。
- PFC QoS は、インターフェイスにポリシー マップが対応付けられない限り、サポート対象外のキーワードが使用されているかどうかを検出しません。
- **conform-action transmit** キーワードによるポリシングでは、一致するトラフィックのポート信頼状態が、trust dscp またはポリシー マップ クラスの **trust** コマンドで設定される信頼状態に設定されます。

名前付き集約ポリサーの使用

名前付き集約ポリサーを使用するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# police aggregate aggregate_name`	定義済みの名前付き集約ポリサーを使用するように、ポリシー マップ クラスを設定します。

- 分散型の集約ポリシングがイネーブルの場合は、次の情報に注意してください。
  - 分散型の集約ポリサーは、DFC を搭載したさまざまなスイッチング モジュールまたは PFC によってサポートされているインターフェイスで、ポリシングを同期します。分散型の集約ポリシングは、次のタイプに分類される最初の 4,096 個の集約ポリサーに適用されます。
    - VLAN、トンネル、ポート チャネル インターフェイスに適用された集約ポリサー。
    - 共有集約ポリサー。
    - 出力ポリシー内の集約ポリサー。
  - ハードウェアでサポートされている機能を超える部分の分散型の集約ポリサーは、非分散型の集約ポリサーとして機能します。
- 分散型の集約ポリシングがイネーブルでない場合は、次の情報に注意してください。
  - 集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
  - 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
    - ポート チャネル インターフェイスに適用されたポリサー。
    - スイッチ仮想インターフェイスに適用されたポリサー。
    - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。
  - この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

インターフェイス別ポリサーの設定

インターフェイス別のポリサーを設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# police` *bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir** *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit** *dscp_value* | **set-prec-transmit** *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	インターフェイス別のポリサーを作成して、それを使用するようにポリシー マップ クラスを設定します。

- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。
- ポリシングでは、レイヤ 2 フレーム サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS に関する制約事項」（P.62-1）を参照してください。
- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小値：32 Kbps（32000 と入力）
  - 最大：256 Gbps（256000000000 と入力）

- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。
- *maximum_burst_bytes* パラメータでは、PIR トークン バケット サイズを設定します。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、トークン バケット サイズには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
  - TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。
  - *maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります。
  - 特定のレートを維持するには、トークン バケット サイズがレート値を 2000 で割った値よりも大きくなるように設定します。
  - 最小トークン バケット サイズは 1 バイトで、1 と入力します。
  - 最大トークン バケット サイズは 512 MB で、512000000 と入力されます。
- 有効な **pir** *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 : 32 kbps（32000 と入力。CIR *bits_per_second* パラメータより小さい値は使用できません）
  - 最大 : 256 Gbps（256000000000 と入力）
- （任意）一致するインプロファイル トラフィックに対応する conform アクションを、次のように指定できます。
  - デフォルトの conform アクションは、**transmit** です。このアクションでは、ポリシー マップ クラスに **trust** コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が *trust dscp* に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマーキングするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマーキングします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してだけサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 一致するトラフィックをすべてドロップするには、**drop** キーワードを入力します。
  - 同じトラフィックに適用する集約ポリサーおよびマイクロフロー ポリサーで、それぞれ同じ conform アクションの動作が指定されていることを確認してください。
- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル トラフィックを送信します。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

    （注） exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致したすべてのアウトオブプロファイル トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

（注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- （任意）PIR を超過するトラフィックについて、violate アクションを次のように指定できます。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル トラフィックを送信します。
  - デフォルトの violate アクションは、exceed アクションと同じものです。
  - 一致したすべてのアウトオブプロファイル トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

次に、**max-pol-ipp5** という名前のポリシー マップを作成する例を示します。このポリシー マップは、クラス マップ **ipp5** を使用し、受信した IP precedence 値に基づいて信頼状態を設定し、最大容量に関する集約ポリサーおよびマイクロフロー ポリサーを設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
```

インターフェイス別マイクロフロー ポリサーの設定

インターフェイス別のマイクロフロー ポリサーを設定するには、次の作業を行います。

コマンド	目的
Router(config-pmap-c)# **police flow** [**mask** {**src-only** | **dest-only** | **full-flow**}] *bits_per_second normal_burst_bytes* [[[**conform-action** {**drop** | **set-dscp-transmit** *dscp_value* | **set-prec-transmit** *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	インターフェイス別のマイクロフロー ポリサーを作成して、それを使用するようにポリシーマップ クラスを設定します。

- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。
- ポリシングでは、レイヤ 2 フレーム サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS に関する制約事項」（P.62-1）を参照してください。
- 送信元アドレスだけに基づいてフローの識別を行うには、**mask src-only** キーワードを入力します。これにより、マイクロフロー ポリサーが、各送信元アドレスからのすべてのトラフィックに適用されます。PFC QoS では、IP トラフィックおよび MAC トラフィック両方に対して **mask src-only** キーワードをサポートします。

- 宛先アドレスだけに基づいてフローの識別を行うには、**mask dest-only** キーワードを入力します。これにより、マイクロフロー ポリサーが、各送信元アドレスへのすべてのトラフィックに適用されます。PFC QoS では、IP トラフィックおよび MAC トラフィック両方に対して **mask dest-only** キーワードをサポートします。リリース 15.1(1) SY1 以降のリリースでは、出力マイクロフロー宛先専用ポリシングをサポートしています。出力ポリシングは VLAN ごとで、レイヤ 3 インターフェイスまたは SVI に適用されます。
- デフォルトおよび **mask full-flow** キーワードを使用する場合は、PFC QoS は送信元 IP アドレス、宛先 IP アドレス、レイヤ 3 プロトコル、レイヤ 4 ポート番号に基づいて IP フローの識別を行います。
- PFC QoS は、プロトコルおよび送信元と宛先 MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、EtherType が違っていても、同じフローの一部であると見なします。
- マイクロフロー ポリサーでは、*maximum_burst_bytes* パラメータ、**pir** *bits_per_second* キーワードおよびパラメータ、または **violate-action** キーワードはサポートされません。

（注） マイクロフロー ポリシング、NetFlow、および NetFlow データ エクスポート（NDE）のフローマスク要件は、競合する可能性があります。

- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小値：32 Kbps（32000 と入力）
  - 最大：256 Gbps（256000000000 と入力）
- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、トークン バケット サイズには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
  - TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。
  - *maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります。
  - 特定のレートを維持するには、トークン バケット サイズがレート値を 2000 で割った値よりも大きくなるように設定します。
  - 最小トークン バケット サイズは 1 バイトで、1 と入力します。
  - 最大トークン バケット サイズは 512 MB で、512000000 と入力されます。
- （任意）一致するインプロファイル トラフィックに対応する conform アクションを、次のように指定できます。
  - デフォルトの conform アクションは、**transmit** です。このアクションでは、ポリシー マップ クラスに **trust** コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が *trust dscp* に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマーキングするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマーキングします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してだけサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 一致するトラフィックをすべてドロップするには、**drop** キーワードを入力します。

  - 同じトラフィックに適用する集約ポリサーおよびマイクロフロー ポリサーで、それぞれ同じ conform アクションの動作が指定されていることを確認してください。
- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - ポリシングなしでマーキングするには、**transmit** キーワードを入力して、一致したすべてのアウトオブプロファイル トラフィックを送信します。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

    （注） exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致したすべてのアウトオブプロファイル トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

    （注） **pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

ポリシー マップの設定の確認

ポリシー マップの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-pmap-c)# end`	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。 **（注）** ポリシー マップで追加クラスを作成するには、追加の **class** コマンドを入力します。
ステップ 2	`Router# show policy-map` *policy_name*	設定を確認します。

次に、設定を確認する例を示します。

```
Router# show policy-map max-pol-ipp5
 Policy Map max-pol-ipp5
  class  ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit
    trust precedence
    police 2000000000 2000000 2000000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit

Router#
```

インターフェイスへのポリシー マップの対応付け

ポリシー マップをインターフェイスに対応付けるには、次の作業を行います。

	コマンド	目的
ステップ1	`Router(config)# interface {{vlan vlan_ID}	{type slot/port[.subinterface]}	{port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ2	`Router(config-if)# service-policy [input	output] policy_map_name`	ポリシー マップをインターフェイスに対応付けます。
ステップ3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。

- EtherChannel のメンバーであるポートに、サービス ポリシーを付加しないでください。
- PFC QoS は、レイヤ 3 インターフェイス（レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイスのいずれか）上だけで **output** キーワードをサポートします。レイヤ 3 インターフェイスには、入力および出力ポリシー マップの両方を付加できます。
- レイヤ 2 ポート上の VLAN ベースまたはポートベースの PFC QoS は、**output** キーワードを使用してレイヤ 3 インターフェイスに対応付けられたポリシーとは関係ありません。
- リリース 15.1(1) SY1 以降のリリースでは、出力マイクロフロー宛先専用ポリシングをサポートしています。出力ポリシングは VLAN ごとで、レイヤ 3 インターフェイスまたは SVI に適用されます。リリース 15.1(1) SY1 よりも前のリリースでは、**output** キーワードで対応付けられたポリシーはマイクロフロー ポリシングをサポートしません。
- **service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを対応付けることができません。
- **output** キーワードを使用して対応付けられたポリシーの IP precedence または DSCP に基づいたフィルタリングでは、受信した IP precedence 値または DSCP 値が使用されます。**output** キーワードを使用して対応付けられたポリシーの IP precedence または DSCP に基づいたフィルタリングは、入力 QoS による IP precedence または DSCP の変更には基づいていません。
- 共有集約ポリサーは、入力と出力の両方の方向には適用できません。
- 分散型の集約ポリシングがイネーブルの場合、集約ポリサーは、DFC を搭載したさまざまなスイッチング モジュールまたは PFC によってサポートされているインターフェイスで、ポリシングを同期します。分散型の集約ポリシングは、次のタイプに分類される最初の 4,096 個の集約ポリサー インスタンスに適用されます。
  - VLAN、トンネル、ポート チャネル インターフェイスに適用された集約ポリサー。
  - 共有集約ポリサー。
  - 出力ポリシー内の集約ポリサー。

  分散型の集約ポリシングがイネーブルの場合、ハードウェアでサポートされている機能を超える部分の集約ポリサーは、非分散型の集約ポリサーとして機能します。

- 非分散型の集約ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。集約ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。集約ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。

  個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。

  - ポート チャネル インターフェイスに適用されたポリサー。
  - スイッチ仮想インターフェイスに適用されたポリサー。
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

- 非集約ポリサーの場合は、個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。

  - ポート チャネル インターフェイスに適用されたポリサー。
  - スイッチ仮想インターフェイスに適用されたポリサー。
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックのドロップのいずれかを実行する必要があります。PFC QoS では、出力ドロップを使用した入力マークダウン、または出力マークダウンを使用した入力ドロップをサポートしません。

次に、ポリシー マップ **pmap1** をギガビット イーサネット ポート 5/36 に対応付ける例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 5/36
Router(config-if)# service-policy input pmap1
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show policy-map interface gigabitethernet 5/36
 gigabitethernet5/36
  service-policy input: pmap1
    class-map: cmap1 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class cmap1
    police 8000 8000 conform-action transmit exceed-action drop
    class-map: cmap2 (match-any)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 2
        0 packets, 0 bytes
        5 minute rate 0 bps
  class cmap2
    police 8000 10000 conform-action transmit exceed-action drop
Router#
```

ポリシー マップの動的セッション単位接続の設定

ポリシー マップの動的セッション単位接続の前提条件

- ユーザが認証されるときに割り当てられる、入力および出力 QoS ポリシー マップを定義します。
- アイデンティティ ポリシーを設定して、割り当てられるポリシー マップを指定します。
- RADIUS サーバのユーザ プロファイルで、Cisco ベンダー固有属性（VSA）を設定して、各ユーザに割り当てられる入力および出力 QoS ポリシー マップを指定します。

ポリシー マップの定義と関連付け

ポリシー マップを定義して、アイデンティティ ポリシーに関連付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# policy-map in_policy_name`	入力 QoS ポリシー マップを設定します。
ステップ 2	`Router(config-pmap)# class class_map_name` `...`	ポリシー マップ クラスを設定します。
ステップ 3	`Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション サブモードを終了します。
ステップ 4	`Router(config)# policy-map out_policy_name`	出力 QoS ポリシー マップを設定します。
ステップ 5	`Router(config-pmap)# class class_map_name` `...`	ポリシー マップ クラスを設定します。
ステップ 6	`Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション サブモードを終了します。
ステップ 7	`Router(config)# identity policy policy1`	アイデンティティ ポリシーを作成し、アイデンティティ ポリシー コンフィギュレーション サブモードを開始します。
ステップ 8	`Router(config-identity-policy)# service-policy type qos input in_policy_name`	入力 QoS ポリシー マップとこのアイデンティティを関連付けます。
ステップ 9	`Router(config-identity-policy)# service-policy type qos output out_policy_name`	出力 QoS ポリシー マップとこのアイデンティティを関連付けます。
ステップ 10	`Router(config-identity-policy)# end`	アイデンティティ ポリシー コンフィギュレーション サブモードを停止して、特権 EXEC モードに戻ります。

アイデンティティ ポリシーを削除するには、**no identity-policy** *policy_name* コマンドを使用します。

ポリシー マップを定義したら、次に示すように、ポリシー マップ名を使用して、RADIUS サーバの各ユーザ プロファイルで Cisco AV ペア属性を設定します。

- cisco-avpair = "ip:sub-policy-In=*in_policy_name*"
- cisco-avpair = "ip:sub-policy-Out=*out_policy_name*"

RADIUS サーバで Cisco AV ペア属性を設定するには、次の作業を行います。

コマンドまたはアクション	目的
sub-policy-In=*in_policy_name* **sub-policy-Out=***out_policy_name*	ユーザ ファイルで RADIUS サーバのサービス ポリシーの 2 つの Cisco AV ペアを入力します。スイッチがポリシー名を要求すると、ユーザ ファイルのこの情報が提供されます。 RADIUS ユーザ ファイルには、RADIUS サーバが認証する各ユーザのエントリが含まれます。各エントリは、*ユーザ プロファイル* とも呼ばれ、ユーザがアクセスできる属性を確立します。 この例で設定されるサービス ポリシーでは、QoS ポリシー マップがインターフェイスに接続され、方向が指定されます（方向は、データ パケットがインターフェイスに送信される場合はインバウンド、データ パケットがインターフェイスから送信される場合はアウトバウンドです）。 インバウンド方向で適用されるポリシー マップは、example_in_qos で、アウトバウンド ポリシー マップは example_out_qos です。

次に、RADIUS サーバのユーザ ファイルのコンフィギュレーションの例を示します。

```
userid    Password ="cisco"
   Service-Type = Framed,
   Framed-Protocol = PPP,
   cisco-avpair = "sub-policy-In=example_in_qos",
   cisco-avpair = "sub-policy-Out=example_out_qos"
```

次に、セッションがアクティブの場合、**show epm session summary** コマンドの出力例を示します。

```
Router# show epm session summary

EPM Session Information
-----------------------
Total sessions seen so far : 5
Total active sessions      : 1
Session IP Address         : 192.0.2.1
-------------------
```

次に、IP アドレスが 192.0.2.1 のインターフェイスでセッションがアクティブの場合の **show epm session ip** *ip_addr* コマンドの出力例を示します。

```
Router# show epm session ip 192.0.2.1

Admission feature       : AUTHPROXY
AAA Policies            :
Input Service Policy    : in_policy_name
Output Service Policy   : out_policy_name
```

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