



## N から P

---

- non-tcp (3 ページ)
- non-tcp contexts (4 ページ)
- oam-bundle (6 ページ)
- platform ip features sequential (9 ページ)
- platform ipsec fips-mode (12 ページ)
- platform ipsec llq (13 ページ)
- platform punt-police queue (14 ページ)
- platform qos marker-statistics (17 ページ)
- platform qos match-statistics per-ace (19 ページ)
- platform qos match-statistics per-filter (21 ページ)
- platform qos-port-channel\_aggregator (23 ページ)
- platform qos-port-channel\_multiple\_active (24 ページ)
- platform vfi dot1q-transparency (25 ページ)
- plim qos input (27 ページ)
- plim qos input map (30 ページ)
- plim qos input map cos (VLAN の CoS 値を分類) (36 ページ)
- police (39 ページ)
- police (EtherSwitch) (50 ページ)
- police (percent) (52 ページ)
- police (ポリシー マップ) (60 ページ)
- police (2 つのレート) (68 ページ)
- police rate (コントロールプレーン) (76 ページ)
- police rate pdp (82 ページ)
- policy-map (86 ページ)
- policy-map copp-peruser (94 ページ)
- precedence (95 ページ)
- precedence (WRED グループ) (99 ページ)
- preempt-priority (102 ページ)
- priority (104 ページ)

- [priority \(10000 シリーズ\)](#) (108 ページ)
- [priority \(SIP400\)](#) (111 ページ)
- [priority-group](#) (114 ページ)
- [priority level](#) (117 ページ)
- [priority-list default](#) (120 ページ)
- [priority-list interface](#) (122 ページ)
- [priority-list protocol](#) (124 ページ)
- [priority-list queue-limit](#) (129 ページ)
- [priority-queue cos-map](#) (131 ページ)
- [priority-queue queue-limit](#) (133 ページ)
- [pvc-bundle](#) (135 ページ)

## non-tcp

IP ヘッダー圧縮 (IPHC) プロファイル内で非 Transmission Control Protocol (非 TCP) ヘッダー圧縮を有効にするには、IPHC プロファイル コンフィギュレーション モードで **non-tcp** コマンドを使用します。IPHC プロファイル内で非 TCP ヘッダー圧縮を無効にするには、このコマンドの **no** 形式を使用します。

**non-tcp**  
**no non-tcp**

**構文の説明** このコマンドには引数またはキーワードはありません。

**コマンド デフォルト** 非 TCP ヘッダー圧縮は有効になっています。

**コマンド モード** IPHC プロファイル コンフィギュレーション

<b>コマンド履歴</b>	リリース	変更箇所
	12.4(9)T	このコマンドが導入されました。

**使用上のガイドライン** IPHC プロファイルでの使用目的

**non-tcp** コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワーク上でヘッダー圧縮を有効にして設定するために使用されます。IPHC プロファイルを使用したヘッダー圧縮の設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、Release 12.4T の「Header Compression」モジュールと「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

### 例

次に、**profile2** という名前の IPHC プロファイルを設定する例を示します。この例では、非 TCP ヘッダー圧縮が設定されます。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# end
```

<b>関連コマンド</b>	コマンド	説明
	<b>iphc-profile</b>	IPHC プロファイルを作成します。

## non-tcp contexts

非 Transmission Control Protocol (TCP) ヘッダー圧縮に使用できるコンテキストの数を設定するには、IPHC プロファイル コンフィギュレーション モードで **non-tcpcontexts** コマンドを使用します。以前に設定したコンテキストの数を削除するには、このコマンドの **no** 形式を使用します。

**non-tcp contexts** {*absolute number-of-connections*|*kbps-per-context kbps*}  
**no non-tcp contexts**

### 構文の説明

<b>absolute</b>	圧縮された非TCP コンテキストの最大数が、固定（絶対）数に基づくことを示します。
<i>number-of-connections</i>	非 TCP 接続の数です。範囲は 1 ～ 1000 です。
<b>kbps-per-context</b>	圧縮された非TCP コンテキストの最大数が、使用可能な帯域幅に基づくことを示します。
<i>kbps</i>	各コンテキストに許可する kbps 数です。範囲は 1 ～ 100 です。

### コマンド デフォルト

**non-tcpcontexts** コマンドは、帯域幅に基づいてコンテキストの数を計算し、コンテキストごとに 4 kbps を割り当てます。

### コマンド モード

IPHC プロファイル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
12.4(9)T	このコマンドが導入されました。

### 使用上のガイドライン

**non-tcpcontexts** コマンドを使用して、非 TCP ヘッダー圧縮に使用できるコンテキストの数を設定します。コンテキストとは、コンプレッサがヘッダーの圧縮に使用し、デコンプレッサがヘッダーの圧縮解除に使用する状態です。コンテキストは、送信された最終ヘッダーの非圧縮バージョンであり、パケットの圧縮と圧縮解除に使用する情報が含まれます。

#### IPHC プロファイルでの使用目的

**non-tcpcontexts** コマンドは、IPHC プロファイルの一部として使用することを目的としています。IPHC プロファイルは、ネットワークでのヘッダー圧縮を有効および設定するために使用されます。IPHC プロファイルを使用してヘッダー圧縮を設定する詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』、リリース 12.4T の「Header Compression」モジュールおよび「Configuring Header Compression Using IPHC Profiles」モジュールを参照してください。

#### 絶対数としてのコンテキストの数の設定

**non-tcpcontexts** コマンドにより、コンテキストの数を絶対数として設定できます。コンテキストの数を絶対数として設定するには、1 ~ 1000 の数を入力します。

#### 帯域幅に基づくコンテキストの数の計算

**non-tcpcontexts** コマンドにより、IPHC プロファイルが適用されるネットワーク リンクで使用できる帯域幅に基づいて、コンテキストの数を計算できます。

使用できる帯域幅に基づいて計算されたコンテキストの数を得るには、**kbps-per-context** キーワードに続けて *kbps* 引数の値を入力します。このコマンドは、使用できる帯域幅を、指定された *kbps* で割ります。たとえば、ネットワーク リンクの帯域幅が 3000 kbps で、*kbps* 引数に 5 を入力すると、このコマンドは 600 のコンテキストを算出します。

#### 例

profile2 という IPHC プロファイルの例を、次に示します。この例では、非 TCP コンテキストの数が 75 に設定されています。

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp contexts absolute 75
Router(config-iphcp)# end
```

#### 関連コマンド

コマンド	説明
<b>iphc-profile</b>	IPHCプロファイルを作成します。

## oam-bundle

バンドル、またはVCバンドルに適用できるVCクラスのすべての仮想回線（VC）メンバーについて、エンドツーエンドF5運用管理および保守（OAM）ループバックセル生成およびOAM管理を有効にするには、SVC-bundle コンフィギュレーションモードまたはVC-class コンフィギュレーションモードで **oam-bundle** コマンドを使用します。バンドルまたはクラスの設定から OAM 管理を削除するには、このコマンドの **no** 形式を使用します。

バンドルのすべての VC メンバーについて、エンドツーエンド F5 OAM ループバック セル生成およびOAM管理を有効にするには、バンドルコンフィギュレーションモードで **oam-bundle** コマンドを使用します。バンドルから OAM 管理を削除するには、このコマンドの **no** 形式を使用します。

**oam-bundle [manage] [frequency]**  
**no oam-bundle [manage] [frequency]**

### 構文の説明

<b>manage</b>	（任意）OAM 管理を有効にします。このキーワードを省略すると、ループバックセルは送信されますが、バンドルは管理されません。
<i>frequency</i>	（任意）送信される OAM ループバック セル間の秒数です。間隔の範囲は、0～600 秒です。 <i>frequency</i> 引数のデフォルト値は 10 秒です。

### コマンド デフォルト

エンドツーエンド F5 OAM ループバック セル生成および OAM 管理は無効になっていますが、OAM セルが受信されるとループバックされます。

### コマンドモード

SVC-bundle コンフィギュレーション（SVC バンドル用）  
 VC-class コンフィギュレーション（VC クラス用）  
 バンドル コンフィギュレーション（ATM VC バンドル用）

### コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.0(26)S	このコマンドが Cisco 10000 シリーズ ルータに追加されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.2(4)T	このコマンドが、SVC バンドル コンフィギュレーション モードで使用できるようになりました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。

リリース	変更箇所
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

### 使用上のガイドライン

このコマンドは、VC バンドルが OAM 管理されるかどうかを定義します。このコマンドがバンドルに設定された場合、バンドルのすべての VC メンバーが OAM 管理されます。OAM 管理が有効になっている場合は、**oamretry** コマンドを使用して、OAM 管理の追加の制御を設定できます。

コマンドを含む VC クラスがスタンドアロン VC (バンドル メンバーではない VC) に付加されている場合、このコマンドは効果がありません。この場合、属性は VC によって無視されません。

VC-class コンフィギュレーション モードでこのコマンドを使用するには、まず **vc-classatm** グローバル コンフィギュレーション コマンドを入力します。

バンドル コンフィギュレーション モードでこのコマンドを使用するには、まず **bundle** サブインターフェイス コンフィギュレーション コマンドを入力してバンドルを作成するか、既存のバンドルを指定します。

VC バンドルの VC は、次の設定継承規則に従います (次に高い優先順位の順にリストされています)。

- bundle-VC モードの VC 設定
- バンドルモードのバンドル設定 (および、割り当てられた VC-class コンフィギュレーションの影響)

### 例

次の例では、「bundle 1」という名前のバンドルの OAM 管理を有効にします。

```
bundle bundle1
oam-bundle manage
```

### 関連コマンド

Command	Description
<b>broadcast</b>	ブロードキャストパケットの複製と、ATM VC クラス、PVC、SVC、または VC バンドルへの送信を設定します。
<b>bundle</b>	バンドル コンフィギュレーション モードに入って、バンドルを作成するか、または既存のバンドルを変更します。
<b>class-bundle</b>	指定された VC クラスに含まれるバンドル レベルのコマンドで VC バンドルを設定します。
<b>encapsulation</b>	インターフェイスで使用するカプセル化方式を設定します。

Command	Description
<b>inarp</b>	ATM PVC、VC クラス、または VC バンドルの Inverse ARP の時間を設定します。
<b>oamretry</b>	ATM PVC、SVC、VC クラス、または、VC バンドルの OAM 管理に関連するパラメータを設定します。
<b>protocol(ATM)</b>	ATM PVC、SVC、VC クラス、または VC バンドルのスタティック マップを設定します。次に、直接 PVC 上、VC バンドル上、または VC クラス内で Inverse ARP を設定することによって、ATM PVC の Inverse ARP または Inverse ARP ブロードキャストを有効にします (IP および IPX プロトコルだけに適用)。
<b>vc-classatm</b>	ATM 相手先固定接続 (PVC)、相手先選択接続 (SVC)、または ATM インターフェイス用の仮想回線 (VC) クラスを作成します。



# platform ip features sequential

Internet Protocol (IP) プレシデンスベースまたは DiffServ コードポイント (DSCP) ベースの出力 Quality of Service (QoS) フィルタリングを有効にして、入力ポリシー フィーチャカード (PFC) QoS によって行われる IP プレシデンスまたは DSCP ポリシングまたはマーキングの変更を使用するには、インターフェイス コンフィギュレーション モードで、**platformipfeaturessequential** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**platform ip features sequential [access-group {ip-acl-nameip-acl-number}]**  
**no platform ip features sequential [access-group {ip-acl-nameip-acl-number}]**

## 構文の説明

<b>access-group ip-acl-name</b>	(任意) 再循環パケットの一致条件を指定するために使用される ACL の名前を指定します。
<b>access-group ip-acl-number</b>	(任意) 再循環パケットの一致条件を指定するために使用される ACL の番号を指定します。有効値は 1 ~ 199 と 1300 ~ 2699 です。

## コマンド デフォルト

IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングは、受信した IP precedence または DSCP 値を使用し、ポリシングまたはマーキングの結果として入力 QoS によって加えられた IP precedence または DSCP の変更を使用しません。

## コマンド モード

インターフェイス コンフィギュレーション (config-if)

## コマンド履歴

リリース	変更箇所
12.2(50)SY	このコマンドが導入されました。
12.2(18)SXE	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

## 使用上のガイドライン



### 注意

スイッチが、再マーキングされた DSCP に対する出力 ACL サポートを設定したが PFC3A モードで動作している場合は、PFC3 はトラフィックを処理して入力 PFC QoS を適用する際、入力 PFC QoS フィルタリングおよび入力 PFC QoS を適用し、入力インターフェイスに設定されたすべての出力 QoS フィルタリングおよび出力 PFC QoS を不正に適用します。この結果、再マーキングされた DSCP に対する出力 ACL サポートが有効になっているインターフェイス上で QoS フィルタリングが設定された場合に、予期しない動作が発生します。この問題は、他の PFC3 モードでは発生しません。

強化出力 QoS フィルタリングにより、IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングで入力 QoS によって加えられた IP precedence または DSCP ポリシング/マーキングの変更を使用することができます。

強化されていない出力 QoS フィルタリングの動作は、QoS がハードウェアで適用されたときの通常の Cisco 7600 シリーズ ルータまたは Catalyst 6500 シリーズ スイッチ動作です。

PFC3 は、出力レイヤ 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）上のレイヤ 3 スイッチドおよびルーテッドトラフィックについてだけ、出力 PFC QoS を提供します。

強化出力 QoS フィルタリングは、入力レイヤ 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）上で設定します。

特定の標準、拡張名前付き、または拡張番号付き IP ACL によってフィルタされたトラフィックについてだけ強化出力 QoS フィルタリングをイネーブルにするには、IP ACL の名前または番号を入力します。

IP ACL の名前または番号を入力しなかった場合、強化出力 QoS フィルタリングはインターフェイス上のすべての IP 入力 IP トラフィックについてイネーブルになります。



- (注) 強化出力 QoS フィルタリングを設定すると、PFC3A はトラフィックを処理して、入力 PFC QoS を適用します。PFC3A は、入力 QoS フィルタリングおよび Cisco 7600 シリーズ ルータまたは Catalyst 6500 シリーズ スイッチ ハードウェア入力 QoS を適用します。PFC3A は、入力インターフェイス上で設定される出力 QoS フィルタリングおよび Cisco 7600 シリーズ ルータまたは Catalyst 6500 シリーズ スイッチ ハードウェア出力 QoS を誤って適用します。



- (注) 入力 QoS マーキングによって変更された IP プレシデンスまたは DSCP のマッチングを行うために、レイヤ 2 機能を使用するインターフェイス上で強化出力 QoS フィルタリングを設定した場合、パケットはリダイレクトまたは破棄されて、出力 QoS によって処理されません。



- (注) 強化出力 QoS フィルタリングをイネーブルにした場合、再帰 ACL、NAT、TCP インターセプトなどの NetFlow ベース機能のハードウェアアクセラレーションはディセーブルになります。

設定を確認するには、**showrunning-configinterface** コマンドを使用します。

次に、強化出力 QoS フィルタリングを有効にする例を示します。

```
Router(config-if)# platform ip features sequential
```

```
Router(config-if)#
```

次に、強化出力 QoS フィルタリングを無効にする例を示します。

```
Router(config-if)# no platform ip features sequential
```

```
Router(config-if)#
```

## 関連コマンド

コマンド	説明
<b>showrunning-configinterface</b>	現在の実行コンフィギュレーションファイルの内容を表示します。

## platform ipsec fips-mode

連邦情報処理標準（FIPS）とハードウェア エントロピーを有効にするには、グローバル コンフィギュレーション モードで **platform ipsec fips-mode** コマンドを使用します。FIPS とハードウェア エントロピーを無効にするには、このコマンドの **no** 形式を使用します。

**platform ipsec fips-mode**  
**no platform ipsec fips-mode**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

なし

### コマンド モード

グローバル設定

### コマンド履歴

リリース

変更箇所

Cisco IOS XE Release  
3.7.3S

このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。

### 例

次に、**platform ipsec fips-mode** コマンドを使用して、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで FIPS モードとハードウェア エントロピーを有効にする例を示します。

```
Router(config)# platform ipsec fips-mode

enable FIPS mode will take effect after reboot!
```

### 関連コマンド

コマンド

説明

show crypto entropy status

## platform ipsec llq

Quality of Service (QoS) グループの低遅延キューイング (LLQ) を有効にするには、グローバル コンフィギュレーション モードで **platform ipsec llq** コマンドを使用します。LLQ を無効にするには、このコマンドの **no** バージョンを使用します。

```
platform ipsec llq qos-group group-number
no platform ipsec llq qos-group group-number
```

構文の説明	<b>qos-group</b>	LLQ を有効化する QoS グループを指定します。
	<i>group-number</i>	グループを識別する番号です。有効な値は 1～99 です。

コマンド デフォルト LLQ は有効になっていません。

コマンド モード グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更箇所
	Cisco IOS XE Release 2.4	このコマンドが導入されました。

使用上のガイドライン このコマンドにより、トンネル保護が使用されているトンネル インターフェイスの IPsec に、指定した QoS グループを高優先順位として設定できます。これにより、優先順位の高いパケットがデフォルトキューにキューイングされることを防ぎ、オーバーサブスクリプション時の遅延とトラフィックの損失を低減します。

例 次の例では、QoS グループ 1 で低遅延キューイングを設定する方法を示します。

```
ASR1006-1(config)# platform ipsec llq qos-group 1
```

関連コマンド	コマンド	説明
	<b>set qos-group</b>	後からパケットの分類に使用できる QoS グループ ID を設定します。

## platform punt-police queue

キューのパント ポリシングを有効にして、キュー単位で最大パント レートとバースト レートを指定するには、グローバル コンフィギュレーション モードで、**platformpunt-policequeue** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

```
platform punt-police queue queue-id max-punt-rate max-burst-rate
no platform punt-police queue queue-id
```

### 構文の説明

<i>queue-id</i>	キューを識別する一意の番号です。有効値の範囲は 0 ~ 28 です。
<i>max-punt-rate</i>	パケット/秒 (pps) 単位のキューの最大パントレートです。有効値の範囲は 10 ~ 10000 です。
<i>max-burst-rate</i>	パケット/秒 (pps) 単位のキューの最大バーストレートです。有効値の範囲は 1000 ~ 10000 です。

### コマンド デフォルト

キューのパント ポリシングは有効になっています。各キューのデフォルトのリストについては、「使用上のガイドライン」のセクションにある表を参照してください。

### コマンド モード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更箇所
Cisco IOS XE 3.5S	このコマンドが、Cisco ASR 903 ルータに追加されました。

### 使用上のガイドライン

パント ポリシングは、ルート プロセッサ (RP) が重要でないトラフィックを処理せずに済むようにします。トラフィックは、さまざまな条件に基づいて異なる CPU キューに配置されます。その後、キュー単位で最大パント レートを設定できます。デフォルトでは、キューに対して明示的なポリシングは行われません。



(注) 特定の CPU キューのトラフィックは、設定されたパント レートとは無関係に、キューのプライオリティ、キューのサイズ、またはトラフィック パント レートに基づいて破棄されることがあります。

設定を確認するには、**show platform software infrastructure punt statistics** コマンドを使用します。

パント ポリシングは、デフォルトで有効になっています。次の表は、各キューのデフォルトのパント ポリシング設定を示しています。

表 1: デフォルトのパント ポリシング設定

リング/キュー	キュー名	パント レート (pps)	バースト レート (pps)
0	SW FORWARDING Q	500	1000
1	ROUTING PROTOCOL Q	500	1000
2	ICMP Q	500	1000
3	HOST Q	1000	2000
4	ACL LOGGIN Q	500	1000
5	STP Q	3000	6000
6	L2 PROTOCOL Q	1000	2000
7	MCAST CONTROL Q	1000	2000
8	BROADCAST Q	500	1000
9	REP Q	3000	6000
10	CFM Q	3000	6000
11	CONTROL Q	1000	2000
12	IP MPLS TTL Q	1000	2000
13	DEFAULT MCAST Q	500	1000
14	MCAST ROUTE DATA Q	500	1000
15	MCAST MISMATCH Q	500	1000
16	RPF FAIL Q	500	1000
17	ROUTING THROTTLE Q	500	1000
18	MCAST Q	500	1000
19	MPLS OAM	1000	2000
20	IP MPLS MTU	500	1000
21	PTP Q	3000	6000
22	LINUX ND Q	500	1000
23	KEEPALIVE Q	1000	2000

リング/キュー	キュー名	パント レート (pps)	バースト レート (pps)
24	ESMC Q	3000	6000
25	FPGA BFD Q	3000	6000
26	FPGA CCM Q	3000	6000
27	FPGA CFE Q	3000	6000
28	L2PT DUP Q	4000	8000

## 例

次に、キュー 20 のパント ポリシングを有効にして、最大パント レートを 9000 pps に設定し、最大バースト レートを 10000 pps に設定する例を示します。

```
Router(config)# platform punt-police queue 20 9000 10000
```

## 関連コマンド

コマンド	説明
<b>show platform hardware pp active infrastructure pi npd rx policer</b>	すべてのキューのパント ポリシング統計情報を表示します。
<b>show platform software infrastructure punt statistics</b>	キューベースのパント ポリシングが有効になっているかどうかを表示します。



# platform qos marker-statistics

システム全体（プラットフォーム）レベルで、変更されたヘッダーを持ち、ローカルルータ処理のカテゴリに分類されたパケット数を表示するには、グローバル コンフィギュレーション モードで **platformqosmarker-statistics** コマンドを使用します。QoS パケット マーキング統計情報機能の表示を無効にするには、このコマンドの **no** 形式を使用します。

**platform qos marker-statistics**  
**no platform qos marker-statistics**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

無効になっています（パケット マーキング統計情報は表示されません）。

## コマンド モード

グローバル コンフィギュレーション（config）

## コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。

## 使用上のガイドライン

システムでポリシーマップがインターフェイスに関連付けられていないことを確認します。関連付けられている場合は、システムによって次のメッセージが返されます。

```
Either a) A system RELOAD or
      b) Remove all service-policies, re-apply the change
         to the statistics, re-apply all service-policies
         is required before this command will be activated.
```

QoS パケット マーキング統計情報機能を有効にすると、拡張設定では CPU 使用率が増加する可能性があります。QoS パケット マーキング統計情報機能を有効にする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

## 例

次の例に、以下をどのように実行するかを示します。

- QoS パケット マーキング統計情報機能の有効化
- 入力インターフェイスでの入力サービス ポリシーの設定
- 設定されたクラスへのトラフィックの分類
- IP プレシデンスを 1 に設定するためのクラスでのマーキングの設定
- **showpolicy-mapinterface** コマンドの出力の表示

```
Router#
platform qos marker-statistics
```

```

class-map test_class
  match access-group 101
  policy-map test_policy
    class test_class
      set ip precedence 1
Interface POS2/0/1
  service-policy input test_policy
Router#
show policy-map interface
POS2/0/1
  Service-policy input: test_policy
    Class-map: test_class (match-all)
      6644560 packets, 757479840 bytes
      5 minute offered rate 8720000 bps, drop rate 0000 bps
    Match: precedence 5
    QoS Set
      precedence 1
      Packets marked 6644560
    Class-map: class-default (match-any)
      18 packets, 1612 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any

```

## 関連コマンド

コマンド	説明
<b>showplatformhardwareqfpactivefeatureqosconfigglobal</b>	QoS パケット マーキング統計情報機能が有効になっているかどうかを表示します。
<b>showpolicy-mapinterface</b>	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスの packets 統計情報を表示します。
<b>showpolicy-mapsession</b>	PPPoE セッションに対して有効な QoS ポリシー マップを表示します。

## platform qos match-statistics per-ace

Quality of Service (QoS) パケット一致統計情報を有効にして、QoS ポリシーで使用される個々のアクセス制御要素 (ACE) に一致するパケット数とバイト数をカウントするには、グローバル コンフィギュレーション モードで **platform qos match-statistics per-ace** コマンドを使用します。ACE 単位の QoS パケット一致統計情報を無効にするには、このコマンドの **no** 形式を使用します。

**platform qos match-statistics per-ace**  
**no platform qos match-statistics per-ace**

構文の説明	このコマンドには引数またはキーワードはありません。
コマンド デフォルト	無効になっています (QoS の ACE 統計情報は増えません)。
コマンド モード	グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更箇所
	Cisco IOS XE Release 3.10S	このコマンドが導入されました。

**使用上のガイドライン** **platform qos match-statistics per-ace** コマンドを設定して QoS の ACE 単位のパケット一致統計情報を有効にする前に、**platform qos match-statistics per-filter** コマンドを設定して QoS のフィルタ単位のパケット一致統計情報を有効にする必要があります。

システムでポリシーマップがインターフェイスに関連付けられていないことを確認します。ある場合は、システムによって次のメッセージが返されます。

```
Either a) A system RELOAD or
      b) Remove all service-policies, re-apply the change
         to the statistics, re-apply all service-policies
         is required before this command will be activated.
```

ACE 単位の QoS 統計情報機能をイネーブルにすると、拡張設定では CPU 使用率が増加する可能性があります。この機能を有効にする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

### 例

次に、QoS ポリシー マップに ACE 単位のフィルタを設定する例を示します。

```
Device(config)# platform qos match-statistics per-filter
Device(config)# platform qos match-statistics per-ace
```

関連コマンド	コマンド	説明
	<b>class-map match-any</b>	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
	<b>platformqos match-statistics per-filter</b>	システム全体（プラットフォーム）レベルで、QoS のフィルタ単位のパケット一致統計情報を有効にします。
	<b>showaccesslists</b>	QoS サービス ポリシーで使用される ACL を含む、すべての設定済み ACL の ACE 統計情報を表示します。
	<b>showplatformhardwareqfpactivefeatureqosconfigglobal</b>	QoS パケット一致統計情報機能が有効になっているかどうかを表示します。
	<b>showpolicy-mapinterface</b>	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

## platform qos match-statistics per-filter

システム全体（プラットフォーム）レベルで QoS パケットフィルタを定義して、そのフィルタに一致するパケット数とバイト数を表示するには、グローバルコンフィギュレーションモードで **platformqosmatch-statisticsper-filter** コマンドを使用します。フィルタリングを停止するには、このコマンドの **no** 形式を使用します。

**platform qos match-statistics per-filter**  
**no platform qos match-statistics per-filter**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

無効になっています（パケット一致統計情報は表示されません）。

### コマンドモード

グローバル コンフィギュレーション (config)

### コマンド履歴

リリース	変更箇所
Cisco IOS XE リリース 3.3S	このコマンドが導入されました。

### 使用上のガイドライン

システムでポリシーマップがインターフェイスに関連付けられていないことを確認します。関連付けられている場合は、システムによって次のメッセージが返されます。

```
Either a) A system RELOAD or
      b) Remove all service-policies, re-apply the change
         to the statistics, re-apply all service-policies
         is required before this command will be activated.
```

QoS パケット一致統計情報機能を有効にすると、拡張設定では CPU 使用率が増加する可能性があります。QoS パケット一致統計情報を有効にする前に、統計情報の利点とシステムの CPU 使用率の増加とを比較して検討する必要があります。

```
Ensure you have defined a filter using the class-map
command with the match-any
keyword.
```

### 例

次の例は、このコマンドの使用方法を示しています。

```
Router>
enable
Router#
configure terminal
Router(config)#
platform qos match-statistics per-filter
Router# end
```

関連コマンド	コマンド	説明
	<b>class-map match-any</b>	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
	<b>showplatformhardwareqfpactivefeatureqosconfigglobal</b>	QoS パケット一致統計情報機能が現在有効になっているかどうかを表示します。
	<b>showpolicy-mapinterface</b>	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

## platform qos-port-channel\_aggregator

ポートチャンネルでQoS適用ポリシーを有効にするには、グローバルコンフィギュレーションモードで `lcp max-bundle` とともに `platform qos-port-channel_aggregator` コマンドを使用します。

**platform qos-port-channel\_aggregator port-channel-numberenable**

構文の説明	<i>port-channel-number</i>	ポートチャンネルの情報を表示します。
	<b>enable</b>	QoSポリシー設定を有効にします。

コマンドデフォルト デフォルトはありません。

コマンドモード グローバル設定

コマンド履歴	リリース	変更箇所
	XE 3.18 SP	このコマンドのサポートがASR 900シリーズルータに追加されました。

### 例

次の例は、ポートチャンネルアクティブ/アクティブモードを有効にする方法を示しています。

```
enable
configure terminal
platform qos-port-channel_aggregator 1
end
```

関連コマンド	コマンド	説明
	<b>show policy-map interface port-channel</b>	EFPのポリシーマップコンフィギュレーションを検証します。

## platform qos-port-channel\_multiple\_active

バンドルごとにアクティブなポートチャンネルを設定するには、グローバル コンフィギュレーション モードで **platform qos-port-channel\_multiple\_active** コマンドを使用します。

**platform qos-port-channel\_multiple\_active** *port-channel*

### 構文の説明

<i>port-channel</i>	ポート チャンネルの情報を表示します。
---------------------	---------------------

### コマンド デフォルト

デフォルトはありません。

### コマンド モード

グローバル設定

### コマンド履歴

リリース	変更箇所
XE 3.18.1 SP	このコマンドのサポートが ASR 900 シリーズルータに追加されました。

### 使用上のガイドライン

アクティブ アクティブ モードで作成されるポート チャンネルを指定する必要があります。

### 例

次の例は、ポートチャンネル アクティブ/アクティブ モードを有効にする方法を示しています。

```
enable
configure terminal
platform qos-port-channel_multiple_active 10
end
```

### 関連コマンド

コマンド	説明
<b>show sdm prefer current</b>	ポートチャンネルアクティブ/アクティブモードを有効にした後で設定を検証します。
<b>show etherchannel summary</b>	ポートチャンネル概要の詳細を検証します。
<b>show policy-map interface brief</b>	ポートチャンネルインターフェイスでアタッチしたポリシーマップを検証します。



## platform vfi dot1q-transparency

802.1Q 透過性モードを有効にするには、グローバル コンフィギュレーション モードで **platformvfidot1q-transparency** コマンドを使用します。802.1Q 透過性を無効にするには、このコマンドの **no** 形式を使用します。

**platform vfi dot1q-transparency**  
**no platform vfi dot1q-transparency**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

802.1Q 透過性モードは無効になっています。

### コマンド モード

グローバル設定

### コマンド履歴

リリース	変更箇所
12.2(18)SXF2	このコマンドが Supervisor Engine 720 に導入されました。

### 使用上のガイドライン

このコマンドは、オプティカル サービス モジュール (OSM) でのみサポートされています。

802.1Q 透過性により、サービス プロバイダーは、仮想プライベート LAN サービス (VPLS) のカスタマー 802.1p ビットを変更せずに、コアベース QoS ポリシーのマルチプロトコル ラベル スイッチング Experimental (MPLS EXP) ビットを変更できます。

Cisco IOS Release 12.2(18)SXF1 よりも前のリリースでは、すべてに一致して MPLS EXP ビットを設定するサービス ポリシーを VLAN インターフェイスに適用すると、内部ゲートウェイ プロトコル (IGP) ラベルと VC ラベルの両方に影響しました。受信した仮想回線 (VC) MPLS EXP ビットに基づいて出力プロバイダー エッジ (PE) で 802.1p ビットが書き換えられたため、VPLS カスタマーの 802.1p ビットが変更されました。

EoMPLS の Dot1q 透過性機能では、VLAN に適用されたポリシーが IGP ラベル (コア QoS 用) にだけ影響し、VC ラベル EXP ビットと 802.1p ビットを同じにします。一方、出力 PE では、802.1p ビットは受信した VC EXP ビットに基づいて書き換えられますが、EXP ビットは入力 802.1p ビットに一致しているため、VPLS カスタマーの 802.1p ビットは変更されません。

グローバル コンフィギュレーションは、Cisco 7600 シリーズ ルータに設定されたすべての仮想転送インスタンス (VFI) およびスイッチ仮想インターフェイス (SVI) の EoMPLS VC に適用されます。

相互運用性を確保するには、接続されているすべての PE ルータに EoMPLS の Dot1q 透過性機能を適用する必要があります。

### 例

次に、802.1Q 透過性をイネーブルにする例を示します。

```
platform vfi dot1q-transparency
```

次に、802.1Q 透過性をディセーブルにする例を示します。

```
no platform vfi dot1q-transparency
```

## 関連コマンド

コマンド	説明
<b>showwanvfidot1q-transparency</b>	802.1Q 透過性モードを表示します。

## plim qos input

Packet over SONET (POS) SPA、チャネライズド SPA、およびクリアチャネル SPA のインターフェイスに分類テンプレートをアタッチするには、インターフェイス コンフィギュレーションモードで **plim qos input class-map class-map index** コマンドを使用します。クリアチャネル SPA のインターフェイス上の低プライオリティ パケットに超過重み値を割り当てるには、**plim qos input weight weight-value** コマンドを使用します。指定したインデックスの分類テンプレートの割り当てを削除するには、**plim qos input class-map** コマンドの **no**形式を使用します。低プライオリティ パケットの超過スケジューリングをインターフェイスから削除するには、**plim qos input weight** コマンドの **no** 形式を使用します。

```
plim qos input {class-map class-map index|weight weight-value}
no plim qos input {class-map class-map index|weight}
```

### 構文の説明

<b>class-map</b>	入力分類テンプレートのクラス マップをインターフェイスにマッピングします。
<i>class-map index</i>	分類基準がインターフェイスに適用されるインデックス分類テンプレート番号です。
<b>weight</b>	低プライオリティ パケット間で超過帯域幅を共有するためにインターフェイスに割り当てられる重みをスケジュールします。
<i>weight-value</i>	低プライオリティ パケット間で超過帯域幅を共有するためにインターフェイスに割り当てられる重み値です。インターフェイスに割り当てられる超過帯域幅は相対的で、他のインターフェイスに割り当てられた空き帯域幅と使用可能な空き帯域幅に依存します。有効な範囲は 40 ~ 10000 です。

### コマンド デフォルト

たとえば、SIP0 はテンプレート 1 ~ 62 を使用し、SIP1 はテンプレート 63 ~ 124 を使用します。

### コマンド モード

インターフェイス コンフィギュレーション (config-if)

### コマンド履歴

リリース	変更箇所
3.1.0S	分類テンプレートをインターフェイスにアタッチし、インターフェイスに重みを割り当てて、超過帯域幅を分配できるようにするために、このコマンドが導入されました。

### 使用上のガイドライン

分類テンプレート固有の詳細はテンプレートで定義され、テンプレートは **plim qos input class-map class-map index** コマンドを使用してインターフェイスにアタッチされます。このコマンドの **no** 形式を使用することで、分類テンプレートを削除できます。 **plim qos input**

**class-map***class-map index* コマンドは、POS SPA、チャネライズド SPA、およびクリアチャンネル SPA に適用できます。

**plim qos input weight***weight-value* コマンドは、低プライオリティ パケットの超過帯域幅の共有を割り当てるために使用されます。**plim qos input weight***weight-value* コマンドは、インターフェイスに重みを割り当てるために使用され、他のインターフェイスに割り当てられた相対的な重みに応じて、インターフェイス間で帯域幅が共有されます。超過帯域幅は、高プライオリティ パケットが処理された後に割り当てられます。



(注) **plim qos input weight***weight-value* コマンドは、クリアチャンネル SPA にのみ適用できます。



(注) ポートレベル（インターフェイスレベル）で「絶対優先」キューの最小帯域幅を設定するためのこのオプションは、現在の操作モードに適用できないため廃止されました。既存の設定は、エラーが発生して拒否されます。



(注) **plim qos input** コマンドは、Cisco ASR 1000 シリーズ ルータ上の Circuit Emulation over Packet (CEoP) OC-3 SPA の CEM インターフェイスからはサポートされていません。



(注) **plim qos input** は、Cisco ASR 1000 シリーズ ルータ上のチャネライズド T1/E1 (CTE1) CEoP SPA の CEM インターフェイスからはサポートされていません。

コマンドライン インターフェイスには次のコマンドがありますが、Cisco ASR 1000 シリーズ ルータ上の CEoP OC3 SPA および CTE1 CEoP SPA には効果がありません。これらのコマンドのいずれかを設定した場合、そのコマンドが CEoP OC3 SPA でサポートされていないことを示すメッセージが表示されます。これらのコマンドのいずれかを設定すると、Cisco ASR 1000 シリーズ ルータでも同じ内容のメッセージが表示されます。

```
hw-module subslot {slot/subslot} qos input {{policer bandwidth bandwidthstrict-policy} | weight weight}}
```

次に、**plim qos input class-map***class-map index* コマンドを使用して分類テンプレートをインターフェイスにアタッチする例を示します。

```
Router# config
Router(config)# interface POS 0/2/0
Router(config-if)# plim qos input class-map
2
```

次に、**plim qos input weight50** コマンドを使用してインターフェイスに 50 の重みを割り当てて、低プライオリティパケット間で超過帯域幅を共有できるようにする例を示します。

```
Router# config
Router(config)# interface POS 0/2/0
Router(config-if)# plim qos input weight
50
```

#### 関連コマンド

Command	Description
<b>plimqosclass-map</b>	分類テンプレートをインターフェイスにアタッチします。

## plim qos input map

ギガビットイーサネット共有ポートアダプタ（SPA）でのプライオリティキューを設定するには、インターフェイスコンフィギュレーションモードまたはサブインターフェイスコンフィギュレーションモードで **plim qos input map** コマンドを使用します。プライオリティキューを削除するには、このコマンドの **no** 形式を使用します。

```
plim qos input map { cos {enable | cos-valuequeue low-latency} | ip {precedence-based | precedence precedence-valuequeue low-latency} | ipv6 tc tc-value queue low-latency | mpls exp exp-valuequeue low-latency
```

```
no plim qos input map { cos {enable | cos-valuequeue low-latency} | ip {precedence-based | precedence precedence-valuequeue low-latency} | ipv6 tc tc-value queue low-latency | mpls exp exp-valuequeue low-latency
```

### 構文の説明

<b>cos enable</b>	IEEE 802.1Q ネットワーキング標準 TCI プライオリティビットに応じた入力 VLAN トラフィックの分類を有効にします。  (注) このコマンドは、VLAN インターフェイスだけに適用できます。
<b>cos</b> <i>cos-value</i> <b>queue low-latency</b>	サブインターフェイス上の着信 VLAN トラフィックを 802.1Q プライオリティビットに応じて分類し、トラフィックを適切なキューに配置します。デフォルトでは、802.1Q プライオリティビットが 6 または 7 に設定されたトラフィックは高プライオリティキューに配置され、他のすべてのトラフィックは低プライオリティキューに配置されます。  <i>cos-value</i> は、0～7 の IEEE 802.1Q または ISL サービスクラス (CoS) 値を指定します。  (注) QinQ サブインターフェイスで CoS 値を設定すると、同じ外部 VLAN ID を持つすべての QinQ サブインターフェイスに、その CoS 値が適用されます。  <b>low-latency</b> は、高プライオリティキューを指定します。
<b>ip dscp-based</b>	DSCP ビットの値に応じた着信 IP トラフィックの分類を有効にします。  (注) このコマンドは物理インターフェイスにのみ適用されます。

<b>ip dscp dscp-value queue low-latency</b>	<p>DiffServ コード ポイント (DSCP) ビットの値に応じて着信 IP トラフィックを分類し、トラフィックを適切なキューに配置します。デフォルトでは、Expedited Forwarding (EF) と等しい DSCP ビットを持つ IP トラフィックは低遅延キューを使用し、その他の DSCP 値を持つトラフィックは低プライオリティ キューを使用します。</p> <p><b>dscp-value</b> は、DSCP ビットの値です。ハイフンで区切られた値の範囲または値のリストを指定できます。有効な値のリストについては、「使用上のガイドライン」セクションを参照してください。</p> <p><b>low-latency</b> は、高プライオリティ キューを指定します。</p>
<b>ip precedence-based</b>	<p>IP プレシデンス値に応じた着信 IP トラフィックの分類を有効にします。</p> <p>(注) このコマンドは物理インターフェイスにのみ適用されます。</p>
<b>ip precedence precedence-value queue low-latency</b>	<p>IP プレシデンス ビットの値に応じて着信 IP トラフィックを分類し、トラフィックを適切なキューに配置します。IP プレシデンス ビットが 6 または 7 に設定されている IP トラフィックは低遅延キューを使用し、その他のすべてのトラフィックは低プライオリティ キューを使用します。</p> <p><b>precedence-value</b> は、IP プレシデンス ビットの値 (0 ~ 7) です。ハイフンで区切られた値の範囲または値のリストを指定できます。「使用上のガイドライン」セクションを参照してください。</p> <p><b>low-latency</b> は、高プライオリティ キューを指定します。</p>
<b>ipv6 tc tc-value queue low-latency</b>	<p>トラフィック クラス ビットの値に応じて入力 IPv6 トラフィックを分類し、トラフィックを適切なキューに配置します。デフォルトでは、<b>ef</b> と等しいトラフィック クラス値を持つ IPv6 トラフィックは高プライオリティ キューを使用し、その他のすべてのトラフィックは低プライオリティ キューを使用します。トラフィック クラス オクテットの最上位 6 ビットのみが分類に使用されます。</p> <p>(注) このコマンドは物理インターフェイスに適用されます。</p> <p><b>tc-value</b> は、トラフィック クラス ビットの値です。ハイフンで区切られた値の範囲または値のリストを指定できます。有効な値のリストについては、「使用上のガイドライン」セクションを参照してください。</p> <p><b>low-latency</b> は、高プライオリティ キューを指定します。</p>

<b>mpls exp</b> <i>exp-value queue</i> <b>low-latency</b>	<p>EXP ビットの値に応じて着信 MPLS トラフィックを分類し、トラフィックを適切なキューに配置します。デフォルトでは、EXP ビットが 6 または 7 に設定されているトラフィックは高プライオリティキューを使用し、その他のすべてのトラフィックは低プライオリティキューを使用します。</p> <p>(注) このコマンドは物理インターフェイスに適用されます。</p> <p><i>exp-value</i> は、EXP ビットの値 (0 ~ 7) です。ハイフンで区切られた値の範囲または値のリストを指定できます。</p> <p><b>low-latency</b> は、高プライオリティキューを指定します。</p>
-----------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

コマンド デフォルト 無効

コマンド モード

インターフェイス コンフィギュレーション (config-if)  
サブインターフェイス コンフィギュレーション (config-subif)

コマンド履歴

リリース	変更箇所
12.2(33)SB	このコマンドが、PRE3 用と PRE4 用の Cisco 10000 シリーズルータに導入されました。
12.2(33)SCB	このコマンドが Cisco IOS リリース 12.2(33)SCB に統合されました。
3.1.0S	このコマンドが、Cisco ASR 1000 シリーズルータの ATM インターフェイスでサポートされました。

使用上のガイドライン

**plim qos input map** コマンドは、高プライオリティトラフィックと低プライオリティトラフィックを分離し、トラフィックを適切なインターフェイスキューに配置します。このコマンドは、SPA インターフェイスプロセッサ (SIP) でプライオリティトラフィックと非プライオリティトラフィックを分離し、オーバーサブスクリプションシナリオでの高プライオリティトラフィックのドロップを防止します。各 SPA は、1 つのプライオリティキューをサポートします。

ルータは、ギガビットイーサネット SPA での入力トラフィックの優先順位付けのために、次の分類タイプをサポートしています。

- VLAN 802.1Q プライオリティ ビット
- IP DSCP ビット
- IP プレシデンス ビット
- IPv6 トラフィック クラス ビット

**plim qos input map ip dscp dscp-value queue low-latency** コマンドで、*dscp-value* に有効な値は次のいずれかです。

- 0 to 63 : DiffServ コード ポイント値



- af11 : 001010
- af12 : 001100
- af13 : 001110
- af21 : 010010
- af22 : 010100
- af23 : 010110
- af31 : 011010
- af32 : 011100
- af33 : 011110
- af41 : 100010
- af42 : 100100
- af43 : 100110
- cs1 : 優先順位 1 (001000)
- cs2 : 優先順位 2 (010000)
- cs3 : 優先順位 3 (011000)
- cs4 : 優先順位 4 (100000)
- cs5 : 優先順位 5 (101000)
- cs6 : 優先順位 6 (110000)
- cs7 : 優先順位 7 (111000)
- default : 000000
- ef : 101110

**plim qos input map ipv6 tc *tc-value* queue low-latency** コマンドで、*tc-value* に有効な値は次のいずれかです。

- 0 to 63 : DiffServ コード ポイント値
- af11 : 001010
- af12 : 001100
- af13 : 001110
- af21 : 010010
- af22 : 010100

- af23 : 010110
- af31 : 011010
- af32 : 011100
- af33 : 011110
- af41 : 100010
- af42 : 100100
- af43 : 100110
- cs1 : 優先順位 1 (001000)
- cs2 : 優先順位 2 (010000)
- cs3 : 優先順位 3 (011000)
- cs4 : 優先順位 4 (100000)
- cs5 : 優先順位 5 (101000)
- cs6 : 優先順位 6 (110000)
- cs7 : 優先順位 7 (111000)
- default : 000000
- ef : 101110

## 例

次に、**plim qos input map ip dscp-based** コマンドを使用して、Cisco 10000 シリーズルータのスロット 1 の SIP のサブスロット 0 にある SPA で DSCP ベースの分類を有効にする例を示します。

```
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# plim qos input map ip dscp-based
```

次に、**plim qos input map** コマンドを使用して DSCP ビットの値に応じて着信 IP トラフィックを分類し、Cisco ASR 1000 シリーズルータ上の ATM インターフェイスの適切なキューにトラフィックを配置する例を示します。

```
Router# configure terminal
Router(config)# interface ATM0/1/0
Router(config-if)# plim qos input map ip dscp af11 - af12 queue strict-priority
Router(config-if)# plim qos input map ipv6 tc af11 - af12 queue strict-priority
Router(config-if)# plim qos input map mpls exp 7 queue 0
```

## 関連コマンド

コマンド	説明
<b>card</b>	SIP-600 および SPA を事前にプロビジョニングします。

コマンド	説明
<b>mtu</b>	インターフェイスの最大パケットサイズを設定します。デフォルト値は1500バイトです。設定できる最大のMTUは9129バイトです。
<b>negotiation auto</b>	Cisco 10000 SIP-600 上のギガビットイーサネット SPA インターフェイスで、自動ネゴシエーションを有効にします。

## plim qos input map cos (VLAN の CoS 値を分類)

QinQ サブインターフェイスの内部または外部 VLAN タグのサービス クラス (CoS) 値または CoS 範囲に基づいて、イーサネット共有ポートアダプタ (SPA) で入力トラフィックを高プライオリティ (低遅延) または低プライオリティ (キュー0) に分類するには、サブインターフェイス コンフィギュレーション モードで **plim qos input map cos** コマンドを使用します。CoS ベースの分類を無効にするには、このコマンドの **no** 形式を使用します。

内部 VLAN の CoS 値を高プライオリティまたは低プライオリティに分類するための構文  
**plim qos input map cos {enable|inner-based|inner {cos-value|cos-range} queue {strict-priority|0}}**  
**no plim qos input map cos enable**

外部 VLAN の CoS 値を高プライオリティまたは低プライオリティに分類するための構文  
**plim qos input map cos {enable|outer-based|outer {cos-value|cos-range} queue {strict-priority|0}}**  
**no plim qos input map cos enable**

構文の説明	
<b>enable</b>	IEEE 802.1Q CoS ベースの分類を有効にします。
<b>inner-based</b>	内部 VLAN ベースの分類を有効にします。内部 VLAN の CoS 値を設定する前に、まず内部 VLAN ベースの分類を有効にする必要があります。
<b>outer-based</b>	外部 VLAN ベースの分類を有効にします。外部 VLAN の CoS 値を設定する前に、まず外部 VLAN ベースの分類を有効にする必要があります。
<b>inner</b>	内部 VLAN の絶対優先を必要とする CoS の値または範囲を設定できます。
<b>outer</b>	外部 VLAN の絶対優先を必要とする CoS の値または範囲を設定できます。
<b>cos-value</b>	CoS 値を高プライオリティまたは低プライオリティにマッピングしてパケットを分類する内部または外部 VLAN の CoS 値です。
<b>cos-range</b>	CoS 範囲を高プライオリティまたは低プライオリティにマッピングしてパケットを分類する内部または外部 VLAN の CoS 範囲です。
<b>queue</b>	内部または外部 VLAN の CoS 値または CoS 範囲の、高プライオリティまたは低プライオリティへの分類を有効にします。
<b>strict-priority</b>	指定された CoS の値または範囲を高プライオリティ (低遅延) に分類します。
<b>0</b>	指定された CoS の値または範囲を低プライオリティ (キュー0) に分類します。

コマンド デフォルト 外部 VLAN の 6 または 7 の CoS 値は、高プライオリティに分類されます。

コマンド モード

サブインターフェイス コンフィギュレーション モード (config-subif)

## コマンド履歴

リリース	変更箇所
Cisco IOS XE Release 3.1S	このコマンドがイーサネット SPA に導入され、Cisco ASR 1000 シリーズ ルータ上の ATM インターフェイスでサポートされました。

## 内部 VLAN の CoS ベースの分類の設定

内部 VLAN の CoS 値に基づいて入力トラフィックを分類する前に、まず **plimqosinputmapcosinner-based** コマンドを使用して内部 VLAN の CoS ベースの分類を有効にする必要があります。

## 外部 VLAN の CoS ベースの分類の設定

外部 VLAN の CoS 値に基づいて入力トラフィックを分類する前に、まず **plimqosinputmapcosouter-based** コマンドを使用して外部 VLAN の CoS ベースの分類を有効にする必要があります。

サブインターフェイス レベルでの CoS ベースの分類を無効にし、メインインターフェイス レベルでのレイヤ 3 情報ベースの分類を有効にするには、サブインターフェイス コンフィギュレーション モードで **no plimqosinputmapcosenable** コマンドを使用します。

**no plimqosinputmapcosenable** コマンドを設定すると、メインインターフェイス レベルの分類設定が適用可能になることを示すメッセージが表示されます。



- (注) CSCtd91658 では、外部 VLAN に基づく分類がすでにあるサブインターフェイスで内部 VLAN に CoS ベースの分類を設定しようとした場合（またはその逆を設定しようとした場合）や、存在しない CoS ベースの分類を削除しようとした場合は、警告メッセージが表示されます。



- (注) **plimqosinputmapcos** コマンドは、イーサネット SPA でのみサポートされています。  
**plimqosinputmapcos** コマンドは、QinQ サブインターフェイスの VLAN サブインターフェイス コンフィギュレーション モードから実行されます。

## 例

次に、内部 VLAN の CoS 値 3 を高プライオリティに分類する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# plim qos input map cos inner-based
Router(config-subif)# plim qos input map cos inner 3 queue strict-priority
```

次に、外部 VLAN の CoS 値 3 を高プライオリティに分類する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# plim qos input map cos outer-based
Router(config-subif)# plim qos input map cos outer 3 queue strict-priority
```

次に、QinQ サブインターフェイス コンフィギュレーションモードで IEEE 802.1Q CoS ベースの分類を有効にする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.2
Router(config-subif)# encapsulation dot1q 2 second-dot1q 100
Router(config-subif)# plim qos input map cos enable
```

次に、QinQ サブインターフェイス コンフィギュレーションモードで IEEE 802.1Q CoS ベースの分類を無効にする例を示します。メインインターフェイスレベルの分類設定が適用可能になることを示すメッセージが表示されます。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.2
Router(config-subif)# encapsulation dot1q 2 second-dot1q 100
Router(config-subif)# no plim qos input map cos enable
%Classification will now be based on Main interface configuration.
```

次に、Dot1Q サブインターフェイス コンフィギュレーションモードで IEEE 802.1Q CoS ベースの分類を有効にする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# encapsulation dot1q 1 native
Router(config-subif)# plim qos input map cos enable
```

次に、Dot1Q サブインターフェイス コンフィギュレーションモードで IEEE 802.1Q CoS ベースの分類を無効にする例を示します。メインインターフェイスレベルの分類設定が適用可能になることを示すメッセージが表示されます。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# encapsulation dot1q 1 native
Router(config-subif)# no plim qos input map cos enable
%Classification will now be based on Main interface configuration.
```

次に、**plim qos input map** コマンドを使用して DSCP ビットの値に応じて着信 IP トラフィックを分類し、Cisco ASR 1000 シリーズルータ上の ATM インターフェイスの適切なキューにトラフィックを配置する例を示します。

```
Router# configure terminal
Router(config)# interface ATM0/1/0
Router(config-if)# plim qos input map ip dscp af11 - af12 queue strict-priority
Router(config-if)# plim qos input map ipv6 tc af11 - af12 queue strict-priority
Router(config-if)# plim qos input map mpls exp 7 queue 0
```

#### 関連コマンド

コマンド	説明
<b>encapsulation</b>	インターフェイスで使用するカプセル化方式を設定します。

# police

トラフィック ポリシングを設定するには、ポリシー マップ クラス コンフィギュレーション モードまたはポリシー マップ クラス ポリス コンフィギュレーション モードで **police** コマンドを使用します。トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

**police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

**no police** *bps* [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

## 構文の説明

<i>bps</i>	平均レート（ビット/秒）です。有効な値は 8000 ～ 128000000000（128 Gb/s）です。
<i>burst-normal</i>	（任意）バイト単位の通常バーストサイズです。有効な値は 1000 ～ 2000000000（2 Gb）です。デフォルトの通常バースト サイズは 1500 です。
<i>burst-max</i>	（任意）バイト単位の最大バーストサイズです。有効な値は 1000 ～ 2000000000（2 Gb）です。デフォルトはプラットフォームによって異なります。
<b>conform-action</b>	レート制限に適合したパケットに対して実行するアクションを指定します。
<b>exceed-action</b>	レート制限を超過したパケットに対して実行するアクションを指定します。
<b>violate-action</b>	通常および超過バーストサイズに違反するパケットに対して実行するアクションを指定します。

<i>action</i>	
---------------	--



パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。

- **drop** : パケットをドロップします。
- **set-clp-transmit value** : ATM セルの 0 から 1 の ATM セル損失率優先度 (CLP) を設定し、ATM CLP ビットを 1 に設定してパケットを送信します。
- **set-cos-inner-transmit value** : 拡張 FlexWAN モジュール、および、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA でブリッジ処理機能の使用時に、ブリッジ処理されたフレームに対するポリシングアクションとして、サービス フィールドの内部クラスを設定します。
- **set-cos-transmit value** : サービス クラス (CoS) パケット値を設定し、送信します。
- **set-discard-class-transmit** : パケットの廃棄クラス属性を設定し、設定した新しい廃棄クラスでパケットを送信します。
- **set-dscp-transmit value** : IP DiffServ コード ポイント (DSCP) 値を設定して、新しい IP DSCP 値でパケットを送信します。
- **set-dscp-tunnel-transmit value** : トンネルマーキングのため、レイヤ 2 Tunnel Protocol Version 3 (L2TPv3) または Generic Routing Encapsulation (GRE) のトンネルヘッダーで DSCP の値 (0 ~ 63) を設定し、新しい値でパケットを送信します。
- **set-frde-transmit value** : フレーム リレー フレーム上のフレーム リレー廃棄適格 (DE) ビットを 0 から 1 に設定し、1 に設定した DE ビットが含まれるパケットを送信します。
- **set-mpls-experimental-imposition-transmit value** : 強制ラベルのヘッダーでマルチプロトコルラベルスイッチング (MPLS) の EXP ビット (0 ~ 7) を設定し、新しい MPLS EXP ビット値でパケットを送信します。
- **set-mpls-experimental-topmost value** : EXP 値を再書き込みします。
- **set-mpls-experimental-topmost-transmit value** : 入力インターフェイスや出力インターフェイスでの最上位 MPLS ラベルヘッダーに MPLS EXP フィールド値を設定します。
- **set-prec-transmit value** : IP プレシデンスを設定して、新しい IP プレシデンス値でパケットを送信します。
- **set-prec-tunnel-transmit value** : トンネルマーキングのため、L2TPv3 または GRE のトンネルヘッダーで優先順位の値 (0 ~ 7) を設定し、新しい値でパケットを送信します。
- **set-qos-transmit value** : QoS グループ値を設定し、設定した新しい QoS グ

ループ値でパケットを送信します。

- **transmit** : パケットを送信します。パケットは変更されません。

#### コマンド デフォルト

トラフィック ポリシングは設定されません。

#### コマンド モード

マークされたパケットに適用される単一のアクションを指定する場合は、ポリシー マップ クラス コンフィギュレーション (config-pmap-c)

マークされたパケットに適用される複数のアクションを指定する場合は、ポリシー マップ クラス ポリシング コンフィギュレーション (config-pmap-c-police)

#### コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが Cisco IOS リリース 12.1(5)T に統合されました。 <b>violate-action</b> キーワードが追加されました。
12.2(2)T	このコマンドが変更されました。 <ul style="list-style-type: none"> <li>• <i>action</i> 引数の <b>set-clp-transmit</b> キーワードが追加されました。</li> <li>• <i>action</i> 引数の <b>set-frde-transmit</b> キーワードが追加されました。</li> </ul> <p>(注) ただし、このリリースでは <b>set-frde-transmit</b> キーワードは AToM トラフィックではサポートされていません。また、<b>set-frde-transmit</b> キーワードは、カプセル化されていない物理インターフェイス上にフレーム リレーが実装されている場合にのみサポートされます。</p> <ul style="list-style-type: none"> <li>• <i>action</i> 引数の <b>set-mpls-experimental-transmit</b> キーワードが追加されました。</li> </ul>
12.2(8)T	このコマンドが、Policer Enhancement (Multiple Actions 機能) のために変更されました。このコマンドが、特定のレートについて適合、超過、または違反しているとマークされたパケットに対して、複数のアクションを適用できるようになりました。
12.2(13)T	このコマンドが変更されました。 <i>action</i> 引数で、 <b>set-mpls-experimental-transmit</b> キーワードの名前が <b>set-mpls-experimental-imposition-transmit</b> に変更されました。

リリース	変更箇所
12.2(28)SB	このコマンドが変更されました。 <i>action</i> 引数の <b>set-dscp-tunnel-transmit</b> および <b>set-prec-tunnel-transmit</b> キーワードが追加されました。これらのキーワードは、Layer 2 Tunnel Protocol Version 3 (L2TPv3) トンネル型パケット用です。
12.2(33)SRA	このコマンドが変更されました。拡張 FlexWAN モジュールでマルチポイントブリッジング (MPB) 機能を使用する場合のために、また、Cisco 7600 シリーズルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB を使用する場合のために、 <i>action</i> 引数に <b>set-cos-inner-transmit</b> キーワードが追加されました。
12.2(31)SB2	このコマンドが変更されました。 <b>set-frde-transmit</b> <i>action</i> 引数のサポートが Cisco 10000 シリーズルータに追加されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
12.2(33)SRC	このコマンドが変更されました。Cisco 7600 シリーズルータのサポートが追加されました。
12.4(15)T2	Generic Routing Encapsulation (GRE) トンネル型パケットのマーキングのサポートが含まれるように、このコマンドが変更されました。  (注) このリリースでは、GRE トンネル型パケットのマーキングは、Cisco MGX ルートプロセッサ モジュール (RPM-XF) に搭載されているプラットフォームでのみ、サポートされます。
12.2(33)SB	GRE トンネル型パケットのマーキングのサポートと、Cisco 7300 シリーズルータのサポートが含まれるように、このコマンドが変更されました。
15.1(1)T	このコマンドが、Cisco ISR 1800、2800、および 3800 シリーズルータの SVI インターフェイスでのポリシングをサポートするように変更されました。
12.2(50)SY	このコマンドが変更されました。 <b>set-mpls-experimental-topmost</b> <i>value</i> 引数のサポートが追加されました。
15.0(1)SY	このコマンドが変更されました。 <i>bps</i> 、 <i>burst-normal</i> 、および <i>burst-max</i> 引数の最大値が増えました。
Cisco IOS XE リリース 3.5S	このコマンドが変更されました。Cisco ASR 903 ルータのサポートが追加されました。

**使用上のガイドライン** **police** コマンドは、サービス レベル契約への準拠に基づいて、異なる Quality of Service (QoS) 値を持つパケットをマークするために使用します。

Cisco IOS リリース 12.2(50)SY では、出力方向で **set-mpls-experimental-topmost value** を適用すると、**set-mpls-experimental-imposition value** がブロックされます。



(注) Cisco IOS リリース 15.0(1)SY 以降では、バースト サイズを指定せずにポリシー マップを設定すると、デフォルト バースト サイズが 2 Gb/s に達することがあります。

高いレートまたは大きいバースト サイズを設定してから、その設定をサポートしていない Cisco IOS ソフトウェア リリースに変更すると、起動時に設定が拒否され、ポリシー マップから **police** コマンドが削除されます。

#### 複数のアクションの指定

**police** コマンドでは、複数のポリシング アクションを指定できます。**police** コマンドの設定時に複数のポリシング アクションを指定する場合は、次の点に注意してください。

- 同時に最大 4 つのアクションを指定できます。
- **conform-action transmit** と **conform-action drop** などの、矛盾するアクションを指定することはできません。

#### **police** コマンドとトラフィック ポリシング機能の使用

**police** コマンドは、トラフィック ポリシング機能とともに使用することができます。トラフィック ポリシング機能は、トークン バケット アルゴリズムで動作します。Cisco IOS リリース 12.1(5)T には、シングル トークン バケット アルゴリズムと 2 トークン バケット アルゴリズムの 2 種類のトークン バケット アルゴリズムがあります。シングル トークン バケット システムは、**violate-action** オプションを指定しなかった場合に使用され、2 トークン バケット システムは、**violate-action** オプションを指定した場合に使用されます。

Cisco IOS リリース 12.0(5)XE で導入された **police** コマンドのトークン バケット アルゴリズムは、Cisco IOS リリース 12.1(5)T で導入された **police** コマンドのトークン バケット アルゴリズムとは異なります。リリース 12.0(5)XE で導入されたトークン バケット アルゴリズムの詳細については、リリース 12.0(5)XE の『*Traffic Policing*』ドキュメントを参照してください。このドキュメントは、www.cisco.com の (Modular QoS CLI 関連の機能モジュールの下にある) 「New Features for 12.0(5)XE」ドキュメント インデックスで利用できます。

次に、Cisco IOS リリース 12.1(5)T で導入されたトークン バケット アルゴリズムの仕組みを説明します。

#### シングル トークン バケットを使用するトークン バケット アルゴリズム

シングル トークン バケット アルゴリズムは、**police** コマンド CLI で **violate-action** オプションが指定されていない場合に使用されます。

適合バケットは、最初はフル サイズに設定されています (フル サイズは、通常バースト サイズとして指定されているバイト数です)。

指定サイズの packets (たとえば、「B」バイト) が特定の時間 (時間「T」) に到着する場合、次のようなアクションが実行されます。

- 適合 packets でトークンが更新されます。前に packets が到着したのが T1 で、現在の時間が T の場合、packets はトークン到着レートに基づいて (T - T1) 相当のビット数で更新されます。トークンの到達レートは次のように計算されます。

(packets 間の時間 (つまり T - T1) x ポリシング レート) / 8 バイト

- 適合 packets B のバイト数が packets サイズ以上の場合、packets は適合し、packets で適合アクションが実行されます。packets が適合した場合、B バイトが適合 packets から削除されて、その packets に対する適合アクションが完了します。
- 適合 packets B のバイト数 (制限されている packets サイズを引いたもの) が 0 未満の場合、超過アクションが実行されます。

## 2 トークン packets を使用するトークン packets アルゴリズム

2 トークン packets アルゴリズムは、**police** コマンドで **violate-action** オプションが指定されている場合に使用されます。

適合 packets は、最初はフルサイズになっています (フルサイズは、通常バーストサイズとして指定されているバイト数です)。

超過 packets は、最初はフルサイズになっています (フル超過サイズは、最大バーストサイズとして指定されているバイト数です)。

適合および超過トークン packets のいずれのトークンも、トークン到着レートまたは認定情報レート (CIR) に基づいて更新されます。

指定サイズの packets (たとえば、「B」バイト) が特定の時間 (時間「T」) に到着する場合、次のようなアクションが実行されます。

- 適合 packets でトークンが更新されます。前の packets が T1 に到達し、現在の packets が T に到達した場合、packets はトークン到達レートに基づいて T - T1 に相当するビット数で更新されます。リフィルトークンは、準拠 packets に置かれます。トークンが準拠 packets でオーバーフローになると、超過 packets にオーバーフロー トークンが置かれます。

トークンの到達レートは次のように計算されます。

(packets 間の時間 (つまり T-T1) x ポリシング レート) / 8 バイト

- 適合 packets B のバイト数が packets サイズ以上の場合、packets は適合し、packets で適合アクションが実行されます。packets が準拠している場合、B バイトが準拠 packets から削除され、準拠処理が実行されます。このシナリオでは、超過 packets には影響ありません。
- 適合 packets B のバイト数が packets サイズ未満の場合、超過トークン packets で packets によるバイトがチェックされます。適合 packets B のバイト数が 0 以上の場合、超過アクションが実行され、超過トークン packets から B バイトが削除されます。適合 packets から削除されるバイトはありません。

- 超過バケット B のバイト数がパケット サイズ未満の場合、パケットはレートに違反しているため、違反アクションが実行されます。パケットに対する処理が完了します。

### Cisco 7600 シリーズ ルータ上の SIP および SPA の **set-cos-inner-transmit** アクションの使用

拡張 FlexWAN モジュールで MPB 機能を使用する場合や、Cisco 7600 シリーズルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB 機能を使用する場合に、内部 CoS 値をポリシングアクションとしてマーキングすることをサポートするために、Cisco IOS リリース 12.2(33)SRA で **set-cos-inner-transmit** キーワードアクションが導入されました。

このコマンドは、Cisco 7600 SIP-600 ではサポートされていません。

Cisco 7600 シリーズルータで、SIP によってサポートされる QoS と **police** コマンドの形式については、『Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide』を参照してください。

### Cisco ASR 903 ルータでの **police** コマンドの使用

Cisco ASR 903 ルータで **police** コマンドを使用する場合は、次の制限が適用されます。

- サブインターフェイスでのクラスベース ポリシングはサポートされていません。
- ポリシングは、入力ポリシー マップでのみサポートされています。
- 階層型ポリシング（親レベルと子レベルの両方でのポリシング）はサポートされていません。
- Cisco ASR 903 ルータは、次のアクション キーワードのみをサポートしています。
  - **drop**
  - **set-cos-transmit**
  - **set-discard-class-transmit**
  - **set-dscp-transmit**
  - **set-mpls-exp-imposition-transmit**
  - **set-mpls-exp-topmost-transmit**
  - **set-precip-transmit**
  - **set-qos-transmit**
  - **transmit**

## 例

### シングル トークン バケットを使用するトークンバケット アルゴリズム：例

次の例では、（**class-map** コマンドを使用して）トラフィック クラスを定義し、（**policy-map** コマンドを使用して）トラフィック クラスからの一致基準をサービス ポリシーに設定されているトラフィック ポリシング設定に関連付ける方法を示します。ここで、**service-policy** コマンドはこのサービス ポリシーをインターフェイスに対応付けるために使用されます。

この特定の例では、トラフィック ポリシングは平均レート 8000 ビット/秒で設定され、ファストイーサネット インターフェイス 0/0 から発信される全パケットに対して通常バースト サイズが 1000 バイトとなります。

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

この例では、初期トークンバケットはフルの1000バイトで開始します。450バイトの packets を受信すると、準拠トークンバケットに使用可能なバイトが十分あるため、 packets は準拠しています。 packets により準拠処理（送信）が実行され、450 バイトが準拠トークンバケットから削除されます（残り550バイト）。

次の packets が0.25秒後に到着すると、250バイトがトークンバケットに追加され（ $(0.25 \times 8000) / 8$ ）、トークンバケットには800バイトが残ります。次の packets が900バイトの場合、 packets が超過して超過アクション（ドロップ）が実行されます。トークンバケットから取り出されるバイトはありません。

## 2 トークンバケットを使用するトークンバケットアルゴリズム：例

この例では、トラフィック ポリシングは平均レート8000ビット/秒で設定され、ファストイーサネットインターフェイス0/0から発信される全 packets に対して通常バーストサイズが1000バイト、超過バーストサイズが1000バイトとなります。

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-qos-transmit 1 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

この例では、初期トークンバケットはフルの1000バイトで開始します。450バイトの packets を受信すると、準拠トークンバケットに使用可能なバイトが十分あるため、 packets は準拠しています。 packets により準拠処理（送信）が実行され、450 バイトが準拠トークンバケットから削除されます（残り550バイト）。

次の packets が0.25秒後に到着すると、250バイトが準拠トークンバケットに追加され（ $(0.25 \times 8000) / 8$ ）、準拠トークンバケットには800バイトが残ります。次の packets が900バイトの場合、準拠トークンバケットでは800バイトしか使用できないため、 packets は準拠していません。

（超過バーストサイズで指定された）フルの1000バイトで始まる超過トークンバケットに、使用可能なバイトがあるかどうかチェックされます。超過トークンバケットには使用可能なバイトが十分あるため、超過アクション（QoS送信値を1に設定）が

実行され、超過バケットから 900 バイトが取られ、超過トークンバケットの残りは 100 バイトになります。

次のパケットが 0.40 秒後に到達し、トークンバケットに 400 バイトが追加されます  $((.40 \times 8000)/8)$ 。これで、適合トークンバケットは 1000 バイト（適合バケットで使用可能な最大トークン数）になり、200 バイトが適合トークンバケットをオーバーフローします（適合トークンバケットの容量を満たすのに 200 バイトだけが必要であったため）。これらのオーバーフローバイトは、超過トークンバケットに置かれ、超過トークンバケットに 300 バイト与えられます。

着信パケットが 1000 バイトの場合、準拠トークンバケットで使用可能なバイト数が十分あるため、パケットは準拠します。パケットにより準拠処理（送信）が実行され、1000 バイトが準拠トークンバケットから削除されます（残り 0 バイト）。

次のパケットが 0.20 秒後に到達し、トークンバケットに 200 バイトが追加されます  $((.20 \times 8000)/8)$ 。これで、準拠バケットの中身は 200 バイトになります。着信パケットが 400 バイトの場合、準拠トークンバケットでは 200 バイトしか使用できないため、パケットは準拠していません。同様に、超過バケットで使用可能なバイト数は 300 バイトだけなので、パケットは超過しません。したがって、パケットは違反となり、違反処理（ドロップ）が実行されます。

#### MPLS EXP 値への適合：例

次の例は、パケットがレート制限に適合する場合に、MPLS EXP フィールドが 5 に設定されることを示しています。パケットがレート制限を超える場合は、MPLS EXP フィールドが 3 に設定されます。

```
Router(config)# policy-map input-IP-dscp
Router(config-pmap)# class dscp24
Router(config-pmap-c)# police 8000 1500 1000 conform-action
set-mpls-experimental-imposition-transmit 5 exceed-action
set-mpls-experimental-imposition-transmit 3
Router(config-pmap-c)# violate-action drop
```

#### Cisco 7600 シリーズ ルータ上の SIP および SPA のアクションとしての内部 CoS 値の設定：例

次に、仮想 LAN (VLAN) 100 のすべてのトラフィックをクラス「vlan-inner-100」にフィルタリングし、vlan-inner-100 クラスのトラフィックシェーピングポリシーを確立する QoS クラスの設定例を示します。このサービスポリシーは、トラフィックの平均レートを 500 kb/s に制限して、1000 バイトの通常バーストと 1500 バイトの最大バーストを使用し、内部 CoS 値を 3 に設定します。内部 CoS 値の設定はブリッジング機能を使用する場合に限ってサポートされるので、**bridge-domain** コマンドを使用して VLAN 100 にトラフィックをブリッジングする ATM SPA インターフェイスの相手先固定接続 (PVC) に出力ポリシーとして適用されるサービスポリシーも示します。

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
```



```

Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap)# class vlan-inner-100
Router(config-pmap-c)# police 500000 1000 1500 conform-action set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end

```

## 関連コマンド

コマンド	説明
<b>bridge-domain</b>	RFC 1483 ATMブリッジングまたはRFC 1490 フレームリレーブリッジングで、ブリッジ処理された VLAN の ATM PVC またはフレームリレー データリンク接続識別子 (DLCI) へのマップを有効にします。
<b>class-map</b>	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
<b>policy-map</b>	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
<b>service-policy</b>	インターフェイスに付加するサービスポリシーの名前を指定します。
<b>showpolicy-map</b>	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
<b>showpolicy-mapinterface</b>	指定されたインターフェイスのすべてのサービス ポリシーに対して設定されている、全クラスの設定を表示するか、または、インターフェイス上の特定のPVCに対するサービスポリシーのクラスを表示します。

## police (EtherSwitch)

分類したトラフィックにポリサーを定義するには、ポリシーマップクラス コンフィギュレーションモードで **police** コマンドを使用します。既存のポリサーを削除するには、このコマンドの **no** 形式を使用します。

```
police {bps|cir bps} [{burst-byte|bc burst-byte}] conform-action transmit [exceed-action
{drop|dscp dscp-value}]
no police {bps|cir bps} [{burst-byte|bc burst-byte}] conform-action transmit [exceed-action
{drop|dscp dscp-value}]
```

### 構文の説明

<i>bps</i>   <b>cir</b> <i>bps</i>	1 秒あたりのビット数 (bps) 単位の平均トラフィック レートまたは認定情報レート (CIR) です。  10/100 ポートの場合、範囲は 1000000 ~ 100000000 で、粒度は 1 Mbps です。  ギガビット対応イーサネット ポートの場合、範囲は 8000000 ~ 128000000000 (128 Gbps) です。16 Mbps を超えるポリサーの粒度はレートの 0.1% で、16 Mbps を下回るポリサーの粒度は 8 Mbps です。
<i>burst-byte</i>   <b>bc</b> <i>burst-byte</i>	(任意) バイト単位の通常バーストサイズまたはバーストカウントです。有効な値は 1000 ~ 2000000000 (2 Gb) です。
<b>conform-action</b> <b>transmit</b>	レート制限に適合するパケットを送信します。
<b>exceed-action</b> <b>drop</b>	(任意) 指定されたレートを超えた場合は、スイッチがパケットをドロップするように指定します。
<b>exceed-action</b> <b>dscp</b> <i>dscp-value</i>	(任意) 指定されたレートを超えた場合は、スイッチがパケットの DiffServ コードポイント (DSCP) を指定された <i>dscp-value</i> に変更し、パケットを送信するよう指定します。

### コマンド デフォルト

ポリサーは定義されません。

### コマンド モード

ポリシー マップ クラス コンフィギュレーション

### コマンド履歴

リリース	変更箇所
12.1(6)EA2	このコマンドが導入されました。
12.2(15)ZJ	このコマンドが変更されました。このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。

リリース	変更箇所
12.3(4)T	このコマンドが変更されました。このコマンドが Cisco 2600 シリーズ、Cisco 3600 シリーズ、および Cisco 3700 シリーズのルータ プラットフォームに実装されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
15.0(1)SY	このコマンドが変更されました。 <i>burst-byte</i> 引数の最大値が増えました。

### 使用上のガイドライン

入力側ファスト イーサネット ポートでは、最大 6 個のポリサーを設定できます。

入力ギガビット対応イーサネット ポートでは、最大 60 個のポリサーを設定できます。

出力側ファスト イーサネットおよびギガビット対応イーサネット ポートでは、ポリサーを設定することはできません。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

設定を確認するには、**showpolicy-map** 特権 EXEC コマンドを使用します。

### 例

次の例では、トラフィックが平均レート 1 Mbps、バーストサイズ 65536 バイトを超えないときに DSCP 値を 46 に設定し、トラフィックがこれらの条件を超えるとパケットを廃棄するポリサーを設定する方法を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 46
Router(config-pmap-c)# police 1000000 65536 conform-action transmit exceed-action drop
Router(config-pmap-c)# end
```

### 関連コマンド

コマンド	説明
<b>policy-map</b>	複数のインターフェイスに適用できるポリシーマップを作成または変更し、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。
<b>showpolicy-map</b>	QoS ポリシー マップを表示します。

## police (percent)

インターフェイスで利用可能な帯域幅のパーセンテージに基づいてトラフィック ポリシングを設定するには、ポリシーマップ クラス コンフィギュレーション モードで **police** コマンドを使用します。トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

**police cir percent percentage [burst-in-msec] [bc conform-burst-in-msec ms] [be peak-burst-in-msec ms] [pir percent percentage] [conform-action action [exceed-action action [violate-action action]]]**

**no police cir percent percentage [burst-in-msec] [bc conform-burst-in-msec ms] [be peak-burst-in-msec ms] [pir percent percentage] [conform-action action [exceed-action action [violate-action action]]]**

**police cir percent percent [burst-in-msec] [bc conform-burst-in-msec ms] [pir percent] [be peak-burst-in-msec ms] [conform-action action] [exceed-action action] [violate-action action]**

**no police cir percent percent [burst-in-msec] [bc conform-burst-in-msec ms] [pir percent] [be peak-burst-in-msec ms] [conform-action action] [exceed-action action] [violate-action action]**

### 構文の説明

<b>cir</b>	情報レートを指定します。CIR がトラフィック ポリシングに使用されることを示します。
<b>percent</b>	帯域幅の割合を使用して CIR を計算するように指定します。
<i>percentage</i>	帯域幅のパーセンテージです。有効値の範囲は 1 ~ 100 です。
<i>burst-in-msec</i>	(任意) ミリ秒単位でのバースト。有効な範囲は 1 ~ 2000 の数字です。
<b>bc</b>	(任意) 最初のトークンバケットでトラフィック ポリシングに使用される適合バースト (bc) サイズを指定します。
<i>conform-burst-in-msec</i>	(任意) ミリ秒単位の bc 値です。有効な範囲は 1 ~ 2000 の数字です。
<b>ms</b>	(任意) バーストの値がミリ秒単位で指定されていることを示します。
<b>be</b>	(任意) 2 番目のトークンバケットでトラフィック ポリシングに使用されるピークバースト (be) サイズを指定します。
<i>peak-burst-in-msec</i>	(任意) ミリ秒単位の be サイズです。有効な範囲は 1 ~ 2000 の数字です。
<b>pir</b>	(任意) 最大情報レート (PIR) がトラフィック ポリシングに使用されることを示します。
<i>percent</i>	(任意) PIR の計算に使用される帯域幅のパーセンテージです。
<b>conform-action</b>	(任意) 適合バーストよりレートが小さいパケットで実行されるアクション。 <b>conform-action</b> を指定する前に、 <i>peak-burst-in-msec</i> の値を指定する必要があります。

<b>exceed-action</b>	(任意) 適合バースト内および適合バーストに超過バーストを加えたレートのパケットで実行されるアクションを指定します。
<b>violate-action</b>	(任意) 適合バーストに超過バーストを加えたレートよりレートが超過しているパケットで実行されるアクションを指定します。violate-action を指定する前に、exceed-action を指定する必要があります。
<b>action</b>	<p>(任意) パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。</p> <p><b>サポートされているすべてのプラットフォーム</b></p> <ul style="list-style-type: none"> <li>• <b>drop</b> : パケットをドロップします。</li> <li>• <b>set-clp-transmit</b> : ATM セルの 0 から 1 の ATM セル損失率優先度 (CLP) を設定して、ATM CLP ビットを 1 に設定してパケットを送信します。</li> <li>• <b>set-dscp-transmit new-dscp</b> : IP DiffServ コードポイント (DSCP) の値を設定して、新しい IP DSCP 値設定でパケットを送信します。</li> <li>• <b>set-frde-transmit</b> : フレーム リレー フレーム上のフレーム リレー廃棄適正 (DE) ビットを 0 から 1 に設定して、1 に設定した DE ビットが含まれるパケットを送信します。</li> <li>• <b>set-prec-transmit new-prec</b> : IP プレシデンスを設定して、その新しい IP プレシデンス値設定でパケットを送信します。</li> <li>• <b>transmit</b> : パケットをそのまま無変更で送信します。</li> </ul> <p><b>Cisco 10000 シリーズ ルータ以外でサポートされるプラットフォーム</b></p> <ul style="list-style-type: none"> <li>• <b>policed-dscp-transmit</b> : (超過アクションと違反アクションのみ) ポリシングされる DSCP マップごとに DSCP の値を変更し、パケットを送信します。</li> <li>• <b>set-cos-inner-transmit value</b> : 拡張 FlexWAN モジュール、および Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 と Cisco 7600 SIP-400 の SPA でブリッジング機能の使用時に、ブリッジ処理されたフレームに対するポリシングアクションとして、サービス フィールドの内部クラスを設定します。</li> <li>• <b>set-cos-transmit value</b> : パケットのサービスクラス (CoS) の値を設定して、パケットを送信します。</li> <li>• <b>set-mpls-exposition-transmit</b> : マルチプロトコル ラベル スイッチング (MPLS) の EXP ビットを 0 から 7 に設定して、新しい MPLS EXP ビット値設定でパケットを送信します。</li> <li>• <b>set-mpls-topmost-transmit</b> : 最上位ラベルにある MPLS EXP ビットを設定して、パケットを送信します。</li> </ul>

<i>action (continued)</i>	<p><b>Cisco 10000 シリーズ ルータ</b></p> <ul style="list-style-type: none"> <li>• <b>drop</b> : パケットをドロップします。</li> <li>• <b>set-clp-transmit value</b> : ATM セルの 0 から 1 の ATM セル損失率優先度 (CLP) を設定し、ATM CLP ビットを 1 に設定してパケットを送信します。</li> <li>• <b>set-cos-inner-transmit value</b> : 拡張 FlexWAN モジュール、および Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 と Cisco 7600 SIP-400 の SPA でブリッジング機能の使用時に、ブリッジ処理されたフレームに対するポリシングアクションとして、サービス フィールドの内部クラスを設定します。</li> <li>• <b>set-cos-transmit value</b> : パケットの COS 値を設定して、送信します。</li> <li>• <b>set-discard-class-transmit</b> : パケットの廃棄クラス属性を設定して、新しい廃棄クラス設定でパケットを送信します。</li> <li>• <b>set-dscp-transmit value</b> : IP DiffServ コードポイント (DSCP) 値を設定して、新しい IP DSCP 値設定でパケットを送信します。</li> <li>• <b>set-frde-transmit value</b> : フレーム リレー フレーム上のフレーム リレー廃棄適格 (DE) ビットを 0 から 1 に設定して、1 に設定した DE ビットが含まれるパケットを送信します。</li> <li>• <b>set-mpls-experimental-imposition-transmit value</b> : 強制ラベルのヘッダーでマルチプロトコル ラベル スイッチング (MPLS) の Experimental (EXP) ビット (0~7) を設定して、新しい MPLS EXP ビット値設定でパケットを送信します。</li> <li>• <b>set-mpls-experimental-topmost-transmit value</b> : 入力インターフェイスや出力インターフェイスでの最上位 MPLS ラベル ヘッダーに、MPLS EXP フィールド値を設定します。</li> <li>• <b>set-prec-transmit value</b> : IP プレシデンスを設定して、新しい IP プレシデンス値設定でパケットを送信します。</li> <li>• <b>set-qos-transmit value</b> : Quality of Service (QoS) グループの値を設定して、新しい QoS グループ値設定でパケットを送信します。有効な値は 0 ~ 99 です。</li> <li>• <b>transmit</b> : パケットを送信します。パケットは変更されません。</li> </ul>
---------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**コマンド デフォルト**

デフォルトの **bc** および **be** の値は 4 ms です。

**conform-action** のデフォルト アクションは **transmit** です。

**exceed-action** および **violate-action** のデフォルト アクションは **drop** です。

## コマンドモード

ポリシーマップクラス コンフィギュレーション (config-pmap-c)

## コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。
12.0(25)SX	このコマンドが変更されました。パーセントベース ポリシング機能が、Cisco 10000 シリーズ ルータに追加されました。
12.1(1)E	このコマンドが Cisco IOS Release 12.2(1)E に統合されました。
12.1(5)T	このコマンドが、Cisco IOS Release 12.1(5)T に統合されました。
12.2(13)T	このコマンドは、パーセントベース ポリシング機能とシェーピング機能のために、変更されました。
12.0(28)S	このコマンドが Cisco IOS Release 12.0(28)S に統合されました。
12.2(18)SXE	このコマンドが Cisco IOS Release 12.2(18)SXE に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが変更されました。拡張 FlexWAN モジュールでマルチポイントブリッジング (MPB) 機能を使用する場合のために、また、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB を使用する場合のために、action 引数に <b>set-cos-inner-transmit</b> キーワードが追加されました。
12.2(31)SB2	このコマンドが変更されました。PRE3 で、Cisco 10000 シリーズ ルータの <b>set-frde-transmit</b> action 引数が追加されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズ ルータに実装されました。
15.0(1)SY	このコマンドが変更されました。CIR および PIR の最大値が増えました。

## 使用上のガイドライン

このコマンドでは、インターフェイスで利用可能な最大帯域幅の割合に基づいて CIR および PIR を計算します。ポリシー マップがインターフェイスに対応付けられている場合、ビット/秒 (bps) 単位の等価 CIR および PIR 値が、インターフェイス帯域幅とこのコマンドで入力したパーセント値に基づいて計算されます。その後、**showpolicy-mapinterface** コマンドを使用して、計算された bps レートを確認できます。

計算された CIR および PIR の bps レートは、8000 ~ 128000000000 bps (128 Gbps) の範囲内であればなりません。レートがこの範囲外の場合、関連ポリシーマップをインターフェイスに対応付けることができません。インターフェイス帯域幅が変更された場合 (帯域幅が追加された場合など)、改訂された帯域幅に基づいて CIR および PIR の bps 値が再計算されます。ポリ

シーマップをインターフェイスに対応付けたあとに CIR および PIR の割合が変更された場合、CIR および PIR の bps 値が再計算されます。

また、このコマンドでは、適合バースト サイズとピーク バースト サイズの値をミリ秒単位で指定することもできます。帯域幅を割合として計算する場合は、適合バースト サイズとピークバースト サイズをミリ秒単位で指定する必要があります。

ポリシーマップは、トップ（または「親」）レベルおよびセカンダリ（または「子」）レベルの、2つのレベルの（ネストされた）階層で設定できます。**police (percent)** コマンドは、親ポリシーマップまたは子ポリシーマップのいずれかで使用するために設定できます。

**police (percent)** コマンドにより、帯域幅のパーセンテージを計算する参照ポイントとして、使用可能な帯域幅の最大レートが使用されます。子ポリシーマップで **police (percent)** コマンドが設定されている場合、**police (percent)** コマンドにより、次に上位のレベルにあるポリシー（この場合は、親ポリシーマップ）で指定されている帯域幅量が使用されます。親ポリシーマップで使用可能な最大帯域幅レートが指定されていない場合、**police (percent)** コマンドにより、次に上位のレベルにあるポリシー（この場合は、物理インターフェイスで、階層の最高ポイント）で使用可能な最大帯域幅レートが、参照ポイントとして使用されます。**police (percent)** コマンドでは、帯域幅の参照ポイントとして、次に上位のレベルが常に参照されます。次に、このポイントについての設定例を示します。

```

Policymap parent_policy
  class parent
    shape average 512000
    service-policy child_policy
Policymap child_policy
  class normal_type
    police cir percent 30

```

この設定例では、**parent\_policy** と **child\_policy** の 2つの階層ポリシーがあります。**child\_policy** と呼ばれるポリシーマップでは、**normal\_type** と呼ばれるクラスで **police** コマンドが設定されました。このクラスでは、**police (percent)** コマンドによって指定されたパーセンテージは 30% です。コマンドにより、**parent\_policy** にある親クラスの帯域幅参照ポイントとして、512 kbps というピーク レートが使用されます。**police (percent)** コマンドでは、cir レート (512 kbps \* 30%) の計算の根拠として、512 kbps が使用されます。

```

interface serial 4/0
  service-policy output parent_policy
Policymap parent_policy
  class parent
    bandwidth 512
    service-policy child_policy

```

前述の例では、**parent\_policy** と呼ばれる 1つのポリシーマップがあります。このポリシーマップでは、ピーク レートが指定されていません。**bandwidth** コマンドが使用されましたが、このコマンドは使用可能な帯域幅の最大レートを表しません。したがって、**police (percent)** コマンドでは、帯域幅の参照ポイントを取得する目的で、次に上位のレベル（この場合は、シリアルインターフェイス 4/0）が参照されます。シリアルインターフェイス 4/0 の帯域幅が 1.5 Mbps とすると、**police (percent)** コマンドでは、cir レート (1500000 \* 30%) の計算の根拠として、1.5 Mbps が使用されます。



**police (percent)** コマンドは、しばしば **bandwidth** コマンドと **priority** コマンドとの組み合わせで使用されます。**bandwidth** コマンドと **priority** コマンドを使用すると、エンティティ（たとえば、物理インターフェイスなど）で使用可能な帯域幅の合計量を計算できます。**bandwidth** コマンドと **priority** コマンドを使用して、エンティティで使用可能な帯域幅の合計量を計算する場合は、次の注意事項に従ってください。

- エンティティが物理インターフェイスの場合、合計帯域幅は、物理インターフェイス上の帯域幅です。
- エンティティが整形 ATM 相手先固定接続（PVC）の場合、合計帯域幅は、次のように計算されます。
  - 可変ビット レート（VBR）の仮想回線（VC）の場合、計算には、平均セル レート（SCR）が使用されます。
  - 使用可能ビット レート（ABR）の VC の場合、計算には、最小セル レート（MCR）が使用されます。

帯域幅割り当ての詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Congestion Management Overview」の章を参照してください。

Cisco 7600 シリーズ ルータ上の SIP および SPA の **set-cos-inner-transmit** アクションの使用

拡張 FlexWAN モジュールで MPB 機能を使用する場合や、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB 機能を使用する場合に、内部 CoS 値をポリシング アクションとしてマーキングすることをサポートするために、Cisco IOS Release 12.2(33)SRA で **set-cos-inner-transmit** キーワード アクションが導入されました。

このコマンドは、Cisco 7600 SIP-600 ではサポートされていません。

Cisco 7600 シリーズ ルータで、SIP によってサポートされる QoS と **police** コマンドの形式の詳細については、『*Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*』を参照してください。

## 例

次に、帯域幅の割合（％）に基づいた CIR と PIR を使用してトラフィック ポリシングを設定する例を示します。この例では、CIR に 20％、PIR に 40％が指定されています。オプションの bc 値と be 値（それぞれ、300 ms、400 ms）も指定されています。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40

Router(config-pmap-c-police)# exit
```

次の例に示したように、ポリシー マップとクラス マップの設定後、ポリシー マップがインターフェイスに付加されます。

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0
```

```
Router(config-if)# service-policy input policy1
Router(config-if)# exit
```

Cisco 7600 シリーズ ルータ上の SIP および SPA のアクションとしての内部 CoS 値の設定

次に、仮想 LAN (VLAN) 100 のすべてのトラフィックをクラス `vlan-inner-100` にフィルタリングし、`vlan-inner-100` クラスのトラフィック シェーピング ポリシーを確立する QoS クラスの設定例を示します。サービス ポリシーで CIR は 20%、PIR は 40% にトラフィックを制限し、適合バースト (bc) を 300 ms、ピーク バースト (be) を 400 ms とし、インナー CoS 値を 3 に設定します。内部 CoS 値の設定はブリッジング機能を使用する場合に限ってサポートされるので、`bridge-domain` コマンドを使用して VLAN 100 にトラフィックをブリッジングする ATM 共有ポートアダプタ (SPA) インターフェイスの相手先固定接続 (PVC) に、出力ポリシーとして適用されるサービスポリシーも示します。

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40
conform-action set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if)# end
```

次に、プライオリティ サービスに `police (percent)` コマンドを設定する例を示します。この例では、`New-Traffic` という名前のポリシー マップで、`Voice` という名前のプライオリティ クラスが設定されています。このルータは、音声トラフィックに認定レートの 25% を割り当て、4 ms の認定バーストと 1 ms の超過バーストを許可します。このルータは、認定レートに適合する音声トラフィックを送信して、バーストサイズを超える音声トラフィックの QoS 送信値を 4 に設定し、認定レートに違反する音声トラフィックをドロップします。

```
Router(config)# policy-map New-Traffic
Router(config-pmap)# class Voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# queue-limit 32
Router(config-pmap-c)# police percent 25 4 ms 1 ms conform-action transmit exceed-action
set-qos-transmit 4 violate-action drop
```

#### 関連コマンド

コマンド	説明
<code>bandwidth(policy-mapclass)</code>	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。

コマンド	説明
<b>bridge-domain</b>	RFC 1483 ATMブリッジングまたはRFC 1490 フレームリレーブリッジングで、ブリッジ処理されたVLANのATM PVCまたはフレームリレーDLCIへのマップをイネーブルにします。
<b>policy-map</b>	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービスポリシーを指定します。
<b>priority</b>	ポリシーマップのトラフィッククラスに、プライオリティを付与します。
<b>service-policy</b>	入力インターフェイスまたはVC、あるいは出力インターフェイスまたはVCに、そのインターフェイスまたはVCのサービスポリシーとして使用するポリシーマップを対応付けます。
<b>shape(percent)</b>	インターフェイスで使用可能な帯域幅の割合 (%) に基づいて、平均レートトラフィックシェーピングとピークレートトラフィックシェーピングを指定します。
<b>showpolicy-map</b>	指定されたサービスポリシーマップに対するすべてのクラスの設定、または、すべての既存ポリシーマップに対するすべてのクラスの設定を表示します。
<b>showpolicy-mapinterface</b>	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、すべてのサービスポリシーに対して設定されているすべてのクラスの packets 統計情報を表示します。

## police (ポリシーマップ)

インターフェイスごとにポリサーを作成し、ポリシーマップクラスを設定して使用するには、ポリシーマップクラス コンフィギュレーション モードで **police** コマンドを使用します。ポリシーマップクラスからインターフェイスごとのポリサーを削除するには、このコマンドの **no** 形式を使用します。

```

police bps [[bc normal-burst-bytes [{maximum-burst-bytes|be [burst-bytes]}]] [pir bps [be
burst-bytes]] [conform-action action [exceed-action action [violate-action action]]]
no police bps
police aggregate name
no police aggregate name
police cir bps [[bc normal-burst-bytes [{maximum-burst-bytes|be [burst-bytes]}]] [pir bps [be
burst-bytes]] [conform-action action [exceed-action action [violate-action action]]]
no police cir bps
police cir percent percent [burst ms [be [burst ms]]] [pir percent percent [be burst ms]]
[conform-action action [exceed-action action [violate-action action]]]
no police cir percent
police flow bps [normal-burst-bytes] [conform-action action [exceed-action action]]
police flow mask {dest-only|full-flow|src-only} bps [normal-burst-bytes] [conform-action action
[exceed-action action]]
no police flow

```

構文の説明	<i>bps</i>	ビット/秒 (bps) 単位でのターゲットビットレート。ポストフィックスの値は、小数点として、 <b>k</b> 、 <b>m</b> および <b>g</b> を使用できます。有効な範囲は 8000 (または 8k) ~ 128000000000 (または 128 Gbps) です。
	<i>normal-burst-bytes</i>	(任意) バーストを処理するための、バイト単位での CIR トークンバケットサイズ。有効な値は 1000 ~ 2000000000 (2 Gb) です。
	<i>maximum-burst-bytes</i>	(任意) バーストを処理するための、バイト単位での PIR トークンバケットサイズ。有効な値は 1000 ~ 2000000000 (2 Gb) です。
	<i>burst-bytes</i>	(任意) バーストを処理するための、バイト単位でのトークンバケットサイズ。有効な値は 1000 ~ 2000000000 (2 Gb) です。
	<b>bc</b>	(任意) 使用可能な (適合) バーストサイズをバイト単位でサイズを指定します。
	<b>be</b>	(任意) 使用可能な超過バーストサイズをバイト単位でサイズを指定します。
	<b>pir</b>	(任意) 最大情報レート (PIR) を指定します。
	<b>cir</b>	認定情報レート (CIR) を指定します。

<b>conform-action</b> アクション	(任意) レートリミットに適合するパケットで実行されるアクションを指定します。 <i>action</i> 引数で有効な値については、「使用上のガイドライン」セクションを参照してください。
<b>exceed-action</b> アクション	(任意) <i>maximum-burst-bytes</i> 引数での指定レートよりもパケットレートが大きい場合に、パケットで実行されるアクションを指定します。 <i>action</i> 引数で有効な値については、「使用上のガイドライン」セクションを参照してください。
<b>violate-action</b> アクション	(任意) <i>maximum-burst-bytes</i> 引数での指定レートよりもパケットレートが大きい場合に実行されるアクションを指定します。 <i>action</i> 引数で有効な値については、「使用上のガイドライン」セクションを参照してください。
<b>aggregate</b> 名前	前に定義した集約ポリサーの名前を指定し、指定された集約ポリサーで使用するポリシー マップ クラスを設定します。
<b>percent</b> パーセント	使用可能なインターフェイス帯域幅の割合 (%) を指定します。有効な範囲は 1 ~ 100 です。
バースト	(任意) バーストを処理するための、ミリ秒 (ms) 単位でのトークンパケット サイズです。有効な範囲は 1 ~ 2000 です。
<b>ms</b>	ミリ秒を示します。帯域幅をパーセンテージで指定する場合、 <i>burst</i> 引数の次に、このキーワードを指定する必要があります。
<b>flow</b>	各フローをポリシングするマイクロフロー ポリサーを指定します。
<b>mask</b>	ポリシングに使用するフロー マスクを指定します。
<b>dest-only</b>	宛先だけのフロー マスクを指定します。
<b>full-flow</b>	フルフロー マスクを指定します。
<b>src-only</b>	発信元だけのフロー マスクを指定します。

コマンド デフォルト      ポリシングは実行されません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション (config-pmap-c)

コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドが Supervisor Engine 720 に導入されました。
12.2(17d)SXB	このコマンドが、Cisco IOS Release 12.2(17d)SXB に統合され、Supervisor Engine 2 に実装されました。

リリース	変更箇所
12.2(17d)SXB3	このコマンドが変更されました。FlexWAN インターフェイスでのみ、 <b>police bps</b> の最小レートが 32,000 から 8,000 に下げられました。
12.2(18)SXD	このコマンドが次のように変更されました。 <ul style="list-style-type: none"> <li>• <b>conform-action</b> キーワードの有効な値に <b>set-mpls-exp-topmost-transmit</b> が追加されました。</li> <li>• <b>set-mpls-exp-transmit</b> キーワードが <b>set-mpls-exp-imposition-transmit</b> に変更されました。</li> </ul>
12.2(18)SXE	このコマンドが変更されました。10 ギガビット イーサネットをサポートするため、bps の最大レートが、4,000,000,000 bps から 10,000,000,000 bps に増加されました。
12.2(18)SXF	このコマンドが変更されました。CIR の最大レートが、10,000,000,000 bps に増加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB	このコマンドが変更されました。コマンドの動作が変更され、ポリシングアクションは変更せずにポリシング レート パラメータだけを変更する場合、ポリシングアクションのデフォルトアクションは、 <b>conform-action transmit</b> 、 <b>exceed-action drop</b> 、および <b>violate-action drop</b> になりました。これは、PRE3 用の Cisco 10000 シリーズ ルータに実装されました。
12.2(33)SB	このコマンドが変更されました。コマンドの動作が変更され、ポリシングアクションは変更せずにポリシング レート パラメータだけを変更する場合、ポリシングアクションが保存されます。これは、PRE3 用と PRE4 用の Cisco 10000 シリーズ ルータに実装されました。詳細については、「使用上のガイドライン」セクションを参照してください。
12.2(33)SXH2	このコマンドが変更されました。CIR の最大レートが、64,000,000,000 bps に増加されました。
12.2(33)SXI	このコマンドが変更されました。CIR の最小トークンバケットサイズが、1 バイトに削減されました。
15.0(1)SY	このコマンドが変更されました。 <i>normal-burst-bytes</i> 、 <i>maximum-burst-bytes</i> 、および <i>burst-bytes</i> 引数の最大値が 2 Gb に増えました。bps 引数の最大値が 128 Gb に増えました。

**使用上のガイドライン** Cisco IOS Release 12.2(17d)SXB3 では、FlexWAN インターフェイスのみ *bps* 引数の範囲は、8,000 ~ 4,000,000,000 bps です。

名前付き集約ポリサーを作成するには、**mls qos aggregate-policer name** コマンドを使用します。

名前付きとインターフェイスごとの、2つのタイプの集約ポリサーを作成できます。両方のタイプとも、次のように、複数のポートに付加できます。

- **mlsqosaggregate-policer** コマンドを使用して、名前付き集約ポリサーを作成します。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。
- ポリシーマップクラスにあるインターフェイスごとの集約ポリサーは、**police** コマンドを使用して定義します。インターフェイス別集約ポリサーを複数の入力ポートに対応付けると、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。

名前付き集約ポリサーの使用をクリアするには、**nopoliceaggregate name** コマンドを使用します。

マイクロフローポリサーを定義するには、**policeflow** コマンドを入力します（ARPトラフィックには、マイクロフローポリシングは適用できません）。

インターフェイスごとの（名前付きではない）集約ポリサーを定義するには、**police** コマンドを入力します。

トラフィックが集約とマイクロフローの両方でポリシングされている場合、集約とマイクロフローの両方のポリサーは同じポリシーマップクラスにあり、それぞれで **conform-action** キーワードおよび **exceed-action** キーワードを使用する必要があります。

### アクション引数の値

*action* 引数の有効値は、次のとおりです。

- **drop** : *bps* 引数に設定されているレートを超えないパケットをドロップします。
- **set-clp-transmit** : ATM セル損失率優先度 (CLP) を設定し、送信します。
- **set-cos-inner-transmit{ new-cos }** : *new-cos* 引数の新しい内部サービスクラス (CoS) の値に一致するトラフィックにマーク付けします。*new-cos* 引数の有効値の範囲は 0 ~ 7 です。
- **set-cos-transmit{ new-cos }** : *new-cos* 引数の新しい CoS の値に一致するトラフィックにマーク付けします。*new-cos* 引数の有効値の範囲は 0 ~ 7 です。
- **set-cos-transmit** : ATM セル損失率優先度 (CLP) を設定し、送信します。
- **set-dscp-transmit{ dscp-bit-pattern | dscp-value | default|ef }** : 新しい DSCP の値に一致するトラフィックにマーク付けします。
  - *dscp-bit-pattern* : DSCP ビットパターンを指定します。表 1 に、有効な値のリストを示します。
  - *dscp-value* : DSCP の値を指定します。有効な値は 0 ~ 63 です。
  - **default** : パケットをデフォルト DSCP 値 (000000) と一致させます。
  - **ef** : Expedited Forwarding (EF) Per-Hop Behavior (PHB) DSCP の値 (101110) とパケットが一致します。

表 2: 有効な DSCP ビット パターンの値

キーワード	定義
af11	パケットが AF11 DSCP (001010) と一致します。
af12	パケットが AF12 DSCP (001100) と一致します。
af13	パケットが AF13 DSCP (001110) と一致します。
af21	パケットが AF21 DSCP (010010) と一致します。
af22	パケットが AF22 DSCP (010100) と一致します。
af23	パケットが AF23 DSCP (010110) と一致します。
af31	パケットが AF31 DSCP (011010) と一致します。
af32	パケットが AF32 DSCP (011100) と一致します。
af33	パケットが AF33 DSCP (011110) と一致します。
af41	パケットが AF41 DSCP (100010) と一致します。
af42	パケットが AF42 DSCP (100100) と一致します。
af43	パケットが AF43 DSCP (100110) と一致します。
cs1	パケットが CS1 (Precedence 1) DSCP (001000) と一致します。
cs2	パケットが CS2 (Precedence 2) DSCP (010000) と一致します。
cs3	パケットが CS3 (Precedence 3) DSCP (011000) と一致します。
cs4	パケットが CS4 (Precedence 4) DSCP (100000) と一致します。
cs5	パケットが CS5 (Precedence 5) DSCP (101000) と一致します。
cs6	パケットが CS6 (Precedence 6) DSCP (110000) と一致します。
cs7	パケットが CS7 (Precedence 7) DSCP (111000) と一致します。

- **set-frde-transmit** : フレーム リレー 廃棄適性 (FR DE) ビットを設定し、送信します。これは、**exceed-action** *action* キーワードと引数との組み合わせで有効です。
- **set-mpls-exp-imposition-transmit new-mpls-exp** : 強制ラベル エントリのマルチプロトコル ラベル スイッチング (MPLS) Experimental (EXP) ビットを再書き込みして、ビットを送信します。*new-mpls-exp* 引数により、ポリシー マップによって定義される MPLS EXP ビットの設定に使用される値が指定されます。*new-mpls-exp* 引数の有効値の範囲は 0 ~ 7 です。



- **set-mpls-exp-topmost-transmit** : 最上位ラベルにある EXP ビットを設定し、パケットを送信します。



(注) **set-mpls-exp-topmost-transmit** キーワードは、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの一部のリリースではサポートされていません。

- **set-prec-transmit** *new-precedence* [ **exceed-action** ] : 新しい IP プレシデンスの値に一致するトラフィックにマーク付けし、送信します。*new-precedence* 引数の有効値の範囲は 0 ~ 7 です。このアクションには、**exceed-action** キーワードを付けることもできます。
- **set-qos-transmit** : qos-group を再書き込みし、パケットを送信します。
- **transmit** : *bps* 引数に設定されているレートを超えないパケットを送信します。**transmit** キーワードのオプションのキーワードと引数の組み合わせは、**exceed-action action** です。

続くキーワードが指定されない場合、デフォルトアクションは、次のとおりです。

- **conform-action** は **transmit**
- **exceed-action** は **drop**
- **violate-action** は **drop**

#### Cisco 10000 シリーズ ルータ

Cisco IOS Release 12.2(31)SB よりも前のリリースでは、ポリシング レートパラメータを変更してアクションパラメータを変更しない場合、アクションパラメータはデフォルトのアクションに戻ります。

たとえば、次の設定例は、**test** という名前のポリシー マップで設定された **police** コマンドを示しています。適合するトラフィック、超過するトラフィック、および違反するトラフィックのポリシング アクションが、**set-clp-transmit** に設定されます。その後、ポリシング レートパラメータがそれぞれ 500000、250、および 200 に変更されますが、アクションは変更されません。**test** ポリシー マップを再度表示すると、ポリシング アクションはそれぞれデフォルトの **transmit**、**drop**、および **drop** になっています。

```
Router# show policy-map test
Policy Map test
Class precl
police 248000 100 10 conform-action set-clp-transmit exceed-action set-clp-transmit
violate-action set-clp-transmit
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class precl
Router(config-pmap-c)# police 500000 250 200
Router(config-pmap-c)# end
Router# show policy-map test
Policy Map test
Class precl
police 500000 250 200 conform-action transmit exceed-action drop violate-action drop
```

Cisco IOS Release 12.2(33)SB 以降のリリースは、デュアルポリシングアクションとポリシングサブモードをサポートしています。そのため、レートパラメータのみを変更するために **police** コマンドを使用した場合、ポリシングアクションはデフォルトのアクションにならず、以前のアクションが保持されます。

たとえば、次の設定例は、**test** という名前のポリシーマップの **precl** という名前のトラフィッククラスで設定された **police** コマンドを示しています。ポリシングレートが指定され、ポリシングサブモードでポリシングアクションが指定されます。ポリシングレートパラメータのみを変更した後は、ポリシングアクションはデフォルトにならず、元の設定が保持されます。

```
Router# show policy-map test
Policy Map test
Class precl
police 248000 1000 100
conform-action set-clp-transmit
exceed-action set-clp-transmit
violate-action set-clp-transmit
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class precl
Router(config-pmap-c)# police 500000 100 200
Router(config-pmap-c)# end
Router# show policy-map test
Policy Map test
Class precl
police 500000 100 200
conform-action set-clp-transmit
exceed-action set-clp-transmit
violate-action set-clp-transmit
```

## 例

次に、前に定義した集約ポリサーの名前を指定し、指定された集約ポリサーで使用するポリシーマップクラスを設定します。

```
Router(config-pmap-c)# police aggregate aggl
```

次に、クラスマップ **access-match** を使用する、**police-setting** という名前のポリシーマップを作成する例を示します。これは、受信する IP precedence の値を信頼するよう設定され、証明書信頼リストの集約ポリサーおよびマイクロフローポリサーで設定されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 1000000000 200000 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)# exit
```

## 関連コマンド

コマンド	説明
<b>class-map</b>	QoS クラス マップ コンフィギュレーション モードにアクセスし、QoS クラス マップを設定します。
<b>mlsqosaggregate-policer</b>	ポリシー マップで使用するために、名前付き集約ポリサーを定義します。
<b>police</b>	トラフィック ポリシングを、QoS ポリシー マップ クラス コンフィギュレーション モードまたは QoS ポリシー マップ クラス ポリシング コンフィギュレーション モードで設定します。
<b>service-policy</b>	ポリシー マップをインターフェイスに付加します。
<b>showclass-map</b>	クラス マップ情報を表示します。
<b>showpolicy-map</b>	ポリシー マップ情報を表示します。
<b>showpolicy-mapinterface</b>	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

## police (2つのレート)

認定情報レート (CIR) と最大情報レート (PIR) の2つのレートを使用してトラフィック ポリシングを設定するには、ポリシーマップ クラス コンフィギュレーション モードで **police** コマンドを使用します。2レートトラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

**police cir cir [bc conform-burst] [pir pir] [be peak-burst] [conform-action action [exceed-action action [violate-action action]]]**

**no police cir**

### 構文の説明

<b>cir</b>	最初のトークンバケットが更新される認定情報レート (CIR) を指定します。
<i>cir</i>	ビット/秒単位の CIR 値です。値は 8000 ~ 128000000000 (128 Gbps) までの数字です。
<b>bc</b>	(任意) 最初のトークンバケットでポリシングに使用される適合バースト (bc) サイズを指定します。
<i>conform-burst</i>	(任意) バイト単位の bc 値です。値は 1000 ~ 2000000000 (2 Gb) までの数字です。
<b>pir</b>	(任意) 2 番目のトークンバケットが更新される最大情報レート (PIR) を指定します。
<i>pir</i>	(任意) ビット/秒単位の PIR 値です。値は 8000 ~ 128000000000 (128 Gbps) までの数字です。
<b>be</b>	(任意) 2 番目のトークンバケットでポリシングに使用されるピークバースト (be) サイズを指定します。
<i>peak-burst</i>	(任意) バイト単位のピークバースト (be) サイズです。サイズは、使用するインターフェイスとプラットフォームによって異なります。
<b>conform-action</b>	(任意) CIR および PIR に適合するパケットに対して実行するアクションを指定します。
<b>exceed-action</b>	(任意) PIR に適合するものの CIR には適合しないパケットに対して実行するアクションを指定します。
<b>violate-action</b>	(任意) PIR を超過するパケットに対して実行するアクションを指定します。

<i>action</i>	<p>(任意) パケットに対して実行するアクションを指定します。次のいずれかのキーワードを指定します。</p> <ul style="list-style-type: none"> <li>• <b>drop</b> : パケットをドロップします。</li> <li>• <b>set-clp-transmit</b> : ATM セルの 0 から 1 の ATM セル損失率優先度 (CLP) を設定して、ATM CLP ビットを 1 に設定してパケットを送信します。</li> <li>• <b>set-cos-inner-transmit value</b> : 拡張 FlexWAN モジュール、および Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 と Cisco 7600 SIP-400 の SPA でブリッジ機能の使用時に、ブリッジ処理されたフレームに対するポリシングアクションとして、サービスフィールドの内部クラスを設定します。</li> <li>• <b>set-dscp-transmit new-dscp</b> : IP DiffServ コードポイント (DSCP) の値を設定して、新しい IP DSCP 値設定でパケットを送信します。</li> <li>• <b>set-dscp-tunnel-transmit value</b> : トンネルマーキングのため、レイヤ 2 Tunnel Protocol Version 3 (L2TPv3) または Generic Routing Encapsulation (GRE) トンネル型パケットのトンネルヘッダーで DSCP の値 (0 ~ 63) を設定して、新しい値でパケットを送信します。</li> <li>• <b>set-frde-transmit</b> : フレームリレーフレーム上のフレームリレー廃棄適正 (DE) ビットを 0 から 1 に設定して、1 に設定した DE ビットが含まれるパケットを送信します。</li> <li>• <b>set-mpls-exp-transmit</b> : マルチプロトコルラベルスイッチング (MPLS) の EXP ビットを 0 から 7 に設定して、新しい MPLS EXP ビット値設定でパケットを送信します。</li> <li>• <b>set-prec-transmit new-prec</b> : IP プレシデンスを設定して、その新しい IP プレシデンス値設定でパケットを送信します。</li> <li>• <b>set-prec-tunnel-transmit value</b> : トンネルマーキングのため、L2TPv3 または GRE トンネル型パケットのトンネルヘッダーで優先順位の値 (0 ~ 7) を設定して、新しい値でパケットを送信します。</li> <li>• <b>set-qos-transmit new-qos</b> : Quality of Service (QoS) グループの値を設定して、新しい QoS グループ値設定でパケットを送信します。</li> <li>• <b>transmit</b> : パケットをそのまま無変更で送信します。</li> </ul>
---------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

コマンドデフォルト 2つのレートを使用するトラフィック ポリシングがディセーブルにされます。

コマンドモード

ポリシーマップクラス コンフィギュレーション (config-pmap-c)

コマンド履歴

リリース	変更箇所
12.0(5)XE	このコマンドが導入されました。

リリース	変更箇所
12.1(1)E	このコマンドが Cisco IOS Release 12.1(1)E に統合されました。
12.1(5)T	このコマンドが変更されました。 <b>violate-action</b> キーワードが追加されました。
12.2(2)T	このコマンドが変更されました。 <i>action</i> 引数に次のキーワードが追加されました。 <ul style="list-style-type: none"> <li>• <b>set-clp-transmit</b></li> <li>• <b>set-frde-transmit</b></li> <li>• <b>set-mpls-exp-transmit</b></li> </ul>
12.2(4)T	このコマンドが変更されました。2レートトラフィックポリシングに対応するために、 <b>cir</b> および <b>pir</b> キーワードが追加されました。
12.2(28)SB	このコマンドが変更されました。 <i>action</i> 引数の <b>set-dscp-tunnel-transmit</b> および <b>set-prec-tunnel-transmit</b> キーワードが追加されました。これらのキーワードは、Layer 2 Tunnel Protocol Version 3 (L2TPv3) トンネル型パケット用です。
12.2(33)SRA	このコマンドが変更されました。拡張 FlexWAN モジュールでマルチポイントブリッジング (MPB) 機能を使用する場合のために、また、Cisco 7600 シリーズルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB を使用する場合のために、 <i>action</i> 引数に <b>set-cos-inner-transmit</b> キーワードが追加されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
12.2(33)SRC	このコマンドが、Cisco マルチレイヤスイッチフィーチャカード3 (MSFC3) に搭載されている Cisco 7600 シリーズルータをサポートするために変更されました。
12.4(15)T2	Generic Routing Encapsulation (GRE) トンネル型パケットのマーキングのサポートが含まれるように、このコマンドが変更されました。  (注) このリリースでは、GRE トンネル型パケットのマーキングは、Cisco MGX ルートプロセッサモジュール (RPM-XF) に搭載されているプラットフォームでのみ、サポートされます。
12.2(33)SB	GRE トンネル型パケットのマーキングのサポートと、Cisco 7300 シリーズルータのサポートが含まれるように、このコマンドが変更されました。
12.4(20)T	このコマンドが変更されました。モジュラ Quality of Service (QoS) コマンドラインインターフェイス (CLI) (MQC) を使用した階層型キューイングフレームワーク (HQF) のサポートが追加されました。
15.0(1)SY	このコマンドが変更されました。 <i>cir</i> 、 <i>conform-burst</i> 、 および <i>pir</i> 引数の最大値が増えました。

## 使用上のガイドライン 明示的なポリシング レートでのプライオリティの設定

明示的なポリシング レートでプライオリティ クラスを設定する場合、輻輳条件に関係なく、トラフィックはポリシング レートに限定されます。つまり、帯域幅が使用可能な場合、プライオリティトラフィックは、明示的なポリサーで指定されたレートを超えることはできません。

### トークンバケット

2レートトラフィックポリシングでは、2つの独立したレートでのトラフィックのポリシングに、2つのトークンバケット (Tc と Tp) を使用します。2つのトークンバケットに関して次の点に注意してください。

- Tc トークンバケットは、パケットが2レートポリサーで到着するたびに CIR 値で更新されます。Tc トークンバケットには、適合バースト (Bc) 値まで含めることができます。
- Tp トークンバケットは、パケットが2レートポリサーで到着するたびに PIR 値で更新されます。Tp トークンバケットには、ピークバースト (Be) 値まで含めることができます。

### トークンバケットの更新

次のシナリオは、トークンバケットの更新方法について説明したものです。

B バイトのパケットは時間 t に着信します。最後のパケットは時間 t1 に着信しました。時間 t での CIR と PIR トークンバケットは、それぞれ Tc(t) および Tp(t) で表されます。これらの値をこのシナリオで使用する場合、トークンバケットは次のように更新されます。

$$Tc(t) = \min(CIR \times (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = \min(PIR \times (t-t1) + Tp(t1), Be)$$

### トラフィックのマーキング

2レートポリサーは、指定レートに適合しているか、超過しているか、または違反しているとしてパケットをマークします。次のポイント (B バイトのパケットを使用) は、パケットがどのようにマークされるかを示しています。

- $B > Tp(t)$  の場合、パケットは指定レートに違反しているとマークされます。
- $B > Tc(t)$  の場合、パケットは指定レートを超過しているとマークされ、Tp(t) トークンバケットは  $Tp(t) = Tp(t) - B$  として更新されます。

これ以外の場合、パケットは指定レートに適合しているとマークされ、Tc(t) および Tp(t) のトークンバケットが次のように更新されます。

$$Tp(t) = Tp(t) - B$$

$$Tc(t) = Tc(t) - B$$

たとえば、CIR が 100 kbps、PIR が 200 kbps で、250 kbps のレートのデータストリームが2レートポリサーで到着した場合、パケットは次のようにマークされます。

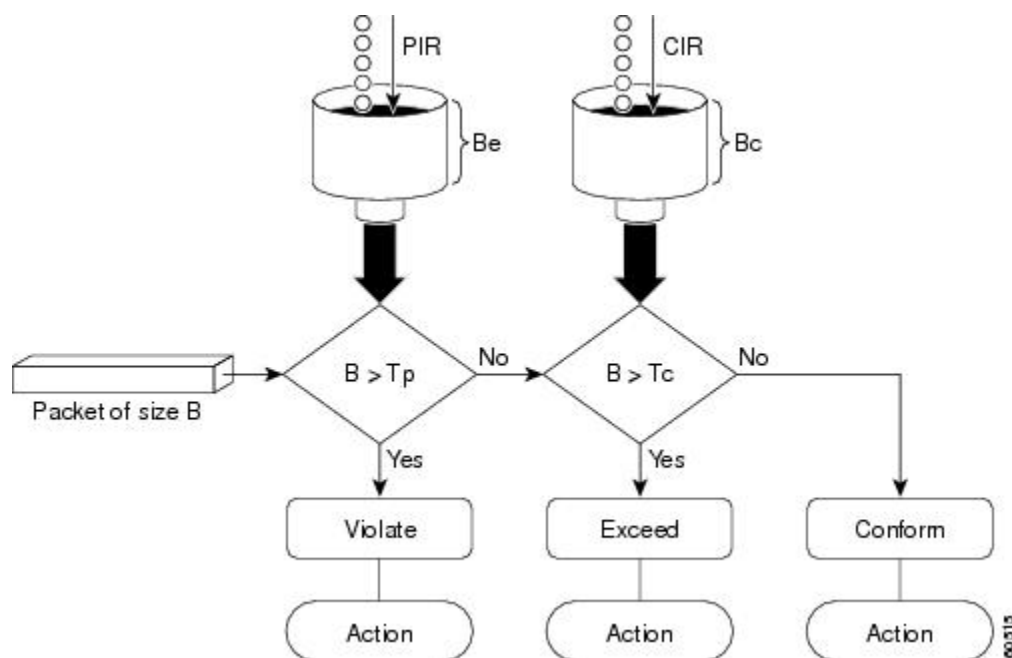
- 100 kbps は、レートに適合しているとマークされます。
- 100 kbps は、レートを超過しているとマークされます。

- 50 kbps は、レートに違反しているとマークされます。

### パケットのマーキングとアクションの割り当てのフローチャート

この図のフローチャートは、2レートポリサーによるパケットのマーキング方法と、パケットへの対応アクション（違反、超過、または適合）の割り当て方法を示したものです。

図 3: 2レートポリサーでのパケットのマーキングとアクションの割り当て



### Cisco 7600 シリーズ ルータ上の SIP および SPA の `set-cos-inner-transmit` アクションの使用

拡張 FlexWAN モジュールで MPB 機能を使用する場合や、Cisco 7600 シリーズ ルータの Cisco 7600 SIP-200 および Cisco 7600 SIP-400 の SPA で MPB 機能を使用する場合に、内部 CoS 値をポリシングアクションとしてマーキングすることをサポートするために、Cisco IOS Release 12.2(33)SRA で `set-cos-inner-transmit` キーワードアクションが導入されました。

このコマンドは、Cisco 7600 SIP-600 ではサポートされていません。

Cisco 7600 シリーズ ルータで、SIP によってサポートされる QoS と `police` コマンドの形式については、『Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide』を参照してください。

### 明示的なポリシング レートでのプライオリティの設定

次に、ネットワークの輻輳条件に関係なく、プライオリティトラフィックが 1000 kbps の認定レートに限定される例を示します。

```
Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police cir 1000000 conform-action transmit exceed-action drop
```



## 2 レート ポリシング機能

次の例では、500 kbps の平均認定レートと 1 Mbps のピーク レートにトラフィックを限定するために、2 レート トラフィック ポリシングがクラスに設定される例を示します。

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
Policy Map policy1
Class police
  police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

平均認定レート (500 kbps) に準拠するとしてマークされたトラフィックは、そのまま送信されます。500 kbps を超過しているものの 1 Mbps は超過していないとマークされたトラフィックは、IP precedence 2 でマークされてから送信されます。1 Mbps を超過しているとマークされたトラフィックはすべてドロップされます。バーストパラメータは 10000 バイトに設定されています。

次に、1.25 Mbps のトラフィックがポリサー クラスに送信 (「提供」) される例を示します。

```
Router# show policy-map interface serial3/0
Serial3/0
Service-policy output: policy1
Class-map: police (match all)
  148803 packets, 36605538 bytes
  30 second offered rate 1249000 bps, drop rate 249000 bps
Match: access-group 101
police:
  cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
  conformed 59538 packets, 14646348 bytes; action: transmit
  exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
  violated 29731 packets, 7313826 bytes; action: drop
  conformed 499000 bps, exceed 500000 bps violate 249000 bps
Class-map: class-default (match-any)
  19 packets, 1990 bytes
  30 seconds offered rate 0 bps, drop rate 0 bps
Match: any
```

2 レート ポリサーにより、500 kbps のトラフィックが指定レートに適合とマークされ、500 kbps のトラフィックが指定レートを超過とマークされ、250 kbps のトラフィックが指定レートに違反とマークされます。レートに適合しているとマークされたパケットはそのまま送信され、レートを超過しているとマークされたパケットは IP precedence

2でマークされてから送信されます。レートに違反しているとマークされたパケットはドロップされます。

### Cisco 7600 シリーズ ルータ上の SIP および SPA のアクションとしての内部 CoS 値の設定：例

次に、仮想 LAN (VLAN) 100 のすべてのトラフィックをクラス「vlan-inner-100」にフィルタリングし、vlan-inner-100 クラスのトラフィック シェーピング ポリシーを確立する QoS クラスの設定例を示します。このサービス ポリシーは、500 kbps の平均認定レートと 1 Mbps のピーク レートにトラフィックを制限し、内部 CoS 値を 3 に設定します。内部 CoS 値の設定はブリッジング機能を使用する場合に限ってサポートされるので、**bridge-domain** コマンドを使用して VLAN 100 にトラフィックをブリッジングする ATM SPA インターフェイスの相手先固定接続 (PVC) に、出力ポリシーとして適用されるサービス ポリシーも示します。

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end
```

#### 関連コマンド

コマンド	説明
<b>bridge-domain</b>	RFC 1483 ATM ブリッジングまたは RFC 1490 フレーム リレー ブリッジングで、ブリッジ処理された VLAN の ATM PVC またはフレーム リレー DLCI へのマップをイネーブルにします。
<b>police</b>	トラフィック ポリシングを設定します。
<b>policy-map</b>	1つ以上のインターフェイスに対応付けることができるポリシーマップを作成または修正し、サービス ポリシーを指定します。
<b>service-policy</b>	ポリシー マップを入力インターフェイスまたは出力インターフェイスに付加して、そのインターフェイスのサービス ポリシーとして使用します。
<b>showpolicy-map</b>	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。

コマンド	説明
<b>showpolicy-mapinterface</b>	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、すべてのサービスポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。

## police rate (コントロールプレーン)

コントロールプレーンを宛先とするトラフィックのトラフィック ポリシングを設定するには、QoS ポリシーマップ クラス コンフィギュレーション モードまたはコントロールプレーン コンフィギュレーション モードで、**policerate** コマンドを使用します。トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

```
police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps]
[peak-burst peak-burst-in-packets packets] [conform-action action]
no police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps]
[peak-burst peak-burst-in-packets packets] [conform-action action]
```

パケット/秒 (pps) の場合の構文

```
police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps]
[peak-burst peak-burst-in-packets packets]
no police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps]
[peak-burst peak-burst-in-packets packets]
```

バイト/秒 (bps) の場合の構文

```
police rate units bps [burst burst-in-bytes bytes] [peak-rate peak-rate-in-bps bps] [peak-burst
peak-burst-in-bytes bytes]
no police rate units bps [burst burst-in-bytes bytes] [peak-rate peak-rate-in-bps bps]
[peak-burst peak-burst-in-bytes bytes]
```

割合の構文

```
police rate percent percentage [burst ms ms] [peak-rate percent percentage] [peak-burst ms
ms]
no police rate percent percentage [burst ms ms] [peak-rate percent percentage] [peak-burst
ms ms]
```

Cisco 10000 シリーズ ルータの場合の構文

```
police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps]
[peak-burst peak-burst-in-packets packets] [conform-action action] [exceed-action action]
[violate-action action]
no police rate units pps [burst burst-in-packets packets] [peak-rate peak-rate-in-pps pps]
[peak-burst peak-burst-in-packets packets] [conform-action action] [exceed-action action]
[violate-action action]
```

SIP-400 搭載の Cisco 7600 シリーズ ルータの場合の構文

```
police rate units [{pps burst burst-in-packets packets|bps burst burst-in-bytes bytes}]
no police rate units [{pps burst burst-in-packets packets|bps burst burst-in-bytes bytes}]
```

構文の説明	<p><i>units</i></p> <p>ポリシング レートです。ポリシング レートが pps 単位で指定される場合、値の有効な範囲は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 500000 です。</li> <li>• Cisco SIP-400 搭載の Cisco 7600 シリーズ ルータ：有効な範囲は 1 ～ 100 です。</li> <li>• その他のプラットフォーム：有効な範囲は 1 ～ 2000000 です。</li> </ul> <p>ポリシング レートが bps 単位で指定される場合、値の有効な範囲は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Cisco SIP-400 搭載の Cisco 7600 シリーズ ルータ：有効な範囲は 80 ～ 8000 です。</li> <li>• その他のプラットフォーム：有効な範囲は 8000 ～ 128000000000 (128 Gbps) です。</li> </ul>
<b>pps</b>	トラフィックがポリシングされるレートの決定に使用されるパケット/秒 (pps) を指定します。
<b>burst</b> <i>burst-in-packets</i> <b>packets</b>	<p>(任意) トラフィック ポリシングに使用されるバースト レートをパケット単位で指定します。値の有効な範囲は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 25000 です。</li> <li>• Cisco SIP-400 搭載の Cisco 7600 シリーズ ルータ：有効な範囲は 1 ～ 1000 です。</li> <li>• その他のプラットフォーム：有効な範囲は 1 ～ 512000 です。</li> </ul>
<b>peak-rate</b> <i>peak-rate-in-pps</i> <b>pps</b>	<p>(任意) トラフィック ポリシングと PIR の計算に使用される最大情報レート (PIR) を指定します。値の有効な範囲は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 500000 です。</li> <li>• その他のプラットフォーム：有効な範囲は 1 ～ 512000 です。</li> </ul>
<b>peak-burst</b> <i>peak-burst-in-packets</i> <b>packets</b>	<p>(任意) トラフィック ポリシングに使用されるピーク バースト値をパケット単位で指定します。値の有効な範囲は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Cisco 10000 シリーズ ルータ：有効な範囲は 1 ～ 25000 です。</li> <li>• その他のプラットフォーム：有効な範囲は 1 ～ 512000 です。</li> </ul>
<b>bps</b>	(任意) トラフィックがポリシングされるレートの決定に使用されるビット/秒 (bps) を指定します。

<b>burst</b> <i>burst-in-bytes</i> <b>bytes</b>	(任意) トラフィック ポリシングに使用されるバースト レートをバイト単位で指定します。値の有効な範囲は次のとおりです。  <ul style="list-style-type: none"> <li>• Cisco SIP-400 搭載の Cisco 7600 シリーズルータ：有効な範囲は 100 ~ 10000 です。</li> <li>• その他のプラットフォーム：有効な範囲は 1000 ~ 2000000000 (2 Gb) です。</li> </ul>
<b>peak-rate</b> <i>peak-rate-in-bps</i> <b>bps</b>	(任意) ピーク レートのピーク レート値をバイト単位で指定します。有効な範囲は 1000 ~ 512000000 です。
<b>peak-burst</b> <i>peak-burst-in-bytes</i> <b>bytes</b>	(任意) トラフィック ポリシングに使用されるピーク バースト値をバイト単位で指定します。有効な範囲は 1000 ~ 2000000000 (2 Gb) です。
<b>percent</b>	トラフィックがポリシングされるレートを決定するために使用されるインターフェイス帯域幅のパーセンテージを指定します。
<i>percentage</i>	帯域幅のパーセンテージです。有効な範囲は 1 ~ 100 です。
<b>burst</b> <i>ms</i> <b>ms</b>	(任意) トラフィック ポリシングに使用されるバースト レートをミリ秒単位で指定します。有効な範囲は 1 ~ 2000 です。
<b>peak-rate</b> <i>percent</i> <i>percentage</i>	(任意) PIR の決定に使用されるインターフェイス帯域幅のパーセンテージを指定します。有効な範囲は 1 ~ 100 です。
<b>peak-burst</b> <i>ms</i> <b>ms</b>	(任意) トラフィック ポリシングに使用されるピークバースト レートをミリ秒単位で指定します。有効な範囲は 1 ~ 2000 です。
<b>conform-action</b> <i>action</i>	(任意) ポリシングレートリミットに適合するパケットで実行されるアクションを指定します。指定可能なアクションについては、「使用上のガイドライン」セクションを参照してください。
<b>exceed-action</b> <i>action</i>	(任意) レートリミットを超過するパケットで実行されるアクションを指定します。指定可能なアクションについては、「使用上のガイドライン」セクションを参照してください。
<b>violate-action</b> <i>action</i>	(任意) ポリシングレートリミットを継続的に超過するパケットで実行されるアクションを指定します。指定可能なアクションについては、「使用上のガイドライン」セクションを参照してください。

コマンド デフォルト 無効

コマンド モード

QoS ポリシーマップ クラス コンフィギュレーション (config-pmap)

コントロールプレーン コンフィギュレーション (config-cp)

コマンド履歴	リリース	変更箇所
	12.3(7)T	このコマンドが導入されました。
	12.2(18)SXD1	このコマンドが変更されました。このコマンドのサポートが Supervisor Engine 720 に追加されました。
	12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
	12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
	12.2(31)SB2	このコマンドが Cisco IOS Release 12.2(31)SB2 に統合され、Cisco 10000 シリーズ ルータに実装されました。
	12.2(33)SRC	このコマンドが、Cisco 7600 SIP-400 での CoPP 拡張をサポートするように変更されました。
	15.0(1)SY	このコマンドが変更されました。 <i>burst-in-bytes</i> 、 <i>peak-burst-in-bytes</i> 、および <i>units</i> 引数の最大値が増えました。

### 使用上のガイドライン

パケット/秒 (pps)、バイト/秒 (bps)、またはインターフェイス帯域幅のパーセンテージでコントロールプレーンを宛先とするトラフィックを制限するには、**police rate** コマンドを使用します。

**policerate** コマンドが発行される場合で、レートが指定されていない場合、コントロールプレーンを宛先とするトラフィックは bps に基づいてポリシングされます。

次の表に、*action* 引数で指定できるアクションのリストを示します。

表 3: *action* 引数の値

アクション	説明
<b>drop</b>	パケットをドロップします。これは、認定ポリシングレートを超過するか、認定ポリシングレートに違反するトラフィックに対するデフォルトアクションです。
<b>set-clp-transmit value</b>	ATM セルで、ATM セル損失率優先度 (CLP) ビットを設定します。有効な値は、0 または 1 です。
<b>set-discard-class-transmit value</b>	パケットの廃棄クラス属性を設定し、設定した新しい廃棄クラスでパケットを送信します。有効な値は 0 ~ 7 です。
<b>set-dscp-transmit value</b>	IP Diffserv コードポイント (DSCP) の値を設定し、設定した新しい IP DSCP 値でパケットを送信します。有効な値は 0 ~ 63 です。
<b>set-dscp-tunnel-transmit value</b>	トンネルパケット DSCP を再書き込みし、新しい DSCP の値でパケットを送信します。有効な値は 0 ~ 63 です。

アクション	説明
<b>set-frde-transmit</b> <i>value</i>	フレームリレーフレーム上のフレームリレー廃棄適格 (DE) ビットを 0 から 1 に設定し、1 に設定した DE ビットが含まれるパケットを送信します。
<b>set-mpls-exp-imposition-transmit</b> <i>value</i>	強制ラベルのヘッダーでマルチプロトコル ラベル スイッチング (MPLS) の EXP ビットを設定し、設定した新しい MPLS EXP ビット値でパケットを送信します。有効な値は 0 ~ 7 です。
<b>set-mpls-exp-transmit</b> <i>value</i>	入力インターフェイス、出力インターフェイス、または両方の MPLS ラベルヘッダーで、MPLS EXP フィールドの値を設定します。有効な値は 0 ~ 7 です。
<b>set-prec-transmit</b> <i>value</i>	IP precedence を設定し、設定した新しい IP precedence 値でパケットを送信します。有効な値は 0 ~ 7 です。
<b>set-prec-tunnel-transmit</b> <i>value</i>	トンネルパケットの IP precedence を設定し、設定した新しい IP precedence 値でパケットを送信します。有効な値は 0 ~ 7 です。
<b>set-qos-transmit</b> <i>value</i>	QoS グループを設定し、設定した新しい QoS グループ値でパケットを送信します。有効な値は 0 ~ 63 です。
<b>transmit</b>	パケットを送信します。パケットは変更されません。

## 例

次に、ポリシングレートリミットに適合するパケットで実行されるアクションを設定する例を示します。

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
Router(config)# access-list 140 permit tcp any any eq telnet
Router(config)# class-map match-any pps-1
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map copp-pps
Router(config-pmap)# class pps-1
Router(config-pmap)# police rate 10000 pps burst 100 packets peak-rate 10100 pps peak-burst
150 packets conform-action transmit
Router(config-cmap)# exit
Router(config)# control-plane
Router(config-cp)# service-policy input copp-pps
Router(config-cp)# exit
```

## 関連コマンド

コマンド	説明
<b>policy-map</b>	1 つ以上のインターフェイスに対応付けることができるポリシー マップを作成または修正し、サービス ポリシーを指定します。



コマンド	説明
<b>showpolicy-map</b>	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。

## police rate pdp

ポリシング レートを使用してパケット データ プロトコル (PDP) トラフィック ポリシングを設定するには、ポリシーマップ クラス コンフィギュレーション モードまたはポリシーマップ クラス ポリシング コンフィギュレーション モードで、**policeratepdp** コマンドを使用します。PDP トラフィック ポリシングを設定から削除するには、このコマンドの **no** 形式を使用します。

```
police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]] conform-action action
exceed-action action [violate-action action]
no police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]] conform-action action
exceed-action action [violate-action action]
```

### 構文の説明

<b>burst bytes</b>	(任意) 認定バーストサイズをバイト単位で指定します。サイズは、使用するインターフェイスとプラットフォームによって異なります。有効な範囲は 1000 ~ 2000000000 (2 Gb) です。デフォルトは 1500 です。
<b>peak-ratepdp</b>	(任意) PDP トラフィックのポリシング時に、セッションのピーク レートが考慮されるように指定します。
<b>peak-burst bytes</b>	(任意) ピークバーストサイズをバイト単位で指定します。サイズは、使用するインターフェイスとプラットフォームによって異なります。有効な範囲は 1000 ~ 2000000000 (2 Gb) です。デフォルトは 2500 です。
<b>conform-action</b>	適合バーストを下回るレートのパケットに対して実行するアクションを指定します。
<b>exceed-action</b>	適合バーストを超えるレートのパケットに対して実行するアクションを指定します。
<b>violate-action</b>	(任意) 適合バーストを違反するレートのパケットに対して実行するアクションを指定します。
<b>action</b>	パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 <ul style="list-style-type: none"> <li>• <b>drop</b> : パケットをドロップします。</li> <li>• <b>set-dscp-transmit new-dscp-value</b> : IP DiffServ コードポイント (DSCP) 値を設定して、新しい IP DSCP 値でパケットを送信します。</li> <li>• <b>set-prec-transmit new-prec-value</b> : IP プレシデンスを設定して、その新しい IP プレシデンス値でパケットを送信します。</li> <li>• <b>transmit</b> : パケットをそのまま無変更で送信します。</li> </ul>

コマンド デフォルト PDP トラフィック ポリシングは無効になっています。

## コマンドモード

ポリシーマップクラス コンフィギュレーション (config-pmap-c)  
 ポリシーマップクラス ポリシング コンフィギュレーション (config-pmap-c-police)

## コマンド履歴

リリース	変更箇所
12.3(8)XU	このコマンドが導入されました。
12.3(11)YJ	このコマンドが、Cisco IOS Release 12.3(11)YJ に組み込まれました。
12.3(14)YQ	このコマンドが、Cisco IOS Release 12.3(14)YQ に組み込まれました。
12.4(9)T	このコマンドが Cisco IOS Release 12.4(9)T に統合されました。
15.0(1)SY	このコマンドが変更されました。bytes 引数の最大値が増えました。

## 使用上のガイドライン

**policeratepdp** コマンドは、Cisco IOS Release 12.4(9)T で使用できる Flow-Based QoS for GGSN 機能に含まれています。

Flow-Based QoS for GGSN 機能は、Gateway General Packet Radio Service (GPRS) Support Node (GGSN) 専用に設計されています。

### PDP ごとのポリシング

Flow-Based QoS for GGSN 機能には、PDP ごとのポリシング (セッションベースのポリシング) が含まれています。

PDP ごとのポリシングは Gateway GPRS Support Node トラフィック コンディショナ (3G TS 23.107) の機能の 1 つで、特定の PDP コンテキストの Gi インターフェイス上で受信されるトラフィックの最大レートを制限するために使用できます。

このポリシング機能は、PDP コンテキストにコールアドミッション制御 (CAC) ネゴシエーションデータ レートを適用します。輻輳が発生した場合に、不適合トラフィックをドロップするか、または不適合トラフィックを優先ドロップとしてマーキングするように GGSN を設定できます。

使用されるポリシングパラメータは、次のように PDP コンテキストに依存します。

- R99 Quality of Service (QoS) プロファイルを持つ GTPv1 PDP の場合、CAC ネゴシエーション QoS プロファイルの最大ビットレート (MBR) および保証ビットレート (GBR) パラメータが使用されます。非リアルタイムトラフィックの場合、MBR パラメータだけが使用されます。
- R98 QoS プロファイルを持つ GTPv1 PDP および GTPv0 PDP の場合、CAC ネゴシエーション QoS ポリシーのピーク スループットパラメータが使用されます。

PDP ごとのポリシングを設定する前に、次の点に注意してください。

- GGSN で、Universal Mobile Telecommunications System (UMTS) QoS マッピングが有効になっている必要があります。

- Gi インターフェイスで、Cisco Express Forwarding (CEF) が有効になっている必要があります。
- ダウンリンク トラフィック用に PDP ごとのポリシングがサポートされるのは、Gi インターフェイスにおいてだけです。
- PDP コンテキストの初期パケットは、ポリシングされません。
- 階層型ポリシングはサポートされません。
- フローベースのポリシングを Access Point Network (APN) にアタッチされているポリシーマップ内で設定した場合、**showpolicy-mapapn** コマンドによって、ポリシングの前に受信されたパケットの総数が表示され、ポリシングカウンタは表示されません。



(注) **showpolicy-mapapn** コマンドによって表示されたポリシングカウンタをクリアするには、**cleargpraccess-pointstatisticsaccess-point-index** コマンドを使用します。

- APN に適用されているサービスポリシーは変更できません。サービスポリシーを変更するには、APN からサービスポリシーを削除し、サービスポリシーを変更してから再適用します。
- それぞれに **matchflowpdp** が設定され、異なる DiffServ コードポイント (DSCP) 値が指定されている複数のクラスマップは、DSCP が信頼されている (**gprsumts-qosdscpunmodified** グローバル コンフィギュレーション コマンドが GGSN 上で設定されていない) 場合のみ、ポリシーマップでサポートされます。

### 詳細情報

GGSN の詳細と、Flow-Based QoS for GGSN 機能の設定手順については、『*Cisco GGSN Release 6.0 Configuration Guide*』、Cisco IOS Release 12.4(2)XB を参照してください。



(注) Flow-Based QoS for GGSN 機能を設定するには、「Configuring Per-PDP Policing」セクションの手順に従います。

**showpolicy-mapapn** コマンド、**gprsumts-qosdscpunmodified** コマンド、**cleargpraccess-pointstatistics** コマンド、およびその他の GGSN 固有のコマンドの詳細については、『*Cisco GGSN Release 6.0 Command Reference*』、Cisco IOS Release 12.4(2)XB を参照してください。

次に、APN に適用される PDP ごとのポリシングのポリシーマップの例を示します。

```
class-map match-all class-pdp
  match flow pdp
  !
  ! Configures a policy map and attaches this class map to it.
policy-map policy-gprs
```

```

class class-pdp
  police rate pdp
    conform-action set-dscp-transmit 15
    exceed-action set-dscp-transmit 15
    violate-action drop
! Attaches the policy map to the APN.

gprs access-point-list gprs
  access-point 1
    access-point-name static
    service-policy input policy-gprs

```

## 関連コマンド

コマンド	説明
<b>cleargprsaccess-pointstatistics</b>	GGSN 上の特定のアクセス ポイントまたはすべてのアクセス ポイントの統計カウンタをクリアします。
<b>gprsumts-qosdscpunmodified</b>	加入者データグラムが、DSCP を変更することなしに GTP パスを介して転送されるように指定します。
<b>matchflowpdp</b>	PDP フローを、クラス マップ内の一致基準として指定します。
<b>showpolicy-mapapn</b>	APN にアタッチされているすべての入力および出力ポリシーの統計情報と設定情報を表示します。

## policy-map

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、サービス ポリシーを指定する1つまたは複数のインターフェイスにアタッチできるポリシーマップを作成または変更するには、グローバル コンフィギュレーションモードで **policy-map** コマンドを使用します。ポリシーマップを削除するには、このコマンドの **no** 形式を使用します。

**Cisco 10000** および **Cisco 7600** シリーズ ルータ以外でサポートされるプラットフォーム

```
policy-map [type {stack|access-control|port-filter|queue-threshold|logging log-policy}]  
policy-map-name
```

```
no policy-map [type {stack|access-control|port-filter|queue-threshold|logging log-policy}]  
policy-map-name
```

**Cisco 10000** シリーズ ルータ

```
policy-map [type {control|service}] policy-map-name
```

```
no policy-map [type {control|service}] policy-map-name
```

**Cisco CMTS**、および **7600** シリーズ ルータ

```
policy-map [type {class-routing ipv4 unicast unicast-name|control control-name|service  
service-name}] policy-map-name
```

```
no policy-map [type {class-routing ipv4 unicast unicast-name|control control-name|service  
service-name}] policy-map-name
```

### 構文の説明

<b>type</b>	(任意) ポリシーマップタイプを指定します。
<b>stack</b>	(任意) 該当するプロトコルスタックで検索する完全一致パターンを決定します。
<b>access-control</b>	(任意) Flexible Packet Matching (FPM) 機能用のポリシーマップをイネーブルにします。
<b>port-filter</b>	(任意) ポートフィルタ機能用のポリシーマップをイネーブルにします。
<b>queue-threshold</b>	(任意) キューのしきい値機能用のポリシーマップをイネーブルにします。
<b>logging</b>	(任意) コントロールプレーンのパケット ロギング機能用のポリシーマップをイネーブルにします。
<i>log-policy</i>	(任意) コントロールプレーン ロギングのログ ポリシーのタイプです。
<i>policy-map-name</i>	ポリシーマップ名です。
<b>control</b>	(任意) 制御ポリシーマップを作成します。
<i>control-name</i>	制御ポリシーマップの名前です。
<b>service</b>	(任意) サービス ポリシーマップを作成します。

<i>service-name</i>	ポリシー マップ サービスの名前です。
<b>class-routing</b>	クラス ルーティング ポリシー マップを設定します。
<b>ipv4</b>	クラス ルーティング IPv4 ポリシー マップを設定します。
<b>unicast</b>	クラス ルーティング IPv4 ユニキャスト ポリシー マップを設定します。
<i>unicast-name</i>	ユニキャスト ポリシー マップ名です。

コマンド デフォルト      ポリシー マップは設定されません。

コマンド モード          グローバル コンフィギュレーション (config)

コマンド履歴

リリース	変更箇所
12.0(5)T	このコマンドが導入されました。
12.4(4)T	このコマンドが変更されました。Flexible Packet Matching をサポートするために、 <b>type</b> キーワードと <b>access-control</b> キーワードが追加されました。コントロールプレーン保護機能をサポートするために <b>port-filter</b> キーワードと <b>queue-threshold</b> キーワードが追加されました。
12.4(6)T	このコマンドが変更されました。コントロールプレーンパケットロギングをサポートするために、 <b>logging</b> キーワードが追加されました。
12.2(31)SB	このコマンドが変更されました。Cisco 10000 シリーズ ルータをサポートするために、 <b>control</b> キーワードと <b>service</b> キーワードが追加されました。
12.2(18)ZY	このコマンドが変更されました。 <ul style="list-style-type: none"> <li>• <b>type</b> キーワードと <b>access-control</b> キーワードが、Supervisor 32/Programmable Intelligent Services Accelerator (PISA) エンジンが搭載されている Catalyst 6500 シリーズ スイッチの Cisco IOS リリース 12.2(18)ZY に統合されました。</li> <li>• このコマンドが、Supervisor 32/PISA エンジンが搭載されている Catalyst 6500 シリーズ スイッチの Network-Based Application Recognition (NBAR) 機能を拡張するため、変更されました。</li> </ul>
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
12.2(33)SRC	このコマンドが変更されました。このコマンドのサポートが Cisco 7600 シリーズ ルータに実装されました。

リリース	変更箇所
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE Release 2.1 に統合され、Cisco ASR 1000 シリーズ ルータに実装されました。
12.2(33)SCF	このコマンドが、Cisco IOS リリース 12.2(33)SCF に統合されました。

## 使用上のガイドライン

一致基準がクラスマップに定義されているクラスのポリシーを設定する前に、作成、追加、または変更するポリシーマップの名前を指定するには、**policy-map** コマンドを使用します。**policy-map** コマンドにより、ポリシーマップ コンフィギュレーションモードが開始されます。このモードでは、ポリシーマップのクラスポリシーを設定または変更することができます。

クラスポリシーをポリシーマップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。**class-map** コマンドと **match** コマンドを使用して、クラスの一貫基準を設定します。設定できるクラスマップは最大 64 個のため、Cisco 7600 システム上の Quality of Service (QoS) クラスマップ用に示されている場合を除いて、ポリシーマップに 64 個を超えるクラスポリシーを含めることはできません。



- (注) Cisco 7600 シリーズ ルータの QoS クラス マップでは、この制限はクラス マップが 1024 個、ポリシー マップのクラスが 256 個です。

ATM 設定セル損失率優先度 (CLP) ビット QoS を含むポリシーマップは、PPP over X (PPPoX) セッションにアタッチできません。このポリシーマップは、**set atm-clp** コマンドを指定しない場合のみ適用できます。

1つのポリシーマップは、同時に複数のインターフェイスに付加できます。特に注意が示されている場合以外では、ポリシーマップをインターフェイスに付加しようとするときに、インターフェイス上の使用可能な帯域幅が、ポリシーマップを構成しているクラスポリシーに必要な合計帯域幅に満たない場合、付加は拒否されます。このとき、ポリシーマップが他のインターフェイスにすでにアタッチされている場合、そのインターフェイスからマップが削除されます。



- (注) この制限は、Session Initiation Protocol (SIP) -400 アクセス対向ラインカードを搭載した Cisco 7600 シリーズ ルータには適用されません。

適用されたポリシーマップ内のクラスポリシーを変更する場合、常にクラスベース均等化キューイング (CBWFQ) が通知され、新しいクラスは CBWFQ システムのポリシーマップの一部としてインストールされます。





- (注) サブスクリバプロファイルを介したポリシー マップのインストールは、サポートされません。サポートされていないポリシーマップを設定した場合で、多数のセッションがある場合、同等数の多数のメッセージがコンソールに表示されます。たとえば、32,000 のセッションがある場合、32,000 のメッセージが 9,600 ボーでコンソールに表示されます。

### クラス キュー (Cisco 10000 シリーズ ルータのみ)

Performance Routing Engine (PRE) 2 では、ポリシー マップで 31 個のクラス キューを設定できます。

ポリシー マップでは、PRE3 により 1 つのプライオリティ レベル 1 のキュー、1 つのプライオリティ レベル 2 のキュー、12 個のクラス キュー、および 1 つのデフォルト キューを設定できます。

### 制御ポリシー (Cisco 10000 シリーズ ルータのみ)

制御ポリシーは、指定されたイベントと条件に対応してシステムが実行するアクションを定義します。

制御ポリシーは 1 つ以上の制御ポリシー ルールで作成されます。制御ポリシー ルールは、制御クラスと 1 つ以上のアクションを関連付けたものです。制御クラスは、アクションが実行される前に満たされる必要がある条件を定義します。

制御ポリシーの定義には次の 3 つの手順があります。

1. **class-maptypecontrol** コマンドを使用して、1 つ以上の制御クラス マップを作成します。
2. **policy-maptypecontrol** コマンドを使用して、制御ポリシー マップを作成します。

制御ポリシー マップには 1 つ以上の制御ポリシー ルールが含まれます。制御ポリシー ルールは、制御クラス マップを 1 つ以上のアクションに関連付けます。アクションに番号が付けられ、順に実行されます。

1. **service-policytypecontrol** コマンドを使用して、コンテキストに制御ポリシーマップを適用します。

### サービス ポリシー (Cisco 10000 シリーズ ルータのみ)

サービス ポリシー マップとサービス プロファイルには、トラフィック ポリシーとその他の機能のコレクションが含まれています。トラフィック ポリシーとは、どのセッショントラフィックにどの機能を適用するかを定義するものです。また、サービス ポリシー マップまたはサービス プロファイルには、ネットワーク転送ポリシーという、セッションデータパケットをネットワークに転送する方法を指定する、特定のタイプのトラフィック ポリシーが含まれています。

### ポリシー マップの制限 (Catalyst 6500 シリーズ スイッチのみ)

Cisco IOS Release 12.2(18)ZY には、Supervisor 32/PISA エンジンが搭載された Catalyst 6500 シリーズ スイッチ用のソフトウェアが含まれています。このリリースおよびプラットフォームには、ポリシー マップと **match** コマンドの使用に関する次の制限があります。

- ポリシー マップがインターフェイスにアタッチされている場合、既存のポリシー マップを変更することはできません。ポリシー マップを変更するには、**service-policy** コマンドの **no** 形式を使用して、インターフェイスからポリシー マップを削除します。
- ポリシー マップにはトラフィック クラスが含まれています。トラフィック クラスには、プロトコルタイプまたはアプリケーションに基づいてパケットを照合する（およびグループにまとめる）ために使用できる、1つ以上の **match** コマンドが含まれています。必要に応じて任意の数のトラフィック クラスを作成できます。ただし、次の制限が適用されます。
  - 1つのトラフィック クラスは、最大 8 個のプロトコルまたはアプリケーションに一致するように設定できます。
  - 複数のトラフィック クラスは、累積で最大 95 個のプロトコルまたはアプリケーションに一致するように設定できます。

#### 例

次に、「**policy1**」と呼ばれるポリシー マップの作成方法と、そのポリシー マップに含まれる 2 つのクラス ポリシーの設定方法の例を示します。「**class1**」という名前のクラス ポリシーにより、アクセスコントロールリスト (ACL) 136 に一致するトラフィックのためのポリシーが指定されます。2 つ目のクラスは、設定されている一致基準を満たさないパケットが誘導されるデフォルト クラスです。

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
  match access-group 136
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1
class class1
  bandwidth 2000
  queue-limit 40
class class-default
  fair-queue 16
  queue-limit 20
```

次に、「**policy9**」という名前のポリシー マップの作成方法と、そのマップに属する 3 つのクラス ポリシーの設定方法の例を示します。これらのクラスのうち、2 つのクラスにより、番号付き ACL またはインターフェイス名のいずれかに基づいた一致基準を指定するクラス マップのクラスに対し、ポリシーが指定されます。また、1 つのクラスにより、設定されている一致基準を満たさないパケットが誘導される、「**class-default**」という名前のデフォルト クラスに対し、ポリシーが指定されます。

```
policy-map policy9

class acl136
  bandwidth 2000
  queue-limit 40
```

```
class ethernet101
  bandwidth 3000
  random-detect exponential-weighting-constant 10
class class-default
  fair-queue 10
  queue-limit 20
```

次に、セッションの開始時に QoS サービスを開始するように設定されたモジュラ QoS コマンドライン インターフェイス (MQC) ポリシー マップの例を示します。

```
Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1
  service-policy type service name QoS_Service
Router(config-control-policymap-class-control)# end
```

### Cisco 10000 シリーズ ルータのみの例

次の例は、「rule4」という名前の制御ポリシーマップの設定を示しています。制御ポリシーマップ rule4 には、「class3」という名前の制御クラスと、ネットワーク アクセス サーバ (NAS) ポート ID を使用してサブスライバを承認するためのアクションを関連付ける、1つのポリシールールが含まれています。制御ポリシーマップをグローバルに適用するために、**service-policytypecontrol** コマンドが使用されています。

```
class-map type control match-all class3
  match vlan 400
  match access-type pppoe
  match domain cisco.com
  available nas-port-id
!
policy-map type control rule4
  class type control class3
  authorize nas-port-id
!
service-policy type control rule4
```

次の例は、「redirect-profile」という名前のサービスポリシーマップの設定を示しています。

```
policy-map type service redirect-profile
  class type traffic CLASS-ALL
  redirect to group redirect-sg
```

### Cisco CMTS ルータの例

次に、802.1p ドメインのポリシー マップを定義する例を示します。

```
enable
configure terminal
policy-map cos7
  class cos7
```

```
set cos 2
end
```

次に、MPLS ドメインのポリシー マップを定義する例を示します。

```
enable
configure terminal
policy-map exp7
class exp7
set mpls experimental topmost 2
end
```

## 関連コマンド

Command	Description
<b>bandwidth(policy-mapclass)</b>	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
<b>class(policy-map)</b>	ポリシーを作成または変更するクラスの名前を指定し、ポリシーを設定する前にそのデフォルトクラスを指定します。
<b>classclass-default</b>	帯域幅が設定または変更されるデフォルトクラスを指定します。
<b>class-map</b>	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。
<b>fair-queue(class-default)</b>	デフォルトクラス ポリシーの一部として <b>class-default</b> クラスで使用するために予約するダイナミック キューの数を指定します。
<b>matchaccess-group</b>	指定した ACL をベースにクラスマップに対して一致基準を設定します。
<b>queue-limit</b>	ポリシー マップで設定されているクラス ポリシー用にキューで維持できるパケットの最大数の指定または修正を行います。
<b>random-detect(interface)</b>	WRED または DWRED をイネーブルにします。
<b>random-detectexponential-weighting-constant</b>	キューの平均サイズ計算のための WRED および DWRED 指数加重係数を設定します。
<b>random-detectservice-policyprecedence</b>	特定の IP precedence に対する WRED パラメータと DWRED パラメータを設定します。
<b>service-policy</b>	インターフェイスまたは VC のサービスポリシーとして使用されるポリシー マップを入力インターフェイスまたは VC (あるいは出力のインターフェイスまたは VC) にアタッチします。

Command	Description
<b>set atm-clpprecedence</b>	ポリシーマップを設定するときのATMCLPビットを設定します。

## policy-map copp-peruser

コントロールプレーン ポリシングおよび保護 (CoPP) のユーザごとのポリシーを定義するポリシー マップを作成するには、グローバル コンフィギュレーション モードで **policy-mapcopp-peruser** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

**policy-map copp-peruser**  
**no policy-map copp-peruser**

### 構文の説明

このコマンドにはキーワードまたは引数はありません。

### コマンド デフォルト

ポリシー マップは設定されません。

### コマンド モード

グローバル設定

### コマンド履歴

リリース	変更箇所
12.2(33)SRB	このコマンドが導入されました。

### 使用上のガイドライン

CoPP を設定するときに、このコマンドを使用して CoPP のユーザごとのポリシーを作成します。

### 例

次の例では、CoPP のユーザごとのポリシー マップを作成します。

```
Router(config)# policy-map copp-peruser
Router(config-pmap)# class arp-peruser
Router(config-pmap-c)# police rate 5 pps burst 50 packets
Router(config-pmap-c)# class dhcp-peruser
Router(config-pmap-c)# police rate 10 pps burst 100 packets
```

### 関連コマンド

コマンド	説明
<b>class-maparp-peruser</b>	ARP のユーザごとのパケットの照合に使用するクラス マップを作成します。
<b>matchsubscriberaccess</b>	ポリシー マップに対する加入者アクセス トラフィックに一致します。

# precedence

仮想回線（VC）バンドルへの割り当て、つまりそのバンドルのすべての VC メンバーへの適用が可能な VC クラスに優先レベルを設定するには、VC-class コンフィギュレーションモードで **precedence** コマンドを使用します。VC クラスから優先レベルを削除するには、このコマンドの **no** 形式を使用します。

バンドルの VC または相手先固定接続（PVC）メンバーの優先レベルを設定するには、ATM VC バンドル メンバーの **bundle-VC** コンフィギュレーションモード、または ATM 相手先選択接続（SVC）の **SVC-bundle-member** コンフィギュレーションモードで **precedence** を使用します。VC または PVC から優先レベルを削除するには、このコマンドの **no** 形式を使用します。

**precedence** [{*other**range*}]

**no precedence**

構文の説明	<b>other</b>	(任意) 明示的には設定されない、0～7の範囲の任意の優先レベルです。
	<i>range</i>	(任意) 0～7の数値で指定される単一の優先レベル、またはハイフンで連結した範囲で指定される優先レベルの範囲です。

コマンド デフォルト デフォルトの設定は、**other** で、明示的に設定されない、0～7の範囲の任意の優先レベルになります。

## コマンドモード

VC-class コンフィギュレーション (VC クラスの場合)

Bundle-VC コンフィギュレーション (ATM VC バンドル メンバーの場合)

SVC-bundle-member コンフィギュレーション (ATM SVC の場合)

コマンド履歴	リリース	変更箇所
	11.1(22)CC	このコマンドが導入されました。
	12.0(3)T	このコマンドが、Cisco IOS Release 12.0(3)T に統合されました。バンドルの VC メンバーの優先レベルを設定できるように拡張されました。
	12.2(4)T	このコマンドが、SVC-bundle-member コンフィギュレーションモードで使用できるようになりました。
	12.0(23)S	このコマンドが、Cisco 12000 シリーズ インターネット ルータで 8 ポートの OC-3 STM-1 ATM ライン カードの VC-class および bundle-vc コンフィギュレーションモードで使用できるようになりました。
	12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更箇所
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

## 使用上のガイドライン

VC または PVC バンドル メンバーに優先レベルを割り当てると、IP precedence レベルを複数の VC/PVC バンドルメンバーに分散できるため、差別化サービスを作成できます。単一の優先レベルまたはレベルの範囲をバンドル内の個々の VC/PVC にマップできます。これにより、バンドル内の VC/PVC がさまざまな優先レベルによってマーク付けされたパケットを伝送できます。または、**precedence other** コマンドを使用して、他の VC/PVC については、明示的に設定されない優先レベルにマーク付けされたトラフィックを VC/PVC によって伝送できることを示します。**precedence other** コマンドを使用して設定可能なバンドル内の VC/PVC は 1 つのみです。この VC/PVC は、デフォルトと見なされます。

VC-class コンフィギュレーション モードでこのコマンドを使用するには、まずグローバル コンフィギュレーション モードで **vc-class atm** コマンドを入力します。**precedence** コマンドを含む VC クラスがスタンドアロン VC (バンドルメンバーではない VC) に付加されている場合、このコマンドは効果がありません。

**precedence** コマンドを使用して **bundle-VC** コンフィギュレーション モードで個々のバンドルメンバーを設定するには、まず **bundle** コマンドを入力して、設定対象の VC メンバーを追加または変更するバンドルにバンドル コンフィギュレーション モードを指定します。その後、**pvc-bundle** コマンドを使用して、作成または変更する VC を指定し、バンドル VC コンフィギュレーション モードにします。

VC バンドルの VC は、次の設定継承ガイドラインに従います (2 番目に高い優先順位の順にリストされています)。

- bundle-VC モードの VC 設定
- バンドル モードのバンドル コンフィギュレーション (および、割り当てられた VC-class コンフィギュレーションの影響)
- サブインターフェイス モードのサブインターフェイス設定

## 例

次は **precedence** コマンドを含む「control-class」という名前のクラスの設定例です。このコマンドは、バンドルに適用すると、そのバンドルのすべての VC メンバーが IP precedence レベル 7 のトラフィックを伝送するように設定します。ただし、このバンドルの VC メンバーは **precedence** コマンドを使用して、**bundle-VC** レベルで個々に設定される場合があることに注意してください。

```
vc-class atm control-class
  precedence 7
```

次は PVC 401 (名前は「control-class」) の設定例で、4 ~ 2 の範囲の IP precedence レベルを持ったトラフィックを伝送し、VC-class コンフィギュレーションを使用した VC の優先レベル マッピング設定を上書きします。



```
pvc-bundle control-class 401
precedence 4-2
```

## 関連コマンド

Command	Description
<b>bump</b>	VC バンドルに割り当てることができる VC クラスのバンピン グルールを設定します。
<b>bundle</b>	バンドルを作成するか、または既存のバンドルを修正してバンドル コンフィギュレーションモードを開始します。
<b>class-vc</b>	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
<b>dscp(frame-relayvc-bundle-member)</b>	特定のフレーム リレー PVC バンドル メンバーに対して DSCP 値を指定します。
<b>matchprecedence</b>	IP precedence 値を一致基準として識別します。
<b>mplsexperimental</b>	VC バンドルへのマッピング、つまりそのバンドルのすべての VC メンバーに適用する、VC クラスの MPLS EXP ビット値を設定します。
<b>protect</b>	VC バンドル メンバーへのアプリケーションの保護されたグループまたは保護された VC ステータスを持つ VC クラスを設定します。
<b>pvc-bundle</b>	バンドルに対してバンドルのメンバーとして PVC を追加し、PVC バンドル メンバーを設定するために bundle-vc コンフィギュレーションモードに入ります。
<b>pvc</b>	ATM PVC に名前を割り当て、ATM PVC のカプセル化タイプを指定し、interface-ATM-VC コンフィギュレーションモードに入ります。
<b>ubr</b>	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピークセル レートを指定します。
<b>ubr+</b>	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピークセル レートと出力最小保証セル レートを指定します。

Command	Description
<b>vbr-nrt</b>	可変ビットレート非リアルタイム（VBR-NRT）QoSを設定し、ATM PVC、SVC、VC クラス、または VC バンドルメンバーの出力ピークセルレート、出力平均セルレート、および、出力最大バーストセル サイズを指定します。
<b>vc-classatm</b>	ATM VC またはインターフェイスの VC クラスを設定します。

## precedence (WRED グループ)

特定の IP プレシデンスの重み付けランダム早期検出 (WRED) または VIP 分散 WRED (DWRED) を設定するには、ランダム検出グループ コンフィギュレーション モードで **precedence** コマンドを使用します。グループの各 IP プレシデンスの値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**precedence** *precedence min-threshold max-threshold mark-probability-denominator*  
**no precedence** *precedence min-threshold max-threshold mark-probability-denominator*

構文の説明		
	<i>precedence</i>	IP プレシデンス番号です。値の範囲は 0 ～ 7 です。
	<i>min-threshold</i>	パケット数での最小しきい値。値の範囲は 1 ～ 4096 です。キューの平均の長さがこの数に達すると、WRED または DWRED は指定された IP プレシデンスを持つパケットをドロップし始めます。
	<i>max-threshold</i>	パケット数での最大しきい値。値の範囲は、 <i>min-threshold</i> ～ 4096 です。平均キューの長さがこの数を超えると、WRED または DWRED は指定された IP プレシデンスを持つすべてのパケットをドロップします。
	<i>mark-probability-denominator</i>	平均キューの深さが <i>max-threshold</i> の場合にドロップされるパケットの割合の分母です。たとえば、分母が 512 の場合、平均キューが <i>max-threshold</i> のときに、512 パケットごとに 1 パケットがドロップされます。値は 1 ～ 65536 です。デフォルトは 10 です。つまり、 <i>max-threshold</i> に達したときに、10 パケットにつき 1 つのパケットがドロップされます。

### コマンドデフォルト

すべての IP プレシデンスについて、*mark-probability-denominator* 引数は 10 で、*max-threshold* 引数は出力バッファリング容量とインターフェイスの伝送速度に基づきます。

デフォルトの *min-threshold* 引数は IP プレシデンスに応じて異なります。IP プレシデンス 0 の *min-threshold* 引数は、*max-threshold* 引数の半分になります。残りの IP プレシデンスの値は、*max-threshold* 引数の半分から *max-threshold* 引数までの間に、等間隔に配置されます。各 IP プレシデンスのデフォルトの最小値の一覧については、以下の「使用上のガイドライン」のセクションにある表を参照してください。

### コマンドモード

Random-detect-group コンフィギュレーション

### コマンド履歴

リリース	変更箇所
11.1(22)CC	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

リリース	変更箇所
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

### 使用上のガイドライン

WREDは、輻輳が存在するときにランダムにパケットをドロップすることでトラフィックを遅くする輻輳回避メカニズムです。DWREDはWREDに類似していますが、Route Switch Processor (RSP) の代わりに Versatile Interface Processor (VIP) が使用されます。

使用する場合、このコマンドは **random-detect-group** コマンドの後に発行します。

インターフェイスで **random-detectgroup** コマンドを設定すると、パケットの IP プレシデンスに基づいて、パケットに対する優先処理が行われます。異なる IP プレシデンスに対する処理を調節するには、**precedence** コマンドを使用します。

WRED または DWRED でドロップするパケットを決定する際に IP プレシデンスを無視する場合は、各 IP プレシデンスに同じパラメータでこのコマンドを入力します。最小しきい値および最大しきい値には、妥当な値を設定します。



- (注) デフォルトの WRED または DWRED パラメータ値は、最適な使用可能データに基づきます。値を変更することでアプリケーションに利点があると判断した場合を除き、パラメータのデフォルト値を変更しないことを推奨します。

次の表に、各 IP プレシデンスのデフォルトの最小値を示します。

表 4: デフォルト WRED 最小しきい値

IP precedence	最小しきい値 (最大しきい値の分数)
0	8/16
1	9/16
2	10/16
3	11/16
4	12/16
5	13/16
6	14/16
7	15/16

## 例

次の例では、異なる IP プレシデンスについて、sanjose という名前の WRED パラメータグループのパラメータを指定します。

```
random-detect-group sanjose
precedence 0 32 256 100
precedence 1 64 256 100
precedence 2 96 256 100
precedence 3 128 256 100
precedence 4 160 256 100
precedence 5 192 256 100
precedence 6 224 256 100
precedence 7 256 256 100
```

## 関連コマンド

Command	Description
<b>exponential-weighting-constant</b>	WRED パラメータグループの平均キューサイズ計算のための指数加重係数を設定します。
<b>random-detect(perVC)</b>	per-VC WRED または per-VC DWRED をイネーブルにします。
<b>random-detect-group</b>	WRED または DWRED パラメータグループを定義します。
<b>random-detectprecedence</b>	特定の IP Precedence の WRED パラメータと DWRED パラメータを設定します。
<b>showqueueing</b>	すべてまたは選択した設定済みキューイング戦略を表示します。
<b>showqueueinginterface</b>	インターフェイスまたは VC のキューイングの統計情報を表示します。

## preempt-priority

アップストリームかダウンストリーム ネイバーまたはローカル クライアント アプリケーションからのシグナルがなかった場合に PATH および RESV メッセージに挿入するリソース予約プロトコル (RSVP) サービス品質 (QoS) 優先順位を指定するには、ローカルポリシー設定モードで **preempt-priority** コマンドを使用します。優先順位を削除するには、このコマンドの **no** 形式を使用します。

```
preempt-priority [traffic-eng x] setup-priority [hold-priority]
no preempt-priority [traffic-eng x] setup-priority [hold-priority]
```

### 構文の説明

<b>traffic-eng</b> <i>x</i>	(任意) トラフィック エンジニアリング (TE) 予約の優先順位の上限を示します。 <i>x</i> 値の範囲は 0 ~ 7 で、番号が小さいほど予約の優先順位が高くなります。非 TE 予約の場合は、 <i>x</i> 値の範囲は 0 ~ 65535 で、番号が大きくなるほど予約の優先順位が高くなります。
<b>setup-priority</b>	初回にインストールされる場合の予約の優先順位を示します。値の範囲は 0 ~ 7 です。0 は優先順位が最も高いことを意味します。TE 予約の場合、デフォルト値は 7 です。TE 以外の予約ではデフォルトは 0 です。
<b>hold-priority</b>	(任意) インストール済みの場合の予約の優先順位を示します。省略すると、この引数のデフォルトは <b>setup-priority</b> になります。値の範囲は 0 ~ 7 です。0 は優先順位が最も高いことを意味します。TE 予約の場合、デフォルト値は 7 です。TE 以外の予約ではデフォルトは 0 です。

### コマンド デフォルト

これらの値を設定した後に RSVP QoS 優先順位を指定します。

### コマンド モード

ローカル ポリシー設定

### コマンド履歴

リリース	変更箇所
12.2(13)I	このコマンドが導入されました。

### 使用上のガイドライン

RSVP QoS または MPLS/TE セッションから発信できるセットアップまたは保持の最大優先度を指定するには、**preempt-priority** コマンドを使用します。これらの制限を超えると、PATHERROR、RESVERROR、またはローカル アプリケーション エラーが返されます。

受信メッセージに、このポリシーで許可されるよりも高い優先順位を要求するプリエンブション優先順位がある場合、メッセージは拒否されます。TE トンネルにプリエンブション優先順位を設定する場合は、**tunnel mpls traffic-eng priority** コマンドを使用します。

1つのポリシーには、**preempt-priority traffic-eng** および **preempt-priority** コマンドを指定でき、このコマンドは、TE および TE 以外のエンドポイントまたはミッドポイントが混同して含まれる

サブネットを識別するアクセス コントロール リスト (ACL) にポリシーをバインドする場合に便利です。

プリエンプションの予約を選択すると、RSVP は低い優先順位の予約をプリエンプション処理した後に高い優先順位の予約を処理します。プリエンプション優先順位が同じ TE 以外の予約が複数ある場合、RSVP は最も古い予約を最初に選択します。

### 例

次は、セットアップ優先順位が 0 で、保持優先度が 5 の例です。

```
Router(config-rsvp-local-policy)# preempt-priority 0 5
```

### 関連コマンド

コマンド	説明
<b>iprsvppolicylocal</b>	RSVP 要求に対する認証の実行方法を決定します。
<b>iprsvppolicypreempt</b>	RSVP は低い優先順位の予約から帯域幅を取得して、新規の優先順位が高い予約に割り当てます。
<b>tunnelmplstraffic-engpriority</b>	MPLS TE トンネルのセットアップおよび予約優先順位を設定します。

# priority

ポリシーマップ内のトラフィックのクラスに優先順位を割り当てるには、ポリシーマップクラス コンフィギュレーション モードで **priority** コマンドを使用します。以前に指定したクラスのプライオリティを削除するには、このコマンドの **no** 形式を使用します。

**priority** {*bandwidth-kbps*|**percent** *percentage*} [*burst*]

**no priority** {*bandwidth-kbps*|**percent** *percentage*} [*burst*]

## 構文の説明

<i>bandwidth-kbps</i>	プライオリティトラフィックに許可される保証帯域幅（キロビット/秒（kbps））。帯域幅の量は、使用中のインターフェイスとプラットフォームによって異なります。保証帯域幅を超えると、非プライオリティトラフィックがなくならないようにするため、プライオリティトラフィックが輻輳のイベントでドロップされます。値は1～2,000,000 kbps である必要があります。
<b>percent</b>	保証帯域幅の分量が、使用可能な帯域幅の割合（%）によって指定されることを、指定します。
<i>percentage</i>	プライオリティクラス用に確保する使用可能な帯域幅の合計。指定できる値の範囲は1～100 です。
<i>burst</i>	（任意）バイト単位のバースト サイズ。バースト サイズは、トラフィックの一時的なバーストに対応するネットワークを設定します。デフォルトバースト値は、設定されている帯域幅レートで、200 ミリ秒のトラフィックとして計算され、burst 引数が指定されていない場合に使用されます。バーストの範囲は32～2000000 バイトです。

## コマンド デフォルト

プライオリティは設定されません。

## コマンド モード

ポリシーマップ クラス コンフィギュレーション (config-pmap-c)

## コマンド履歴

リリース	変更箇所
12.0(7)T	このコマンドが導入されました。
12.0(5)XE5	このコマンドが Cisco IOS Release 12.0(5)XE5 に統合されて、Versatile Interface Processor (VIP) に分散型低遅延キューイング (VIP 用の低遅延キューイング) 機能の一部として実装されました。
12.0(9)S	このコマンドが Cisco IOS Release 12.0(9)S に統合されて、VIP に分散型低遅延キューイング (VIP 用の低遅延キューイング) 機能の一部として実装されました。
12.1(2)E	このコマンドが変更されました。burst 引数がキーワードが追加されました。



リリース	変更箇所
12.1(3)T	このコマンドが Cisco IOS Release 12.1(3)T に統合されました。
12.1(5)T	このコマンドが Cisco IOS Release 12.1(5)T に統合されて、VIP に分散型低遅延キューイング（VIP用の低遅延キューイング）機能の一部として実装されました。
12.2(2)T	このコマンドが変更されました。 <b>percent</b> キーワードおよび <i>percentage</i> 引数が追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィッチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。
Cisco IOS XE Release 2.1	このコマンドが Cisco IOS XE 2.1 に統合され、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。
15.1(1)T	このコマンドが変更されました。 <i>bandwidth-kbps</i> 引数に使用できる値が変更されました。値は 8 ～ 2,000,000 kbps である必要があります。
15.2(1)T	このコマンドが変更されました。 <i>bandwidth-kbps</i> 引数に使用できる値が変更されました。値は 1 ～ 2,000,000 kbps である必要があります。
15.4(1)S	このコマンドが、Cisco ASR 901 シリーズ ルータに実装されました。

### 使用上のガイドライン

このコマンドは、クラスベース均等化キューイング（CBWFQ）の絶対優先キューイング（PQ）の場合に、低遅延キューイング（LLQ）を設定します。完全 PQ では、音声などの遅延に敏感なデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。

**priority** コマンドを使用すると、（User Datagram Ports（UDP）ポートだけではなく）さまざまな基準に基づいてクラスを設定し、優先順位を割り当てることができます。これは、シリアルインターフェイスと ATM 相手先固定接続（PVC）で使用できます。類似の **iprtppriority** コマンドを使用すると、UDP ポート番号のみに基づいてプライオリティフローを決定することができます。ATM PVC では使用できません。

デバイスが輻輳していない場合は、プライオリティクラストラフィックの割り当て帯域幅を超えることができます。デバイスが輻輳している場合、割り当てられた帯域幅を超えるプライオリティクラストラフィックは破棄されます。

同じポリシーマップ内では、**bandwidth** コマンドおよび **priority** コマンドは、同じクラスに使用できません。しかしこれらのコマンドは、同じポリシーマップでは一緒に使用できます。

ポリシーマップで、1つまたは複数のクラスにプライオリティステータスを指定できます。単一ポリシーマップ内の複数のクラスがプライオリティクラスとして設定されると、これらのクラスからのすべてのトラフィックが、同じ単一のプライオリティキューにキューイングされます。

クラスポリシー設定が含まれているポリシーマップがインターフェイスに付加されて、そのインターフェイスのサービスポリシーが決定される場合、使用可能な帯域幅が評価されます。インターフェイスの帯域幅が不十分なことが原因で、特定のインターフェイスにポリシーマップがアタッチできない場合、そのポリシーは、正常にアタッチされていたすべてのインターフェイスから削除されます。

帯域割り当ての詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide』の「Congestion Management Overview」を参照してください。



- (注) Cisco ASR 1000 シリーズアグリゲーションサービスルータでは、*bandwidth-kbps* や *percentage* などの条件付きプライオリティレートリミッタの使用は、3 レイヤポリシーマップ設定の最下位レベル（孫またはリーフ）ではサポートされません。3 レベルポリシーの最下位レベルでは、条件付きリミッタは適用されません。ただし、完全ポリサーによるプライオリティは、このレベルの階層でサポートされます。この制約は、フラットまたは2 レベル階層型ポリシーマップには適用されません。

## 例

次に、`policy1` という名前のポリシーマップで、50 kbps の保証帯域幅と 60 バイトの 1 回限りのバーストサイズで PQ を設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

次に、`policy1` という名前のポリシーマップが適用されているインターフェイス上で、使用可能な帯域幅の 10% を `voice` という名前のクラス用に予約する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

## 関連コマンド

コマンド	説明
<b>bandwidth</b>	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
<b>iprtppriority</b>	UDP 宛先ポートの範囲に属する RTP パケットフローセットについて、完全プライオリティキューを予約します。
<b>iprtppreserve</b>	UDP 宛先ポートの範囲に属する RTP パケットフローのセット用に、特殊キューを確保します。

コマンド	説明
<b>max-reserved-bandwidth</b>	CBWFQ、LLQ、およびIP RTPプライオリティに割り当てるインターフェイス帯域幅のパーセント比率を変更します。
<b>show interfaces fair-queue</b>	VIP ベースのインターフェイスの WFQ について、情報と統計情報を表示します。
<b>show policy-map</b>	指定されたサービス ポリシー マップに対するすべてのクラスの設定、または、すべての既存ポリシー マップに対するすべてのクラスの設定を表示します。
<b>show policy-map interface</b>	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、すべてのサービス ポリシーに対して設定されているすべてのクラスの packets 統計情報を表示します。
<b>show queue</b>	特定のインターフェイスまたは VC のキュー内部の packets のコンテンツを表示します。

## priority (10000 シリーズ)

ポリシー マップでトラフィック クラスに優先順位を割り当てるには、Cisco 10000 シリーズ ルータの QoS ポリシー マップ クラス コンフィギュレーション モードで **priority** コマンドを使用します。クラスの優先処理を削除するには、このコマンドの **no** 形式を使用します。

**priority**  
**no priority**

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

QoS ポリシー クラス コンフィギュレーション (config-pmap-c)

### コマンド履歴

リリース	変更箇所
12.0(17)SL	このコマンドが導入されました。
12.0(20)ST	このコマンドが拡張され、パーセントベース帯域幅レートをサポートするようになりました。
12.0(25)S	このコマンドが変更され、ESR-PRE1 で絶対優先キューイングが使用できるようになりました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。
12.3(7)XI1	このコマンドが変更され、ESR-PRE2 で絶対優先キューイングが使用できるようになりました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。

### 使用上のガイドライン

Cisco IOS Release 12.0(25)S および Release 12.3(7)XI1 以降の **priority** コマンドでは、絶対優先キューイングを使用できます。帯域幅レートをキロビット/秒 (kbps) またはリンク帯域幅のパーセンテージで指定するには、**police** または **police percent** コマンドを使用します。

絶対優先キューイングを使用すると、リンク上の現在の輻輳レベルに関係なく、優先キューに入れるパケットの低遅延を保証します。



(注) Cisco IOS Release 12.0(25)S および Release 12.3(7)XI1 より前のリリースで帯域幅レートを指定する場合、**priority** コマンドを使用します。

**priority** コマンドを使用すると、ポリシー マップでトラフィック クラスに優先順位を割り当てられます。ルータは優先処理をプライオリティ クラスに割り当てるため、プライオリティ

キューイングでは音声など遅延の影響を受けやすいデータを、他のキューの packets より前にキュー解除して送信できます。

`police` コマンドで帯域幅パラメータを指定すると、プライオリティクラスに帯域幅を保証し、そのプライオリティクラスからの packets のフローを制限します。

`priority` コマンドを使用すると、次のインターフェイスでプライオリティキューイングがサポートされます。

- Physical

- マルチリンク PPP およびマルチリンク フレーム リレー

- ATM 整形 (ピーク セル レートを指定) 未指定ビット レート (UBR) の相手先固定接続 (PVC) およびポイントツーポイント サブインターフェイス

- ATM 固定ビット レート (CBR) PVC およびポイントツーポイント サブインターフェイス

- ATM 可変ビット レート (VBR) PVC およびポイントツーポイント サブインターフェイス

- ラベル制御 ATM (LC-ATM) サブインターフェイス

- フレーム リレー PVC、ポイントツーポイント サブインターフェイス、およびマップ クラス

- イーサネット VLAN

`priority` コマンドを使用しても、次のインターフェイスではプライオリティ キューイングはサポートされません。

- ATM 非整形 (ピーク セル レートを指定しない) UBR PVC およびポイントツーポイント サブインターフェイス

- IP トンネル

- 仮想アクセス

### Cisco 10000 シリーズ ルータ

Cisco 10000 シリーズルータでは、発信インターフェイスでのみ `priority` コマンドをサポートしています。着信インターフェイスでは、`priority` コマンドはサポートされません。

### プライオリティ キューイングの制限事項

- 各ポリシー マップで指定できるプライオリティクラスは1つのみです。

- プライオリティ サービスでは `random-detect` または `bandwidth` コマンドを設定できません。

### 例

次の例では、ポリシー マップ `policy1` の `class-default` に優先順位を割り当てます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# priority
```

## 関連コマンド

Command	Description
<b>bandwidth(policy-mapclass)</b>	ポリシーマップに属しているクラスに割り当てる帯域幅を指定します。
<b>police</b>	インターフェイスで送受信するトラフィックの最大レートを制御します。
<b>police (percent)</b>	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
<b>randomdetect (perVC)</b>	VC 単位 WRED または VC 単位 VIP 分散 WRED を有効にします。

## priority (SIP400)

クラスマップに絶対スケジュール優先を設定するには、ポリシーマップクラス コンフィギュレーションモードで **priority** コマンドを使用します。以前に指定したクラスの優先度レベルを削除するには、このコマンドの **no** 形式を引数を指定せずに使用します。

**priority** [level {1|2}] [{*kbps* [*burst*]|**percent** *percentage* [*burst*]}]  
**no priority**

### 構文の説明

<b>level</b> {1 2}	(任意) 複数レベルの絶対優先サービスモデルを定義します (1は高レベル、2は低レベル)。特定のレベルの優先サービスが設定されたトラフィッククラスをイネーブルにすると、その特定のレベルの優先サービスがイネーブルにされたすべてのトラフィックに、単一の優先キューが関連付けられることとなります。デフォルトは1です。
<i>kbps</i>	(任意) プライオリティトラフィックに対して許可される、kbps 単位での保証帯域幅です。帯域幅の量は、使用中のインターフェイスとプラットフォームによって異なります。保証帯域幅を超えると、非プライオリティトラフィックがなくならないようにするため、プライオリティトラフィックが輻輳のイベントでドロップされます。範囲: 1 ~ 2480000。
<i>burst</i>	(任意) バーストサイズをバイト単位で指定します。バーストサイズは、トラフィックの一時的なバーストに対応するネットワークを設定します。 <i>burst</i> 引数を指定しないと、デフォルトのバースト値が使用されます。範囲: 18 ~ 2000000。デフォルト: 設定された帯域幅レートで 200 ミリ秒のトラフィックです。
<b>percent</b> <i>percentage</i>	(任意) プライオリティクラス用に残しておく合計の利用可能な帯域幅のパーセンテージを指定します。範囲は 1 ~ 100 です。

### コマンド デフォルト

すべてのトラフィックで低いプライオリティ キューが使用されます。

### コマンド モード

ポリシーマップクラス コンフィギュレーション (config-pmap-c)

### コマンド履歴

リリース	変更箇所
12.2(33)SXI	このコマンドが導入されました。

### 使用上のガイドライン

1つのポリシーマップ内に2つのレベルのプライオリティ キューを作成するには、**priority** コマンドを入力します。レベル2のプライオリティキューからのパケットは、レベル1プライオリティ キューが空のときのみ送信されるようにスケジュールされます。

優先帯域幅およびパーセンテージには次の制限事項があります。

- 出力方向のみでサポートされます。

- ATM 共有ポート アダプタ (SPA) ではサポートされません。

優先度レベルには次の制限事項があります。

- 2つの優先度レベル (priority または priority level 1 と priority level 2) のみがサポートされます。
- 優先順位は出力方向のみでサポートされます。
- 優先順位は、ATM SPA でサポートされていません。

プライオリティ機能の厳密なレベルおよびレベルごとのカウントを表示するには、**showpolicy-mapinterface** コマンドを入力します。

同じポリシー マップ内では、**bandwidth** コマンドおよび **prioritylevel** コマンドは、同じクラスに使用できません。ただし、これらのコマンドは、同じポリシー マップでは使用できます。

同じポリシー マップ内では、**shape** コマンドおよび **prioritylevel** コマンドは、同じクラスに使用できません。ただし、これらのコマンドは、同じポリシー マップでは使用できます。

ポリシー マップで、1つまたは複数のクラスにプライオリティ ステータスを指定できます。ルータは単一のプライオリティ キューを同じ優先度レベルが有効になっているすべてのトラフィックに関連付け、ハイレベルプライオリティ キューが空になると、次レベルのプライオリティ キューと非プライオリティ キューを処理します。

同じポリシー マップ内の異なる2つのクラスに同じ優先度レベルを指定することはできません。

同じポリシー マップ内の異なる2つのクラスに **priority** コマンドおよび **prioritylevel** コマンドは指定できません。たとえば、**prioritykbps** または **prioritypercentpercentage** コマンドおよび **prioritylevel** コマンドを異なるクラスに指定することはできません。

**prioritylevel** コマンドが特定レベルのプライオリティ サービスで設定されている場合、**queue-limit** および **random-detect** コマンドは、その優先度レベルの単一クラスが設定されている場合のみ使用できます。

いかなる優先度レベルであっても、デフォルト キューをプライオリティ キューに設定することはできません。

## 例

次の例は、複数レベルのプライオリティ キューの設定方法を示しています。この例では、Customer1 という名前のトラフィック クラスに高い優先順位 (レベル1) が割り当てられており、Customer2 という名前のクラスにはレベル2の優先順位が割り当てられています。Customer2 トラフィックが妨げられないように、Customer1 トラフィックは使用可能な帯域幅の30%でポリシングされています。

```
Router# config terminal
Router(config)# policy-map Business
Router(config-pmap)# class Customer1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 30
Router(config-pmap-c)# exit
```



```
Router(config-pmap)# class Customer2
Router(config-pmap-c)# priority level 2
```

次に、`policy1` という名前のポリシーマップで、50 kbps の保証された帯域幅と 60 パイットの 1 回限りのバースト サイズでプライオリティ キューを設定する例を示します。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

次の例では、`policy1` という名前のポリシーマップが付加されているインターフェイス上で、使用可能な帯域幅の 10% が音声クラス用に確保されます。

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

#### 関連コマンド

コマンド	説明
<b>bandwidth</b>	ポリシーマップに属するクラスに割り当てる帯域幅を指定または変更します。
<b>priority</b>	トラフィック クラスに優先順位を割り当てます。
<b>queue-limit</b>	ポリシーマップに設定されたクラス ポリシー用にキューが保持できる最大パケット数を指定します。
<b>random-detect</b>	インターフェイスで重み付けランダム早期検出 (WRED) を有効にします。
<b>shape</b>	発信トラフィックのクラスに最大データ レートを指定します。
<b>showpolicy-mapinterface</b>	インターフェイスに対応付けられているポリシーの統計情報および設定を表示します。

# priority-group



- (注) Cisco IOS Release 15.1(3)T では、**priority-group** コマンドは表示されません。このコマンドは Cisco IOS ソフトウェアで引き続き使用できますが、CLI のインタラクティブ ヘルプでは、コマンドラインで疑問符を入力して表示しようとしても表示されません。このコマンドは、将来のリリースで完全に削除されます。つまり、適切な代替コマンド（またはコマンドシーケンス）を使用する必要があります。代わりに使用するコマンドのリストなど、詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide』の「Legacy QoS Command Deprecation」機能ドキュメントを参照してください。

指定された優先リストをインターフェイスに割り当てるには、インターフェイスコンフィギュレーションモードで **priority-group** コマンドを使用します。指定された優先度グループの割り当てを削除するには、このコマンドの **no** 形式を使用します。

**priority-group** *list-number*  
**no priority-group** *list-number*

## 構文の説明

<i>list-number</i>	インターフェイスに割り当てられた優先リスト番号。1～16の数字。
--------------------	----------------------------------

## コマンド デフォルト

無効

## コマンド モード

インターフェイス コンフィギュレーション

## コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
15.1(3)T	このコマンドが変更されました。このコマンドが非表示になりました。

## 使用上のガイドライン

1つのインターフェイスに1つのリストのみを割り当てることができます。優先出力キューイングには、インターフェイスから送信されるパケットの優先順位付け機能があります。

出力キューの現在のステータスを表示するには、**showqueueing** および **showinterfaces** コマンドを使用します。

## 例

次の例では、シリアルインターフェイス 0 の伝送パケットが優先リスト 1 に分類されます。

```
interface serial 0
  priority-group 1
```

次は、シリアルトンネル (STUN) 接続のシリアルリンクのアドレスに基づいてキューイングプライオリティを確立する例です。優先度グループを出カインターフェイスに割り当てるには、**priority-group** インターフェイス コンフィギュレーション コマンドを使用する必要があることに注意してください。

```
stun peer-name 172.16.0.0
stun protocol-group 1 sdlc
!
interface serial 0
! Disable the ip address for interface serial 0:
no ip address
! Enable the interface for STUN:
encapsulation stun
!
stun group 2
stun route address 10 tcp 172.16.0.1 local-ack priority
!
! Assign priority group 1 to the input side of interface serial 0:
priority-group 1
! Assign a low priority to priority list 1 on serial link identified
! by group 2 and address A7:
priority-list 1 stun low address 2 A7
```

## 関連コマンド

Command	Description
<b>locaddr-priority-list</b>	LUアドレスに基づいてキューイングプライオリティを確立する手順の1つとして、LUをキューイングプライオリティにマップします。
<b>priority-listdefault</b>	優先リストの他の規則に一致しないパケット用にプライオリティ キューを割り当てます。
<b>priority-listinterface</b>	特定のインターフェイスから着信するパケットのキューイングプライオリティを確立します。
<b>priority-listprotocol</b>	プロトコルタイプに基づいてキューイングの優先順位を設定します。
<b>priority-listprotocolti tcp</b>	TCPポートに基づいてBSTUNまたはSTUNキューイングプライオリティを確立します。
<b>priority-listprotocolstunaddress</b>	シリアルリンクのアドレスに基づいて、STUNキューイングプライオリティを確立します。
<b>priority-listqueue-limit</b>	各プライオリティ キューで待機可能なパケットの最大数を指定します。

Command	Description
<b>showinterfaces</b>	ルータまたはアクセス サーバで設定されているすべてのインターフェイスの統計情報を表示します。
<b>showqueue</b>	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
<b>showqueueing</b>	すべてまたは選択した設定済みキューイング戦略を表示します。

## priority level

複数のプライオリティ キューを設定するには、ポリシーマップクラス コンフィギュレーション モードで **priority level** コマンドを使用します。以前に指定したクラスの優先度レベルを削除するには、このコマンドの **no** 形式を使用します。

**priority level level**  
**no priority level level**

### 構文の説明

<i>level</i>	<p>複数レベルの絶対優先サービス モデルを定義します。特定のレベルのプライオリティ サービスが設定されたトラフィック クラスを有効にすると、その特定のレベルのプライオリティ サービスが有効にされたすべてのトラフィックに、単一のプライオリティ キューが関連付けられることとなります。</p> <p>有効な値は、1（高プライオリティ）～4（低プライオリティ）です。デフォルトは1です。Cisco ASR 1000 シリーズルータおよびCisco ASR 903 シリーズルータの有効な値は、1（高プライオリティ）～2（低プライオリティ）です。デフォルトは1です。</p>
--------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### コマンド デフォルト

優先度レベルのデフォルト レベルは1です。

### コマンド モード

ポリシーマップ クラス コンフィギュレーション (config-pmap-c)

### コマンド履歴

リリース	変更箇所
12.2(31)SB2	このコマンドが、複数レベルの絶対優先キューイングをサポートするために追加され、PRE3 用の Cisco 10000 シリーズルータに実装されました。
Cisco IOS XE Release 2.1	このコマンドが Cisco ASR 1000 シリーズルータに実装されました。
Cisco IOS XE リリース 3.7S	このコマンドが Cisco ASR 903 シリーズルータに実装されました。

### 使用上のガイドライン

同じポリシー マップ内では、**bandwidth** および **priority level** コマンドを同じクラスに使用できません。ただし、これらのコマンドは、同じポリシー マップでは使用できます。

同じポリシー マップ内では、**shape** および **priority level** コマンドを同じクラスに使用できません。ただし、これらのコマンドは、同じポリシー マップでは使用できます。

ポリシー マップで、1 つまたは複数のクラスにプライオリティ ステータスを指定できます。ルータは単一のプライオリティ キューを同じ優先度レベルが有効になっているすべてのトラフィックに関連付け、空になるまでハイレベル プライオリティ キューを処理した後、次レベルのプライオリティ キューと非プライオリティ キューを処理します。

同じポリシー マップ内の異なる 2 つのクラスに同じ優先度レベルを指定することはできません。

同じポリシー マップ内の異なる 2 つのクラスに **priority** コマンドおよび **priority level** コマンドは指定できません。たとえば、**priority bandwidth kbps** または **priority percent percentage** コマンドおよび **priority level** コマンドを異なるクラスに指定することはできません。

**priority level** コマンドが特定レベルのプライオリティ サービスで設定されている場合、**queue-limit** および **random-detect** コマンドは、その優先度レベルの単一クラスが設定されている場合のみ使用できます。

いかなる優先度レベルであっても、デフォルトキューをプライオリティ キューに設定することはできません。

### Cisco 10000 シリーズ ルータ、Cisco ASR 1000 シリーズ ルータ、および Cisco ASR 903 シリーズ ルータ

Cisco 10000 シリーズ ルータ、Cisco ASR 1000 シリーズ ルータ、および Cisco ASR 903 シリーズ ルータでは、プライオリティ サービスの 2 つのレベルであるレベル 1（高）およびレベル 2（低）がサポートされます。優先度レベルを指定しないと、ルータではデフォルトのレベル 1 が使用されます。レベル 1 では、トラフィック クラスに低遅延動作が割り当てられる必要があります。ハイレベルキューが空になるまで処理された後、次レベルキューと非プライオリティ キューが処理されます。

#### 例

次の例は、複数レベルのプライオリティ キューの設定方法を示しています。この例では、Customer1 という名前のトラフィック クラスに高い優先順位（レベル 1）が割り当てられており、Customer2 という名前のクラスにはレベル 2 の優先順位が割り当てられています。Customer2 トラフィックでの帯域幅不足を防ぐために、Customer1 トラフィックは使用可能な帯域幅の 30% でポリシングされています。

```
Router> enable
Router# config terminal
Router(config)# policy-map Business
Router(config-pmap)# class Customer1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 30
Router(config-pmap-c)# exit
Router(config-pmap)# class Customer2
Router(config-pmap-c)# priority level 2
```

#### 関連コマンド

コマンド	説明
<b>bandwidth</b>	ポリシー マップに属するクラスに割り当てる帯域幅を指定または変更します。
<b>priority</b>	トラフィック クラスに優先順位を割り当てます。

コマンド	説明
<b>showpolicy-mapinterface</b>	指定したインターフェイスまたはサブインターフェイス上か、インターフェイス上の特定のPVCに対し、すべてのサービスポリシーに対して設定されているすべてのクラスのパケット統計情報を表示します。設定されているすべての優先度レベルの統計情報が表示されます。

## priority-list default

優先リストの他のどのルールにも一致しないパケットにプライオリティキューを割り当てるには、グローバルコンフィギュレーションモードで **priority-listdefault** コマンドを使用します。デフォルトに戻すか、デフォルトとして **normal** を割り当てるには、このコマンドの **no** 形式を使用します。

**priority-list list-number default {high|medium|normal|low}**  
**no priority-list list-number default**

構文の説明	<i>list-number</i>	優先リストを識別する 1 ～ 16 の番号。
	<b>high   medium   normal   low</b>	プライオリティ キューのレベル。このコマンドの <b>no</b> 形式を使用する場合は、 <b>normal</b> キューになります。

コマンド デフォルト このコマンドはデフォルトではディセーブルになっています。

コマンド モード グローバル設定

コマンド履歴	リリース	変更箇所
	10.0	このコマンドが導入されました。
	12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
	12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン 複数のルールを使用する場合、システムでは表示された順序で優先順位設定が読み取られることに注意してください。パケットの分類時に、システムは **priority-list** コマンドで指定されたルールリストから一致するプロトコルまたはインターフェイス タイプを検索します。一致すると、パケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

例 次は、優先リストの他のどのルールにも一致しないパケットのプライオリティキューを低プライオリティに設定する例です。

```
priority-list 1 default low
```

関連コマンド	<b>Command</b>	<b>Description</b>
	<b>priority-group</b>	指定した優先リストをインターフェイスに割り当てます。



Command	Description
<b>priority-listinterface</b>	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
<b>priority-listprotocol</b>	プロトコルタイプに基づいてキューイングの優先順位を設定します。
<b>priority-listqueue-limit</b>	各プライオリティキューで待機可能なパケットの最大数を指定します。
<b>showqueue</b>	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
<b>showqueueing</b>	すべてまたは選択した設定済みキューイング戦略を表示します。

## priority-list interface

特定のインターフェイスから着信するパケットのキューイングプライオリティを確立するには、グローバルコンフィギュレーションモードで **priority-listinterface** コマンドを使用します。リストからエントリを削除するには、このコマンドの **no** 形式を適切な引数を指定して使用します。

**priority-list** *list-number* **interface** *interface-type* *interface-number* {**high**|**medium**|**normal**|**low**}  
**no priority-list** *list-number* **interface** *interface-type* *interface-number* {**high**|**medium**|**normal**|**low**}

### 構文の説明

<i>list-number</i>	優先リストを識別する 1～16 の番号。
<i>interface-type</i>	インターフェイスのタイプ。
<i>interface-number</i>	インターフェイスの番号。
<b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b>	プライオリティ キューのレベル。

### コマンド デフォルト

デフォルトでは、キューイングプライオリティは確立されません。

### コマンド モード

グローバル設定

### コマンド履歴

リリース	変更箇所
10.0	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

### 使用上のガイドライン

複数のルールを使用する場合、システムでは表示された順序で優先順位設定が読み取られることに注意してください。パケットの分類時に、システムは **priority-list** コマンドで指定されたルールリストから一致するプロトコルまたはインターフェイスタイプを検索します。一致すると、パケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

### 例

次は、シリアルインターフェイス 0 に着信するリストを中プライオリティのキューレベルに割り当てる例です。

```
priority-list 3 interface serial 0 medium
```



- (注) このコマンドは、インターフェイスへのパケットの割り当て方法を指定するルールを定義します。ルールを定義したら、**priority-group** コマンドを使用してパケットを実際にインターフェイスへ割り当てます。

#### 関連コマンド

Command	Description
<b>priority-group</b>	指定した優先リストをインターフェイスに割り当てます。
<b>priority-listdefault</b>	優先リストの他の規則に一致しないパケット用にプライオリティキューを割り当てます。
<b>priority-listprotocol</b>	プロトコルタイプに基づいてキューイングの優先順位を設定します。
<b>priority-listqueue-limit</b>	各プライオリティキューで待機可能なパケットの最大数を指定します。
<b>showqueue</b>	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
<b>showqueueing</b>	すべてまたは選択した設定済みキューイング戦略を表示します。

## priority-list protocol

プロトコルタイプに基づいてキューイングプライオリティを確立するには、グローバル コンフィギュレーション モードで **priority-listprotocol** コマンドを使用します。プロトコルタイプ別に割り当てられた優先リスト エントリを削除するには、このコマンドの **no** 形式を適切な引数を指定して使用します。

**priority-list** *list-number* **protocol** *protocol-name* {**high**|**medium**|**normal**|**low**} *queue-keyword*  
*keyword-value*

**no priority-list** *list-number* **protocol** *protocol-name* {**high**|**medium**|**normal**|**low**} *queue-keyword*  
*keyword-value*

構文の説明		
	<i>list-number</i>	優先リストを識別する 1 ~ 16 の番号。
	<i>protocol-name</i>	プロトコルタイプ : <b>aarp</b> 、 <b>appletalk</b> 、 <b>arp</b> 、 <b>bridge</b> (透過)、 <b>clns</b> 、 <b>clns_es</b> 、 <b>clns_is</b> 、 <b>compressedtcp</b> 、 <b>cmns</b> 、 <b>decnet</b> 、 <b>decnet_node</b> 、 <b>decnet_router-l1</b> 、 <b>decnet_router-l2</b> 、 <b>dls</b> 、 <b>ip</b> 、 <b>ipx</b> 、 <b>pad</b> 、 <b>rsrb</b> 、 <b>stun</b> 、および <b>x25</b> 。
	<b>high</b>   <b>medium</b>   <b>normal</b>   <b>low</b>	プライオリティ キューのレベル。
	<i>queue-keyword</i> <i>keyword-value</i>	使用可能なキーワードは、 <b>fragments</b> 、 <b>gt</b> 、 <b>list</b> 、 <b>lt</b> 、 <b>tcp</b> 、および <b>udp</b> です。キーワードと値の詳細については、「使用上のガイドライン」セクションの表 20 を参照してください。

コマンド デフォルト キューイング プライオリティは確立されません。

コマンド モード グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更箇所
	10.0	このコマンドが導入されました。
	12.2(13)T	このコマンドが変更されました。 <b>apollo</b> 、 <b>vines</b> 、および <b>xns</b> キーワードはプロトコルタイプのリストから削除されました。これらのプロトコルは、Release 12.2(13)T で Apollo Domain、Banyan VINES、および Xerox Network Systems (XNS) が削除されたため、削除されました。
	12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
	12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレーンでサポートされます。このトレーニングの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

**使用上のガイドライン** 単一プロトコルで複数のルールを使用する場合、システムでは表示された順序で優先順位設定が読み取られることに注意してください。パケットの分類時に、システムは **priority-list** コマンドで指定されたルールリストから一致するプロトコルタイプを検索します。一致すると、パケットが適切なキューに割り当てられます。システムは指定された順序でリストを検索し、ルールとの初回の一致で検索は終了します。

**decnet\_router-l1** キーワードはすべてのレベル 1 ルータ（エリア内ルータ）のマルチキャストアドレスを示し、**decnet\_router-l2** キーワードはすべてのレベル 2 ルータ（エリア間ルータ）を示します。

**dls**、**rsrb**、および **stun** キーワードはダイレクトカプセル化のみを意味します。

次の表を使用して、ご使用のシステムに対応したキューイングプライオリティを設定します。

表 5: プロトコルプライオリティ キューのキーワードと値

オプション	説明
<b>fragments</b>	定義済みの優先度レベルをフラグメント化された IP パケットに割り当てます（IP のみで使用する場合）。具体的には、このコマンドはフラグメント オフセット フィールドがゼロではない IP パケットに一致します。フラグメント化された IP パケットの最初のフラグメントはフラグメント オフセットがゼロのため、このようなパケットはこのコマンドでは一致しません。  (注) フラグメント オフセットがゼロではないパケットには、TCP または User Datagram Protocol (UDP) ヘッダーがないため、 <b>tcp</b> または <b>udp</b> キーワードを使用するこのコマンドの他のインスタンスでは、このようなパケットが一致することはありません。
<b>gt byte-count</b>	バイト数の最小値を指定します。パケットサイズが <i>byte-count</i> 引数に入力された値よりも大きい場合に、割り当てられた優先度レベルが有効になります。  (注) 発信インターフェイスで MAC カプセル化を行うためのバイト数もパケットサイズに追加する必要があります。
<b>list list-number</b>	AppleTalk、ブリッジング、IP、IPX、VINES、または XNS で使用する場合、トラフィック プライオリティを指定されたリストに従って割り当てます。 <i>list-number</i> 引数は、指定された <i>protocol-name</i> に対応した、 <b>access-list</b> グローバル コンフィギュレーション コマンドで指定したアクセス リスト番号です。たとえば、プロトコルが AppleTalk の場合、 <i>list-number</i> は AppleTalk の有効なアクセス リスト番号である必要があります。
<b>lt byte-count</b>	バイト数の最大値を指定します。パケットサイズが <i>byte-count</i> 引数に入力された値よりも小さい場合に、割り当てられた優先度レベルが有効になります。  (注) 発信インターフェイスで MAC カプセル化を行うためのバイト数もパケットサイズに追加する必要があります。

オプション	説明
tcp ポート	定義済みの優先度レベルを、指定されたポートで送受信する TCP セグメントに割り当てます (IP のみで使用する場合)。表 21 に一般的な TCP サービスとそのポート番号を示します。
udp ポート	定義済みの優先度レベルを、指定されたポートで送受信する UDP パケットに割り当てます (IP のみで使用する場合)。表 22 に一般的な UDP サービスとそのポート番号を示します。

表 6: 一般的な TCP サービスとそのポート番号

サービス	ポート
FTP data	20
FTP	21
簡易メール転送プロトコル (SMTP)	25
Telnet	23



- (注) TCP サービスとそのポート番号の完全なリストを表示するには、Router(config)# などのヘルプ文字列を入力します。 **prioritylist4protocolipmediumtcp?**

表 7: 一般的な UDP サービスとそのポート番号

サービス	ポート
ドメイン ネーム システム (DNS)	53
ネットワークファイルシステム (NFS)	2049
リモートプロシージャコール (RPC)	111
SNMP	161
TFTP	69



- (注) UDP サービスとそのポート番号の完全なリストを表示するには、Router(config)# などのヘルプ文字列を入力します。 **prioritylist4protocolipmediumudp?**



- (注) 上の表には、より一般的な TCP および UDP ポート番号の一部が示されています。ただし、任意のポート番号を指定して優先順位付けができるため、このリストに制限されるわけではありません。TFTP、FTP などのプロトコルでは、初回のリクエストのみポート 69 を使用します。後続のパケットで使用するのは、ランダムに選択されたポート番号です。これらのプロトコルタイプの場合、ポート番号を使用すると、キュー登録済みのトラフィックを管理する方法としては有効に機能しません。

## 例

次の例では、任意の優先リスト番号として 1 を割り当て、DECnet をプロトコルタイプに指定し、このインターフェイスから送信する DECnet パケットの優先度レベルを高にします。

```
priority-list 1 protocol decnet high
```

次の例では、200 バイトよりも大きいサイズのすべての DECnet パケットで優先度レベルを中にする方法を示します。

```
priority-list 2 protocol decnet medium gt 200
```

次の例では、200 バイトよりも小さいサイズのすべての DECnet パケットで優先度レベルを中にする方法を示します。

```
priority-list 4 protocol decnet medium lt 200
```

次の例は、IP アクセスリスト 10 に一致するトラフィックの優先度レベルを高にする方法を示します。

```
priority-list 1 protocol ip high list 10
```

次の例は、Telnet パケットの優先度レベルを中にする方法を示します。

```
priority-list 4 protocol ip medium tcp 23
```

次の例は、UDP DNS パケットの優先度レベルを中にする方法を示します。

```
priority-list 4 protocol ip medium udp 53
```

次の例は、イーサネットタイプコードアクセスリスト 201 に一致するトラフィックの優先度レベルを高にする方法を示します。

```
priority-list 1 protocol bridge high list 201
```

次の例は、TCP カプセル化を使用した Data-Link Switching Plus (DLSw+) の優先度レベルを高にする方法を示します。

```
priority-list 1 protocol ip high tcp 2065
```

次の例は、ダイレクトカプセル化を使用した DLSw+ トラフィックの優先度レベルを高にする方法を示します。

```
priority-list 1 protocol dls w high
```



- (注) このコマンドは、インターフェイスへのパケットの割り当て方法を指定するルールを定義します。ルールを定義したら、**priority-group** コマンドを使用してパケットを実際にインターフェイスへ割り当てます。

#### 関連コマンド

Command	Description
<b>priority-group</b>	指定した優先リストをインターフェイスに割り当てます。
<b>priority-listdefault</b>	優先リストの他の規則に一致しないパケット用にプライオリティキューを割り当てます。
<b>priority-listinterface</b>	特定のインターフェイスから着信するパケットのキューイングプライオリティを確立します。
<b>priority-listqueue-limit</b>	各プライオリティキューで待機可能なパケットの最大数を指定します。
<b>showqueue</b>	特定のインターフェイスまたは VC のキュー内部のパケットのコンテンツを表示します。
<b>showqueueing</b>	すべてまたは選択した設定済みキューイング戦略を表示します。



## priority-list queue-limit

各プライオリティキューに待機可能なパケットの最大数を指定するには、グローバルコンフィギュレーションモードで **priority-listqueue-limit** を使用します。normal キューを選択するには、このコマンドの **no** 形式を使用します。

**priority-list** *list-number* **queue-limit** *high-limit medium-limit normal-limit low-limit*  
**no priority-list** *list-number* **queue-limit**

構文の説明	<i>list-number</i>	優先リストを識別する 1 ~ 16 の番号。
	<i>high-limit medium-limit normal-limit low-limit</i>	プライオリティ キューの最大長。4 つの引数のいずれかに 0 値を指定すると、その特定のキューではサイズが無制限になります。これらの引数のデフォルト値については、次の表を参照してください。

コマンド デフォルト なし。このコマンドの「使用上のガイドライン」セクションの次の表で、デフォルトのキュー制限引数のリストを参照してください。

コマンド モード グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更箇所
	10.0	このコマンドが導入されました。
	12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
	12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン プライオリティキューがオーバーフローすると、超過したパケットは破棄され、該当する場合はそのプロトコルに関するメッセージを送信できます。

次の表にデフォルトのキュー制限値を示します。

表 8: デフォルトのプライオリティ キューのパケット制限数

プライオリティ キューの引数	パケットの制限
<i>high-limit</i>	20
<i>medium-limit</i>	40
<i>normal-limit</i>	60

プライオリティ キューの引数	パケットの制限
<i>low-limit</i>	80



- (注) プライオリティ キューイングが有効で、キュー内にアクティブな統合サービス デジタル網 (ISDN) コールがある場合、**priority-listqueue-limit** コマンドの設定を変更すると、キューからそのコールがドロップされます。プライオリティ キューイングの詳細については、『Cisco IOS Quality of Service Solutions Configuration Guide』を参照してください。

## 例

次に、プライオリティ キューの最大パケット数を 10 に設定する例を示します。

```
Router(config)# priority-list 2 queue-limit 10 40 60 80
```

## 関連コマンド

Command	Description
<b>priority-group</b>	指定した優先リストをインターフェイスに割り当てます。
<b>priority-listdefault</b>	優先リストの他の規則に一致しないパケット用にプライオリティ キューを割り当てます。
<b>priority-listinterface</b>	特定のインターフェイスから着信するパケットのキューイング プライオリティを確立します。
<b>priority-listprotocol</b>	プロトコルタイプに基づいてキューイングの優先順位を設定します。
<b>showqueue</b>	特定のインターフェイスまたはVCのキュー内部のパケットのコンテンツを表示します。
<b>showqueueing</b>	すべてまたは選択した設定済みキューイング戦略を表示します。

## priority-queue cos-map

インターフェイス コンフィギュレーション コマンド モードで CoS 値を受信/送信絶対優先キューにマップするには、**priority-queue cos-map** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

```
priority-queue cos-map queue-id cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7 [cos8]]]]]]]
no priority-queue cos-map
```

### 構文の説明

<i>queue-id</i>	キュー番号。有効値は <b>1</b> です。
<i>cos1</i>	CoS 値。有効値は 0 ~ 7 です。
<i>...cos8</i>	(任意) CoS 値。有効値は、0 ~ 7 です。

### コマンド デフォルト

デフォルト マッピングはキュー 1 で、次の受信および送信完全プライオリティ キューで CoS 5 にマッピングされます。

- 1p1q4t 受信キュー
- 1p1q0t 受信キュー
- 1p1q8t 受信キュー
- 1p2q2t 送信キュー
- 1p3q8t 送信キュー
- 1p7q8t 送信キュー
- 1p3q1t 送信キュー
- 1p2q1t 送信キュー

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更箇所
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	このコマンドが、Supervisor Engine 2 に実装され、Cisco IOS Release 12.2(17d)SXB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(50)SY	このコマンドがサポートされるようになりました。

---

 使用上のガイドライン


(注) Cisco IOS Release 12.2(50)SY 以降では、**platform qos queuing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

---

完全優先キューに CoS 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に **1** です。
- キューにマッピングする、最大 8 つの CoS 値を入力できます。

---

 例

次に、ギガビットイーサネットポート 1/1 の完全プライオリティ キューに、CoS 値 7 をマッピングする例を示します。

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

---

 関連コマンド

コマンド	説明
show queueing interfaces	キューイング情報を表示します。

## priority-queue queue-limit

インターフェイスにプライオリティ キューのサイズを設定するには、インターフェイス コンフィギュレーションモードで **priority-queue queue-limit** コマンドを使用します。デフォルトのプライオリティ キュー サイズに戻すには、このコマンドの **no** 形式を使用します。

**priority-queue queue-limit** パーセント

**no priority-queue queue-limit** パーセント

### 構文の説明

パーセント	プライオリティ キュー サイズ (%)。有効な値は 1～100 です。
-------	-------------------------------------

### コマンド デフォルト

グローバル サービス品質 (QoS) が有効な場合は、プライオリティ キュー サイズは 15 です。グローバル QoS が無効な場合は、プライオリティ キュー サイズは 0 です。

### コマンド モード

インターフェイス コンフィギュレーション

### コマンド履歴

リリース	変更箇所
12.2(18)SXF2	このコマンドが導入されました。
12.2(50)SY	このコマンドがサポートされるようになりました。

### 使用上のガイドライン



(注) Cisco IOS Release 12.2(50)SY 以降では、**platform qos queuing-only** コマンドまたは **auto qos default** コマンドが設定されている場合のみ、このコマンドを有効にできます。

このコマンドは、次のモジュールでサポートされています。

- WS-X6501-10GE--1p2q1t<sup>1</sup>
- WS-X6148A-GE--1p3q8t<sup>2</sup>
- WS-X6148-45--1p3q8t
- WS-X6148-FE-SFP--1p3q8t
- WS-X6748-SFP--1p3q8t
- WS-X6724-SFP--1p7q8t<sup>3</sup>

<sup>1</sup> 1p2q1t: 絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 1 つ、設定不可 (100%) のテールドロップしきい値が 1 つ指定された標準キューが 2 つ。

<sup>2</sup> 1p3q8t: 絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 8 つ指定された標準キューが 3 つ。

<sup>3</sup> 1p7q8t: 絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 8 つ指定された標準キューが 7 つ。

- WS-X6704-10GE--1p7q4t<sup>4</sup>
- WS-SUP32-10GB-3E--1p7q4t
- WS-SUP32-GB-3E--1p3q8t
- WS-X6708-10GE--1p7q4t

## 例

次の例では、インターフェイスにプライオリティキューサイズを設定する方法を示しています。

```
priority-queue queue-limit 15
```

## 関連コマンド

コマンド	説明
<b>showqueueinginterface</b>	キューイング情報を表示します。

<sup>4</sup> 1p7q4t : 絶対優先キューが 1 つ、各キューに WRED 廃棄しきい値が 4 つ指定された標準キューが 7 つ。

## pvc-bundle

仮想回線（VC）をバンドルのメンバーとしてバンドルに追加し、**bundle-VC** コンフィギュレーションモードにして VC バンドル メンバーを設定するには、バンドル コンフィギュレーションモードで **pvc-bundle** コマンドを使用します。バンドルから VC を削除するには、このコマンドの **no** 形式を使用します。

```
pvc-bundle pvc-name [vpi/] [vci]
no pvc-bundle pvc-name [vpi/] [vci]
```

### 構文の説明

<i>pvc-name</i>	相手先固定接続（PVC）バンドルの名前。
<i>vpi /</i>	<p>（任意）この PVC の ATM ネットワーク仮想パス識別子（VPI）。/と <i>vpi</i> 値がない場合の <i>vpi</i> 値のデフォルトは 0 です。</p> <p>Cisco 7200 および 7500 シリーズルータでは、値の範囲は 0～255 です。Cisco 4500 および 4700 ルータでの値の範囲は 0～1 で、8192 を <b>atmvc-per-vp</b> コマンドで設定した値で割ったときの商より小さい値です。</p> <p><i>vpi</i> および <i>vci</i> 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。</p>
<i>vci</i>	<p>（任意）この PVC の ATM ネットワーク仮想チャネル識別子（VCI）。この値は 0～1 の範囲で、<b>atmvc-per-vp</b> コマンドによってこのインターフェイスに対して設定された最大値未満です。一般的に、低い値 0～31 は、特定のトラフィック（運用管理および保守（OAM）、相手先選択接続（SVC）シグナリング、統合ローカルマネジメントインターフェイス（ILMI）など）のために予約されており、使用できません。</p> <p>VCI は、ATM セルのヘッダーの 16 ビットフィールドです。VCI 値はローカルにだけ意味があるため、単一リンク上でだけ一意であり、ATM ネットワーク全体では一意ではありません。</p> <p><i>vpi</i> および <i>vci</i> 引数は両方を 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。</p>

### コマンドデフォルト

なし

### コマンドモード

バンドル コンフィギュレーション

### コマンド履歴

リリース	変更箇所
12.0(3)T	このコマンドが導入されました。
12.0(26)S	このコマンドが Cisco 10000 シリーズルータに実装されました。
12.2(16)BX	このコマンドが ESR-PRE2 に実装されました。

リリース	変更箇所
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(31)SB	このコマンドが Cisco IOS Release 12.2(31)SB に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

## 使用上のガイドライン

各バンドルには、異なるサービス品質（QoS）属性を持つ複数の VC を追加できます。このコマンドは、VC をバンドルに関連付け、そのバンドルのメンバーにします。VC をバンドルに追加するには、バンドルが必要です。 **bundle** コマンドを使用してバンドルを作成します。バンドルに追加済みの VC を設定する場合もこのコマンドを使用できます。同様にコマンドを入力して、VC バンドル メンバーの名前を指定します。

**pvc-bundle** コマンドで **bundle-VC** コンフィギュレーションモードにして、VC に VC 固有および VC クラスの属性を指定できます。

## 例

次の例では、**bundle1** という名前の既存のバンドルを指定して、バンドルコンフィギュレーションモードにします。その後には 2 つの VC をバンドルに追加します。追加する VC それぞれで、**bundle-VC** モードにして、VC クラスを VC に割り当て、設定します。

```
bundle bundle1
pvc-bundle bundle1-control 207
class control-class
pvc-bundle bundle1-premium 206
class premium-class
```

次の例は、**bundle1-control** という名前の PVC（**bundle1** という名前のバンドルの既存のメンバー）を設定し、クラスベース均等化キューイング（CBWFQ）を使用します。この設定例では、**policy1** という名前のポリシーマップを PVC に割り当てます。ポリシーマップを割り当てると、**policy1** を含むクラスによって、PVC **bundle1-control** のサービスポリシーが決定されます。

```
bundle bundle1
pvc-bundle bundle1-control 207
class control-class
service-policy output policy1
```

## 関連コマンド

Command	Description
<b>atmvc-per-vp</b>	VPI ごとにサポートする VCI の最大数を設定します。
<b>bump</b>	VC バンドルに割り当てることができる VC クラスのバンピングルールを設定します。
<b>class-bundle</b>	指定された VC クラスに含まれるバンドル レベルのコマンドで VC バンドルを設定します。



Command	Description
<b>class-vc</b>	VC クラスを ATM PVC、SVC、または VC バンドル メンバーに割り当てます。
<b>precedence</b>	バンドルの VC メンバーまたは VC バンドルに割り当て可能な VC クラスに優先レベルを設定します。
<b>protect</b>	VC バンドル メンバーへのアプリケーションの保護されたグループまたは保護された VC ステータスを持つ VC クラスを設定します。
<b>pvc</b>	ATM PVC に名前を割り当て、ATM PVC のカプセル化タイプを指定し、 <b>interface-ATM-VC</b> コンフィギュレーション モードに入ります。
<b>ubr</b>	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートを指定します。
<b>ubr+</b>	UBR QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レートと出力最小保証セル レートを指定します。
<b>vbr-nrt</b>	可変ビット レート非リアルタイム (VBR-NRT) QoS を設定し、ATM PVC、SVC、VC クラス、または VC バンドル メンバーの出力ピーク セル レート、出力平均セル レート、および、出力最大バーストセル サイズを指定します。

