QoS：ポリシングおよびシェーピング コンフィギュレーション ガイド、Cisco IOS XE Release 3S（Cisco ASR 1000）

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

ポリシングとシェーピングの概要

Cisco IOS XE QoS は、ポリシングとシェーピングという 2 種類のトラフィック規制メカニズムを提供します。

パケットまたはデータ ソースが所定の契約に確実に準拠するようにするため、およびパケットに使用する QoS を決定するために、これらのトラフィック規制メカニズム（ポリサーともシェーパーとも呼ばれます）をネットワーク全体に配置できます。 ポリシングとシェーピングのメカニズムは、準拠とサービスを確実に行うために、パケットの分類によって表されるトラフィック記述子をパケットに対して使用します。

ポリサーとシェーパーは、通常、トラフィック記述子の違反を同一の方法で識別します。 ただし、通常、違反に対処する方法が異なります。たとえば、

- ポリサーは通常、トラフィックをドロップしますが、パケットの設定または「マーキング」を変更することもできます。 （たとえば、ポリサーは、パケットをドロップするか、ポリサーの IP precedence を書き換えて、パケット ヘッダーのタイプ オブ サービス（ToS）ビットをリセットします）。
- シェーパーは、通常、バッファ、またはキューイング メカニズムを使用し、過剰なトラフィックを遅延してパケットを保持し、データ レートが予想より高い場合にフローをシェーピングします。 （たとえば、クラス ベース シェーピングは、フローをシェーピングするために、パケットを遅らせる均等化キューを使用します）。

トラフィック シェーピングとトラフィック ポリシングは連携して機能します。 たとえば、優れたトラフィック シェーピング スキームを使用すると、ネットワーク内のノードは動作の不正なフローを簡単に検出できます。 このアクティビティは、フローのトラフィックのポリシングと呼ばれる場合もあります。

この章では、Cisco IOS XE QoS トラフィック ポリシングおよびシェーピングのメカニズムについて簡単に説明します。 ポリシングとシェーピングは、両方ともトークン バケット メカニズムを使用するため、この章ではまずトークン バケットがどう機能するかについて説明します。 この章は、次の項で構成されています。

• パケット フローを規制するトラフィック シェーピング，3 ページ

トークン バケットとは

トークン バケットは、転送レートの正式な定義です。 バースト サイズ、平均レート、時間間隔（Tc）という 3 つの構成要素があります。 通常は中間レートがビット/秒の単位で表されますが、次に示す関係式によって、2 つの値が残る 3 つめの値から導き出される場合もあります。

```
mean rate = burst size / time interval
```

これらの用語の定義は次のとおりです。

- 平均レート：認定情報レート（CIR）とも呼ばれ、単位時間に送信または転送できるデータ量の平均値を指定します。
- バースト サイズ：認定バースト（Bc）サイズとも呼ばれ、スケジューリングの問題が発生しない特定の単位時間内に送信可能なトラフィック量をビット（またはバイト）/バースト単位で指定します （GTS などのシェーパーの場合はバースト当たりのビット数を指定し、CAR などのポリサーの場合はバーストおよび 1 秒当たりのバイト数を指定します）。
- 時間間隔：測定間隔とも呼ばれ、バースト当たりの秒数で時間を指定します。

定義では、間隔が整数倍の場合は、インターフェイスのビット レートは中間レートを超えません。 ただし、ビット レートは間隔内で任意に早くなる場合があります。

トークンバケットは、フロー内のデータを規制するデバイスの管理に使用されます。調整デバイスは、たとえば CAR のようなトラフィック ポリサーの場合もあれば、FRTS や GTS のようなトラフィック シェーパーの場合もあります。 トークン バケット自体には、廃棄ポリシーまたはプライオリティ ポリシーはありません。 むしろ、トークン バケットは、フローによって規制機能が過剰に働く場合に、トークンを廃棄し、送信キューの管理の問題はフローに任せます。 （CAR、FRTS、および GTS は、真のトークン バケットまたは真のリーキー バケットを実装しません）。

トークン バケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。 バケット自体には指定された容量があります。 バケットがいっぱいになると、新しく到着するトークンは廃棄されます。 各トークンは、送信元が一定の数のビットをネットワークに送信するための権限です。 パケットを送信するため、規制機能はパケット サイズに等しい数のトークンをバケットから削除する必要があります。

パケットを送信できるだけの十分なトークンがバケット内に存在しない場合、パケットは、バケットに十分な量のトークンが蓄積されるまで送信待ちの状態になるか（GTS の場合）、廃棄またはマークダウンされます（CAR の場合）。 バケットがすでにトークンで満たされている場合、着信トークンはオーバーフローし、以降のパケットには使用できません。 したがって、いつでも、送信元がネットワークに送信できる最大のバーストは、バケットのサイズにほぼ比例します。

トラフィック シェーピングに使用されるトークン バケット メカニズムは、トークン バケットとデータ バッファまたはキューの両方を持っています。データ バッファを持たない場合は、ポリシング機能になります。 トラフィック シェーピングの場合、到着したパケットですぐに送信できないものは、データ バッファで遅延されます。

トラフィック シェーピングでは、トークン バケットはバースト性を許可する一方で、それを抑制します。 トラフィック シェーピングは、トークン バケットの容量を時間間隔で割った値にトークンに対してトークン バケットで設定された所定のレートを加えた値より速くフローが送信されないように、バースト性を抑制します。 次の式を参照してください。

```
(token bucket capacity in bits / time interval in seconds) + established rate in bps =
maximum flow speed in bps
```

このようなバースト性抑制方法は、長期的な送信レートが、バケットで設定されたトークンの所定レートを超えないことも保証します。

トラフィック ポリシング

トラフィック ポリシングでは、インターフェイス上で送受信するトラフィックの最大レートを制御し、ネットワークを複数のプライオリティ レベル、またはサービスクラス（CoS）に区切ります。

トラフィック ポリシングでは、トークン バケット アルゴリズムを介して、トラフィックの最大レートを管理します。 トークン バケット アルゴリズムでは、ユーザが設定した値を使用して、特定の瞬間にインターフェイス上で許可されるトラフィックの最大レートを決定できます。 トークン バケット アルゴリズムは、（トラフィック ポリシングを伴うトラフィック ポリシーがどこに設定されているかに応じて）入力または出力されるすべてのトラフィックによって影響を受けます。大きなパケットが同じトラフィック ストリームで複数送信される際のネットワーク帯域幅の管理に役立ちます。

トークンバケットアルゴリズムは、ユーザに各パケットに対する、準拠（conform）アクション、超過（exceed）アクション、およびオプションの違反（violate）アクションの 3 つを提供します。トラフィック ポリシングを設定され、インターフェイスに入ってくるトラフィックは、これらのカテゴリのいずれかに分類されます。 これら 3 つのカテゴリ内で、ユーザはパケットの処理を決定できます。 たとえば、適合したパケットは送信するように設定し、超過したパケットはプライオリティを下げて送信するように設定し、違反したポリシーはドロップするように設定できます。

トラフィック ポリシングは、多くの場合、ネットワークに出入りするトラフィックのレートを制限するためにネットワークのエッジのインターフェイスで設定されます。最も一般的なトラフィック ポリシングの設定では、適合したトラフィックは送信され、超過したトラフィックはプライオリティを下げて送信されるかドロップされます。 ユーザはネットワークのニーズに合わせてこれらの設定オプションを変更できます。

パケット フローを規制するトラフィック シェーピング

ネットワーク上のパケットフロー（つまり、トラフィックのフロー）は、トラフィック シェーピングともいいます。トラフィック シェーピングでは、インターフェイスから出るトラフィックの速度を制御できます。 このようにして、トラフィックのフローとパケットを受信するインターフェイスの速度を一致させることができます。

第 2 章

IPv6 QoS：MQC トラフィック シェーピング

トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 QoS の概要：MQC トラフィック シェーピング

QoS for IPv6 の実装方針

IPv6 パケットは、IPv4 パケットとは別のパスで転送されます。 IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、重み付けランダム早

期検出（WRED）、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含まれます。 これらの機能は、IPv6 のプロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスのどちらでも使用できます。

IPv6 環境で使用可能な QoS 機能はすべて、モジュラ QoS コマンドライン インターフェイス（MQC）から管理します。 MQC を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシーマップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに対応付けることができます。

IPv6 が稼働しているネットワークに QoS を実装するには、IPv4 だけが稼働しているネットワークに QoS を実装する手順に従ってください。 高度なレベルで QoS を実装するための基本手順は、次のとおりです。

- QoS を必要とするネットワーク内のアプリケーションを特定します。
- どの QoS 機能が適切であるかを判断するために、アプリケーションの特性を理解します。
- 変更と転送がリンク層ヘッダー サイズに及ぼす影響を理解するために、ネットワーク トポロジについて理解します。
- ネットワークに確立する基準に基づいて、クラスを作成します。 具体的には、同じネットワークで IPv6 トラフィックとともに IPv4 トラフィックも伝送されている場合、IPv6 トラフィックと IPv4 トラフィックを同様に処理するか、それとも別の方法で処理し、それぞれに応じた一致基準を指定するかを決定します。 両者を同様に処理する場合は、**match precedence**、**match dscp**、**set precedence**、**set dscp** などの match 文を使用します。 両者を別の方法で処理する場合は、match-all クラス マップ内に **match protocol ip** や **match protocol ipv6** などの一致基準を追加します。
- 各クラスにマーキングするためのポリシーを作成します。
- QoS 機能を適用する際は、エッジからコアに向かって作業します。
- トラフィックを処理するためのポリシーを構築します。
- ポリシーを適用します。

IPv6 環境でのトラフィック ポリシング

IPv6 での輻輳管理は、IPv4 と同様で、IPv6 環境でのキューイングおよびトラフィック シェーピング機能の設定に使用するコマンドは、IPv4 で使用されるものと同じコマンドです。 トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケットデキュー レートを制限できます。 トラフィック シェーピングでは、デフォルトでフローベース キューイングが使用されます。 パケットの分類およびプライオリティ設定には、CBWFQ を使用できます。 トラフィックのコンディショニングおよびポリシングには、クラスベース ポリシング機能と汎用トラフィック シェーピング（GTS）、またはフレーム リレー トラフィック シェーピング（FRTS）を使用できます。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	*IPv6 の RFC*

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 QoS の機能情報：MQC トラフィック シェーピング

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*IPv6 QoS* の機能情報：*MQC* トラフィック シェーピング

機能名	リリース	機能情報
IPv6 QoS：MQC トラフィック シェーピング	Cisco IOS XE Release 2.1	トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。

第 3 章

残りの帯域幅使用比率の分配

残りの帯域幅使用比率の分配機能を使用すると、すべてのサービス プロバイダーが、サブインターフェイスおよびクラス キューに帯域幅余剰比率を設定することができます。 この比率は、他のサブインターフェイスまたはキューに関して、サブインターフェイスまたはキューに対する相対的重みを指定します。 輻輳時に、ルータはこの帯域幅余剰比率を使用して、非プライオリティ トラフィック クラスに割り当てる超過帯域幅（プライオリティ トラフィックで未使用）の量を指定します。 ルータは物理インターフェイスに設定された他のサブインターフェイス レベルのキューとクラス キューに対して超過している帯域幅を割り当てます。 帯域幅余剰比率の管理では、トラフィック プライオリティはスピードだけを基準とするわけではありません。 代わりに、サービス プロバイダーは、サービス製品や登録料などの代替要因を基準にすることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

残りの帯域幅使用比率の分配の前提条件

残りの帯域幅使用比率の分配機能をイネーブルにする前に、class-map コマンドを使用して、必要な数のトラフィック クラスを作成します。

残りの帯域幅使用比率の分配に関する制約事項

- 帯域幅余剰比率は、発信インターフェイスでのみ使用できます。
- bandwidth remaining ratio コマンドは、同じポリシー マップの異なるトラフィック クラスにある別の bandwidth コマンドとは共存できません。 たとえば、次の設定は無効で、エラー・メッセージが表示される原因となります。

```
policy-map Prec1
 class precedence_0
  bandwidth remaining ratio 10
 class precedence_2
  bandwidth 1000
```

- bandwidth remaining ratio コマンドは、同じクラスにある別の bandwidth コマンドとは共存できません。 たとえば、次の設定は無効で、エラー・メッセージが表示される原因となります。

```
policy-map Prec1
 class precedence_0
  bandwidth 1000
  bandwidth remaining ratio 10
```

- bandwidth remaining ratio コマンドは、同じクラスにある別の priority コマンドとは共存できません。 たとえば、次の設定は無効で、エラー・メッセージが表示される原因となります。

```
policy-map Prec1
 class precedence_1
  priority percent 10
  bandwidth remaining ratio 10
```

残りの帯域幅使用比率の分配の概要

残りの帯域幅使用比率の分配機能の利点

残りの帯域幅使用比率の分配機能を使用すると、サービス プロバイダーが輻輳時の加入者トラフィックに優先順位を付けることができます。 帯域幅余剰比率は、ルータが非プライオリティ トラフィック クラスに超過帯域幅（プライオリティ トラフィックで未使用）を割り当てる方法を反映するために使用されます。 ルータは、帯域幅レートだけを使用する代わりに、超過帯域幅の割り当てを決定する際、最小帯域幅レート、最大帯域幅レート、帯域幅余剰比率を設定することを考慮します。 帯域幅余剰比率は、トラフィックの優先順位付けの柔軟性が向上させ、速度以外の要因に帯域幅余剰比率を基準とすることにより、超過帯域幅割り当てに反映させることができます。

帯域幅余剰比率を使用すると、サービス プロバイダーが輻輳時にサブインターフェイスとキューに優先順位を割り当てる際の柔軟性が向上します。 速度に加えて、サービス製品や登録料などの代替要因に帯域幅余剰比率を基準とすることができます。 このようにすると、ビジネス サービスを伝送するサブインターフェイスに対する重みを増し、個人サービスを伝送するサブインターフェイスに対する重みを抑えることができます。

帯域幅余剰比率機能

帯域幅余剰比率は、**bandwidth remaining ratio** コマンドで指定される 1～1000 の値で、キューまたはサブインターフェイス レベルのキューに割り当てる未使用（超過）帯域幅の量の指定に使用します。 ルータは物理インターフェイスに設定された他のクラス レベル キューとサブインターフェイス レベル キューに対して超過している帯域幅を割り当てます。 帯域幅余剰比率の値はパーセンテージを示すものではありません。名前が示すとおり、比率が使用されます。たとえば、帯域幅余剰比率が 100 であるサブインターフェイスは、帯域幅余剰比率が 10 であるサブインターフェイスと比較して、輻輳中に受信する未使用（超過）帯域幅は 10 倍になります。

帯域幅余剰比率がなければ、ルータのキューイング メカニズムまたはスケジューラはクラスまたはサブインターフェイス間に均等に未使用（超過）帯域幅を割り当てます。

帯域幅余剰比率があると、未使用（超過）帯域幅の割り当ては、帯域幅レート（サービス製品または登録料など）以外の要素に基づいて行うことができます。

帯域幅余剰比率は、bandwidth remaining ratio コマンドを使用して、各サブインターフェイスまたはクラスに別々に設定できます。 帯域幅余剰比率は 1～1000 の範囲で指定できます。 加入者が 3 人で、帯域幅余剰比率が 9、7、1 に設定されている場合にプライオリティ トラフィックが実行された後の超過帯域幅が 1700 kbps の場合、加入者は、900 kbps、700 kbps、100 kbps をそれぞれ受け取ります。

残りの帯域幅使用比率の分配の設定方法

サブインターフェイスまたはクラス キュー、あるいはこの両方に帯域幅余剰比率を適用することができます。

帯域幅余剰比率のサブインターフェイスに対する設定と適用

（注） 発信サブインターフェイスのみに帯域幅余剰比率を適用することができます。

>

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *child-policy-name*
4. **class** *class-map-name*
5. **bandwidth** *bandwidth-kbps*
6. ステップ「帯域幅余剰比率のサブインターフェイスに対する設定と適用」と「帯域幅余剰比率のサブインターフェイスに対する設定と適用」を繰り返して、必要に応じて追加のトラフィック クラスを設定します。
7. **exit**
8. **exit**
9. **policy-map** *parent-policy-name*
10. **class class-default**
11. **bandwidth remaining ratio** *ratio*
12. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
13. **service-policy** *child-policy-name*
14. **exit**
15. **exit**
16. **interface** *type slot* / *module* / *port* . *subinterface* [**point-to-point** | **multipoint**]
17. **service-policy output** *parent-policy-name*
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map** *child-policy-name* 例： `Router(config)# policy-map Child`	子ポリシー マップを作成または変更して、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。 • 子ポリシー マップの名前を入力します。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class precedence_0`	クラス マップを設定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**bandwidth** *bandwidth-kbps* 例： `Router(config-pmap-c)# bandwidth 10000`	このトラフィック クラスに割り当てられるように kbps 単位で帯域幅を指定します。 • キロ ビット/秒（kbps）単位で帯域幅の量を入力します。
ステップ 6	ステップ「帯域幅余剰比率のサブインターフェイスに対する設定と適用」と「帯域幅余剰比率のサブインターフェイスに対する設定と適用」を繰り返して、必要に応じて追加のトラフィック クラスを設定します。	
ステップ 7	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 9	**policy-map** *parent-policy-name* 例： `Router(config)# policy-map Parent`	親ポリシー マップを作成または変更して、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。 • 親ポリシー マップの名前を入力します。
ステップ 10	**class class-default** 例： `Router(config-pmap)# class class-default`	class-default クラスを設定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 （注） ルータは、サブインターフェイスの集約機能として class-default クラスで設定された任意の機能を解釈します。
ステップ 11	**bandwidth remaining ratio** *ratio* 例： `Router(config-pmap-c)# bandwidth remaining ratio 10`	サブインターフェイスの帯域幅余剰比率を指定します。 • 比率を入力します。 ratio は、輻輳時にサブインストールの各キューに割り当てるための未使用帯域幅の量を決定する際に使用する値です。他のサブインターフェイスに対して超過している帯域幅がスケジューラにより割り当てられます。 有効値は 1 ～ 1000 です。 デフォルト値は、1 です
ステップ 12	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] 例： `Router(config-pmap-c)# shape average 100000000`	（任意）average または peak レートを指定するレートにシェーピングします。 • CIR およびオプションの引数とともに **average** または **peak** キーワードを入力します。 次の点に注意してください。 • average：平均レート シェーピングを指定します。 • peak：ピーク レート シェーピングを指定します。 • cir：認定情報レート（CIR）を bps で指定します。 • （任意）bc：認定バースト サイズをビットで指定します。 • （任意）bc：超過バースト サイズをビットで指定します。

	コマンドまたはアクション	目的
ステップ 13	**service-policy** *child-policy-name* 例： `Router(config-pmap-c)# service-policy Child`	指定する子のポリシー マップをトラフィック クラスに適用します。 • 前に設定された子ポリシー マップの名前を入力します。 ルータは、子ポリシー マップで指定された QoS アクション（機能）をトラフィック クラスに適用します。 （注） **service-policy** コマンドは、通常、input または output キーワードを使用してトラフィックの方向を指定する必要があります。 ただし、子ポリシーを親ポリシーに適用する場合、トラフィックの方向を指定しないでください。
ステップ 14	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 15	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。

ステップ 16	**interface** *type slot* / *module* / *port* . *subinterface* [**point-to-point** | **multipoint**]
	
	例：
	`Router(config)# interface GigabitEthernet 1/0/0.1`
		指定するインターフェイスを作成または変更し、サブインターフェイス コンフィギュレーション モードを開始します。
		• インターフェイスのタイプを入力します。 次の点に注意してください。
		  • type：インターフェイスのタイプ（ギガビット イーサネットなど）を指定します。
		  • slot/module/port.subinterface：サブインターフェイスを識別するサブインターフェイスの番号（1/0/0.1 など）を指定します。
		  • （任意）point-to-point：サブインターフェイスがポイントツーポイント サブインターフェイスであることを示します。
		  • （任意）multipoint：サブインターフェイスがポイントツー マルチポイント サブインターフェイスであることを示します。

	コマンドまたはアクション	目的
ステップ 17	**service-policy output** *parent-policy-name* 例： `Router(config-subif)# service-policy output Parent`	サブインターフェイスに親ポリシー マップを適用します。 • 親ポリシーマップの **output** キーワードと名前を入力します。 （注） ルータは、親の class-default クラスで指定されたシェーピング レートにサブインターフェイス トラフィックをシェーピングし、子ポリシー マップで指定された QoS アクション（機能）を適用します。 （注） 輻輳時は、ルータは親ポリシー マップで指定された帯域幅余剰比率を使用して、他のサブインターフェイスを基準としてこのサブインターフェイス上で未使用の帯域幅を割り当てます。
ステップ 18	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。

帯域幅余剰比率のクラス キューに対する設定と適用

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *child-policy-name*
4. **class** *class-map-name*
5. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
6. **bandwidth remaining ratio** *ratio*
7. ユーザが定義する各クラス キューにステップ「帯域幅余剰比率のクラス キューに対する設定と適用」、「帯域幅余剰比率のクラス キューに対する設定と適用」、「帯域幅余剰比率のクラス キューに対する設定と適用」を繰り返し、必要に応じて帯域幅余剰比率を指定します。
8. **exit**
9. **exit**
10. **policy-map** *parent-policy-name*
11. **class class-default**
12. **shape** {**average** | **peak**} *cir* [*bc*] [*be*]
13. **bandwidth remaining ratio** *ratio*
14. **service-policy** *child-policy-name*
15. **exit**
16. **exit**
17. **interface** *type slot / module / port . subinterface* [**point-to-point** | **multipoint**]
18. **service-policy output** *parent-policy-name*
19. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**policy-map** *child-policy-name* 例： `Router(config)# policy-map Child`	子ポリシーマップを作成または変更して、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。 • 子ポリシー マップの名前を入力します。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class precedence_0`	クラス マップを設定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] 例： `Router(config-pmap-c)# shape average 100000000`	（任意）average または peak レートを指定するレートにシェーピングします。 • CIR およびオプションの引数とともに **average** または **peak** キーワードを入力します。 次の点に注意してください。 • average：平均レート シェーピングを指定します。 • peak：ピーク レート シェーピングを指定します。 • cir：認定情報レート（CIR）を bps で指定します。 • （任意）bc：認定バーストサイズをビットで指定します。 • （任意）bc：超過バーストサイズをビットで指定します。
ステップ 6	**bandwidth remaining ratio** *ratio* 例： `Router(config-pmap-c)# bandwidth remaining ratio 10`	トラフィック クラスの帯域幅余剰比率を指定します。 • 帯域幅余剰比率を入力します。 ratio は、輻輳時にサブインストールの各キューに割り当てるための未使用帯域幅の量を決定する際に使用する値です。 他のサブインターフェイスに対して超過している帯域幅がキューイング メカニズムまたはスケジューラにより割り当てられます。 有効値は 1 ～ 1000 です。 デフォルト値は、1 です （注） 階層型ポリシー マップ構造では、**bandwidth remaining ratio***ratio* コマンドは、少なくとも 1 個のクラスに使用する必要があります。 これを他のクラスで使用することは任意です。 このコマンドが他のクラスに明示的にイネーブルにされていない場合、キューイング メカニズムはデフォルトとして 1 を使用します。
ステップ 7	ユーザが定義する各クラス キューにステップ「帯域幅余剰比率のクラス キューに対する設定と適	

	コマンドまたはアクション	目的
	用」、「帯域幅余剰比率のクラス キューに対する設定と適用」、「帯域幅余剰比率のクラス キューに対する設定と適用」を繰り返し、必要に応じて帯域幅余剰比率を指定します。	
ステップ 8	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 9	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 10	**policy-map** *parent-policy-name* 例： `Router(config)# policy-map Parent`	親ポリシーマップを作成または変更して、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。 • 親ポリシー マップの名前を入力します。
ステップ 11	**class class-default** 例： `Router(config-pmap)# class class-default`	class-default クラスを設定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 （注） ルータは、サブインターフェイスの集約機能として class-default クラスで設定された任意の機能を解釈します。
ステップ 12	**shape** {**average** | **peak**} *cir* [*bc*] [*be*] 例： `Router(config-pmap-c)# shape average 100000000`	（任意）average または peak レートを指定するレートにシェーピングします。 • CIR およびオプションの引数とともに **average** または **peak** キーワードを入力します。 次の点に注意してください。 • average：平均レート シェーピングを指定します。 • peak：ピーク レート シェーピングを指定します。 • cir：認定情報レート（CIR）を bps で指定します。 • （任意）bc：認定バースト サイズをビットで指定します。 • （任意）bc：超過バースト サイズをビットで指定します。

	コマンドまたはアクション	目的
ステップ 13	**bandwidth remaining ratio** *ratio* 例： `Router(config-pmap-c)# bandwidth remaining ratio 10`	（階層型ポリシー マップ構造内の class-default または他のクラスで任意）サブインターフェイスの帯域幅残存率を指定します。 • 帯域幅余剰比率を入力します。 ratio は、輻輳時にサブインストールの各キューに割り当てるための未使用帯域幅の量を決定する際に使用する値です。 他のサブインターフェイスに対して超過している帯域幅がキューイング メカニズムまたはスケジューラにより割り当てられます。 有効値は 1 ～ 1000 です。 デフォルト値は、1 です （注） 階層型ポリシー マップ構造では、**bandwidth remaining ratio***ratio* コマンドは、少なくとも 1 個のクラスに使用する必要があります。 これを他のクラスで使用することは任意です。 このコマンドが他のクラスに明示的にイネーブルにされていない場合、キューイング メカニズムはデフォルトとして 1 を使用します。
ステップ 14	**service-policy** *child-policy-name* 例： `Router(config-pmap-c)# service-policy Child`	指定する子のポリシーマップをトラフィック クラスに適用します。 • 子ポリシーマップの名前を入力します。ルータは、子ポリシーマップで指定された QoS アクション（機能）をトラフィック クラスに適用します。 （注） **service-policy** コマンドは、通常、input または output キーワードを使用してトラフィックの方向を指定する必要があります。 ただし、子ポリシーを親ポリシー マップに適用する場合、トラフィックの方向を指定しないでください。
ステップ 15	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 16	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 17	**interface** *type slot* / *module* / *port* **.** *subinterface* [**point-to-point** | **multipoint**]	指定するインターフェイスを作成または変更し、サブインターフェイス コンフィギュレーション モードを開始します。 • インターフェイスのタイプを入力します。 次の点に注意してください。

	コマンドまたはアクション	目的
	例： `Router(config)# interface GigabitEthernet 1/0/0.1`	• type：インターフェイスのタイプ（ギガビットイーサネットなど）を指定します。 • slot/module/port.subinterface：サブインターフェイスを識別するサブインターフェイスの番号（1/0/0.1 など）を指定します。 •（任意）point-to-point：サブインターフェイスがポイントツーポイント サブインターフェイスであることを示します。 •（任意）multipoint：サブインターフェイスがポイントツーマルチポイント サブインターフェイスであることを示します。
ステップ 18	**service-policy output** *parent-policy-name* 例： `Router(config-subif)# service-policy output Parent`	サブインターフェイスに親ポリシー マップを付加します。 • 親ポリシー マップの **output** キーワードと名前を入力します。 （注） 輻輳が発生すると、このクラス キューは指定クラス レベル帯域幅余剰比率に応じて帯域幅を受け取ります。
ステップ 19	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。

残りの帯域幅使用比率の分配の設定例

イーサネット サブインターフェイスでの帯域幅余剰比率の設定例

次に、階層型ポリシーを使用してイーサネット サブインターフェイスに帯域幅余剰比率を設定する例を示します。 この例では、ギガビットイーサネット サブインターフェイス 1/0/0.1 は 100 Mbps にシェーピングされます。 輻輳時、ルータは 10 の帯域幅余剰比率を使用して、インターフェイス上の他のサブインターフェイス レベルとクラス レベルのキューに対して、サブインターフェイス 1/0/0.1 上の非プライオリティ トラフィックに割り当てる超過帯域幅（プライオリティ トラフィックで未使用）の量を指定します。

```
policy-map Child
 class precedence_0
```

```
  bandwidth 10000
 class precedence_1
  shape average 100000
  bandwidth 100
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  shape average 100000000
  service-policy Child
interface GigabitEthernet1/0/0.1
 encapsulation dot1Q 100
 ip address 10.1.0.1 255.255.255.0
 service-policy output Parent
```

クラス キューでの帯域幅余剰比率の確認例

次の設定例では、vlan10_policy はギガビット イーサネット サブインターフェイス 1/0/0.10 に適用され、vlan20_policy はギガビット イーサネット サブインターフェイス 1/0/0.20 に適用されます。サブインターフェイス ギガビット イーサネット 1/0/0.20 の帯域幅余剰比率はサブインターフェイス ギガビット イーサネット 1/0/0.10 の帯域幅余剰比率の 10 倍であるため（サブインターフェイス 1/0/0.20 では 100、サブインターフェイス 1/0/0.10 では 10）、インターフェイス輻輳時に、サブインターフェイス ギガビット イーサネット 1/0/0.20 にはサブインターフェイス ギガビット イーサネット 1/0/0.10 の 10 倍の帯域幅が使用できます。

輻輳がサブインターフェイス レベル内で発生すると、このクラス キューはクラス レベル帯域幅余剰比率に応じて帯域幅を使用します。 例では、クラス precedence_0、precedence_1 および precedence_2 の帯域幅は、それぞれクラス 20、40、および 60 の余剰比率に基づいて割り当てられます。

Router# **show policy-map**

```
Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20 <---- Class-level ratio
    Class precedence_1
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 40 <---- Class-level ratio
    Class precedence_2
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 60 <---- Class-level ratio
Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10 <---- Subinterface-level ratio
      service-policy child-policy
Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 100 <---- Subinterface-level ratio
      service-policy child-policy
interface GigabitEthernet1/0/0.10
 encapsulation dot1Q 10
 snmp trap link-status
 service-policy output vlan10_policy
interface GigabitEthernet1/0/0.20
 encapsulation dot1Q 20
```

```
 snmp trap link-status
 service-policy output vlan20_policy
```

帯域幅余剰比率の確認例

次の show policy-map interface コマンドの出力例では、ギガビット イーサネット サブインターフェイス 1/0/0.10 に付加されている vlan10_policy というポリシー マップと子ポリシーのクラス レベル キューに帯域幅余剰比率が設定されています。

```
Router# show policy-map interface GigabitEthernet 1/0/0.10
GigabitEthernet1/0/0.10
  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 10
      Service-policy : child-policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

次の show policy-map interface コマンドの出力例では、ギガビット イーサネット サブインターフェイス 1/0/0.20 に付加されている vlan20_policy というポリシー マップと子ポリシーのクラス レベル キューに帯域幅余剰比率が設定されています。

```
Router# show policy-map interface GigabitEthernet 1/0/0.20
GigabitEthernet1/0/0.20
  Service-policy output: vlan20_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 100
      Service-policy : child-policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

show policy-map コマンドの次の出力例では、vlan10_policy というポリシー マップの親 class-default クラスで帯域幅余剰比率が 10 に設定されています。

```
Router# show policy-map vlan10_policy
  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
```

```
      bandwidth remaining ratio 10
      service-policy child-policy
```

show policy-map コマンドの次の出力例では、vlan20_policy というポリシーマップの親 class-default クラスで帯域幅余剰比率が 100 に設定されています。

```
Router# show policy-map vlan20_policy
  Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 100
      service-policy child-policy
```

show policy-map コマンドの次の出力例では、クラス キュー precedence_0、precedence_1 および precedence_2 で、帯域幅余剰比率がそれぞれ 20、40、60 に設定されています。

```
Router# show policy-map child-policy
  Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20
    Class precedence_1
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 40
    Class precedence_2
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 60
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
輻輳回避	「輻輳回避の概要」モジュール
クラス マップ、ポリシー マップ、階層型ポリシー マップ、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）	「MQC を使用した QoS 機能の適用」モジュール
トラフィック シェーピング、トラフィック ポリシング	「ポリシングとシェーピングの概要」モジュール

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

残りの帯域幅使用比率の分配の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *2*：残りの帯域幅使用比率の分配の機能情報

機能名	リリース	機能情報
MQC：残りの帯域幅使用比率の分配	Cisco IOS XE Release 2.1	残りの帯域幅使用比率の分配機能を使用すると、すべてのサービス プロバイダーが、サブインターフェイスおよびクラス キューに帯域幅余剰比率を設定することができます。 この比率は、他のサブインターフェイスまたはキューに関して、サブインターフェイスまたはキューに対する相対的重みを指定します。 輻輳時に、ルータはこの帯域幅余剰比率を使用して、非プライオリティ トラフィック クラスに割り当てる超過帯域幅（プライオリティ トラフィックで未使用）の量を指定します。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ ルータに導入されました。 この機能により、**bandwidth remaining ratio**、 **show policy-map**、 **show policy-map interface** コマンドが導入または変更されました。

第 4 章

QoS パーセントベース シェーピング

QoS：パーセントベース シェーピングを使用すると、インターフェイスで使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 シェーピングを設定することができます。 この機能を使用すると、認定（準拠）バースト（bc）サイズおよび超過（ピーク）バースト（be）サイズ（トラフィック シェーピングの設定に使用）をミリ秒（ms）単位で指定することもできます。この方法でトラフィック シェーピングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

QoS パーセントベース シェーピングの概要

QoS パーセントベース シェーピングの利点

この機能を使用すると、インターフェイスで使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 シェーピングを設定し、バースト サイズをミリ秒単位で指定できます。 この方法でトラフィック シェーピングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。 つまり、各インターフェイスの帯域幅を再計算したり、インターフェイスのタイプごとに別のポリシー マップを設定したりする必要はありません。

QoS パーセントベース シェーピングのクラスおよびポリシー マップ

QoS：パーセントベース シェーピング機能を設定するには、トラフィック クラスを定義し、ポリシーマップを設定してから、そのポリシーマップを適切なインターフェイスにアタッチする必要があります。

MQC では、**class-map** コマンドは、トラフィック クラスの定義に使用されます（トラフィック クラスは、その後、トラフィック ポリシーに関連付けされます）。 トラフィック クラスの目的は、トラフィックを分類することです。

MQC は、次の 3 つのプロセスで構成されます。

- **class-map** コマンドを使用したトラフィック クラスの定義
- トラフィック クラスを 1 つまたは複数の QoS 機能と関連付けてトラフィック ポリシーを作成（**policy-map** コマンドを使用）
- **service-policy** コマンドを使用した、トラフィック ポリシーのインターフェイスへのアタッチ

トラフィック クラスには、3 つの主な要素が含まれます。名前、一連の match コマンド、そしてトラフィック クラスに **match** コマンドが複数存在する場合にこれらの **match** コマンド（match-all または match-any）の評価の仕方についての指定です。 トラフィック クラスの名前は、**class-map** コマンド ラインで付けます。たとえば、CLI でトラフィック クラスを設定するときに **class-map cisco** コマンドを入力すると、トラフィック クラスの名前は「cisco」になります。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。 パケットは、**match** コマンドで指定された基準に合っているかどうかを判断するために、チェックされます。 指定された基準に合っていれば、パケットはクラスのメンバーと見なされ、トラフィック ポリシーで設定された QoS 仕様に従って転送されます。 一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

トラフィック規制メカニズムと帯域幅のパーセンテージ

Cisco IOS XE Quality of Service（QoS）では、トラフィック ポリシングとトラフィック シェーピングという 2 種類のトラフィック規制メカニズムが提供されています。 トラフィック ポリサーは、通常、特定のレートに違反するトラフィックをドロップします。 トラフィック シェーパーは、通常、パケットを保持するバッファを使用して過剰なトラフィックを遅延し、キューに対するデータ レートが予想より高い場合に、フローをシェーピングします。

トラフィック シェーピングとトラフィック ポリシングは連携して機能し、クラス マップで設定できます。 クラス マップは、データ パケットを特定のカテゴリ（「クラス」）に編成します。 ポリシー マップ（しばしば「サービス ポリシー」とも呼ばれる）で使用すると、ユーザ定義の QoS 処理を受信できます。

この機能が導入されるまでは、トラフィック ポリシングおよびトラフィック シェーピングはインターフェイスで使用可能な帯域幅のユーザ指定の量に基づいて設定されています。 ポリシーマップは、その後で特定の量の帯域幅に基づいて設定されていました。 このため、各インターフェイスに別々のポリシー マップが必要とされていました。

この機能を使用すると、インターフェイスで使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 ポリシングおよびトラフィック シェーピングを設定できます。 この方法でトラフィック ポリシングおよびトラフィック シェーピングを設定すると、顧客は帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

帯域幅のパーセンテージに基づいたトラフィック ポリシングおよびトラフィック シェーピングの設定は、**police** (percent) コマンドおよび **shape** (percent) コマンドを使用して実行されます。

ミリ秒オプションで指定されたバースト サイズ

バースト パラメータ（bc および be）の目的は、トラフィックがドロップまたは遅延する前の正常な動作状況で予測されるトラフィック量を指定することです。 十分に高いバースト値を設定すると、適切なスループットを確実に実現できます。

この機能を使用すると、トラフィック シェーピングを設定する際、認定（準拠）バースト（bc）サイズおよび超過（ピーク）バースト（be）サイズをクラス帯域幅のミリ秒（ms）単位で指定することができます。 ミリ秒の値は、QoS：パーセントベース シェーピング機能が使用するバイト数を計算するために使用されます。

ミリ秒単位でこれらのバースト サイズを指定する場合、**shape** (percent) コマンドの **bc** キーワードと **be** キーワード（および関連付けられている引数）を使用して実行します。

QoS パーセントベース シェーピングの設定方法

クラスおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name*| **class-default**}
5. **shape** {**average** | **peak**} **percent** *percentage* [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map** *policy-name* 例： `Router(config)# policy-map policy1`	作成するポリシー マップの名前を指定します。 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。 • ポリシー マップ名を入力します。
ステップ 4	**class** {*class-name*| **class-default**} 例： `Router(config-pmap)# class class1`	ポリシーを設定または変更できるようにクラスを指定します。 ポリシーマップ クラス コンフィギュレーション モードを開始します。 • クラス名を入力するか、デフォルト クラス（class-default）を指定します。

	コマンドまたはアクション	目的
ステップ 5	**shape** {**average** | **peak**} **percent** *percentage* [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**] 例： `Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms`	指定された帯域幅のパーセンテージとオプションのバーストサイズに基づいて、平均またはピーク レート トラフィック シェーピングを設定します。 • 帯域幅のパーセンテージとオプションのバーストサイズを入力します。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	ポリシーマップ クラス コンフィギュレーション モードを終了します。

ポリシー マップのインターフェイスへの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**interface** *type number*
	
	例：
	`Router(config)#`
	`interface serial4/0/0`
		インターフェイス（サブインターフェイス）タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
		• インターフェイスのタイプ番号を入力します。
		（注） ネットワークのニーズにより、ポリシーマップをサブインターフェイス、ATM PVC、フレームリレー DLCI、または他のタイプのインターフェイスにアタッチする必要がある場合もあります。

ステップ 4	**pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**] 例： `Router(config-if)# pvc cisco 0/16 ilmi`	（任意）ATM PVC に名前を作成するか割り当て、ATM PVC でカプセル化タイプを指定します。 ATM VC コンフィギュレーション モードを開始します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。 ATM PVC にポリシー マップをアタッチしない場合は、この手順をスキップして、ポリシー マップのインターフェイスへの適用 に進みます。

ステップ 5	**service-policy** {**input**| **output**} *policy-map-name*
	
	例：
	`Router(config-if)#`
	`service-policy input policy1`
	
	例：
		インターフェイスの入力または出力方向にアタッチするポリシー マップの名前を指定します。
		（注） ポリシー マップは、入力または出力ルータで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。 ポリシー マップを適用する方向（入力または出力）とルータ（入力または出力）は、ネットワーク構成に従って変わります。 **service-policy** コマンドを使用してポリシー マップをインターフェイスに適用する場合、ネットワーク構成に適したルータおよびインターフェイスの方向を選択してください。
		（注） トラフィック シェーピングは、出力インターフェイスや出力 VC にアタッチされているサービス ポリシーでのみサポートされます。
		• ポリシー マップ名を入力します。

ステップ 6	**end** 例： `Router(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了します。

QoS パーセントベース シェーピングの設定確認

手順の概要

1. **enable**
2. **show class-map** [*class-map-name*]
3. **show policy-map interface** *interface-name*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show class-map** [*class-map-name*] 例： `Router# show class-map class1`	一致基準を含めて、クラスマップに関するすべての情報が表示されます。 • クラス マップ名を入力します。
ステップ 3	**show policy-map interface** *interface-name* 例： `Router# show policy-map interface serial4/0/0`	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。 • インターフェイス タイプと番号を入力します。
ステップ 4	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

トラブルシューティングのヒント

QoS パーセントベース シェーピングの設定確認, （35 ページ）に示すコマンドを使用すると、意図した設定を実現し、機能が正しく働いていることを確認できます。 上記の **show** コマンドの使用後に、設定が正しくない、または機能が予想どおりに働いていないと判明した場合は、次の操作を実行します。

意図したとおりに設定が行われていない場合は、次の手順を完了します。

1. **show running-config** コマンドを使用して、コマンドの出力を分析します。
2. ポリシー マップが **show running-config** コマンドの出力に表示されない場合は、**logging console** コマンドをイネーブルにします。
3. ポリシー マップをインターフェイスに再度アタッチします。

パケットが正確に一致していない場合は（たとえば、パケット カウンタが正しく増加していないなど）、次の手順を完了します。

1. **show policy-map** コマンドを実行して、コマンドの出力を分析します。
2. **show running-config** コマンドを実行して、コマンドの出力を分析します。
3. **show policy-map interface** コマンドを実行して、コマンドの出力を分析します。 次の内容を確認します。
    1. ポリシー マップにキューイングが適用され、パケットが正しいクラスに一致しているにもかかわらず、予期しない結果が生じる場合は、キューのパケット数と一致したパケット数を比較します。
    2. インターフェイスが混雑していて、一致するパケット数が少ない場合、送信（tx）リングの調整を確認し、tx リングでキューイングが実行されているかどうかを評価します。 このためには、**show controllers** コマンドを使用し、コマンドの出力で、tx 回数の値を確認します。

QoS パーセントベース シェーピングの設定例

帯域幅のパーセンテージに基づいたトラフィックシェーピングを指定する例

次に、帯域幅の割合に基づいた平均シェーピング レートを使用するトラフィック シェーピングの設定例を示します。 この例では、帯域幅の 25% が指定されています。 さらに、オプションの be 値と bc 値（それぞれ、300 ms と 400 ms）が指定されています。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1

Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms

Router(config-pmap-c)# end
```

ポリシーマップとクラスマップの設定後、ポリシーマップは次の例に示すように、インターフェイスにアタッチされます。

```
Router> enable
Router# configure terminal
Router(config)#
```

```
interface serial4/0/0
Router(config-if)#

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

QoS パーセントベース シェーピングを確認する例

次に、**show policy-map** コマンドおよび **show policy-map interface** コマンドの出力例を示します。これらのコマンドの出力は、ネットワーク上の設定の確認およびモニタに使用できます。

次は、**show policy-map** コマンドの出力例です。 この出力例には、「policy3」というポリシーマップの内容が表示されています。policy 3 では、30% の認定情報レート（CIR）に基づく平均レートのトラフィック シェーピングが設定されており、bc および be がミリ秒の単位で指定されています。

```
Router# show policy-map
  Policy Map policy3
    Class class-default
      Average Rate Traffic Shaping
      cir 30% bc 10 (msec) be 10 (msec)
```

次は、**show policy-map interface** コマンドのサンプル出力です。 このサンプルには、平均レートのトラフィック シェーピングがイネーブルにされている、シリアル 2/0 インターフェイスの統計情報が表示されています。

```
Router# show policy-map interface serial2/0/0
 Serial2/0/0
  Service-policy output: policy3 (1032)
    Class-map: class-default (match-any) (1033/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1034)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 0/0
      shape (average) cir 614400 bc 6144 be 6144
      target shape rate 614400
```

この例では、CIR は bps で表示され、認定バースト（bc）と超過バースト（be）の両方が、ビットで表示されます。

CIR、bc、および be は、以下に説明する式に基づいて計算されます。

CIR 計算用の式

CIR を計算する場合は、次の式を使用します。

指定された CIR パーセンテージ（**show policy-map** コマンドの出力に示すとおり）X インターフェイスの帯域幅（BW）（ **show interfaces** コマンドの出力に示すとおり）= 合計ビット/秒単位

シリアル 2/0 インターフェイスでは、帯域幅（BW）は 2048 kbps です。 インターフェイスの帯域幅を確認するには、**show interfaces** コマンドを使用します。 次に例を示します。

```
Router # show interfaces serial2/0/0
Serial2/0 is administratively down, line protocol is down
```

```
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

したがって、次の値が式で使用されます。

30% X 2048 kbps = 614400 bps

認定バースト（bc）および超過バースト（be）の計算式

bc および be の両方を計算する場合は、次の式を使用します。

ミリ秒単位の bc（または be）（**show policy-map** コマンドに示すとおり）X キロバイト単位の CIR（**show policy-map** コマンドに示すとおり）/ 1000 = 総ビット数。

したがって、次の値が式で使用されます。

10 ms X 614400 bps = 6144 bits

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
インターフェイスへのポリシーマップの付加についてのモジュラ QoS コマンドライン インターフェイス（CLI）（MQC）情報	「MQC を使用した QoS 機能の適用」モジュール
トラフィック シェーピングの概念と概要	「ポリシングとシェーピングの概要」モジュール
トラフィック ポリシング	「トラフィック ポリシング」モジュール

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

QoS パーセントベース シェーピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *3*：*QoS*：パーセントベース シェーピングの機能情報

機能名	リリース	機能情報
QoS：パーセントベース シェーピング	Cisco IOS XE Release 2.1	QoS：パーセントベース シェーピングを使用すると、インターフェイスで使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 シェーピングを設定することができます。 この機能を使用すると、認定（準拠）バースト（bc）サイズおよび超過（ピーク）バースト（be）サイズ（トラフィック シェーピングの設定に使用）をミリ秒（ms）単位で指定することもできます。 この方法でトラフィック シェーピングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能により、**shape (percent)**、 **show policy-map**、**show policy-map interface** コマンドが導入または変更されました。

第 5 章

イーサネットオーバーヘッドアカウンティング

イーサネット オーバーヘッド アカウンティング機能は、パケットにシェーピングを適用するとき、ルータがダウンストリーム イーサネット フレーム ヘッダーを考慮に入れるようにします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

イーサネットオーバーヘッドアカウンティングの制約事項

- イーサネット オーバーヘッド アカウンティングでは、ダウンストリーム イーサネット フレーム ヘッダーをシェーピングされたレートに自動的に含めることができます。 ただし、イーサネット オーバーヘッド アカウンティングではポリシングはサポートされません。
- ルータは、shapeおよびbandwidthコマンドに限りオーバーヘッドアカウンティングをサポートします。
- 子ポリシーでオーバーヘッド アカウンティングをイネーブルにする場合は、親ポリシーでオーバーヘッド アカウンティングをイネーブルにする必要があります。
- ポリシー マップで、ポリシーのすべてのクラスに対してオーバーヘッド アカウンティングをイネーブルにするか、またはディセーブルにする必要があります。 同じポリシー内の一部のクラスに対してオーバーヘッドアカウンティングをイネーブルにし、残りのクラスに対してオーバーヘッド アカウンティングをディセーブルにすることはできません。
- オーバーヘッド アカウンティングは、どの QoS カウンタ（分類、ポリシング、キューイング）にも反映されません。
- 最上位親ポリシー、中位子ポリシー、最下位子ポリシーで、シェーピングおよび帯域幅のオーバーヘッド アカウンティングをイネーブルにできます。 子ポリシーは、親または親の親レベルで設定するオーバーヘッド アカウンティング ポリシーを継承します。

イーサネットオーバーヘッドアカウンティングに関する情報

イーサネット オーバーヘッド アカウンティングの利点

イーサネット オーバーヘッド アカウンティング機能は、パケットにシェーピングを適用するとき、ルータがダウンストリーム イーサネット フレーム ヘッダーを考慮に入れるようにします。 ユーザ定義のオフセットにより、パケット単位オーバーヘッドを計算するときに、ルータが使用するオーバーヘッド バイト数が指定されます。 有効なオフセット値は、オーバーヘッドの +63～-63 バイトです。 シェーピングを適用する前に、ルータはオーバーヘッドを計算します。

イーサネットインターフェイスおよびサブインターフェイスは、オーバーヘッドアカウンティングをサポートします。 **shape** または **bandwidth** コマンドを使用して、VLAN 単位およびポート単位でアカウンティングを設定できます。

加入者線カプセル化タイプ

shape コマンドおよび **bandwidth** コマンドの *subscriber-encapsulation* 引数は、加入者線でのカプセル化タイプを指定します。 ルータは、次の加入者線カプセル化タイプをサポートします。

- snap-1483routed
- mux-1483routed
- snap-dot1q-rbe
- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-rbe
- mux-rbe

ルータ上のオーバーヘッド計算

トラフィック シェーピングのオーバーヘッドを計算するとき、ルータはBRASとDigital Subscriber Line Access Multiplexer（DSLAM）の間と、DSLAMとCustomer Premises Equipment（CPE）の間で使用するカプセル化タイプを考慮します。

次の表は、ルータがATMオーバーヘッドを計算するときにさまざまなカプセル化タイプに使用するフィールドを示します。

表 *4*：オーバーヘッド計算

カプセル化タイプ	バイト数	説明
802.1Q	18	6バイト宛先MACアドレス＋6バイト発信元MACアドレス＋2バイト プロトコルID（0x8100）＋2バイトVLAN ID（VID）/Canonical Format Indicator（CFI）/PRIORITY＋2バイト長/タイプ
802.3	14	6バイト宛先MACアドレス＋6バイト発信元MACアドレス＋2バイト プロトコルID（0x8000）
AAL5 MUX プラス 1483	8	8バイト AAL5 トレーラ

カプセル化タイプ	バイト数	説明
AAL5 MUX プラス PPP over ATM（PPPoA）	10	8 バイト AAL5 トレーラ + 2 バイト プロトコル ID（0x002）
AAL5 SNAP プラス 1483	18	8 バイト AAL5 トレーラ + 3 バイト LLC ヘッダー（0xAAAA03） + 3 バイト OUI（0x0080c2） + 2 バイト プロトコル ID（0x0007） + 2 バイト PAD（0x0000）
AAL5 SNAP プラス PPPoA	12	8 バイト AAL5 トレーラ + 3 バイト LLC ヘッダー（0xFEFE03） + 1 バイト プロトコル ID（0xCF）
PPPoE	6	1 バイト バージョン/タイプ（0x11） + 1 バイト コード（0x00） + 2 バイト セッション ID + 2 バイト長
qinq	22	6 バイト宛先 MAC アドレス + 6 バイト発信元 MAC アドレス + 2 バイト プロトコル ID（0x8100） + 2 バイト VID/CFI/PRIORITY + 2 バイト プロトコル ID + 2 バイト内側タグ + 2 バイト長またはタイプ

オーバーヘッド アカウンティングと階層型ポリシー

階層型ポリシーでは、最上位親ポリシー、中位子ポリシー、最下位子ポリシーで、シェーピングおよび帯域幅のオーバーヘッドアカウンティングを設定できます。親または親の親レベルで設定したオーバーヘッド アカウンティング ポリシーは子のキューイング機能で継承されます。 子ポリシーで設定したオーバーヘッドアカウンティングも親ポリシーで設定する必要があります。これで、親または親の親レベルでの設定が容易になります。

親クラスおよび子クラスは、**bandwidth**（ポリシー マップ クラス）コマンドの **user-defined** *offset* [**atm**] 引数を使用してオーバーヘッド アカウンティングをイネーブルにしてオフセットを設定するときに、同じカプセル化タイプを指定する必要があります。

次の表は、オーバーヘッド アカウンティングの設定要件について説明します。

表 *5*：オーバーヘッド アカウンティングの設定要件

ポリシー マップまたはクラス	現在の設定	設定要件
親	イネーブル	子ポリシーでイネーブル
子	イネーブル	親ポリシーでイネーブル
子クラス	イネーブル	ポリシング付きのプライオリティ クラスを除く、子ポリシー マップのすべてのクラスでイネーブル
子クラス（ポリシングなしの非プライオリティ）	ディセーブル	子ポリシー マップのすべてのクラスでディセーブル
子クラス（ポリシング付きのプライオリティ）	ディセーブル	子ポリシー マップのすべての非プライオリティ クラスでディセーブルまたはイネーブル

イーサネットオーバーヘッドアカウンティングの設定方法

階層型ポリシーでのイーサネット オーバーヘッド アカウンティングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. **bandwidth** {*bandwidth-kbps* | [**remaining**] **percent** *percentage*} **account** {**qinq** | **dot1q**} {**aal5** | **aal3**} *subscriber-encapsulation* **user-defined** *offset* [**atm**]
6. exit
7. **policy-map** *policy-map-name*
8. **class class-default**
9. **shape** [**average**] *rate* **account** {{**qinq** | **dot1q**} {**aal5** | **aal3**} *subscriber-encapsulation* | **user-defined** *offset* [**atm**]}
10. **service-policy** *policy-map-name*
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**policy-map** *policy-map-name* 例： `Router(config)# policy-map Business`	子ポリシーを作成または変更します。 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。 • *policy-map-name* 引数は子ポリシー マップの名前です。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class video`	指定するトラフィック クラスをポリシー マップに割り当てます。 ポリシーマップ クラス コンフィギュレーション モードを開始します。 • *class-map-name* 引数は設定済みのクラス マップの名前です。
ステップ 5	**bandwidth** {*bandwidth-kbps* | [**remaining**] **percent** *percentage*} **account** {**qinq** | **dot1q**} {**aal5** | **aal3**} *subscriber-encapsulation* **user-defined** *offset* [**atm**] 例： `Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`	クラスベース均等化キューイングおよびオーバーヘッド アカウンティングをイネーブルにします。 • *bandwidth-kbps*：ポリシー マップに属しているクラスに割り当てる最小帯域幅。 有効な値は、リンク帯域幅の 1～99% に相当する 8～2,488,320 です。 • *percentage*：ポリシー マップに属するクラスに割り当てられるリンク帯域幅の最大パーセンテージ。 有効値は 1 ～ 99 です。 • **remaining** *percentage*：ポリシーマップに属するクラスに割り当てられる使用されていないリンク帯域幅の最小パーセンテージ。 有効値は 1 ～ 99 です。 • **account**：ATM オーバーヘッド アカウンティングをイネーブルにします。 • **qinq**：QinQ カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **dot1q**：IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **aal5**：コネクション型可変ビット レート（VBR）サービスをサポートする ATM アダプテーション層 5 を指定します。 • **aal3**：コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。 • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。 詳細については、「階層型ポリシーでのイーサネット オーバーヘッド アカウンティングの設定」の項を参照してください。 • **user-defined**：ATM オーバーヘッドを計算するときに、指定したオフセット値をルータが使用することを示します。 • *offset*：オーバーヘッドを計算するときにルータが使用するバイト数を指定します。 -63 ～ 63 バイトの範囲内の値を指定できます。

	コマンドまたはアクション	目的
		• **atm**：（任意）ATM オーバーヘッド計算に ATM セル タックスを適用します。
ステップ 6	exit 例： `router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 7	**policy-map** *policy-map-name* 例： `Router(config-pmap)# policy-map Test`	最上位親ポリシーを作成または変更します。 • *policy-map-name*：親ポリシー マップの名前を指定します。
ステップ 8	**class class-default** 例： `Router(config-pmap)# class class-default`	デフォルト クラスを指定します。
ステップ 9	**shape** [**average**] *rate* **account** {{**qinq** | **dot1q**} {**aal5** | **aal3**} *subscriber-encapsulation* | **user-defined** *offset* [**atm**]} 例： `Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1-rbe`	指示されたビット レートにトラフィックをシェーピングし、オーバーヘッド アカウンティングをイネーブルにします。 • **average**：（任意）各間隔で送信される最大ビット数を指定する認定バースト（Bc）です。 このオプションがサポートされるのは Performance Routing Engine 3（PRE3）だけです。 • **rate**：トラフィックのシェーピングに使用されるビット レート（bps）です。 このコマンドを逆方向明示的輻輳通知（BECN）の近似値と併用すると、ビット レートは許容ビット レート範囲の上限値になります。 • **account**：ATM オーバーヘッド アカウンティングをイネーブルにします。 • **qinq**：QinQ カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • dot1q：IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **aal5**：コネクション型可変ビット レート（VBR）サービスをサポートする ATM アダプテーション層 5 を指定します。 • **aal3**：コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。

	コマンドまたはアクション	目的
		• *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、「階層型ポリシーでのイーサネット オーバーヘッド アカウンティングの設定」の項を参照してください。 • **user-defined**：ATM オーバーヘッドを計算するときに、指定したオフセット値をルータが使用することを示します。 • *offset*：オーバーヘッドを計算するときにルータが使用するバイト数を指定します。 -63 ～ 63 バイトの範囲内の値を指定できます。 • **atm**：（任意）ATM オーバーヘッド計算に ATM セル タックスを適用します。 offset オプションと atm オプションの両方を設定すると、パケット サイズがオフセット サイズに調整され、ATM セル タックスが追加されます。
ステップ 10	**service-policy** *policy-map-name* 例： `Router(config-pmap-c)# service-policy map1`	親 class-default クラスに子ポリシーを適用します。 *policy-map-name*：設定済みの子ポリシー マップの名前を指定します。 （注） 子ポリシーを親 class-default クラスに適用する場合、入力キーワードまたは出力キーワードを指定しないでください。
ステップ 11	**end** 例： `Router(config-pmap-c)# end`	

オーバーヘッド アカウンティングの検証

手順の概要

1. **enable**
   - パスワードを入力します（要求された場合）。
2. **show policy-map** [*policy-map-name*]
   - （任意）ポリシーマップ名を入力します。名前には最大40文字までの英数字を指定できます。
3. **show policy-map interface**
4. **show running-config**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** • パスワードを入力します（要求された場合）。 例： `Router> enable`	特権EXECモードなど、高位の権限レベルをイネーブルにします。
ステップ2	**show policy-map** [*policy-map-name*] • （任意）ポリシー マップ名を入力します。 名前には最大 40 文字までの英数字を指定できます。 例： `Router# show policy-map unit-test`	（任意）指定したポリシーマップに関する全クラスの設定、または、既存の全ポリシーマップに関する全クラスの設定を表示します。
ステップ3	**show policy-map interface** 例： `Router# show policy-map serial2/0`	（任意）インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	**show running-config** 例： `Router# show running-config`	（任意）現在実行中のコンフィギュレーション ファイルの内容を表示します。
ステップ 5	**exit** 例： `Router(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了します。

イーサネットオーバーヘッドアカウンティングの設定例

例：イーサネット オーバーヘッド アカウンティングのイネーブル化

次の設定例は、イーサネットオーバーヘッドアカウンティングをイネーブルにする方法を示します。 次の例では、ethernet_ovrh ポリシー マップの設定は 200,000 kbps のレートで class-default トラフィックをシェーピングし、ユーザ定義値 18 を使用してオーバーヘッド アカウンティングをイネーブルにします。 ethernet_ovrh ポリシーはサブインターフェイス ギガビット イーサネット 1/0/0.100 に関連付けられているため、サブインターフェイスでオーバーヘッド アカウンティングがイネーブルになります。

```
Router# configure-terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map ethernet_ovrh
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 200000 account user-defined 18
!
Router(config)# interface GigabitEthernet1/0/0.100
Router(config-subif)# service-policy output ethernet_ovrh
!
Router# show running-config | begin 1/0/0.100
interface GigabitEthernet1/0/0.100
encapsulation dot1Q 101
pppoe enable group group_pta
service-policy output ethernet_ovrh
```

例：イーサネット オーバーヘッド アカウンティングの確認

次の例は、ATM オーバーヘッド アカウンティングがシェーピングに対してイネーブルであることを示す、**show running-config** コマンドの出力の一部を示します。 BRAS-DSLAM カプセル化は dot1q で、加入者線カプセル化は AAL5 サービスに基づく snap-rbe です。

```
subscriber policy recording rules limit 64
```

```
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average 10 account dot1q aal5 snap-rbe
```

例：ユーザ定義オプションを使用したイーサネット オーバーヘッド アカウンティングの確認

次の例は、イーサネットオーバーヘッドアカウンティングがシェーピングに対してイネーブルであり、ユーザ定義オフセットが 18 バイトであることを示す、ethernet_ovrh ポリシーマップの出力を示します。 **show policy-map** コマンドの出力例は、ethernet_ovrh ポリシーマップがサブインターフェイス ギガビット イーサネット 1/0/0.100 に関連付けられており、サブインターフェイスでオーバーヘッド アカウンティングがイネーブルになっていることを示します。

```
Router# show policy-map ethernet_ovrh
Policy Map ethernet_ovrh
Class class-default
Average Rate Traffic Shaping
cir 200000 (bps) account user-defined 18
Router# show policy-map interface GigabitEthernet1/0/0.100
GigabitEthernet1/0/0.100
Service-policy output: ethernet_ovrh
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 8 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 200000, bc 800, be 800
target shape rate 200000
Overhead Accounting Enabled
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『Cisco IOS Quality of Service Solutions Command Reference』
ポリシングとシェーピング	「ポリシングとシェーピングの概要」モジュール
クラス マップ	「MQC を使用した QoS 機能の適用」モジュール
ポリシー マップ	「MQC を使用した QoS 機能の適用」モジュール

標準

標準	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

イーサネットオーバーヘッドアカウンティングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *6*：イーサネット オーバーヘッド アカウンティングの機能情報

機能名	リリース	機能情報
イーサネット オーバーヘッド アカウンティング	Cisco IOS XE Release 2.4	イーサネット オーバーヘッド アカウンティング機能が Cisco ASR 1000 シリーズ ルータに導入されました。 これで、パケットにシェーピングを適用する際に、ルータがダウンストリーム イーサネット フレーム ヘッダーを考慮できるようになります。

機能名	リリース	機能情報
親レベルのオーバーヘッド アカウンティング	Cisco IOS XE Release 3.9S	親レベルのオーバーヘッド アカウンティング機能が Cisco ASR 1000 シリーズ ルータに導入されました。 これで、子ポリシーが親または親の親レベルで設定するオーバーヘッド アカウンティング ポリシーを継承できるようになります。

QoS：ポリシングおよびシェーピング コンフィギュレーション ガイド、**Cisco IOS XE Release 3S**（**Cisco ASR 1000**）

第 6 章

ATMのMQCトラフィックシェーピングオーバーヘッドアカウンティング

ATM の MQC トラフィック シェーピング オーバーヘッド アカウンティング機能を使用すれば、ブロードバンド集約システム（BRAS）で、パケットに Quality of Service（QoS）機能を適用するときにさまざまなカプセル化タイプを考慮できます。 一般的に、イーサネット デジタル加入者線（DSL）環境では、ルータからデジタル加入者線アクセス マルチプレクサ（DSLAM）までのカプセル化がギガビット イーサネットで、DSLAM から加入者宅内機器（CPE）までのカプセル化が ATM です。 ATM オーバーヘッド アカウンティングを使用すれば、ルータで、加入者線上の ATM カプセル化と、セル分割で増加したオーバーヘッドを考慮できます。 この機能を使用すれば、サービス プロバイダーは加入者線でのオーバーランを防止することができ、ルータでは ATM パケットで使用される実際の帯域幅に対して QoS 機能を実行できるようになります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する前提条件

トラフィックは **class-map** コマンドを使用して設定する必要があります。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する制約事項

- ポリシー マップ内で使用されるカプセル化タイプと、親ポリシー マップと子ポリシー マップ間で使用されるカプセル化タイプを同じにする必要があります。
- ATM オーバーヘッド アカウンティングを含むように設定されたポリシー マップは、イーサネット インターフェイス（またはイーサネット インターフェイス上の IP セッション）以外に対応付けないようにする必要があります。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングについて

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの利点

ATM のトラフィック シェーピング オーバーヘッド アカウンティング機能を使用すれば、BRAS でパケットに QoS を適用するときにさまざまなカプセル化タイプを考慮できます。 一般的に、イーサネット DSL 環境では、BRAS から DSLAM までのカプセル化がギガビット イーサネット

で、DSLAM から CPE までのカプセル化が ATM です。 ATM オーバーヘッド アカウンティングを使用すれば、BRAS で、加入者線上の ATM カプセル化と、セル分割で増加したオーバーヘッドを考慮できます。 この機能を使用すれば、サービスプロバイダーは加入者線でのオーバーランを防止することができ、ルータでは ATM 加入者トラフィックで使用される実際の帯域幅に対して QoS 機能を実行できるようになります。

BRAS とカプセル化タイプ

BRAS は、DSLAM-CPE 側用に設定されたカプセル化タイプを使用して、パケット当たりの ATM オーバーヘッドを計算します。

DSLAM-CPE カプセル化タイプは、サブネットワーク アクセス プロトコル（SNAP）と、ATM アダプテーション層 5（AAL5）の後ろに Routed BridgE（RBE）、x-1483、x-dot1q-rbe、IP、PPP over Ethernet（PPPoE）、または PPP over ATM（PPPoA）カプセル化が続くマルチプレクサ（MUX）フォーマットに基づいています。 DSLAM は IP パケットと PPPoE パケットをペイロードとして扱うため、BRAS は IP カプセル化と PPPoE カプセル化を考慮しません。

BRAS-DSLAM 側のカプセル化は IEEE 802.1Q VLAN または Q-in-Q（qinq）です。 ただし、DSLAM は BRAS-DSLAM カプセル化を削除するため、BRAS は 802.1Q または qinq カプセル化を考慮しません。

AAL5 の分割処理によって、5 バイトのセルヘッダー、AAL5 コンバージェンス副層共通部（CPCS）パディング、および AAL5 トレーラのオーバーヘッドが追加されます。 詳細については、ATM オーバーヘッドの計算, （60 ページ）を参照してください。

加入者線カプセル化タイプ

ルータは、次の加入者線カプセル化タイプをサポートします。

- snap-rbe
- mux-rbe
- snap-dot1q-rbe
- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-1483routed
- mux-1483routed
- snap-rbe-dot1q
- mux-rbe-dot1q

（注） 上記カプセル化タイプは、AAL5、qinq、および dot1q カプセル化用です。 使用されているプラットフォームに基づくオフセットを使用したユーザ定義のカプセル化もサポートされます

ATM オーバーヘッドの計算

ATM のトラフィック シェーピング オーバーヘッド アカウンティング機能は、BRAS での ATM カプセル化オーバーヘッドを考慮することによって、加入者線のオーバーサブスクリプションを防止します。 ATM オーバーヘッドを計算するときに、ATM のトラフィック シェーピング オーバーヘッド アカウンティング機能は次の要素を考慮します。

- BRAS で使用されるカプセル化タイプ
- CPCS トレーラ オーバーヘッド
- DSLAM と CPE 間で使用されるカプセル化タイプ

次の式を使用してオフセット サイズ（ATM オーバーヘッド アカウンティングの計算に使用されるパラメータ）が計算されます。

バイト単位のオフセット サイズ = (CPCS トレーラ オーバーヘッド) + (DSLAM と CPE 間) - (BRAS カプセル化タイプ)

この公式から得られたバイト単位のオフセット サイズについては、次の表を参照してください。

このオフセット サイズと一緒に CPCS 内のパケット サイズとパケット アセンブラ/ディスアセンブラ（PAD）がルータでの ATM オーバーヘッド アカウンティング レートの計算に使用されます。

（注） 8 バイトの CPCS トレーラ オーバーヘッドが AAL5 に対応します。 4 バイトの CPCS トレーラ オーバーヘッドが AAL3 に対応しますが、AAL3 はサポートされません。

表 7：***ATM*** **オーバーヘッドの計算に使用されるバイト単位のオフセット サイズ**

使用されているカプセル化タイプ	**BRAS**	**CPCS** トレーラ オーバーヘッド	**DSLAM** と **CPE** 間	オフセット サイズ
dot1q mux-1483routed	18	8	3	-7
dot1q snap-1483routed	18	8	6	-4
dot1q mux-rbe	18	8	14	4
dot1q snap-rbe	18	8	24	14
dot1q mux-dot1q-rbe	18	8	18	8

使用されているカプセル化タイプ	BRAS	CPCS トレーラ オーバーヘッド	DSLAM と CPE 間	オフセット サイズ
dot1q snap-dot1q-rbe	18	8	28	18
qot1q mux-pppoa	18 + 6	8	2	-14
qot1q snap-pppoa	18 + 6	8	4	-12
qinq mux-1483routed	22	8	3	-11
qinq snap-1483routed	22	8	6	-8
qinq mux-rbe	22	8	14	0
qinq snap-rbe	22	8	24	10
qinq mux-dot1q-rbe	22	8	18	4
qing snap-dot1q-rbe	22	8	28	14
qinq mux-pppoa	22 + 6	8	2	-18
qinq snap-pppoa	22 + 6	8	4	-16

ATM オーバーヘッド アカウンティングと階層型ポリシー

階層型ポリシーでは、親ポリシーと子ポリシー上でシェーピングと帯域幅に対する ATM オーバーヘッド アカウンティングをイネーブルにすることができます。 **bandwidth** コマンドまたは **shape** コマンドを含まないトラフィック クラス上の ATM オーバーヘッド アカウンティングはイネーブルにする必要がありません。 子ポリシー上の ATM オーバーヘッド アカウンティングをイネーブルにした場合は、親ポリシー上の ATM オーバーヘッド アカウンティングもイネーブルにする必要があります。 ATM オーバーヘッド アカウンティングをイネーブルにする場合は、親クラスと子クラスで同じカプセル化タイプを指定する必要があります。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定方法

階層型ポリシーでの ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}}
6. **bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**|**aal3**] {*subscriber-encapsulation* | **user-defined***offset*[atm]}]
7. **shape** [**average** |**peak**] mean-*rate*[*burst-size*] [*excess-burst-size*] account {{{qinq | dot1q} {aal5 | aal3} {subscriber-encapsulation}} | {user-defined offset [atm]}}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map** *policy-map-name* 例： `Router(config)# policy-map Business`	子ポリシーを作成または変更して、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。 • ポリシー マップ名を入力します。 これは、子ポリシーの名前です。

	コマンドまたはアクション	目的
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class video`	ポリシー マップに対して指定されたトラフィック クラスを割り当て、ポリシー マップ クラス コンフィギュレーション モードを開始します。 • トラフィック クラス名を入力します。 これは設定済みのクラス マップの名前です。
ステップ 5	bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}} 例： `Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`	次のように、指定されたキーワードと引数に基づいてクラスベース重み付け均等化キューイング（CBWFQ）をイネーブルにします。 • *bandwidth-kbps*：ポリシー マップに属しているクラスに対して割り当てる最小帯域幅を指定または変更します。 有効な値は、リンク帯域幅の 1 ～99% に相当する 8～2488320 です。 • **percent** *percentage*：ポリシー マップに属しているクラスに対して割り当てるリンク帯域幅の最小パーセンテージを指定または変更します。 有効値は 1 ～ 99 です。 • **remaining percent** *percentage*：ポリシー マップに属するクラスに割り当てられる未使用のリンク帯域幅の最小パーセンテージを指定または変更します。 有効値は 1 ～ 99 です。 • **account** ：ATM オーバーヘッド アカウンティングをイネーブルにします。 • **qinq** ：QinQ カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **dot1q** ：IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **aal5** ：コネクション型可変ビット レート（VBR）サービスをサポートする ATM アダプテーション層 5 を指定します。 • **aal3** ：コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。 • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、加入者線カプセル化タイプ，（59 ページ）を参照してください。 • **user-defined** ：ルータでの ATM オーバーヘッド計算に使用されるオフセット サイズを指定します。 • *offset*：ATM オーバーヘッドを計算する際のオフセット サイズを指定します。 有効値は –63～+63 バイトです。 • **atm** ：（任意）ATM オーバーヘッド計算に ATM セル タックスを適用します。

	コマンドまたはアクション	目的
ステップ 6	**bandwidth remaining ratio** *ratio* [**account** {**qinq** | **dot1q**} [**aal5**|**aal3**] {*subscriber-encapsulation* | **user-defined***offset*[atm]}] 例： `Router(config-pmap-c)# bandwidth remaining ratio 10 account dot1q aal5 snap-pppo`	（任意）ATMアカウンティングパラメータと一緒にサブインターフェイスの帯域幅残存率を指定します。 • *ratio*：サブインターフェイスの帯域幅余剰比率を指定します。 有効な値は 1 ～ 100 です。 デフォルト値は、1 です （注） Cisco 7600 シリーズ ルータの有効値は 1 ～ 10,000 です。 デフォルト値は、1 です • **account** ：ATM オーバーヘッド アカウンティングをイネーブルにします。 • **qinq** ：QinQ カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **dot1q** ：IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **aal5** ：コネクション型 VBR サービスをサポートする AAL5 を指定します。 • **aal3** ：コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。 • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、加入者線カプセル化タイプ，（59 ページ）を参照してください。 • **user-defined** ：ルータでの ATM オーバーヘッド計算に使用されるオフセット サイズを指定します。 • *offset*：ATM オーバーヘッドを計算する際のオフセット サイズをバイト単位で指定します。 有効な値は -63～+63 です。 • **atm** ：（任意）ATM オーバーヘッド計算に ATM セル タックスを適用します。
ステップ 7	**shape** [**average** |**peak**] mean-*rate*[*burst-size*] [*excess-burst-size*] account {{{qinq | dot1q} {aal5 | aal3} {subscriber-encapsulation}} | {user-defined offset [atm]}} 例： `Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1q-rbe`	次のように、指定されたビット レートにトラフィックをシェーピングし、指定されたキーワードと引数に基づいて ATM オーバーヘッド アカウンティングをイネーブルにします。 • **average** ：（任意）インターバルごとに送出される最大ビット数を指定する認定バースト（Bc）。 • **peak** ：（任意）インターバルごとに送出される最大ビット数を指定します（Bc＋超過バースト [Be]）。 Cisco 10000 ルータと SIP400（Cisco 7600 シリーズ ルータ上）は、このオプションをサポートしません。

	コマンドまたはアクション	目的
		• *mean-rate*：認定情報速度（CIR）とも呼ばれます。 トラフィックのシェーピングに使用されるビット レートを bps 単位で指定します。 • *burst-size*：（任意）測定インターバル内のビット数（Bc）。 • *excess-burst-size*：（任意）Be の超過が許可される受け入れ可能なビット数。 • **account** ：ATM オーバーヘッド アカウンティングをイネーブルにします。 • **qinq** ：QinQ カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **dot1q** ：IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **aal5** ：コネクション型可変ビット レート（VBR）サービスをサポートする AAL5 を指定します。 • **aal3** ：コネクションレス型リンクとコネクション型リンクの両方をサポートする ATM アダプテーション層 5 を指定します。 aal3 または aal5 のいずれかを指定する必要があります。 • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、加入者線カプセル化タイプ，（59 ページ）を参照してください。 • **user-defined** ：ルータでの ATM オーバーヘッド計算に使用されるオフセット サイズを指定します。 • *offset*：ATM オーバーヘッドを計算する際のオフセット サイズを指定します。 有効値は –63～+63 バイトです。 • **atm** ：（任意）ATM オーバーヘッド計算に ATM セル タックスを適用します。 *offset* オプションと **atm** オプションの両方を設定すると、オフセット サイズに対するパケット サイズの調整が行われてから、ATM セル タックスが追加されます。
ステップ 8	**end** 例： `Router(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定の確認

手順の概要

1. **enable**
2. **show policy-map** [*policy-map-name*]
3. **show policy-map session**
4. **show running-config**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show policy-map** [*policy-map-name*] 例： `Router# show policy-map unit-test`	（任意）指定したポリシー マップに関する全クラスの設定、または、既存の全ポリシー マップに関する全クラスの設定を表示します。 • （任意）ポリシー マップ名を入力します。
ステップ 3	**show policy-map session** 例： `Router# show policy-map session`	（任意）IPoE/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。
ステップ 4	**show running-config** 例： `Router# show running-config`	（任意）現在実行中のコンフィギュレーション ファイルの内容を表示します。
ステップ 5	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定例

ATM のトラフィック シェーピング オーバーヘッド アカウンティングをイネーブルにする例

次に、階層型ポリシー マップ構造を使用して ATM オーバーヘッド アカウンティングをイネーブルにする例を示します。 子ポリシー マップに Business と Non-Business の 2 つのクラスがあります。 Business クラスは、プライオリティが設定され、128,000 kbps にポリシングされています。 Non-Business クラスは、ATM オーバーヘッド アカウンティングがイネーブルにされ、使用可能な帯域幅の 20 % が割り当てられています。 親ポリシー マップは集約トラフィックを 256,000 Kbps にシェーピングし、ATM オーバーヘッド アカウンティングをイネーブルにします。

レイヤ 2 オーバーヘッド アカウンティングがビジネス トラフィック クラス用に明示的に設定されていないことに注意してください。 親ポリシーの class-default クラスで ATM オーバーヘッド アカウンティングがイネーブルになっている場合は、**bandwidth** コマンドまたは **shape** コマンドを含まない子トラフィック クラス上で ATM オーバーヘッド アカウンティングをイネーブルにする必要がありません。 したがって、この例では、親 class-default クラスで ATM オーバーヘッド アカウンティングがイネーブルになっているため、Business プライオリティ キューで ATM オーバーヘッド アカウンティングが黙示的にイネーブルにされます。

```
policy-map Child
 class Business
  priority
  police 128000
 class Non-Business
  bandwidth percent 20 account dot1q aal5 snap-rbe-dot1q
  exit
 exit
policy-map Parent
 class class-default
  shape 256000 account dot1q aal5 snap-rbe-dot1q
  service-policy Child
```

次の例では、subscriber_classes という名前の子ポリシー マップの gaming クラスと class-default クラス、および、subscriber_line という名前の親ポリシー マップの class-default クラスでオーバーヘッド アカウンティングが帯域幅に対してイネーブルになっています。 voip クラスと video クラスには明示的にイネーブルになっているアカウンティングはありません。これらのクラスは親ポリシーでオーバーヘッドアカウンティングがイネーブルであるため、ATM オーバーヘッドアカウンティングが黙示的にイネーブルにされます。 親ポリシーと子ポリシーの機能で同じカプセル化タイプが使用されていることに注意してください。

```
policy-map subscriber_classes
 class voip
  priority level 1
  police 8000
 class video
  priority level 2
  police 8000
 class gaming
  bandwidth remaining percent 80 account dot1q aal5 snap-rbe-dot1q
```

```
 class class-default
  bandwidth remaining percent 20 account dot1q aal5 snap-rbe-dot1q
policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
  shape average 512 account aal5 dot1q snap-rbe-dot1q
  service policy subscriber_classes
```

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの確認例

```
Router# show policy-map interface

Service-policy output:unit-test
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000

Router# show policy-map session output

SSS session identifier 2 -
Service-policy output:  ATM_OH_POLICY
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 2500 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
       Overhead Accounting Enabled
```

次の **show running-config** コマンドの出力は、ATM オーバーヘッド アカウンティングがシェーピングに対してイネーブルになっていることを示しています。 BRAS-DSLAM カプセル化は dot1q で、加入者線カプセル化は AAL5 サービスに基づく snap-rbe です。

```
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account dot1q aal5 snap-rbe
!
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
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）、階層型ポリシー、ポリシー マップ	「MQC を使用した QoS 機能の適用」モジュール
トラフィックのポリシングとシェーピング	「ポリシングとシェーピングの概要」モジュール

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ATM の MQC トラフィック シェーピング オーバーヘッド アカウンティングに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *8*：*ATM* の *MQC* トラフィック シェーピング オーバーヘッド アカウンティングに関する機能情報

機能名	リリース	機能情報
ATM の MQC トラフィック シェーピング オーバーヘッド アカウンティング	Cisco IOS XE Release 2.4	ATM の MQC トラフィック シェーピング オーバーヘッド アカウンティング機能を使用すれば、BRAS で、パケットに QoS機能を適用するときにさまざまなカプセル化タイプを考慮できます。 この機能により、**bandwidth (policy-map class)**、**bandwidth remaining ratio**、**shape (policy-map class)**、**show policy-map interface**、**show policy-map session**、**show running-config** コマンドが導入または変更されました。

第 7 章

QoS ポリシー アカウンティング

QoS ポリシー アカウンティング機能により、システムのトラフィックを正確に示すことができます。 加入者に対する Quality of Service（QoS）構成の割り当ての柔軟性も高くなります。 また、QoS アカウンティングのハイ アベイラビリティ機能により、QoS アカウンティング統計情報の有効性が持続し、RADIUS アカウンティングの課金サーバにより、計画中の予期せぬルート プロセッサ（RP）スイッチオーバー時にアカウンティング カウンタが引き続き報告されます。 このモジュールでは、QoS ポリシー アカウンティングの設定、ユーザ テンプレートの使用、サブスクライバ アカウンティングの精度のアクティブ化の各方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

QoS ポリシー アカウンティングの前提条件

- PPP over Ethernet（PPPoE）または PPP over Ethernet over ATM（PPPoEoA）セッションはイネーブルです。
- RADIUS サーバが設定されます。
- 認証、許可、アカウンティング（AAA）はイネーブルです。
- RADIUS サーバの加入者のユーザ プロファイルが作成されます。
- ポリシー マップが設定されます。
- サービス テンプレートが設定されます。
- トラフィック クラスが作成されます。
- Stateful Switchover（SSO）および In-Service Software Upgrades（ISSU）の前提条件を満たす必要があります。 詳細については、『*Cisco IOS High Availability Configuration Guide*』を参照してください。

QoS ポリシー アカウンティングに関する制約事項

- システムのフェールオーバーでは、次が発生します。
  - ポリシー マップに静的に設定された QoS アカウンティングの場合、QoS アカウンティング統計情報はゼロにリセットされます。
  - サービス テンプレートを使用して動的に設定された QoS アカウンティングの場合、新しいアクティブなルート プロセッサ（RP）にセッションは存在しなくなります。

（注） Cisco IOS XE Release 3.5S 以降のリリースでは、ハイ アベイラビリティ（HA）のサポートは、サービス テンプレートを通じて有効になるアカウンティング サービスに使用できます。 そのため、QoS アカウンティング統計情報およびサービス セッションは、システムのフェールオーバー中に保持され、新しいアクティブ RP で使用できます。

- マルチキャストは、QoS ポリシー アカウンティング サービスではサポートされません。
- 次の QoS アクションはサービス テンプレートではサポートされていません。
  - account
  - fair-queue
  - netflow-sampler
  - random-detect

- 次の QoS フィルタはサービス テンプレートではサポートされていません。
  - atm
  - class-map
  - cos
  - destination-address
  - discard-class
  - fr-de
  - fr-dlci
  - input-interface
  - mpls
  - not
  - packet
  - source-address
  - vlan
- サービス テンプレート定義の行は、Cisco IOS CLI によって許可された設定の最大行の長さを超えることはできません。 この範囲内に抑えるためにシェル変数名を短くすることができます。
- セッションでアクティブになっているテンプレート サービスは変更できません。代わりに、これを非アクティブにし、別のテンプレート サービスをアクティブにすることができます。
- テンプレート サービスがアクティブである場合、従来の複雑なパラメータ化された文字列を使用して QoS ポリシーをセッションでアクティブに変更できない場合があります。
- IP アドレスのパラメータ化は IPv4 および注釈のない名前付き ACL でのみサポートされます。パラメータ化されたサービス アクティベーションで指定された IP アドレスは、「permit ip network mask any」および「permit ip any network mask」の固定パターンでクローン ACL に必ず追加されます。
- サービス テンプレートは、PPP セッションのみでサポートされ、サブインターフェイスではアクティブにできません。
- セッションでアクティブにできるのは常に 1 つの Turbo Button サービスのみです。 Turbo Button サービスは、親ポリシーの class-default における「service-policy xxxx」以外の QoS アクションを変更する（子ポリシーを変更する）すべてのサービスです。
- シェル変数、QoS クラス マップ、アクセス コントロール リスト（ACL）の名前には、次の文字を含めることはできません。
  - !
  - $
  - #

- -
- ,
- >
- <

- サービス名は、グループ アカウンティングに対してのみのアカウンティング レコードにエコーバックされます（サービス テンプレートで $_acctgrp を使用する場合）。
- セッションでアクティブな入力/出力 QoS ポリシー名は、以前アクティブであった QoS ポリシー（または最後のマルチサービス許可変更（CoA）または Access-Accept で指定されたスタティック QoS ポリシー）を連結することで形成されます。
- 同じサービス テンプレートからインスタンス化された 2 個のテンプレート サービスは、セッションで同時にアクティブにすることはできません。 ただし、無関係なサービス テンプレートからインスタンス化された複数のテンプレート サービスは、セッションで同時にアクティブにすることができます。
- テンプレート サービスのサポートが提供されるのは、ローカルに終端された PPP に対して、および Layer 2 Tunneling Protocol（L2TP）アクセス コンセントレータ（LAC）で PPP によって転送されるセッションに対してのみです。
- LAC で PPP によって転送されたセッションの場合、Access-Accept を介してテンプレート サービスを適用するには、次の設定を使用します。
  - vpdn authen-before-forward。
  - 認証プロファイルではなくユーザ許可プロファイル（PPP 認証後に受信される Access-Accept）にのみテンプレート サービスを指定します。
- テンプレート サービスをアクティブにするのは、親の class-default の下の子ポリシー（2 レベルまで）に対して、および親ポリシー（Turbo Button サービス）に対してのみです。
- デフォルトの QoS ポリシーは、2 レベルの深さ（親 + class-default の下の子）に限られ、class-default 以外のクラスの下には子ポリシーを設定しません。
- テンプレート サービスを子レベルでアクティブにするために、デフォルトの親ポリシーの class-default の下で子ポリシーを設定する必要があります。
- 構文エラー チェックに起因するロールバックのみがサポートされます。
- サービスのアクティブ化または非アクティブ化が単一の CoA メッセージに複数含まれる場合、操作（アクティブ化または非アクティブ化）の失敗は、CoA 処理の開始前のセッション状態に復元するために、CoA が以前のすべての動作をロールバックする（取り消す）必要があることを意味します。 つまり、すべての操作が CoA で正常に処理されるか、まったく処理されないことになります。 CoA の否定 ACK（NACK）は RADIUS に送信されます。
- ロールバックが Access-Accept の処理中に動作するようにするには、加入者サービスの複数承認処理を設定する必要があります。 Access-Accept でサービスの処理に失敗すると、Access-Accept での以前のすべてのサービスがロールバックされる（取り消される）ことになります。 Access-Accept サービス処理が失敗してもセッションが立ち上がります。

- プラットフォームまたはデータ プレーンで発生するエラーは、ロールバックをトリガーしません（ロールバックが不完全なサービスに終わる可能性があります）。
- テンプレート サービスがセッションで使用中またはアクティブである場合、サービス テンプレートを変更しないでください。 使用中のテンプレート サービスを表示するには、**show subscriber policy ppm-shim-db** コマンドを使用します。

QoS ポリシー アカウンティングの概要

RADIUS は AAA 管理を提供するネットワーキング プロトコルです。 特に、各 RADIUS アカウンティング メッセージには、入力と出力のカウンタが含まれます。 QoS ポリシー アカウンティング機能を使用するとカウンタ間の誤差を解消することができます。

グループでの QoS ポリシー アカウンティング機能

QoS ポリシー アカウンティング機能は、RADIUS サーバに対する次の情報をセッション単位に収集してレポートします。

- Acct-Session-Id
- 入出力パケット数/バイト数/ギガワード数、パケット数、および正常に送信されたパケットのバイト数
- Parent-Session-Id
- ポリシー名とクラス名またはグループ名（QoSポリシーアカウンティング機能がグループでイネーブルの場合）
- サービス名
- ユーザ名

QoS ポリシー アカウンティング機能をグループでイネーブルにして、グループ名を割り当てる場合は、この機能は次の条件を満たすパケットを集計します。

- 同じグループのトラフィック クラスで分類する
- 同じターゲットに適用される入出力 QoS ポリシーに含まれている

別のアカウンティング ストリーム

トラフィック クラスをグループに割り当てない代わりに AAA 方式リストに割り当てた場合、トラフィック クラスごとに別の QoS ポリシー アカウンティング ストリームが作成されます。 別のアカウンティング ストリームにより、複数のクラスに適合するトラフィックを区別することができます。 ターゲット、方向、ポリシー名、クラス名にはそれぞれ固有の RADIUS Acct-Session-Id 値があります。

サービス テンプレート

サービス テンプレートを使用すると、CLI に新しい QoS ポリシーを定義せずに QoS パラメータを動的に変更することができます。 QoS ポリシーは、セッションの開始時、またはセッション確立後の任意の時点で変更できます。 アクティブな QoS を動的に変更する前に、現在のサービスを非アクティブ化します。

サービス テンプレートを理解するには、次の用語について知っておく必要があります。

- サービス テンプレートは：
  - Cisco IOS シェル機能です
  - 入力 QoS ポリシー マップ定義を含みます
  - 出力 QoS ポリシー マップ定義を含みます
  - プログラム的に呼び出されます
  - シェル変数のデフォルト値を指定します
- テンプレート サービスは：
  - 括弧付きの QoS サービス名です
  - 一致するシェル マップ テンプレート定義を含みます
  - サービス テンプレートのシェル関数の実行中に動的に作成されます
- 最終的に有効な入力ポリシー マップ
- 最終的に有効な出力ポリシー マップ

QoS ポリシー アカウンティング機能は、Cisco IOS シェルが、サービス テンプレートのシェル関数で使用される変数のデフォルト値を上書きする方法について説明します。 シェル マップ内の QoS ポリシー定義には、QoS アクション パラメータ値の代わりにシェル変数が含まれる場合があります。

サービス テンプレートの使用

サービス テンプレートを作成するには、テキスト エディタでサービス テンプレートを作成し、CLI にそのテンプレートをコピーします。 シェルマップ ブロックの内容はテキストとして扱われます。

サービス テンプレート ポリシー マップ（ポリシー マップ $_outgoing/$_incoming）を定義する際には、使用可能な CLI ヘルプまたはプロンプトはありません。 たとえば次の CLI 支援にはアクセスできません。

- パーサーの自動実行
- コマンド オプション

- 範囲ヘルプ
- 構文チェック

（注） CLIで使用可能なエディタはありません。そのため間違えた場合はサービステンプレート全体を削除し、最初から再度設定する必要があります。

サービス テンプレートの確認

テキスト エディタにサービス テンプレートを作成する際の構文をチェックする機能はありません。 したがって、サービステンプレートをアクティブにする前に、構文を確認する必要があります。 次のコード サンプルは、*voice-service1* サービス テンプレートを確認する方法を示します。 独自のテンプレートを確認するには、*voice-service1* をサービス テンプレート名で置き換えます。

```
(shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1)
configure terminal
no policy-map test-svc_IN <-------- Removes previous service template verifications.
no policy-map test-svc_OUT <-------- Removes previous service template verifications.
no aaa-accounting group test_svc_GRP <-------- Removes previous service template
verifications.
end
trigger voice-service1 _incoming=test-svc_IN _outgoing=test-svc_OUT _acctgrp=test-svc_GRP
show policy-map test-svc-IN <--------
Ensure that the output matches the expected service template template service with default
 values.
show policy-map test-svc-OUT <--------
Ensure that the output matches the expected service template template service with default
 values.
```

サービス テンプレートの削除

サービス テンプレートを削除するには、コマンドラインで次のように入力します。

```
no shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1 in_h=class-default
 out_h=class-default
```

voice-service1 は、サービス テンプレートの名前を意味します。

サンプル サービス テンプレート

サービス テンプレート

次に、サービス テンプレートの例を示します。

```
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voip
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
 exit
```

```
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit $queue_size packets
        set precedence 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
}
```

処理パラメータのオーバーライド

処理パラメータのオーバーライドは、シェル変数が、QoS ポリシー内のクラスで入力されたポリシング、シェーピング、帯域幅、設定などの QoS アクションのパラメータの代わりに使用されるサービス テンプレートのタイプです。

テンプレート サービスを無効にすると、システムは以前アクティブだった QoS ポリシーを復元します。 QoS ポリシーは、名前は異なっている可能性がありますが、テンプレート サービスがアクティブになる前にアクティブになっている QoS ポリシーと構造的かつ機能的に同じです。

この例では、次のパラメータを使用したサービスが生成されます。

```
Reserved variable initialization before executing the service template shell function:
$_incoming = voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN
$_outgoing = voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT
$_acctgrp = aaa-accounting group
voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP list default
```

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

voice-service1(police_rate=200000,prec_value=5,queue_size=32) をターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
```

```
 class class-default
   shape average 10000000
   service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

      class voip
        police 200000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
        set precedence 5
        set cos 6
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 32 packets
        set precedence 6
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

voice-service1(police_rate=200000,prec_value=5,queue_size=32) をターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

 class class-default
   police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

 class-default
```

処理のパラメータ化のデフォルト パラメータ

処理のパラメータ化のデフォルト パラメータは、シェル変数が、QoS ポリシー内のクラスで入力されたポリシング、シェーピング、帯域幅、設定などの QoS アクションのパラメータの代わりに使用されるサービス テンプレートのタイプです。

テンプレート サービスを無効にすると、システムは以前アクティブだった QoS ポリシーを復元します。 QoS ポリシーは、名前は異なっている可能性がありますが、テンプレート サービスがアクティブになる前にアクティブになっている QoS ポリシーと構造的かつ機能的に同じです。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
class class-default
   shape average 10000000
   service-policy output_child
```

```
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
ip access-list extended voip-acl
 permit ip 10.1.1.0 0.0.0.255 any
ip access-list extended voip-control-acl
 permit ip 10.2.2.0 0.0.0.255 any
class-map match-any voip
 match access-group name voip-acl
!
class-map match-any voip-control
 match access-group name voip-control-acl
!
shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1 in_h=class-default
out_h=class-default
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voip
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
 exit
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit $queue_size packets
        set precedence 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
}
```

voice-service1 をターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map output_parent$class-default$voice-service1><_OUT$class-default class
  class-default
  shape average 10000000
  service-policy output_child$voice-service1><_OUT$class-default
policy-map output_child$voice-service1><_OUT$class-default
  class voip
   police 10000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 4
   set cos 6
   aaa-accounting group voice-service1><_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 16 packets
   set precedence 6
```

```
   aaa-accounting group voice-service1><GRP
 class class-default
```

voice-service1 をターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map input_parent$class-default$voice-service1><_IN$class-default
 class class-default
 police cir 10000000 bc 312500 conform-action transmit exceed-action drop
 service-policy input_child$voice-service1><_IN$class-default
policy-map input_child$voice-service1><_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1><_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1><_GRP
 class-default
```

クラス名のオーバーライド

クラス名のオーバーライドは、シェル変数が、QoSポリシー内のクラスで入力されたポリシング、シェーピング、帯域幅、設定などのQoSアクションのパラメータの代わりに使用されるサービステンプレートのタイプです。シェル変数は、サービステンプレートのポリシー定義におけるクラス名の代わりに使用される可能性があります。 シェル変数は、クラス名を完全に置き換える場合があります。または、固定プレフィックス付きの可変サフィックスとして設定される可能性があります。

テンプレート サービスを無効にすると、システムは以前アクティブだったQoSポリシーを復元します。QoSポリシーは、名前は異なっている可能性がありますが、テンプレート サービスがアクティブになる前にアクティブになっている QoS ポリシーと構造的かつ機能的に同じです。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
! Pre-configured ACLs/class-maps
ip access-list extended aol_classifier_acl         ! Locally pre-configured
 permit ip host 10.1.30.194 any
class-map match-all voice-control-aol_classifier_reference      ! Locally pre-configured
  match access-group name aol_classifier_acl
! Other pre-configured ACLs/classes here (e.g., voice-aol_classifier_reference,
voice-t_online, etc.)
! Service template:
shell map voice-aol-service1 prec_value=3 police_rate=100000 class_ref=t_online
in_h=class-default out_h=class-default
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voice-control-$class_ref
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
```

```
        queue-limit 16 packets
        set precedence 6
        aaa-accounting group $_acctgrp
      class voice-$class_ref
       police $poice_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voice-control-$class_ref
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
      class voice-$class_ref
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence $prec_value
        aaa-accounting group $_acctgrp
}
```

voice-aol-service1(class_ref=aol_classifier_reference) をターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map
output_parent$class-default$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default

 class class-default
    shape average 10000000
   service-policy
output_child$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default
policy-map
output_child$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default
      class voice-control-aol_classifier_reference     ! Reference to pre-configured class
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
      class voice-aol_classifier_reference     ! reference to pre-configured class
        police 100000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
        set precedence 3
        set cos 6
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
class class-default
```

voice-aol-service1(class_ref=aol_classifier_reference) をターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map
input_parent$class-default$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default

 class class-default
    police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default
policy-map input_child$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default

      class voice-control-aol_classifier_reference     ! reference to pre-configured class
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
      class voice-aol_classifier_reference     ! reference to pre-configured class
```

```
       police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
       set precedence 3
       aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
      class-default
```

IP アドレスのパラメータ化

IPアドレスのパラメータ化は、分類子がACLにエントリを追加することによって、動的に変更できる処理のパラメータ化サービス テンプレートのタイプです。 ACL に追加されるエントリは、シェル変数の IP アドレスのリストです。

テンプレート サービスを無効にすると、システムは以前アクティブだったQoSポリシーを復元します。QoSポリシーは、名前は異なっている可能性がありますが、テンプレート サービスがアクティブになる前にアクティブになっている QoS ポリシーと構造的かつ機能的に同じです。

（注） クラスは事前定義する必要があります。これらは動的に作成されません。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
! Base ACLs:
ip access-list extended IPOne-control-acl     ! Base ACL locally pre-configured
  permit ip any host 10.0.132.118
  permit ip host 10.0.132.118 any
  permit ip any host 10.1.245.122
  permit ip host 10.1.245.122 any
ip access-list extended IPOne-combined-acl      ! Base ACL pre-configured
 permit ip any 10.0.132.0 0.0.0.127
 permit ip 10.0.132.0 0.0.0.127 any
 permit ip any 10.1.245.64 0.0.0.63
 permit ip 10.1.245.64 0.0.0.63 any
! Base class-maps:
class-map match-any voice-control      ! Base class map pre-configured
  match access-list name IPOne-control-acl      !   Match on the base ACL
class-map match-any voice      ! base class-map pre-configured
  match access-list name IPOne-combined-acl      !   Match on the base ACL
! Service template:
shell map voice-toi  prec_value=3 police_rate=100000 ip_list=10.2.1.0/28,10.2.1.0/29
in_h=class-default out_h=class-default
{
    configure terminal
    ! Class-map templates:
    classmap-template voice-control  $ip_list
    classmap-template voice  $ip_list
    ! Service parameter templates:
    policy-map $_outgoing
      class voice-control-$ip_list     ! class names MUST end with -$ip_list
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
```

```
        set precedence 6
        aaa-accounting group IPOne-aol
      class voice-$ip_list
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        aaa-accounting group IPOne-aol
   policy-map $_incoming
     class voice-control-$ip_list
      police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group IPOne-aol
      class voice-$ip_list
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence $prec_value
        aaa-accounting group IPOne-aol
```

ターゲット セッションで voice-toi(ip_list=10.1.30.0/28,10.1.40.0/29) をアクティブにすると、これがアクティブな出力 QoS ポリシーになります。

```
policy-map output_parent$class-default$
voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
 class class-default
    shape average 10000000
   service-policy output_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
policy-map output_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
      class voice-control-10.1.30.0/28,10.1.40.0/29
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group IPOne-aol
      class voice-10.1.30.0/28,10.1.40.0/29
        police 100000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
        set precedence 3
        aaa-accounting group IPOne-aol
class class-default
```

ターゲット セッションで voice-toi(ip_list=10.1.30.0/28,10.1.40.0/29) をアクティブにすると、これがアクティブな入力 QoS ポリシーになります。

```
policy-map
input_parent$class-default$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
 class class-default
    police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy input_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
policy-map input_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
      class voice-control-10.1.30.0/28,10.1.40.0/29
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group IPOne-aol
      class voice-10.1.30.0/28,10.1.40.0/29
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 3
        aaa-accounting group IPOne-aol
 class-default
```

（注） 次の設定が動的に作成されます。

```
! Internally created ACLs:
ip access-list extended IPOne-control-acl-10.1.30.0/28,10.1.40.0/29
  permit ip any host 10.0.132.118
  permit ip host 10.0.132.118 any
  permit ip any host 10.1.245.122
  permit ip host 10.1.245.122 any
  permit ip 10.1.30.0 0.0.0.15 any  ! ACEs derived from $ip_list
  permit ip any  10.1.30.0 0.0.0.15
  permit ip 10.1.40.0 0.0.0.7 any
  permit ip any 10.1.40.0 0.0.0.7
ip access-list extended IPOne-combined-acl-10.1.30.0/28,10.1.40.0/29
  permit ip any 10.0.132.0 0.0.0.127
  permit ip 10.0.132.0 0.0.0.127 any
  permit ip any 10.1.245.64 0.0.0.63
  permit ip 10.1.245.64 0.0.0.63 any
  permit ip 10.1.30.0 0.0.0.15 any  ! ACEs derived from $ip_list
  permit ip any 10.1.30.0 0.0.0.15
  permit ip 10.1.40.0 0.0.0.7 any
  permit ip any 0.0.0.7 10.1.40.0
! internally created class-maps:
class-map match-any voice-control-10.1.30.0/28,10.1.40.0/29
   match access-group name IPOne-control-acl-10.1.30.0/28,10.1.40.0/29
class-map match-any voice-10.1.30.0/28,10.1.40.0/29
   match access-group name IPOne-combined-acl-10.1.30.0/28,10.1.40.0/29
```

Turbo Button サービス

Turbo Button サービスは、入力親 class-default でのポリシング パラメータと、出力親 class-default でのシェーピングパラメータだけが、動的に変更可能な処理のパラメータ化サービステンプレートのタイプです。

次に、Turbo Button サービスのサービス テンプレートの作成方法を示します。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
shell map turbo-button in_police_val=20000000 $out_shape=20000000
configure terminal
accounting group $_acctgrp list default
policy-map $_outgoing
class class-default
shape average $out_shape
aaa-accounting group $_acctgrp
policy-map $_incoming
class class-default
police $in_police_val
aaa-accounting group $_acctgrp
```

Turbo Button のアクティブ化

次に、デフォルト値を使用して Turbo Button サービスをアクティブにする例を示します。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
accounting group turbo-button>< list default

accounting group turbo-button>< list default
! Service outgoing:
 policy-map  turbo-button><_OUT
 class class-default
 shape average 20000000
 aaa-accounting group turbo-button>< list default
! Service incoming:
 policy-map  turbo-button><_IN
 class class-default
 police 20000000
aaa-accounting group turbo-button>< list default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map output_parent$turbo-button><_OUT$
class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 class class-default
 shape average 20000000
aaa-accounting group turbo-button>< list default
service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class voip
police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
 priority level 1
 queue-limit 8 packets
 set precedence 5
 set cos 6

aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class voip-control
 police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
 queue-limit 32 packets
 set precedence 6
aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map input_parent$turbo-button>
<_IN$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
class class-default
   police cir 20000000 bc 312500 conform-action transmit exceed-action drop
```

```
   aaa-accounting group turbo-button>< list default

service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

   class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

   class voip-control
        police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class-default
```

Turbo Button の非アクティブ化

次に、VSA 252 0c turbo-button() のデフォルト値を使用して Turbo Button サービスを非アクティブにする例を示します。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class class-default
  shape average 10000000
  service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

class class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

   class class-default
   police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  class voip
   police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
   set precedence 5
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop

   set precedence 7
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class-default
```

Turbo Button のオーバーライド

次に、VSA 250 Aturbo-button(in_police_val=30000000, out_shape_val=30000000) (Activation from Access-Accept) または VSA 252 0b turbo-button(in_police_val=30000000, out_shape_val=30000000) (Activation from CoA) のデフォルト値を使用して Turbo Button サービスをアクティブにする方法を示します。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000 list default

! Service outgoing:
 policy-map turbo-button>in_police_val=30000000#out_shape_val=30000000<_OUT
 class class-default
  shape average 30000000
  accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
! Service incoming:
  policy-map turbo-button>in_police_val=30000000#out_shape_val=30000000<_IN
  class class-default
   police 30000000
   accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map output_parent$turbo-button>
in_police_val=30000000#out_shape_val=30000000<_OUT$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class class-default
```

```
 shape average 20000000
 accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
 service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class voip
 police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
 priority level 1
 queue-limit 8 packets
 set precedence 5
 set cos 6
 aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class voip-control
 police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
 queue-limit 32 packets
 aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map
input_parent$turbo-button>in_police_val=30000000#out_shape_val=30000000<_IN$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
class class-default
 police cir 20000000 bc 312500 conform-action transmit exceed-action drop
 accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
 service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class-default
```

Turbo Button オーバーライドの非アクティブ化の例

次に、VSA 252 0c turbo-button (in_police_val=30000000, out_shape_val=30000000) のデフォルト値を使用して Turbo Button オーバーライドを非アクティブにする例を示します。

セッションでアクティブな出力 QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな入力 QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
```

```
 class class-default
  shape average 10000000
  service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

  class class-default
  police cir 10000000 bc 312500 conform-action transmit exceed-action drop
  service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  class voip
   police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
   set precedence 5
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop

   set precedence 7
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class-default
```

中間アカウンティング インターバルのオーバーライドの例

中間アカウンティング インターバルのオーバーライドは、アカウント中間値の動的な変更が可能なアカウンティング方式リスト定義での中間インターバル値の代わりに、シェル変数を使用できる処理のパラメータ化サービス テンプレートのタイプです。

次に、VSA 252 0b voice-service1(police_rate=200000,prec_value=5,acct_interval=600) のデフォルト値を使用して、アカウンティング グループのオーバーライドを実行する例を示します。

この例では、次のパラメータを使用したサービスが生成されます。

```
! Global AAA method list and accounting group parameters
aaa accounting network list-600
 action-type start-stop periodic interval 600
  accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600 <_GRP
list list-600
! OUT policy-map:
 policy-map voice-service1>policy_rate=200000#prec_value-5#acct_interval=600 <_OUT
  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
```

```
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group


OUT:
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
IN:
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな出力ポリシーとなります。

```
policy-map
output_parent$class-default$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
 <_OUT$class-default
 class class-default
 shape average 10000000
 service-policy output_child$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
 <_OUT$class-default
 policy-map output_child$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
<_OUT$class-default
 class voip
  police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
  priority level 1
  queue-limit 8 packets
  set precedence 5
  set cos 6
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
  class voip-control
  police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
  queue-limit 32 packets
  set precedence 6
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class class-default
```

サービスをターゲット セッションでアクティブにすると、これがアクティブな入力ポリシーとなります。

```
policy-map
input_parent$class-default$voice-service1>policy_rate=200000#prec_value-5#acct_interval=600
 <_IN$class-default
class class-default
 police cir 10000000 bc 312500 conform-action transmit exceed-action drop
 service-policy input_child$voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
 <_IN$class-default
policy-map input_child$voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
```

```
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class class-default
```

サブスクライバ アカウンティングの精度

サブスクライバアカウンティングの精度機能により、Accounting-Stop レコードの入出力パケット/バイト統計情報は、1 秒内まで正確であることが保証されます。

サブスクライバ アカウンティング データは、次のイベント中に認証、許可、アカウンティング（AAA）サーバに送信されます。

- セッションまたはサービスのライフタイム中に設定されたインターバル
- サービスのログオフ
- セッションの切断

サブスクライバアカウンティングの精度機能に値を設定するには、**subscriber accounting accuracy** *milliseconds* コマンドを使用します。

許可変更（CoA）ACK の順序指定

CoA ACK 順序指定は、QOS アカウンティング レコードがこの CoA に送信される前に、個々の CoA イベント用に CoA-ACK を送信します。 CoA は、単一または複数のサービスのアクティブ化または非アクティブ化を含む場合があります。

サービスがセッションにインストールできない場合、次の状況が発生します。

- CoA 全体が失敗します。
- Policy Manager は RADIUS サーバに CoA-NAK を送信します。
- 前のサービス コンフィギュレーションが復元されます。

失敗が検出される前に 1 つ以上のサービスがインストールされると、次の状況が発生します。

- CoA 全体が失敗します。
- サービスはバックアウトされます。
- Policy Manager は RADIUS サーバに CoA-NAK を送信します。
- 前のサービス コンフィギュレーションが復元されます。

マルチサービス CoA は次のいずれかで構成されます。

- QoS サービス：Policy Manager は、最終的に有効な 1 個のポリシー マップにサービスを組み合わせます。 すべてのサービスのセッションに適用されるのは、1 個の QoS ポリシーだけで

す。 ポリシーをインストールできない場合、システムはセッションを復元して前のポリシー マップを使用します。 事実上、セッションは CoA の前の状態に復元されます。

- QoS およびインテリジェント サービス ゲートウェイ（ISG）サービス：Policy Manager は ISG サービスを最初に適用し、次に QoS サービスを適用します。 QoS ポリシーをインストールできない場合、システムはセッションを前のポリシー マップに復元します。 ISG と QoS の両方のサービスは、以前の状態に戻るまでロールバックされます。

マルチサービス CoA の場合、すべてのサービスが正常にインストールされると、1 個の CoA ACK のみが送信されます。

許可変更のロールバック

CoA のロールバック機能により、QoS ポリシー アカウンティングが CoA が発行される前の状態に復元されます。 また、CoA のロールバックは、CoA-NAK を使用して RADIUS サーバを正しく認知します。

CoA のロールバック機能は、構文の間違いと、アドミッション制御やリソース割り当ての失敗などのポリシー インストール障害に適用されます。

CoA が失敗すると、システムは CoA-NAK を送信し、QoS アカウンティング レコードを送信しません。既存のサービスのアカウンティング レコードは前のカウンタを保持し、新しいパケットをカウントし続けます。

QoS アカウンティングのハイ アベイラビリティ

QoS アカウンティングがクラスでイネーブルになると、ポリシー アカウンティング機能は、次の 3 種類のイベントをサポートします。

- 開始：新しいアカウンティング フローを示します。 開始レコードには、このフローに固有の統計情報と属性が含まれます。
- 中間：どのくらいの頻度でフロー統計情報が報告されるかを示します。
- 停止：アカウンティング フローの終りを示します。 停止レコードにも、このフローに固有の統計情報と属性が含まれます。

ポリシー アカウンティング機能は、アカウンティング フローの統計情報を収集し、RADIUS アカウンティングの課金サーバに情報を送信します。

QoS アカウンティングのハイ アベイラビリティ機能により、計画的または予想外のフェールオーバーが発生した場合に、開始、中間、停止の各アカウンティング レコードが影響を受けないようにします。 計画的または予想外のフェールオーバーが発生すると、QoS アカウンティングの HA 機能により、RADIUS アカウンティングの課金サーバへの情報のフローを中断せずに RP スイッチオーバーを発生させることができます。 この機能により、すべてのアクティブセッションのすべての QoS サービスが中断することなく続行され、サービス アカウンティング カウンタが RP スイッチオーバー中保持するようになります。

ポリシー アカウンティング ステートの永続性

開始、停止、中間アカウンティングが Stateful Switchover（SSO）または In-Service Software Upgrade（ISSU）による影響を受けないようにするため、Policy Manager は、すべての QoS サービスおよびパラメータ化された CoA 機能をフェールオーバー時のスタンバイ RP と同期します。 さらに、ダイナミックな QoS の設定とポーリング間隔は、アクティブ RP とスタンバイ RP 間で同期化されます。

スタンバイ RP にパラメータ化された CoA イベントを同期するには、Policy Manager は次の機能を実行します。

- プロビジョニング イベントをスタンバイ RP で同期するように CoA のリプレイを管理します。
- アクティブ RP とスタンバイ RP の両方で同じサービス テンプレートを使用します。
- アクティブ RP とスタンバイ RP の両方でセッションに適用する同じポリシー マップ名とクラス マップ名を作成します。
- サービス テンプレートのアクティベーション中に定義済みの QoS ポリシー マップとクラス マップを使用します。

ポリシー アカウンティング カウンタの永続性

QoS アカウンティングの HA 機能により、ポリシー アカウンティング カウンタが SSO またはフェールオーバー中持続するようになります。 スイッチオーバーが発生すると、スタンバイ RP がアクティブ RP になり、以前アクティブだった RP からの統計情報を集計します。 新しくアクティブになった RP がスイッチオーバー後に定期的な更新を受信した場合は、集計した統計情報と、定期的な更新から取得した値を使用して、中間レコードが生成されます。 新しくアクティブになった RP がスイッチオーバー後に定期的な更新を受信しない場合は、以前アクティブだった RP から集計した統計情報だけを使用して、中間レコードが生成されます。

SSO と ISSU の詳細については、『*Cisco IOS High Availability Configuration Guide*』を参照してください。

QoS ポリシー アカウンティングを使用する方法

QoS ポリシー アカウンティングを使用する場合、トラフィック クラスにグループまたは AAA 方式リストを割り当て、次にポリシーアカウンティングのサービステンプレートを設定し、最後にサブスクライバ アカウンティングの精度機能をアクティブにする必要があります。

（注） デフォルトでは、QoS ポリシー アカウンティングはトラフィック クラスに割り当てられていません。

トラフィック クラスにグループまたは AAA 方式リストを割り当てる

はじめる前に

グループまたは AAA 方式リストがすでに存在している必要があります。 トラフィック クラスに未定義のグループまたは AAA 方式リストを追加しようとすると、エラー メッセージが表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp** *list-name method1*
4. **aaa accounting network** *methodlist-name*
5. **action-type start-stop**
6. **periodic interval** *minutes*
7. **accounting group group_name** *list list-name*
8. **policy-map** *policy-map-name*
9. **class class-default**
10. **accounting aaa list** *list-name* [*group-name*]
11. **end**
12. **show policy-map session**
13. **show accounting group** *group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authentication ppp** *list-name method1* 例： `Router(config)# aaa authentication ppp group radius`	有効な AAA 認証方式を指定します。 • グループ RADIUS はグローバル RADIUS 認証をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa accounting network** *methodlist-name* 例： `Router(config)# aaa accounting network list1`	RADIUS を使用する場合のサービスの AAA をイネーブルにします。 • クラスまたはグループの中間インターバルを決定するアルゴリズムは、ここで指定した方式リストを使用します。
ステップ 5	**action-type start-stop** 例： `Router(config)# action-type start-stop`	プロセスの開始時に start アカウンティング通知を送信し、プロセスの終了時に stop アカウンティング通知を送信します。
ステップ 6	**periodic interval** *minutes* 例： `Router(config)# periodic interval 1`	指定された場合、方式リストに中間インターバル値（1～71,582 分）を追加します。 • 中間インターバルを定義していない場合、AAA で定義されたグローバル値が使用されます。 • 方式リストが中間アップデートをディセーブルにすると、この方式リストを使用しているアカウンティング フローからは中間更新は生成されません。
ステップ 7	**accounting group group_name** *list list-name* 例： `Router(config)# accounting group group_name AAAmethodlist AAAmethodlist1`	AAA 方式リストにプロパティを設定します。 • 既存のトラフィック クラスに割り当てられたグループまたは AAA 方式リストで一時的にプロパティを上書きすることによって、このクラスにセッション単位の変更を加えることができます。 これで、各加入者に動的にカスタマイズされた QoS 設定を提供できるようになります。
ステップ 8	**policy-map** *policy-map-name* 例： `Router(config)# policy-map p1`	ポリシー マップを作成します。
ステップ 9	**class class-default** 例： `Router(config)# class class-default`	トラフィック クラスを作成します。

	コマンドまたはアクション	目的
ステップ 10	**accounting aaa list** *list-name* [*group-name*] 例： `Router(config)# accounting aaa list AAAmethodlist1`	グループまたは AAA 方式リストにトラフィック クラスを割り当てます。 • 次に、グループのないリスト AAAmethodlist1 を使用してトラフィック クラスのインスタンスに対してイネーブルにされた QoS ポリシー アカウンティング機能を示します。
ステップ 11	**end** 例： `Router(config)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show policy-map session** 例： `Router# show policy-map session`	（任意）グループまたは AAA 方式リストのあるトラフィック クラスの QoS ポリシー アカウンティング機能の情報を表示します。
ステップ 13	**show accounting group** *group-name* 例： `Router# show accounting group acc-group1`	（任意）グループから方式リストへの関連付けをすべて表示します。 • グループ名を入力すると、そのグループに固有の情報が表示されます。

サブスクライバ アカウンティング精度のアクティブ化

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber accounting accuracy** *milliseconds*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**subscriber accounting accuracy** *milliseconds* 例： `Device(config)# subscriber accounting accuracy 1000`	サブスクライバ アカウンティング精度機能の値を設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードを開始します。

トラブルシューティング サービス テンプレート

サービス テンプレートに問題がある場合、これを修復するには、ルータのすべてのテンプレートのサービス ポリシー マップの使用情報を表示できます。

手順の概要

1. **enable**
2. **show subscriber policy ppm-shim-db**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show subscriber policy ppm-shim-db** 例： `Router(config)# show subscriber policy ppm-shim-db`	ルータのすべてのテンプレートのサービス ポリシー マップと最終的に有効なポリシー マップの参照カウント（使用情報）を表示します。

QoS ポリシー アカウンティングの設定例

例：グループでの QoS ポリシー アカウンティング機能の使用

次に、グループ化の例を示します。

```
policy-map my-policy
class voip
police
aaa-accounting group premium-services
class voip-control
police
aaa-accounting group premium-services
```

例：別のアカウンティング ストリームを生成する

次に、voip と voip-control という 2 つの分類子の例を示します。 分類子は、1 つのターゲットに関連付けられた 1 つのポリシーに割り当てられます。 この設定で、2 つの別の QoS ポリシー アカウンティング ストリームが生成されます。

```
policy-map my-policy
class voip
police 200000
accounting aaa list AAA-LIST
class voip-control
police 100000
accounting aaa list AAA-LIST
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド	『*Cisco IOS QoS Command Reference*』
Cisco IOS のハイ アベイラビリティ	『*Cisco IOS High Availability Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2866	『RADIUS Accounting』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

QoS ポリシー アカウンティング機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *9*：*QoS* ポリシー アカウンティング機能の機能情報

機能名	リリース	機能情報
QoS アカウンティング HA	Cisco IOS XE Release 3.5S	QoS アカウンティングのハイアベイラビリティ（HA）機能により、QoSアカウンティング統計情報の有効性が持続し、RADIUSアカウンティングの課金サーバにより、計画中の予期せぬルート プロセッサ（RP）スイッチオーバー時にアカウンティング カウンタが引き続き報告されます。 Cisco IOS XE Release 3.5S では、このサービスは Cisco ASR 1000 シリーズ ルータに導入されました。 コマンド **debug qos accounting** が変更されました。

機能名	リリース	機能情報
QoS ポリシー アカウンティング	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.2S Cisco IOS XE Release 3.8S	QoS ポリシー アカウンティング機能により、システムのトラフィックを正確に示すことができます。 加入者に対する QoS 設定の割り当ての柔軟性も高くなります。 スタティック CLI 駆動型のアカウンティングがサポートされます。 Cisco IOS XE Release 2.6 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE Release 3.2S では、ダイナミックなアクティベーションによって制御されないサービスの場合は、サービステンプレート、加入者のサブセカンド精度、ダイナミック CoA と中断のないアカウンティングがサポートされます。 この機能により、**show subscriber policy ppm-shim-db** コマンドと **subscriber accounting accuracy** コマンドが追加されました。

第 8 章

ATM VC での PPP セッション キューイング

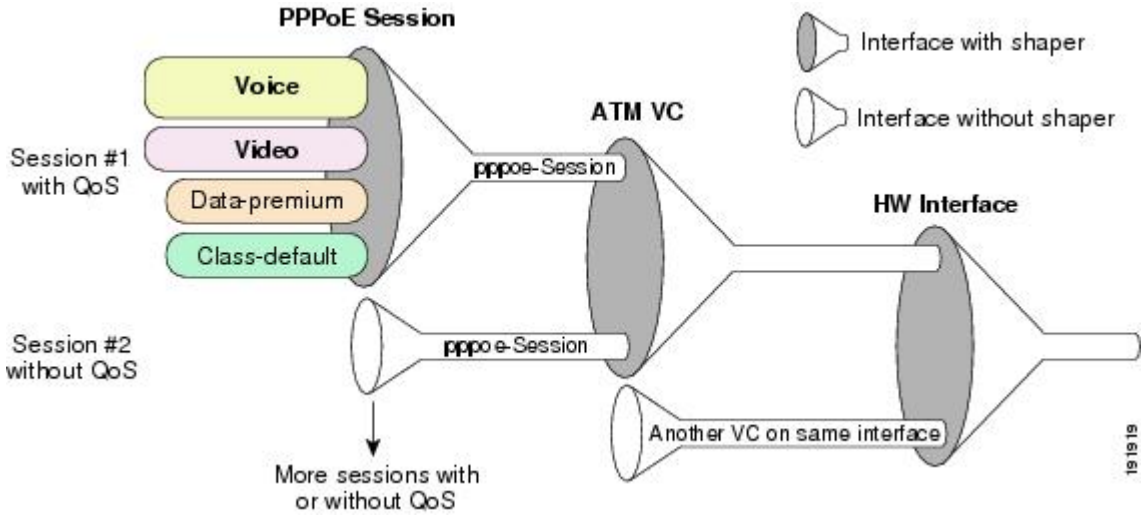
ATM VC 機能での PPP セッション キューイングにより、ユーザが指定したレートに PPP over Ethernet over ATM（PPPoEoA）セッションをシェーピングし、キューに入れることができます。複数のセッションが ATM VC に存在することがあり、Quality of Service（QoS）ポリシーを適用させることも、セッションの一部が QoS ポリシーを所有することもあります。ルータは、VC での PPPoEoA トラフィックに使用するすべての帯域幅の合計をシェーピングします。これで、Digital Subscriber Line Access Multiplexer（DSLAM）への加入者接続が輻輳状態になりません。キューイング関連機能は、PPPoEoA セッション全体で稼働するさまざまなアプリケーションに、異なるサービス レベルを提供します。

ネストされた、2 つのレベルの階層型サービス ポリシーは、Modular Quality of Service Command-Line Interface（MQC）を使用して、ルータに直接シェーピングするセッションを設定するために使用されます。 階層型ポリシーは次のコンポーネントから構成されます。

- 子ポリシー：priority、bandwidth、police などの QoS コマンドを使用して QoS アクションを定義します。
- 親ポリシー：shape コマンドまたは bandwidth remaining ratio コマンド、またはこの両方のコマンドが設定された class-default クラスのみが含まれます。
  - shape コマンド：特定のアルゴリズムに従って、指定されたビット レートにセッション トラフィックをシェーピングします。
  - bandwidth remaining ratio コマンド：輻輳中にセッションに割り当てる未使用帯域幅の量を決定するためにルータが使用する比率の値を指定します。

（注） ATM VC での PPP セッション キューイング機能は、PPP 終端集約（PTA）設定と L2TP アクセス コンセントレータ（LAC）設定の双方で動作します。

以下の図は、ATM VC での PPP セッション キューイングを示します。



機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ATM VC での PPP セッション キューイングの前提条件

- PPPoEoA セッションをイネーブルにする必要があります。

- class-map コマンドを使用してトラフィック クラスを作成し、トラフィックの分類に使用される一致基準を指定します。
- RADIUS を使用するダイナミックな PPPoEoA セッション キューイングの場合、次を実行する必要があります。
  - 認証、許可、アカウンティング（AAA）をルータでイネーブルにする
  - ダイナミックな QoS 用に RADIUS サーバを設定する
  - RADIUS サーバに加入者のユーザ プロファイルを作成する

ATM VC での PPP セッション キューイングに関する制約事項

- 非整型 VC（指定されたピーク セル レート（PCR）または平均セル レート（SCR）のない VC）には、PPP セッション キューイングを設定できません。
- セッション キューイング ポリシーを持つ VC は、整形仮想パス（VP）の一部にすることはできません。
- 同じ ATM カテゴリ（整形未指定ビット レート（UBR）など）に低帯域幅 VC と高帯域幅 VC の両方が含まれる場合、SAR メカニズムにより高帯域幅 VC の低スループットを引き起こす可能性があります。 回避策は、低帯域幅 VC と高帯域幅 VC に異なる ATM クラスを使用することです。 たとえば、低帯域幅 VC を整形 UBR として、高帯域幅 VC を非リアルタイム可変ビット レート（VBR-rt nrt）または固定ビット レート（CBR）として設定します。
- CLASS-BASED QOS MIB には、セッションに適用されるサービス ポリシーの統計情報は含まれません。
- RADIUS アカウンティングには、キューイングの統計情報は含まれません。

ATM VC での PPP セッション キューイングの概要

ATM VC での PPP セッションに QoS ポリシーを動的に適用する

ルータによって、RADIUS を使用して PPPoEoA セッションに QoS ポリシー マップを動的に適用できるようになります。 QoS ポリシーの実際の設定がルータで発生しても、セッションに動的に適用するポリシー マップの名前を指定するように RADIUS に次の属性と値（AV）のペアを設定することができます。

```
"ip:sub-qos-policy-in=<name of the QoS policy in ingress direction>"
"ip:sub-qos-policy-out=<name of egress policy>"
```

AV ペアは、次の RADIUS プロファイルのいずれかに定義できます。

- ユーザ プロファイル：RADIUS サーバ上のユーザ プロファイルには、ユーザに適用されるポリシー マップ名を識別するエントリが含まれます。 ポリシー マップ名は、セッションが承認されると RADIUS がルータにダウンロードするサービスです。
- サービス プロファイル：RADIUS サーバ上のサービス プロファイルは、セッション ID と AV ペアを指定します。 セッション ID は、セッションの IP アドレスなどです。 AV ペアは、ユーザが属するサービス（ポリシー マップ名）を定義します。

ポリシーサーバからサービスログイン要求を受け取った後、すでにログインしている加入者向けのサービスをアクティブにするため、RADIUS はルータに許可変更（CoA）要求を送信します。許可に成功すると、ルータは ip:sub-qos-policy-in[out]= AV ペアを使用して RADIUS からポリシーマップ名をダウンロードし、PPPoEoA セッションに QoS ポリシーを適用します。 サービス ポリシーにはキューイング関連の操作が含まれるため、ルータは適切なクラス キューを設定します。

（注） ルータは RADIUS のベンダー固有属性（VSA）38、Cisco-Policy-Down および Cisco-Policy-Up もサポートしますが、QoS ポリシー定義には ip:sub-qos-policy-in[out]= AV ペアを使用することを推奨します。

PPP セッション キューイングの継承

PPP セッションは、そのユーザの親インターフェイスからキューを継承するか、セッション自身のキューを含みます。 セッション キューイングが設定されている PPPoEoA セッションにはそれぞれ独自のキューのセットがあります。

次の表に、ルータがセッション トラフィックを指示するキューを示します。

表 *10*：*PPP* セッション キューの継承

キューイング ポリシー	セッション トラフィックに使用されるキュー
ポリシーなし	VC のデフォルト キュー
VC に適用	VC キュー
セッションに適用	セッションのキュー

PPP セッション キューイングをサポートするインターフェイス

ルータはアウトバウンド トラフィック専用の整形 ATM VC に対して、PPP セッション キューイングをサポートします。

ルータはインバウンド ATM インターフェイスでの PPP セッション キューイングをサポートされません。

混合設定とキューイング

混合設定とは、QoS が適用されていないセッションが含まれる設定です。 一部の VC ではキューイング ポリシーは VC レベルで適用され、他の VC ではセッションにキューイング ポリシーが適用されます。 一部のセッションにはポリシーがまったく適用されません。 その結果、ルータはトラフィックを階層型キューイング フレームワーク（HQF）を使用して次のようにトラフィックを転送します。

- VC レベルまたはセッション レベルでキューイング ポリシーが適用されていない場合、ルータは policing-only ポリシーが適用されている、またはポリシーが適用されていない VC 上のセッションからのトラフィックを含む、VC 上のすべてのトラフィックをデフォルト キューに送信します。
- キューイング ポリシーがセッション レベルではなく VC レベルで適用されている場合、ルータは VC 上のキューイング ポリシーに関連付けられたキューにトラフィックを送信します。
- キューイング ポリシーが他のセッションにではなく VC 上の一部のセッションに適用されている場合、ルータは policing-only ポリシーが付属したトラフィックまたは VC のデフォルト キューにポリシーが適用されていないトラフィックを送信します。 ルータは、キューイング ポリシーが付属したトラフィックを、セッションに適用されるキューイング ポリシーに関連付けられたキューに送信します。

帯域幅モードおよび ATM ポートのオーバーサブスクリプション

ATM ポートは予約帯域幅モードまたは共有帯域幅モードで動作します。

ポートがオーバーサブスクライブしていない（ポート上のすべての VC の帯域幅の合計がポート帯域幅未満である）場合、ポートは予約帯域幅モード（特定の量の帯域幅がポートの各 VC 用に予約されている）で動作します。 VCが割り当てられた帯域幅の一部だけを使用している場合は、未使用の帯域幅はポート上の VC 間で共有されません。

ATM ポートがオーバーサブスクライブしている（ポート上のすべての VC の帯域幅の合計がポート帯域幅よりも大きい）場合、ポートは共有帯域幅モードで動作します。 このモードでは、すべての未使用帯域幅が、VC の個々のシェーピング レートまで、ポート上の他の VC で再使用できます。VC 上のトラフィックは、その VC のシェーピング レートを超えることはできません。

セッション レベルでのオーバーサブスクリプション

セッション レベルのオーバーサブスクリプションは、セッションのトラフィックのシェーピング後、および集約セッショントラフィックがサブインターフェイスのシェーピング レートを超過した場合に発生します。 すべてのプライオリティ トラフィックが指定されると、ルータは、セッションに適用されるポリシーの親ポリシーに設定した bandwidth remaining ratio コマンドで指定された値に基づいて、VC 上の残りの帯域幅をセッションに分配します。 bandwidth remaining ratio コマンドが親ポリシーで指定されていない場合、ルータはデフォルトの比率である 1 を使用します。

ATM VC での PPP セッション キューイングの設定方法

仮想テンプレートを使用してPPPセッションキューイングを設定する

仮想テンプレートは、その設定が特定の目的に対応する汎用設定情報、ユーザ固有の設定情報とルータ依存情報を指定できる論理インターフェイスです。 インターフェイスに仮想テンプレートを設定し、仮想テンプレートに QoS ポリシー マップを適用します。 仮想テンプレートは、ポリシー マップで指定された QoS 機能を継承します。 ルータがインターフェイスにセッションを確立すると、ルータは仮想テンプレート設定で指定された QoS 機能を、仮想テンプレートに付加されたポリシーマップで指定されたQoS機能を含むセッションに作成された仮想アクセスインターフェイス（VAI）に適用します。

ATMインターフェイスに設定されたブロードバンド集約グループ（bba-group）は、セッションにQoS ポリシーを適用するためにルータが使用する仮想テンプレートを示します。 セッションがATM インターフェイスに到達すると、ルータはセッションに仮想アクセス インターフェイス（VAI）を作成し、仮想テンプレートに関連付けられたポリシーをセッションに適用します。

仮想テンプレートを使用して PPPoEoA セッション キューイングを設定するには、次の設定作業を実行します。

階層型 QoS ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. priority level level
6. **police** *bps* [*burst-normal burst-max*] [**conform-action** *action]* [**exceed-action** *action]* **violate-action** *action*
7. set cos value
8. bandwidth remaining ratio
9. exit
10. **policy-map** *policy-map-name*
11. **class** *class-default*
12. bandwidth remaining ratio
13. **shape** [**average**] *mean-rate*[*burst-size*] [*excess-burst-size*]
14. **service-policy** *policy-map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map** *policy-map-name* 例： `Router(config)# policy-map policy-map-name`	子ポリシーを作成または変更します。 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。 policy-map-name は子ポリシー マップの名前です。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class class-map-name`	指定するトラフィック クラスをポリシーマップに割り当てます。 ポリシーマップ クラス コンフィギュレーション モードを開始します。 class-map-name は設定済みのクラス マップの名前で、QoS アクションを定義するトラフィック クラスです。 子ポリシー マップに含めるトラフィック クラスごとにステップ 2～6 を繰り返して行ってください。
ステップ 5	priority level level 例： `Router(config-pmap-c)# priority level level`	（任意）完全プライオリティ サービス モデルの複数レベルを定義します。 特定のプライオリティ レベルのサービスを持つトラフィック クラスをイネーブルにすると、指定されたプライオリティ サービスのレベルがイネーブルであるすべてのトラフィックに関連付けられた単一のプライオリティ キューに影響します。 level は、特定のプライオリティ レベルを示す番号です。 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:1
ステップ 6	**police** *bps* [*burst-normal burst-max*] [**conform-action** *action]* [**exceed-action** *action]* **violate-action** *action* 例： `Router(config-pmap-c)# police bps [burst-normal] [burst-max] [conform-action action]`	（任意）トラフィック ポリシングを設定します。 bps はビット/秒の平均速度です。 有効値は 8000 ～ 200000000 です。 （任意）burst-normal は標準バースト サイズ（バイト）です。 有効値は 1000 ～ 51200000 です。 デフォルトのノーマル バースト サイズは 1500 バイトです。 （任意）burst-max は超過バースト サイズ（バイト）です。 有効値は 1000 ～ 51200000 です。

	コマンドまたはアクション	目的
	`[exceed-action action] [violate-action action]`	（任意）conform-action action は、レート制限に適合するパケットで実行されるアクションを示します。 （任意）exceed-action action は、レート制限を超過するパケットで実行されるアクションを示します。 （任意）violate-action action は、ノーマルおよび超過バースト サイズに違反するパケットで実行するアクションです。
ステップ 7	set cos value **例：** `Router(config-pmap-c)# set cos value`	（任意）送信パケットのレイヤ 2 サービス クラス（CoS）値を設定します。 値は 0～7 の、IEEE 802.1Q CoS 固有値です。
ステップ 8	bandwidth remaining ratio **例：** `Router(config-pmap-c)# bandwidth remaining ratio`	（任意）クラス レベルまたはサブインターフェイス レベルのキューの BRR を指定します。この BRR は、プライオリティ トラフィックによって使用されていない余分な帯域幅を判断し、非プライオリティ キューに割り当てるために輻輳時に使用します。 比率は、他のサブインターフェイスまたはキューに関して、サブインターフェイスまたはキューに対する相対的重みを指定します。 有効な値は、1 ～ 1000 です。
ステップ 9	exit **例：** `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**policy-map** *policy-map-name* **例：** `Router(config-pmap)#` **policy-map** *policy-map-name*	親ポリシーを作成または変更します。 policy-map-name は親ポリシー マップの名前です。
ステップ 11	**class** *class-default* **例：** `Router(config-pmap)#` **class** *class-default*	親 class-default クラスを設定または変更します。 親ポリシーの class-default クラスは 1 つだけ設定できます。 他のトラフィック クラスは設定しないでください。
ステップ 12	bandwidth remaining ratio **例：** `Router(config-pmap-c)# bandwidth remaining ratio`	（任意）クラス レベルまたはサブインターフェイス レベルのキューの BRR を指定します。この BRR は、プライオリティ トラフィックによって使用されていない余分な帯域幅を判断し、非プライオリティ キューに割り当てるために輻輳時に使用します。

	コマンドまたはアクション	目的
		比率は、他のサブインターフェイスまたはキューに関して、サブインターフェイスまたはキューに対する相対的重みを指定します。 有効な値は、1 ～ 1000 です。
ステップ 13	**shape** [**average**] *mean-rate*[*burst-size*] [*excess-burst-size*] 例： **Router(config-pmap-c)# shape** [**average**] *mean-rate* [*burst-size*] [*excess-burst-size*]	指示されたビット レートにトラフィックをシェーピングし、ATM オーバーヘッド アカウンティングをイネーブルにします。 （任意）average は、各間隔で送信される最大ビット数を指定する認定バースト（Bc）です。 このオプションがサポートされるのは Performance Routing Engine 3（PRE3）だけです。 mean-rate は、認定情報速度（CIR）とも呼ばれます。 トラフィックのシェーピングに使用されるビット レートを bps 単位で指定します。 このコマンドを逆方向明示的輻輳通知（BECN）の近似値と併用すると、ビット レートは許容ビット レート範囲の上限値になります。 （任意）burst-size は測定インターバル内のビット数（Bc）です。 （任意）excess-burst-size は Be の超過が許可される受け入れ可能なビット数です。
ステップ 14	**service-policy** *policy-map-name* 例： `Router(config-pmap-c)#` **service-policy** *policy-map-name*	親の class-default クラスに子ポリシーを適用します。 policy-map-name は、ステップ 1 で設定された子ポリシー マップの名前です。

例

次に、階層型 QoS ポリシーを設定する例を示します。 この例では、child-policy は Premium と Silver という 2 種類のトラフィック クラスに QoS 機能を設定します。 Premium トラフィックが優先され、40 パーセントでポリシングされます。 ルータは Premium トラフィックの IP precedence をレベル 3 に設定します。 Silver トラフィックは 80000 bps でポリシングされ、IP Precedence レベル 3 が設定されます。 トラフィックを 200,000 Kbps にシェーピングする親ポリシーの class-default クラスに child-policy が適用されます。

```
Router(config)# policy-map child-policy
Router(config-pmap)# class Premium
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# set ip precedence 3
Router(config-pmap-c)# class Silver
Router(config-pmap-c)# police 80000 10000 conform-action transmit exceed-action drop
Router(config-pmap-c)# set ip precedence 5
Router(config-pmap-c)# exit
Router(config-pmap)# policy-map Parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 200000
Router(config-pmap-c)# service-policy output child-policy
```

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

仮想テンプレートと階層型ポリシー マップの関連付け

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template template-** *number*
4. **service-policy {input | output} policy-map-name**
5. exit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface virtual-template template-***number* 例： `Router(config)# interface virtual-template template-number`	仮想テンプレートを作成し、インターフェイス コンフィギュレーション モードを開始します。 template-number は識別のために仮想テンプレート インターフェイスに割り当てられる番号です。 有効な値は 1～200 です。 ルータ上に最大 200 個の仮想テンプレート インターフェイスを設定できます。
ステップ 4	**service-policy {input | output} policy-map-name** 例： `Router(config-if)# service-policy {input | output} policy-map-name`	指定したポリシーマップを、指定の着信方向または発信方向で仮想テンプレート インターフェイスに対応付けます。 input は着信トラフィックにポリシー マップを適用するように指定します。 output は発信トラフィックにポリシー マップを適用するように指定します。 policy-map-name は設定済みのポリシー マップの名前です。

	コマンドまたはアクション	目的
ステップ 5	exit 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

例

次に、仮想テンプレートとポリシー マップを関連付ける例を示します。 この例では、Parent という名前のポリシー マップが VirtualTemplate1 という名前の仮想テンプレートに関連付けられます。

```
Router(config)# interface virtual-template1
Router(config-if)# service-policy output Parent
Router(config-if)# exit
Router(config)#
```

ATM サブインターフェイスに仮想テンプレートを適用する

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-group pppoe group-name**
4. **virtual-template template-number**
5. exit
6. interface atm number.subinterface [point-to-point]
7. pvc [name] vpi/vci
8. protocol pppoe group group-name
9. exit
10. exit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bba-group pppoe group-name** 例： `Router(config)#` **bba-group pppoe group-name**	PPP over Ethernet（PPPoE）プロファイルを作成します。 BBA グループ コンフィギュレーション モードを開始します。 group-name は、PPPoE プロファイルの名前です。
ステップ 4	**virtual-template template-number** 例： `Router(config-bba-grp)#` **virtual-template template-number**	仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートに BBA グループを関連付けます。 template-number は仮想テンプレートの識別番号です。
ステップ 5	exit 例： `Router(config-bba-grp)# exit`	BBA グループ コンフィギュレーション モードを終了します。
ステップ 6	interface atm number.subinterface [point-to-point] 例： `Router(config)# interface atm number.subinterface [point-to-point]`	サブインターフェイスを作成または変更します。 サブインターフェイス コンフィギュレーション モードを開始します。 atm はインターフェイス タイプです。 number は、インターフェイスのスロット、モジュール、およびポート番号です（1/0/0 など）。 .subinterface はサブインターフェイスの番号です（1/0/0.1 など）です。 （任意）point-to-point はサブインターフェイスが別のサブインターフェイスに直接接続することを示します。
ステップ 7	pvc [name] vpi/vci 例： `Router(config-subif) pvc [name] vpi/vci`	ATM 相手先固定接続（PVC）を作成または変更します。 ATM 仮想回線コンフィギュレーション モードを開始します。 （任意）name は PVC を識別し、15 文字まで使用できます。 vpi/ はこの PVC の ATM ネットワーク仮想パス識別子（VPI）を指定します。 スラッシュを指定する必要があります。 有効な値は、0 ～ 255 です。 ルータは、有効な値の範囲外にある値を接続 ID として処理します。 デフォルト値は 0 です

	コマンドまたはアクション	目的
		（注） vpi および vci 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。 vci はこの PVC の ATM ネットワーク仮想チャネル識別子（VCI）を指定します。 有効な値は 0～1 で、atm vc-per-vp 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。 値が範囲外の場合、「認識されないコマンド」のエラー メッセージが表示されます。 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。 通常、小さい値である 0～31 は特定のトラフィック（F4 OAM、SVC シグナリング、ILMI など）に予約されているため使用できません。
ステップ 8	protocol pppoe group group-name **例**： `Router(config-atm-vc)# protocol pppoe group group-name`	PPP over Ethernet（PPPoE）セッションを相手先固定接続（PVC）で確立できるようにします。 group は、インターフェイス上の PPPoE セッションで使用される PPPoE プロファイル（bba-group）を示します。 group-name は、インターフェイス上の PPPoE セッションで使用される PPPoE プロファイル（bba-group）の名前です。 group group-name は、QoS ポリシー付きの仮想テンプレート インターフェイスをセッションに適用するために使用される、bba-group を指します。
ステップ 9	exit **例**： `Router(config-atm-vc)# exit`	ATM 仮想回線コンフィギュレーション モードを終了します。
ステップ 10	exit **例**： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了します。

例

次に、ATM インターフェイスを仮想テンプレート インターフェイスを関連付ける方法と、インターフェイス上のセッションに仮想テンプレート内のポリシーを適用する方法の例を示します。この例では、Parent という名前のサービス ポリシーが、pppoeoa-group という bba-group に関連付けられている Virtual-Template 8 に適用されます。 bba-group は ATM サブインターフェイス 4/0/1.10 上の PVC 101/210 に適用されます。

```
bba-group pppoe pppoeoa-group
Virtual-Template 8
```

```
interface ATM4/0/1.10 point-to-point
pvc 101/210
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
interface Virtual-Template8
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
ppp authentication chap
service-policy output Parent
```

RADIUS を使用して PPP セッション キューイングを設定する

RADIUS を使用して PPPoEoA セッション キューイングを設定するには、次の設定作業を実行します。

ポリシー マップの設定

ルータによって、PPPoEoA セッションに RADIUS を使用して QoS ポリシー マップを動的に適用できるようになります。

RADIUS プロファイルに Cisco QoS AV ペアを追加する

シスコの属性と値（AV）のペアは、シスコなどのベンダーが独自の拡張属性をサポートできるようにするベンダー固有属性（VSA）です。 RADIUS 属性 26 は、ルータと RADIUS サーバ間でベンダー固有の情報をやり取りするために使用される Cisco VSA です。

RADIUS ユーザ プロファイルには、RADIUS サーバが認証する各ユーザのエントリが含まれます。エントリごとにユーザがアクセス可能な属性が設定されます。 RADIUS を使用して PPPoEoA セッション キューイングを設定する場合は、適切なユーザ プロファイルに次の Cisco AV ペアを入力してください。

```
Cisco-AVPair = "ip:sub-qos-policy-out=<name of egress policy>"
```

Cisco AV ペアは、QoS 機能を PPPoEoA セッションに適用する場合にルータが使用するポリシー マップを示します。 ポリシー サーバからサービス ログイン要求を受け取った後、すでにログインしているユーザ向けのサービスをアクティブにするため、RADIUS はルータに許可変更（CoA）要求を送信します。 認証に成功すると、ルータは Cisco AV ペアを使用して RADIUS からポリシー マップ名をダウンロードし、セッションに QoS ポリシーを適用します。

（注） ルータは RADIUS のベンダー固有属性（VSA）38、Cisco-Policy-Down および Cisco-Policy-Up もサポートしますが、QoS ポリシー定義には上記の属性を使用することを推奨します。

ATM VC での PPP セッション キューイングの確認

手順の概要

1. **enable**
2. **configure terminal**
3. **show policy-map [interface interface]**
4. show policy-map session [uid uid-number] [input | output [class class-name]]
5. **show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**show policy-map [interface interface]** 例： `Router# show policy-map [interface interface]`	ユーザが指定したインターフェイスに付加されたポリシー マップに関する情報を表示します。 インターフェイスを指定しないと、ルータ上で設定されているすべてのポリシー マップに関する情報が表示されます。 interface interface は、インターフェイスのタイプと番号です（atm 4/0/0 など）。
ステップ 4	show policy-map session [uid uid-number] [input | output [class class-name]] 例： `Router# show policy-map session [uid uid-number] [input | output [class class-name]]`	加入者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。 （任意）uid は一意のセッション ID を定義します。 （任意）uid-number は一意のセッション ID です。 有効な値は 1 ～ 65535 です。 （任意）input には一意のセッションのアップストリーム トラフィックが表示されます。 （任意）output には一意のセッションのダウンストリーム トラフィックが表示されます。

	コマンドまたはアクション	目的
		（任意）class は、QoS ポリシー マップ定義の一部であるクラスを識別します。 （任意）class-name は QoS ポリシー マップ定義の一部であるクラス名を提供します。
ステップ 5	**show running-config** 例： `Router# show running-config`	ルータ上の実行コンフィギュレーションを表示します。出力には、AAA 設定、およびポリシー マップ、ATM VCs、PPPoEoA、ダイナミック帯域幅選択、仮想テンプレート、RADIUS サーバの設定が表示されます。

ATM VC での PPP セッション キューイングの設定例

ATM VC での PPP セッション キューイングの設定例

次に、PPPoEoA セッション キューイングを設定する例を示します。この例では、pppoeoa Group という名前のブロードバンド集約グループに適用される pm_hier2_0_2 という名前の階層型 QoS ポリシーが、Virtual-Template555 に関連付けられています。

```
bba-group pppoe pppoeoa-group
Virtual-Template 555
!
policy-map pm_hier2_child_0_2
class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
class cm_1
shape average percent 80
bandwidth remaining ratio 80
class class-default
shape average percent 50
bandwidth remaining ratio 20
policy-map pm_hier2_0_2
class class-default
shape average percent 100
bandwidth remaining ratio 100
service-policy pm_hier_child_0_2
interface ATM2/0/7.5555 point-to-point
pvc 1/5555
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
!
interface Virtual-Template555
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
```

```
ppp authentication chap
service-policy output pm_hier2_0_2
```

階層型ポリシー マップを設定および適用する例

階層型ポリシーマップを設定および適用する例, （123ページ）に、階層型ポリシーを設定し、仮想テンプレートに適用する例を示します。 この例には、child1 という名前の子ポリシー マップと、gold トラフィック クラスと bronze トラフィック クラス用に定義された QoS 機能が含まれます。 child1 ポリシーは 512000 bps にシェーピングされる、親ポリシー マップに適用されます。 階層型ポリシーは、virtual-template 1 という名前の仮想テンプレートに適用されます。

```
Router(config)# policy-map child1
Router(config-pmap)# class gold
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# class bronze
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 512000
Router(config-pmap-c)# service-policy child1
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface virtual-template 1
Router(config-if)# service-policy output parent
```

ATM VC での PPP セッション キューイング用 RADIUS の設定例

ATM VC での PPP セッション キューイング用 RADIUS の設定例, （123ページ）に、ポリシー マップ名をルータにダウンロードする際に使用される Cisco AV ペアを定義する方法を示します。 加入者のユーザ プロファイルの例の最初の 3 行には、ユーザ パスワード、サービス タイプ、プロトコル タイプが含まれます。 この情報は、ユーザ プロファイルが最初に作成されたときに、加入者のユーザプロファイルに入力されます。 最後の行は、ユーザプロファイルに追加された Cisco QoS AV ペアの例です。 ルータにダウンロードされたポリシー マップ名は p23 です。

```
userid Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
cisco-avpair = "sub-qos-policy-out=p23"
```

ATM VC での PPP セッション キューイングの確認例

ATM VC での PPP セッション キューイングの確認例, （123 ページ）は、show pppoe session コマンドを使用して、ルータに設定されたセッションを表示します。 この場合、セッション ID（SID）6 で 1 個のセッションがアクティブです。

PPP セッション情報の表示：show pxf cpu queue session コマンド

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
```

```
Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC VA-st Type
 14 6 0009.b68d.bb37 ATM2/0/7.5555 555 Vi3.1 PTA
   0009.b68d.bc37 VC: 1/5555    UP
```

ATM VC での PPP セッション キューイングの確認例, （123 ページ）は、show policy-map session コマンドを使用して、ダウンストリーム方向のトラフィックの QoS ポリシーマップ統計情報を表示します。 ポリシー マップ コンフィギュレーションの例も示します。

PPP セッション情報の表示：show policy-map session コマンド

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC VA-st Type
 14 6 0009.b68d.bb37 ATM2/0/7.5555 555  Vi3.1  PTA
 0009.b68d.bc37 VC: 1/5555 UP
Router#
Router#
Router# show policy-map session uid 14
SSS session identifier 14 -
 Service-policy output: pm_hier2_0_2
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 50 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000
bandwidth remaining ratio 100
 Service-policy : pm_hier2_child_0_2
queue stats for all priority classes:
Queueing
priority level 1
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
Class-map: cm_0 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 0
0 packets, 0 bytes
30 second rate 0 bps
Priority: 0% (0 kbps), burst bytes 4470, b/w exceed drops: 0
Priority Level: 1
Police:
104000 bps, 1536 limit, 0 extended limit
conformed 0 packets, 0 bytes; action: transmit
exceeded 0 packets, 0 bytes; action: drop
violated 0 packets, 0 bytes; action: drop
Class-map: cm_1 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 1
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 237 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1600000, bc 6400, be 6400
target shape rate 1600000
bandwidth remaining ratio 80
Class-map: class-default (match-any)
```

```
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1000000, bc 4000, be 4000
target shape rate 1000000
bandwidth remaining ratio 20
Router# show policy-map pm_hier2_0_2
Policy Map pm_hier2_0_2
Class class-default
Average Rate Traffic Shaping
cir 100%
bandwidth remaining ratio 100
service-policy pm_hier2_child_0_2
Router# show policy-map pm_hier2_child_0_2
Policy Map pm_hier2_child_0_2
Class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
Class cm_1
Average Rate Traffic Shaping
cir 80%
bandwidth remaining ratio 80
Class class-default
Average Rate Traffic Shaping
cir 50%
bandwidth remaining ratio 20
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド	『*Cisco IOS QoS Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ATM VC での PPP セッション キューイングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *11*：*ATM VC* での *PPP* セッション キューイングの機能情報

機能名	リリース	機能情報
ATM VC での PPP セッション キューイング	Cisco IOS XE Release 2.5	ATM 仮想回線（VC）での PPP セッション キューイングにより、ユーザが指定したレートに PPP over Ethernet over ATM（PPPoEoA）セッションをシェーピングし、キューに入れることができます。 この機能は、Cisco IOS Release XE 2.5 で、Cisco ASR 1000 シリーズ ルータに導入されました。

QoS：ポリシングおよびシェーピング コンフィギュレーション ガイド、**Cisco IOS XE Release 3S**（**Cisco ASR 1000**）

第 9 章

階層型 Color-Aware ポリシング

階層型 Color-Aware ポリシング機能は、子から親にポリサーの順序付けを評価する場面に 2 つのレベルのポリシングを提供し、親レベルで特定のトラフィックを優先的に扱うことができます。この機能は、次のサポートと変更を通じて、Cisco IOS XE Release 3.2S から Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでイネーブルになります。

- 階層型ポリシーでのデータ プレーンのポリシングの順序を反転させ、このポリシーが子から親に評価されるようにます。 以前のリリースでは、ポリシーは親から子に評価されていました。
- Quality of Service（QoS）ポリシー内の Color-Aware ポリシングの限定的なサポート（RFC 2697、RFC 2698）。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

階層型 Color-Aware ポリシングの前提条件

Cisco IOS XE Release 3.2S 以降のバージョンがインストールされていて、Cisco ASR 1000 シリーズルータで実行されている必要があります。

モジュラ Qos CLI（MQC）、マスター コントロール プロセッサ（MCP）ソフトウェアとハードウェアアーキテクチャなどの関連機能とテクノロジーについて知っておく必要があります。その他の関連資料, （140ページ）の項には、関連機能およびテクノロジーマニュアルへのリンクが記載されています。

階層型 Color-Aware ポリシングに関する制約事項

Color-Aware ポリシング機能には次の制約事項が適用されます。

- Color-Aware クラス マップは、QoS グループのマッチングだけをサポートします。
- Color-Aware クラスごとに 1 フィルタのみ（1 個の match ステートメント）がサポートされます。
- Color-Aware 統計情報はサポートされません。既存のポリサー統計情報だけがサポートされます。
- Color-Aware クラス マップの削除（**no class-map***class-map-name* コマンドを使用）は、クラス マップが Color-Aware ポリサーで参照されている間は許可されません。 これは、すべての Color-Aware ポリサーから取り除く必要があります（**no conform-color***class-map-name* または **no exceed-color***class-map-name* コマンドを最初に使用）。
- 階層型ポリサーの評価は、子から親への順序付けをサポートするために永続的に反転します（設定不可）。

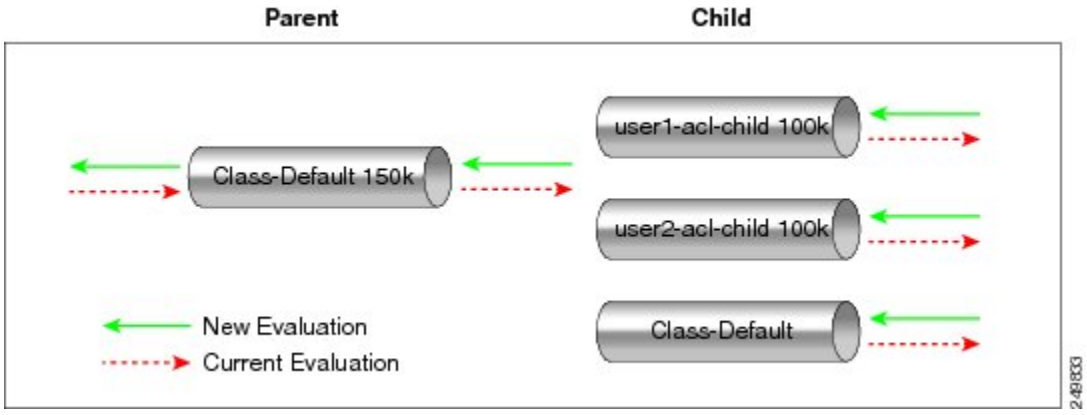
階層型 Color-Aware ポリシングの概要

階層型の順序のポリシング

Cisco IOS XE Release 3.2S 以前は、Cisco ASR 1000 シリーズ プラットフォームは、評価順序が親から子である階層型ポリシーでのポリサーをサポートしていました。 階層型 Color-Aware ポリシング機能の導入により、評価順序が反転し、QoS ポリシーでポリサーが子から親へ評価されるようになります。 この順序はデフォルトの動作に対する永続的な変更で、設定不可です。 逆順ポリサー機能は、入出力方向の両方で共有されます。

次の単純な 2 つのレベルのポリサーの設定により、下記の図に示すように動作が変化します。

```
policy-map child
 class user1
  police 100k
 class user2
  police 100k
policy-map parent
 class class-default
  police 150k
  service-policy child
```



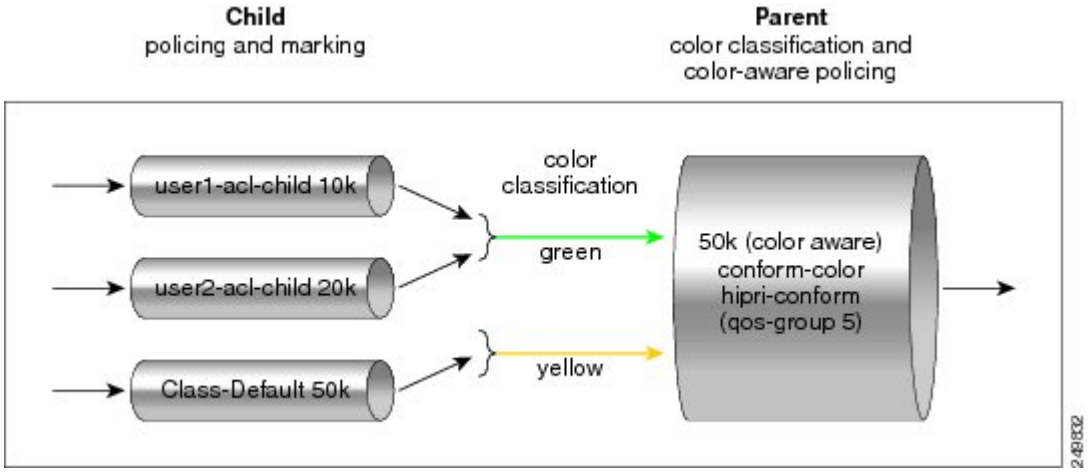
限定的 Color-Aware ポリシング

次の単純な 2 つのレベルの Color-Aware ポリサーの設定により、下記の図に示すように動作が変化します。

```
ip access-list extended user1-acl
 permit ip host 192.168.1.1 any
 permit ip host 192.168.1.2 any
ip access-list extended user2-acl
 permit ip host 192.168.2.1 any
 permit ip host 192.168.2.2 any
class-map match-all user1-acl-child
  match access-group name user1-acl
class-map match-all user2-acl-child
  match access-group name user2-acl
class-map match-all hipri-conform
 match qos-group 5
policy-map child-policy
 class user1-acl-child
   police 10000 bc 1500
    conform-action set-qos-transmit 5
class user2-acl-child
   police 20000 bc 1500
    conform-action set-qos-transmit 5
class class-default
   police 50000 bc 1500
policy-map parent-policy
 class class-default
  police 50000 bc 3000
   exceed-action transmit
   violate-action drop
```

```
 conform-color hipri-conform
service-policy child-policy
```

図 *1*：単純な *2* つのレベルの *Color-Aware* ポリサー



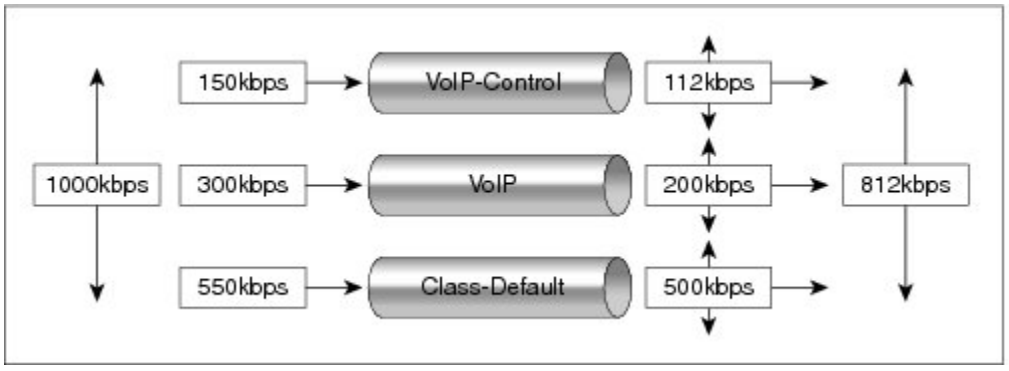
（注） 「適合した」子のトラフィックに対する親レベルでのドロップを回避するには、親ポリサーのレートとバーストが、子の適合レートとバースト サイズの合計以上である必要があります。不適切な（親から子への）レートおよびバースト サイズがコードにないかどうかチェックする機能はありません。 この制限を認識し、適切に設定する必要があります。 次の例では、Color-Aware ポリシングとともに明示的なマーキング アクションがサポートされ、Color-Aware ポリサーのマーキング アクションを同様に実行します。これらのマーキング アクション（「set qos-group」など）が子ポリシーにある場合、結果として生成されるビット値は、親の Color-Aware ポリサー（子ポリサーのマーキング アクションの場合と同じ）によって評価されます：50k>= 10k (user1-acl-child) + 20k (user2-acl-child)

子クラスと親クラスでのトラフィックのポリシング

階層型 Color-Aware ポリシング機能がリリースされるまでは、ポリシングとマーキングは、通常、入力 QoS のオプションとして使用されていました。 たとえば、音声カスタマーは、音声制御では 112 kb/s、音声トラフィックでは 200 Kbps に制限されていました。 class-default クラスにはポリサーがありません。 唯一の制限は、xDSL 接続の物理的な帯域幅のみです。 次の図に示すように、

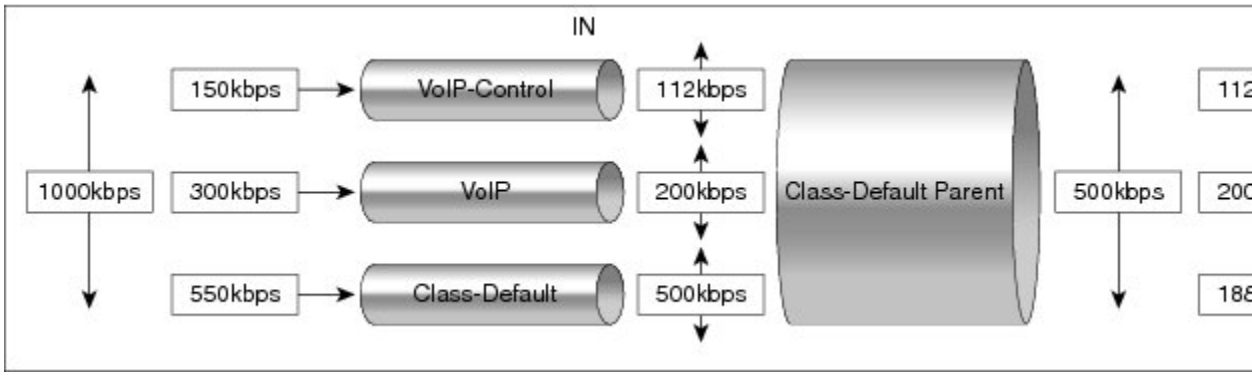
カスタマーは1000 kb/sまで送信できます。ただし、この場合、より多くの音声と音声制御パケットが送信され、両方のクラスに対してトラフィックをポリシングする必要があります。

図 *2*：子クラスでのトラフィックのポリシング



次の図に示すように、入力帯域幅全体を制御することが重要です。 重要な要件は、その全体の制限においてPremiumトラフィックが影響を受けないということです。 次の図に示すように、音声および音声制御パケットは全体の制限ではドロップされません。 子の class-default クラスから発生するパケットのみ、制限を満たすためにドロップされます。

図 *3*：親クラスでのトラフィックのポリシング



最初のクラスは同様に機能します。 音声および音声制御は許容されるレベルにポリシングされ、class-default クラスは影響を受けません。 次のレベルでは、帯域幅全体は 500 Kb/s に制限され、class-default クラスから発生するパケットのみドロップする必要があります。 音声および音声制御は影響を受けないようにしておく必要があります。

ポリサーの実行順序は次のとおりです。

1. 上記の図に示すように、子クラスのトラフィックをポリシングします。VoIP-Control クラスを 112 kb/s に、VoIP クラスを 200 kb/s に、class-default を 500 kb/s にポリシングします。
2. 親ポリシーマップの class default のトラフィックをポリシングしますが、子の class default からのトラフィックのみをドロップし、残りの子クラスはドロップしません。 上の図に示すように、112 Kb/s の VoIP-Control および 200 kb/s の VoIP トラフィックは、親ポリサーでは影響を

受けません。しかし、子からの 500 kb/s の class default は、親レベルでの 500 Kbps のポリシング ポリシー全体に適合するよう 188kb/s にポリシングされます。

階層型 Color-Aware ポリシングの設定方法

階層型 Color-Aware ポリシング機能の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default** [**fragment** *fragment-class-name*]} [**insert-before** *class-name*] [**service-fragment** *fragment-class-name*]
5. **police** [**cir** *cir*][**bc** *conform-burst*] [**pir** *pir*][**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]][**conform-color hipri-conform**]
6. **service-policy** *policy-map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map** *policy-map-name* 例： `Router(config)# policy-map parent-policy`	ポリシー マップ コンフィギュレーション モードを開始して、ポリシー マップを作成します。
ステップ 4	**class** {*class-name* | **class-default** [**fragment** *fragment-class-name*]}	ポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	[**insert-before** *class-name*] [**service-fragment** *fragment-class-name*] 例： `Router(config-pmap)# class class-default`	• 作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。 作成または変更する親クラスまたは子クラスの指定に必要な回数だけ次のコマンドを繰り返します。 • *class name*：設定するクラス、またはポリシーを編集するクラスの名前。 クラス名は、クラス マップに使用するとともに、ポリシー マップのクラスにポリシーを設定する場合にも使用します。 • **class-default**：ポリシーを設定または変更できるようデフォルト クラスを指定します。 • **fragment** *fragment-class-name*：（任意）デフォルト トラフィック クラスをフラグメントに指定し、フラグメント トラフィック クラスに名前を付けます。 • **insert-before** *class-name*：（任意）2 つの既存のクラス マップ間にクラス マップを追加します。 既存の 2 つのクラス マップ間に新しいクラス マップを挿入すると、既存のポリシー マップ コンフィギュレーションの柔軟性が向上します。 このオプションを指定しないと、クラス マップはポリシー マップに付加されます。 （注） このキーワードは、Flexible Packet Matching（FPM）ポリシーでだけサポートされています。 • **service-fragment** *fragment-class-name*：（任意）クラスがフラグメントのコレクションを分類するように指定します。 このクラスにより分類されるフラグメントは、すべて同じフラグメント クラス名を共有している必要があります。

ステップ 5	**police** [**cir** *cir*][**bc** *conform-burst*] [**pir** *pir*][**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]][**conform-color hipri-conform**]
	
	例：
	
	`Router(config-pmap-c)# police 50000 bc 3000`
	`Router(config-pmap-c-police)# exceed-action transmit`
	
	例：
	
	`Router(config-pmap-c-police)# violate-action drop`
		トラフィック ポリシングを設定し、指定のレートに準拠、超過、または違反としてマーク付けされたパケットに適用する複数のアクションを指定します。
		
		• ポリシー マップ クラス ポリス コンフィギュレーション モードを開始します。 1 つのアクションにつき 1 行を使用して、アクションを指定します。
		
		• **cir**：認定情報レート。 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。
		
		• **conform-action**：（任意）レートが適合バースト値よりも少ない場合にパケットで実行されるアクション。
		
		• **exceed-action**：（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。

	コマンドまたはアクション	目的
	例： `Router(config-pmap-c-police)# conform-color hipri-conform`	• **violate-action**：（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。違反アクションを指定する前に、超過アクションを指定する必要があります。 • **conform-color**：（任意）Color-Aware ポリシングを（設定済みポリサーで）イネーブルにし、適合カラーの決定に使用されるクラスマップを割り当てます。 **hipri-conform** キーワードは、使用されるクラス マップ（以前は class-map **コマンド**で設定）です。
ステップ 6	**service-policy** *policy-map-name* 例： `Router(config-pmap-c-police)# service-policy child-policy`	ポリシー マップ内に QoS ポリシーとしてサービス ポリシー（階層型サービス ポリシーと呼ばれます）を作成します。 • *policy-map-name*：QoS ポリシーとして使用する定義済みのポリシーマップの名前。 名前には最大 40 文字までの英数字を指定できます。
ステップ 7	**end** 例： `Router(config-pmap-c-police)# end`	現在のコンフィギュレーション モードを終了します。

例

次は、ポリシングの逆順を示す階層型 Color-Aware ポリシング機能の設定例です。

```
policy-map child-policy
 class user1-acl-child
  police 10000 bc 1500
 class user2-acl-child
  police 20000 bc 1500
 class class-default
  police 50000 bc 1500
policy-map parent-policy
 class class-default
  police 50000 bc 3000
  service-policy child-policy
```

階層型 Color-Aware ポリシングの設定例

階層型 Color-Aware ポリシング機能をイネーブルにする例

次に、階層型 Color-Aware ポリシング機能をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip access-list extended user1-acl
Router(config-ext-nacl)# permit ip host 192.168.1.1 any
Router(config-ext-nacl)# permit ip host 192.168.1.2 any
Router(config-ext-nacl)# ip access-list extended user2-acl
Router(config-ext-nacl)# permit ip host 192.168.2.1 any
Router(config-ext-nacl)# permit ip host 192.168.2.2 any
Router(config-ext-nacl)# exit
Router(config)# class-map match-all user1-acl-child
Router(config-cmap)# match access-group name user1-acl
Router(config-cmap)# class-map match-all user2-acl-child
Router(config-cmap)# match access-group name user2-acl
Router(config-cmap)# class-map match-all hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# exit
Router(config)# policy-map child-policy
Router(config-pmap)# class user1-acl-child
Router(config-pmap-c)# police cir 10000 bc 1500
Router(config-pmap-c-police)# class user2-acl-child
Router(config-pmap-c)# police cir 20000 bc 1500
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map parent-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 50000 bc 3000
Router(config-pmap-c-police)# exceed-action transmit
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# conform-color hipri-conform
Router(config-pmap-c-police)# service-policy child-policy
```

クラス マップでの複数エントリを拒否する例

次に、クラス マップでの複数エントリの設定が拒否された試行の例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# match qos-group 6
Only one match statement is supported for color-aware policing
Router(config-cmap)# no match qos-group 6
```

アクティブな Color-Aware クラス マップの削除を拒否する例

次に、アクティブな Color-Aware クラス マップを許可できない例を示します。

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no class-map hipri-conform
Class-map hipri-conform is being used
```

階層型 Color-Aware ポリシング機能の設定を削除する例

次に、階層型 Color-Aware ポリシング機能の設定を削除する方法の例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no policy-map parent-policy
Router(config)# no policy-map child-policy
Router(config)# no class-map hipri-conform
Router(config)# no class-map user1-acl-child
Router(config)# no class-map user2-acl-child
```

Cisco ASR 1000 シリーズ ルータの階層型 Color-Aware ポリシングの例

次に、Cisco ASR 1000 シリーズ ルータで階層型 Color-Aware ポリシング機能をイネーブルにする設定例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip access-list extended user1-acl
Router(config-ext-nacl)# permit ip host 192.168.1.1 any
Router(config-ext-nacl)# permit ip host 192.168.1.2 any
Router(config-ext-nacl)# ip access-list extended user2-acl
Router(config-ext-nacl)# permit ip host 192.168.2.1 any
Router(config-ext-nacl)# permit ip host 192.168.2.2 any
Router(config-ext-nacl)# class-map match-all user1-acl-child
Router(config-cmap)# match access-group name user1-acl
Router(config-cmap)# class-map match-all user2-acl-child
Router(config-cmap)# match access-group name user2-acl
Router(config-cmap)# class-map match-all hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# policy-map child-policy
Router(config-pmap)# class user1-acl-child
Router(config-pmap-c)# police 10000 bc 1500
Router(config-pmap-c-police)# conform-action set-qos-transmit 5
Router(config-pmap-c-police)# class user2-acl-child
Router(config-pmap-c)# police 20000 bc 1500
Router(config-pmap-c-police)# conform-action set-qos-transmit 5
Router(config-pmap-c-police)# class class-default
Router(config-pmap-c)# police 50000 bc 1500
Router(config-pmap-c-police)# policy-map parent-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 50000 bc 3000
Router(config-pmap-c-police)# exceed-action transmit
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# conform-color hipri-conform
Router(config-pmap-c-police)# service-policy child-policy
Router(config-pmap-c)# end
Router#
*Sep 16 12:31:11.536: %SYS-5-CONFIG_I: Configured from console by console
Router# show class-map
Class Map match-all user1-acl-child (id 4)
Match access-group name user1-acl
Class Map match-all user2-acl-child (id 5)
Match access-group name user2-acl
Class Map match-any class-default (id 0)
Match any
Class Map match-all hipri-conform (id 3)
```

```
Match qos-group 5
Router# show policy-map
Policy Map parent-policy
Class class-default
police cir 50000 bc 3000 be 3000
conform-color hipri-conform
conform-action transmit
exceed-action transmit
violate-action drop
service-policy child-policy
Policy Map police
Class prec1
priority level 1 20000 (kb/s)
Class prec2
bandwidth 20000 (kb/s)
Class class-default
bandwidth 20000 (kb/s)
Policy Map child-policy
Class user1-acl-child
police cir 10000 bc 1500
conform-action set-qos-transmit 5
exceed-action drop
Class user2-acl-child
police cir 20000 bc 1500
conform-action set-qos-transmit 5
exceed-action drop
Class class-default
police cir 50000 bc 1500
conform-action transmit
exceed-action drop
```

階層型 Color-Aware ポリシングが適用された show コマンドの例

次に、階層型 Color-Aware ポリシング ポリシーが適用された場合の **show policy-map interface** コマンドからの出力例を示します。

```
Router# show policy-map interface
GigabitEthernet0/0/0
Service-policy input: parent-policy
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
police:
cir 50000 bps, bc 3000 bytes, be 3000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
transmit
violated 0 packets, 0 bytes; actions:
drop
No color-aware policing statistics available
conformed 0000 bps, exceed 0000 bps, violate 0000 bps
Service-policy : child-policy
Class-map: user1-acl-child (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name user1-acl
police:
cir 10000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions:
set-qos-transmit 5
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceed 0000 bps
Class-map: user2-acl-child (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
```

```
Match: access-group name user2-acl
police:
cir 20000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions:
set-qos-transmit 5
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceed 0000 bps
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
police:
cir 50000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceed 0000 bps
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Quality of Service コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』
Quality of Service 設定情報	『*Cisco IOS QoS Configuration Guide, Cisco IOS XE Release 3S*』

標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

階層型 Color-Aware ポリシングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *12*：階層型 *Color-Aware* ポリシングの機能情報

機能名	リリース	機能情報
階層型 Color-Aware ポリシング	Cisco IOS XE Release 3.2S	階層型 Color-Aware ポリシング機能は、子から親にポリサーの順序付けを評価する場面に2つのレベルのポリシングを提供し、親レベルで特定のトラフィックを優先的に扱うことができます。

第 10 章

IPv6 QoS：MQC トラフィック ポリシング

IPv6 環境でのポリシングの設定またはコマンド使用法は、IPv4 環境と同じです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 QoS の概要：MQC トラフィック ポリシング

QoS for IPv6 の実装方針

IPv6 パケットは、IPv4 パケットとは別のパスで転送されます。 IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、重み付けランダム早期検出（WRED）、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含

まれます。 これらの機能は、IPv6 のプロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスのどちらでも使用できます。

IPv6 環境で使用可能な QoS 機能はすべて、モジュラ QoS コマンドライン インターフェイス（MQC）から管理します。 MQC を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシーマップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに対応付けることができます。

IPv6 が稼働しているネットワークに QoS を実装するには、IPv4 だけが稼働しているネットワークに QoS を実装する手順に従ってください。 高度なレベルで QoS を実装するための基本手順は、次のとおりです。

- QoS を必要とするネットワーク内のアプリケーションを特定します。
- どの QoS 機能が適切であるかを判断するために、アプリケーションの特性を理解します。
- 変更と転送がリンク層ヘッダー サイズに及ぼす影響を理解するために、ネットワーク トポロジについて理解します。
- ネットワークに確立する基準に基づいて、クラスを作成します。 具体的には、同じネットワークで IPv6 トラフィックとともに IPv4 トラフィックも伝送されている場合、IPv6 トラフィックと IPv4 トラフィックを同様に処理するか、それとも別の方法で処理し、それぞれに応じた一致基準を指定するかを決定します。 両者を同様に処理する場合は、**match precedence**、**match dscp**、**set precedence**、**set dscp** などの match 文を使用します。 両者を別の方法で処理する場合は、match-all クラス マップ内に **match protocol ip** や **match protocol ipv6** などの一致基準を追加します。
- 各クラスにマーキングするためのポリシーを作成します。
- QoS 機能を適用する際は、エッジからコアに向かって作業します。
- トラフィックを処理するためのポリシーを構築します。
- ポリシーを適用します。

IPv6 環境でのトラフィック ポリシング

IPv6 での輻輳管理は、IPv4 と同様で、IPv6 環境でのキューイングおよびトラフィック シェーピング機能の設定に使用するコマンドは、IPv4 で使用されるものと同じコマンドです。 トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケットデキュー レートを制限できます。 トラフィック シェーピングでは、デフォルトでフローベース キューイングが使用されます。 パケットの分類およびプライオリティ設定には、CBWFQ を使用できます。 トラフィックのコンディショニングおよびポリシングには、クラスベース ポリシング機能と汎用トラフィック シェーピング（GTS）、またはフレーム リレー トラフィック シェーピング（FRTS）を使用できます。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
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）、階層型ポリシー、ポリシー マップ	「MQC を使用した QoS 機能の適用」モジュール
トラフィックのポリシングとシェーピング	「ポリシングとシェーピングの概要」モジュール

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 QoS の機能情報：MQC トラフィック ポリシング

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *13*：*IPv6 QoS* の機能情報：*MQC* トラフィック ポリシング

機能名	リリース	機能情報
IPv6 QoS：MQC トラフィック ポリシング	Cisco IOS XE Release 2.1	IPv6 環境でのポリシングの設定またはコマンド使用法は、IPv4 環境と同じです。

第 11 章

トラフィック ポリシング

このフィーチャ モジュールでは、トラフィック ポリシング機能について説明します。 トラフィック ポリシングは、次のように機能します。

- ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限します。
- ATM セル損失率優先度（CLP）ビット、フレームリレー廃棄特性（DE）ビット、IP Precedence 値、IP Diffserv コード ポイント（DSCP）値、MPLS EXP 値、Quality of Service（QoS）グループを設定することによりパケットにマーク付けします。

トラフィック ポリシングでは、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。 トラフィック ポリシング機能は、この機能が含まれるサービス ポリシーがインターフェイスに関連付けられる場合に適用されます。 サービス ポリシー（トラフィック ポリシー）はモジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用して設定されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載

されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

トラフィック ポリシングに関する制約事項

- トラフィック ポリシングは、インターフェイスまたはサブインターフェイスで設定できます。
- トラフィック ポリシングは EtherChannel インターフェイスではサポートされていません。

利点

レート制限による帯域幅管理

トラフィック ポリシングでは、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。トラフィックポリシングは、多くの場合、ネットワークの端のインターフェイスで、ネットワークを出入りするトラフィックを制限するように設定されます。 ほとんどのトラフィックポリシング設定では、レートパラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

パケットのマーキング

パケットのマーキングにより、ネットワークを複数のプライオリティ レベルまたはクラスサービス（CoS）に区切ることができます。 パケットがマーキングされ、ダウンストリーム デバイスのトラフィックを識別および分類するためにこれらのマーキングが使用できます。 ATM セル損失率優先度（CLP）マーキングやフレームリレー廃棄特性（DE）マーキングなどでは、マーキングがトラフィックの分類に使用されます。

- トラフィック ポリシングを使用して、ネットワークに入るパケットの IP precedence または DSCP 値を設定します。 その後、ネットワーク内のネットワーキング デバイスは、調整された IP precedence 値を使用してトラフィックの処理方法を決定できます。 たとえば、重み付けランダム早期検出（WRE）機能では、IP precedence 値を使用して、パケットがドロップされる確率を決定します。
- トラフィック ポリシングを使用して、パケットを QoS グループに割り当てます。 ルータは QoS グループを使用して、ルータ内のパケットに優先順位を付ける方法を決定します。

トラフィックには、トラフィック ポリシング機能を使用せずにマークを付けることができます。トラフィックポリシングを使用せずにトラフィックにマークを付ける場合は、「ネットワーク トラフィックのマーキング」モジュールを参照してください。

フレームリレー フレームのパケットの優先順位付け

トラフィック ポリシング機能では、フレームリレー フレームのフレームリレー DE ビットにマーク付けできます。 フレームリレー DE ビットは 1 ビットで、0 または 1 に設定できます。 輻輳環境では、DE ビットが 1 に設定されたフレームは、DE ビットが 0 に設定されたフレームの前に破棄されます。

ATM セルのパケットの優先順位付け

トラフィック ポリシング機能では、ATM セルの ATM CLP にマーク付けできます。 ATM CLP ビットは、ATM ネットワークのパケットに優先順位を付けるために使用されます。 これにより ATM CLP ビットは 1 ビットで、0 または 1 に設定できます。 輻輳環境では、ATM CLP ビットが 1 に設定されたセルは、ATM CLP ビットが 0 に設定されたセルの前に破棄されます。

トラフィック ポリシングの設定方法

トラフィック ポリシングの設定

コマンド	目的
Router(config-pmap-c)# **police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	トラフィック クラスによる最大帯域幅の使用を指定します。 （注） トラフィック ポリシング機能は、トークン バケット メカニズムで動作します。 現在、トークン バケット アルゴリズムには、シングル トークン バケット アルゴリズムとツー トークン バケット アルゴリズムの 2 種類あります。 シングル トークン バケット システムは、**violate-action** オプションが指定されていない場合に使用されます。 ツー トークン バケット システムは、**violate-action** オプションが指定されている場合に使用されます。

トラフィック ポリシングのモニタリングと保守

コマンド	目的
Router# **show policy-map**	設定されたすべてのポリシーマップを表示します。

コマンド	目的
Router# **show policy-map** *policy-map-name*	ユーザ指定ポリシー マップを表示します。
Router# **show policy-map interface**	インターフェイスに適用されたすべての入力および出力ポリシーの統計情報および設定を表示します。

トラフィック ポリシングの設定例

トラフィック ポリシングを含むサービス ポリシーの設定例

次に、（**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）そのトラフィック クラスをトラフィック ポリシーに関連付ける設定例を示します。トラフィック ポリシングはトラフィック ポリシーに適用されます。 **service-policy** コマンドは、トラフィック ポリシーをインターフェイスに適用するために使用されます。

この例では、トラフィック ポリシングは 8,000 ビット/秒の認定情報速度（CIR）、通常バースト サイズは 2000 バイト、超過バースト サイズは 4000 バイトが設定されています。 FastEthernet インターフェイス 1/1/1 に着信するパケットは、パケットが超過基準に準拠しているか、または指定されたパラメータに違反していないかどうかを分析するため、トークンバケットアルゴリズムによって評価されます。 準拠するパケットは送信され、超過するパケットは 4 の QoS グループ値が割り当てられて送信され、違反するパケットはドロップされます。

```
Router(config)# class-map acgroup2
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map police
Router(config-pmap)# class acgroup2
Router(config-pmap-c)# police 8000 2000 4000 conform-action transmit exceed-action
set-qos-transmit 4 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/1/1
Router(config-if)# service-policy input police
Router(config-if)# end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
ポリシングとシェーピングの概念について	「ポリシングとシェーピングの概要」モジュール
MQC	「MQC を使用した QoS 機能の適用」モジュール
ネットワーク トラフィックのマーキング	「ネットワーク トラフィックのマーキング」モジュール
IPv6 トラフィック ポリシング	『*QoS*：ポリシングおよびシェーピング コンフィギュレーション ガイド』の「IPv6 QoS：MQC トラフィック ポリシング」モジュール。

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2697	『*A Single Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

トラフィック ポリシングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *14*：トラフィック ポリシングの機能情報

機能名	リリース	機能情報
トラフィック ポリシング	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能により、**police**、**show policy-map**、**show policy-map interface** コマンドが導入または変更されました。

第 12 章

ポリシング機能拡張（複数のアクション）

機能の履歴

リリース	変更内容
Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。

このマニュアルでは、ポリシング機能拡張（複数のアクション機能）について説明します。具体的な内容は、次のとおりです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

機能の概要

これは、Cisco IOS XE シングルレート ポリシング機能および 2 つのレートを使用したポリシング機能を拡張する機能です。 トラフィック ポリシングと 2 つのレートを使用したポリシング機能は、インターフェイス上で送受信されるトラフィックの最大レートを制御するトラフィック ポリシング メカニズムです。 これらのトラフィック ポリシング メカニズムは、指定されたレートに準拠、超過、または違反しているとしてパケットにマーク付けします。 パケットがマークされた後、そのマーキングに基づいてパケットで実行するアクションを指定できます。

トラフィック ポリシング機能と 2 つのレートを使用したポリシング機能の両方とも、1 つの準拠アクション、1 つの超過アクション、1 つの違反アクションだけしか指定できません。 新しいポリシング機能拡張（複数のアクション機能）を使用すると、マーク付けされたパケットに対して複数の準拠アクション、超過アクション、違反アクションを実行できます。

複数のアクションを指定するには、**police** コマンドの *action* 引数を使用します。 結果のアクションは次の表のとおりです。

表 *15*：*police* コマンドの *Action* 引数

指定された処理	結果
drop	パケットをドロップします。
set-clp-transmit	ATM セルに ATM セル損失率優先度（CLP）ビットとして 0～1 の値を設定し、パケットを送信します。
set-cos-transmit	サービス クラス（CoS）の値を設定し、パケットを送信します。
set-discard-class-transmit	廃棄クラス値を設定し、パケットを送信します。
set-dscp-transmit *new-dscp*	IP Diffserv コード ポイント（DSCP）の値を設定し、ATM CLP ビットを 1 に設定した状態でパケットを送信します。
set-frde-transmit	フレームリレーフレームにフレームリレー廃棄特性（DE）ビットとして 0～1 の値を設定し、パケットを送信します。

指定された処理	結果
set-mpls-exp-transmit	0～7 のマルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）ビットを設定し、パケットを送信します。
set-mpls-exp-imposition-transmit	0～7 の MPLS EXP ビットをタグ インポジションに設定し、パケットを送信します。
set-prec-transmit *new-prec*	IP Precedence レベルを設定し、パケットを送信します。
set-qos-transmit *new-qos*	Quality of Service（QoS）グループの値を設定し、パケットを送信します。
transmit	パケットを送信します。

利点

この機能を使用する前に、パケットの送信に加えて、パケットに *1* つだけマーキング アクションを指定できます。 必要に応じてパケットに複数のマーキング アクションを指定できるようにして、この機能の柔軟性を高めることができます。 たとえば、パケットが TCP/IP 環境とフレームリレー環境の両方で送信されることがわかっている場合、超過パケットまたは違反パケットの DSCP 値を変更し、フレームリレー廃棄特性（DE）ビットを 0 ～ 1 の値に設定して優先度が低いことを示すことができます。

制約事項

shape (percent) コマンドは、「子」（ネストした）ポリシーマップで使用される場合、Cisco 7500、Cisco 7200、または下位シリーズ ルータでサポートされません。 したがって、これらのルータでネストしたポリシー マップに使用できるように **shape** (percent) コマンドを設定することはできません。

関連機能およびテクノロジー

- 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）
- クラスベース重み付け均等化キューイング（CBWFQ）
- クラスベース パケット マーキング
- トラフィック ポリシング
- 2 レート ポリシング機能

関連資料

- 「MQC を使用した QoS 機能の適用」モジュール
- 「重み付け均等化キューイングの設定」モジュール
- 「ネットワーク トラフィックのマーキング」モジュール
- 「ポリシングとシェーピングの概要」モジュール
- 「トラフィック ポリシング」モジュール
- 「2 つのレートを使用したポリシング機能」モジュール
- 「ポリサー機能拡張：複数アクション」モジュール
- 「Cisco Express Forwarding Overview」モジュール
- 『Cisco IOS Quality of Service Solutions Command Reference』
- 『Cisco IOS Switching Services Command Reference』
- RFC 2697『*A Single Rate Three Color Marker*』
- RFC 2698『*A Two Rate Three Color Marker*』

サポートされている規格の MIB および RFC

標準

なし

MIB

- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CLASS-BASED-QOS-CAPABILITY-MIB

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://tools.cisco.com/ITDIT/MIBS/servlet/index

Cisco MIB Locator で必要な MIB 情報がサポートされていない場合、サポート対象 MIB のリストを取得し、次の URL にある Cisco MIB ページから MIB をダウンロードすることもできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco MIB Locator にアクセスするには、Cisco.com のアカウントが必要です。 アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。 自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。 チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細

がEメールで届きます。資格のあるユーザは、Cisco.comのアカウントを作成できます。次のURLにある指示に従ってください。

http://www.cisco.com/register

RFC

なし

前提条件

- Cisco 7500 シリーズ ルータで、ポリシング機能拡張：複数のアクション機能を使用するには、事前に、インターフェイスで CEF または dCEF を設定しておく必要があります。
- ポリシング機能拡張：複数のアクション機能を設定するには、トラフィック クラスとサービス ポリシーを 1 つずつ作成し、作成したサービス ポリシーを指定のインターフェイスにアタッチする必要があります。

設定作業

複数のポリシング機能アクションの設定

手順の概要

1. Router(config)# **policy-map** *policy-map-name*
2. Router(config-pmap)# **class** *class-default*
3. Router(config-pmap-c)# **police** {**cir** *cir*}[**bc** *conform-burst*]{**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **policy-map** *policy-map-name*	ポリシーマップを作成します。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。
ステップ 2	Router(config-pmap)# **class** *class-default*	サービス ポリシーにデフォルトのトラフィック クラスを指定します。ポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Router(config-pmap-c)# **police** {**cir** *cir*}[**bc** *conform-burst*]{**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]	トラフィック ポリシングを設定し、指定のレートに準拠、超過、または違反としてマーク付けされたパケットに適用する複数のアクションを指定します。 1 つのアクションにつき 1 行を使用して、アクションを指定します。 ポリシーマップ クラス ポリス コンフィギュレーション モードを開始します。

複数のポリシング機能アクション設定の確認

コマンド	目的
Router# **show policy-map interface**	インターフェイスに適用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を表示します。

トラブルシューティングのヒント

- インターフェイス タイプをチェックします。インターフェイスが、このモジュールの2 つのレートを使用したポリシング機能に関する制約事項にサポートされていないインターフェイスとして記載されていないことを確認してください。
- Cisco 7500 シリーズ ルータの入力トラフィック ポリシングでは、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングが、トラフィック ポリシングが設定されるインターフェイスで設定されていることを確認します。
- Cisco 7500 シリーズ ルータの出力トラフィック ポリシングでは、着信トラフィックがシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングであることを確認します。 トラフィック ポリシングは、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディング スイッチングがイネーブルになっていない場合はスイッチング パスで使用できません。

複数のポリシング機能アクションのモニタリングと保守

コマンド	目的
`Router#` **show policy-map**	設定されたすべてのポリシーマップを表示します。
`Router#` **show policy-map** *policy-map-name*	ユーザ指定ポリシー マップを表示します。
`Router#` **show policy-map interface**	インターフェイスに適用されたすべての入力および出力ポリシーの統計情報および設定を表示します。

設定例

2 つのレートを使用したポリシング機能での複数のアクションの例

次に、ポリシーマップ「police」がインターフェイスから発信するトラフィックのポリシングを行うときに 2 つのレートを使用したポリシング機能を使用するように設定する例を示します。 認定情報レート（CIR）と最大情報レート（PIR）の 2 つのレートが、それぞれ 1 Mbps と 2 Mbps に指定されています。

```
Router(config)# policy-map police
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 1000000 pir 2000000

Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action set-prec-transmit 4
Router(config-pmap-c-police)# exceed-action set-frde
Router(config-pmap-c-police)# violate-action set-prec-transmit 2
Router(config-pmap-c-police)# violate-action set-frde-transmit

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

ポリシー マップ「police」に関連付けられたパケットでは、次のアクションが実行されます。

- これらのレートに準拠するとしてマーク付けされたすべてのパケット（CIR に準拠するパケット）は、変更されずに送信されます。
- これらのレートに超過するとしてマーク付けされたすべてのパケット（CIR を超えて PIR は超えないパケット）は、IP Precedence レベルに 4 が割り当てられ、DE ビットが 1 に設定されて送信されます。
- これらのレートに違反するとしてマーク付けされたすべてのパケット（PIR を超えるパケット）は、IP Precedence レベルに 2 が割り当てられ、DE ビットが 1 に設定されて送信されます。

複数のポリシング機能アクションを確認する例

次の出力例は、**show policy-map** コマンドを使用してポリシー マップ「police」の設定を表示する方法を示します。 このサービス ポリシーでは、指定の CIR レートを超過するとしてマーク付けされたパケットに対する複数のアクションが設定されています。 これらのパケットは、IP Precedence レベルに 4 が割り当てられ、DE ビットが 1 に設定されてから、パケットが送信されます。 指定の PIR レートを超過するとしてマーク付けされたパケットに対しても、複数のアクションが設定されています。 これらのパケットは、IP Precedence レベルに 2 が割り当てられ、DE ビットが 1 に設定されてから、パケットが送信されます。

```
Router# show policy-map police
  Policy Map police
    Class class-default
     police cir 1000000 bc 31250 pir 2000000 be 31250
       conform-action transmit
       exceed-action set-prec-transmit 4
       exceed-action set-frde-transmit
       violate-action set-prec-transmit 2
       violate-action set-frde-transmit
```

ポリシング機能拡張（複数のアクション）の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *16*：*QoS for dVTI* の機能情報

機能名	リリース	機能情報
ポリシング機能拡張（複数のアクション）	Cisco IOS XE Release 2.1	ポリシング機能拡張（複数のアクション）は、マーク付けされたパケットに対する複数準拠、超過、違反の各アクションを指定します。

第 13 章

コントロール プレーン ポリシング

コントロール プレーン ポリシング機能により、ユーザは、コントロール プレーン パケットのトラフィック フローを管理する Quality of Service（QoS）フィルタを設定し、偵察行為やサービス拒絶（DoS）攻撃から ルータおよびスイッチのコントロール プレーンを保護できます。 このように、ルータやスイッチに対する攻撃や大量トラフィック負荷があったとしても、コントロール プレーン（CP）を利用してパケット転送とプロトコル ステートを維持することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

コントロール プレーン ポリシングの制約事項

出力レート制限サポート

出力レート制限は、サイレント（パケット廃棄）モードで実行されます。 サイレント モードでは、ルータが、**service-policy output** コマンドで出力コントロールプレーン トラフィックに適用されたポリシーマップに従ってパケットを自動的に廃棄できます。詳細については、「出力レート制限とサイレント モード動作」の項を参照してください。

MQC の制約事項

コントロール プレーン ポリシング機能では、パケット分類、パケット マーキング、およびトラフィック ポリシングを設定するためにモジュラ Qos CLI（MQC）を必要とします。 MQC を使用してトラフィック ポリシングを設定するときに適用されるすべての制約事項が、コントロールプレーン ポリシングの設定時にも適用されます。 ポリシー マップでは、**police** と **set** の 2 つの MQC コマンドだけがサポートされます。

一致基準のサポートおよび制約事項

サポートされる分類（一致）基準は次のとおりです。

- 標準および拡張 IP アクセス コントロール リスト（ACL）。
- クラスマップ コンフィギュレーション モードでは、次のコマンドによって一致基準を指定します。
  - **match dscp**
  - **match ip dscp**
  - **match ip precedence**
  - **match precedence**
  - **match protocol arp**
  - **match protocol ipv6**
  - **match protocol pppoe**

（注） **match protocol pppoe** コマンドは、コントロール プレーンに送信されるすべての PPPoE データ パケットを一致させるものです。

- **match protocol pppoe-discovery**

（注） **match protocol pppoe-discovery** コマンドは、コントロール プレーンに送信されるすべての PPPoE コントロール パケットを一致させるものです。

- **match qos-group**

（注） **match input-interface** コマンドはサポートされていません。

（注） Network-Based Application Recognition（NBAR）分類を必要とする機能は、コントロール プレーン レベルで適切に機能しない場合があります。

コントロール プレーン ポリシングに関する情報

コントロール プレーン ポリシングの利点

Cisco ルータまたはスイッチ上でコントロール プレーン ポリシング機能を設定すると、次の効果が得られます。

- インフラストラクチャのルータおよびスイッチに対する DoS 攻撃からの保護
- Cisco ルータまたはスイッチのコントロールプレーン宛てに送信されるパケットに対する QoS 制御
- コントロール プレーン ポリシーの設定の容易さ
- プラットフォームの信頼性と可用性の向上

理解しておく必要があるコントロール プレーンの用語

Cisco ASR 1000 シリーズ ルータでは、コントロール プレーン ポリシング機能に関して次の用語が使用されます。

- コントロール プレーン：ルート プロセッサ（RP）上でプロセス レベルで稼働するプロセスの集合。 これらのプロセスがまとまって、ほとんどの Cisco IOS XE 機能を高いレベルで制御します。 コントロール プレーンへ送信される、またはコントロール プレーンから送信されるトラフィックを、制御トラフィックと呼びます。
- フォワーディング プレーン：IP パケットの高速フォワーディングを担当するデバイス。 ハードウェアによって実装して、高速パケットフォワーディングを実現できるように、そのロ

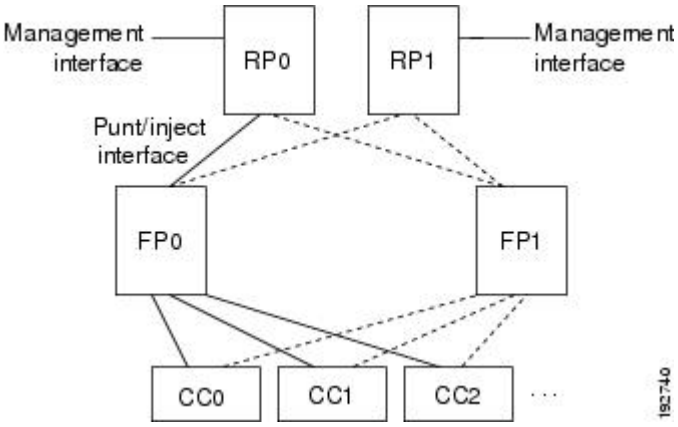
ジックはシンプルに保たれています。 FP によって、複雑な処理を必要とするパケット（IP オプションを持つパケットなど）が、コントロールプレーンの RP にパントされ、処理されます。

コントロール プレーン ポリシングの概要

ルータのコントロール プレーンを DoS 攻撃から保護し、コントロール プレーン間のトラフィックに対する詳細な制御を提供するために、コントロールプレーンポリシング機能では、入出力トラフィックの独自のインターフェイスを持つ別々のエンティティとしてコントロール プレーンを扱います。 このインターフェイスはパント/インジェクト インターフェイスと呼ばれます。パント/インジェクト インターフェイスは、ルータ上の物理インターフェイスと同じです。 パケットは、このインターフェイスを通してフォワーディング プレーンから RP へ（入力方向）パントされ、また、RP からフォワーディング プレーンへ（出力方向）インジェクトされます。 CoPP を実現するために、このインターフェイスに一連の Quality Of Service（QoS）規則を適用することが可能です。

これらの QoS 規則は、パケットの宛先がそのコントロールプレーンであると判定された後またはパケットがそのコントロールプレーンから出て行くときにだけ適用されます。 指定したレート制限に到達した後に不要なパケットがそれ以上進むことがないようにサービス ポリシー（QoS ポリシーマップ）を設定できます。たとえば、システム管理者は、コントロールプレーン宛てのすべての TCP/SYN パケットを 1 メガビット/秒の最大レートに制限できます。

図 *4*：デュアル *RP* とデュアル フォワーディング プレーンを使用した *Cisco ASR 1000* シリーズ ルータの概念図



上の図は、デュアル RP とデュアル フォワーディング プレーンを使用した Cisco ASR 1000 シリーズ ルータの概念図を示します。 いつでも 1 つの RP と 1 つのフォワーディング プレーンだけがアクティブになります。 片方の RP とフォワーディング プレーンはスタンバイ モードになり、キャリア カード（CC）からのトラフィックは受信しません。 コントロール プレーン宛てに送信されるパケットは、キャリアカードを通って入ってきてからアクティブなフォワーディングプレーンを通して出て行き、その後、アクティブな RP へパントされます。 入力 QoS ポリシー マップをコントロールプレーン上で設定すると、パケットがアクティブな RP にパントされる前に、アクティ

ブなフォワーディング プレーンによって QoS アクション（送信、ドロップ、設定アクションなど）が実行されます。これにより、アクティブな RP におけるコントロール プレーンの最適な保護が実現されます。

一方、コントロールプレーンから出て行くパケットはアクティブなフォワーディングプレーンにインジェクトされてから、キャリア カードを通って出て行きます。 出力 QoS ポリシー マップがコントロールプレーン上で設定されていると、RP からインジェクトされたパケットの受信後に、アクティブなフォワーディング プレーンによって QoS アクションが実行されます。 このプロセスにより、重要なリソースが RP に保存されます。

（注） 「コントロール プレーン ポリシングの概要」の項に示すとおり、管理インターフェイスは RP に直接接続されています。そのため、コントロール プレーンに対する、またはコントロール プレーンからの、管理インターフェイスを通るすべてのトラフィックは、フォワーディング プレーンが実行する CoPP 機能の影響を受けません。

ハイアベイラビリティ（HA）モードでは、RP のスイッチオーバーが発生すると、アクティブなフォワーディングプレーンによって、トラフィックが、新しいパント/インジェクトインターフェイスを通って、新しいアクティブな RP に転送されます。 アクティブなフォワーディング プレーンは、新しいアクティブな RP にトラフィックをパントする前に、CoPP 機能を引き続き実行します。フォワーディングプレーンのスイッチオーバーが発生すると、新しいアクティブなフォワーディングプレーンによって、キャリーカードからトラフィックが受信され、トラフィックがアクティブな RP にパントされる前に、CoPP 機能が実行されます。

（注） Cisco ASR 1000 シリーズ ルータでは、フォワーディング プレーン内で従来の制御トラフィックの一部が処理されるので、コントロール プレーンの負荷が軽減されます。 たとえば、IP インターネット制御メッセージ プロトコル（ICMP）エコー要求がこのルータに送信されるのが一例です。 Cisco ASR1000 シリーズ ルータによってこのようなパケットが受信されると、そのパケットは、RP にパントされることなく、フォワーディング プレーン内で直接処理されます。 他の Cisco ルータと整合性を保ち、同じ機能によって、CoPP を使用してこのようなパケットを制御するために、Cisco ASR 1000 シリーズ ルータでは、パケットが RP にパントされなくても、このようなパケットに対する CoPP 機能が拡張されます。 カスタマーが CoPP 機能を使用して、このようなパケットをレート制限したり、マーキングしたりすることも可能です。

出力レート制限とサイレント モード動作

service-policy output *policy-map-name* コマンドを使用してコントロール プレーン トラフィックに出力ポリシングを設定した場合、ルータがパケットを静かに廃棄するように自動的に設定されます。

コントロールプレーンからの出力トラフィックのレート制限（ポリシング）は、サイレントモードで実行されます。 サイレント モードでは、Cisco IOS XE ソフトウェアを稼働しているルータは、いかなるシステム メッセージも送信せずに動作します。 コントロール プレーンから出て行くパケットが出力ポリシングで廃棄されても、エラー メッセージを受け取ることはありません。

コントロール プレーン ポリシングの使用方法

コントロール プレーン サービスの定義

アクティブな RP のパケット レート制御やサイレント パケット廃棄などのコントロール プレーン サービスを定義するには、この作業を実行します。

はじめる前に

コントロール プレーンのコンフィギュレーション モードを開始して既存の QoS ポリシーをコントロールプレーンに付加する前に、MQC でポリシーを作成してコントロールプレーン トラフィック用のクラス マップとポリシー マップを定義しておく必要があります。

（注）
- プラットフォーム固有の制約事項は、あるとしても、サービス ポリシーがコントロール プレーン インターフェイスに適用されるときにチェックされます。
- 出力ポリシングにパフォーマンス上の利点はありません。 単にデバイスから出て行く情報を制御するだけです。

手順の概要

1. **enable**
2. **configure terminal**
3. **control-plane**
4. **service-policy** {**input** | **output** *policy-map-name*}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**control-plane** 例： `Device(config)# control-plane`	（コントロールプレーン サービスを定義するための前提条件である）コントロール プレーン コンフィギュレーション モードを開始します。
ステップ 4	**service-policy** {**input** | **output** *policy-map-name*} 例： `Device(config-cp)# service-policy input control-plane-policy`	QoS サービス ポリシーをコントロールプレーンに付加します。 • **input**：指定したサービス ポリシーをコントロール プレーンで受信されるパケットに適用します。 • **output**：指定したサービス ポリシーをコントロールプレーンから送信されるパケットに適用し、デバイスがパケットを静かに廃棄できるようにします。 • *policy-map-name*：付加されるサービス ポリシー マップ（**policy-map** コマンドで作成）の名前。
ステップ 5	**end** 例： `Device(config-cp)# end`	（任意）特権 EXEC モードに戻ります。

コントロール プレーン サービスの確認

手順の概要

1. **enable**
2. **show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | **output** [*class class-name*]]
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | **output** [*class class-name*]]	コントロール プレーンに関する情報を表示します。

	コマンドまたはアクション	目的
	例： `Device# show policy-map control-plane all`	• **all**：（任意）CP 上で使用されるすべての QoS ポリシーに関するサービス ポリシー情報を表示します。 • **input**：（任意）適用されている入力ポリシーの統計情報を表示します。 • **output**（任意）適用されている出力ポリシーの統計情報を表示します。 • **class** *class-name*：（任意）設定および統計情報を表示するトラフィック クラスの名前を指定します。
ステップ 3	**exit** 例： `Device# exit`	（任意）特権 EXEC モードを終了します。

例

次に、ポリシーマップ TEST がコントロール プレーンに関連付けられている例を示します。 このポリシー マップでは、クラス マップ TEST と一致するトラフィックはポリシングされますが、それ以外のすべてのトラフィック（クラスマップ「class-default」と一致）はそのまま通過することが許可されます。

```
Device# show policy-map control-plane

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
      20 packets, 11280 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 101
      police:
        8000 bps, 1500 limit, 1500 extended limit
        conformed 15 packets, 6210 bytes; action:transmit
        exceeded 5 packets, 5070 bytes; action:drop
        violated 0 packets, 0 bytes; action:drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
      105325 packets, 11415151 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
```

DoS 攻撃を軽減するためのコントロール プレーンの設定

DoS）攻撃を軽減するため、RSVP パケットにコントロール プレーン ポリシング（CoPP）を適用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **permit** *protocol* {**any | host** {*address* | *name*}} {**any | host** {*address* | *name*}}
4. **access-list** *access-list-number* **permit** *protocol* {**tcd | udp**} {**any | host** {*source-addr* | *name*}} **eq** *port number* {**any | host** {*source-addr* | *name*}} **eq** *port number*
5. **class-map** *class-map-name*
6. **match access-group** *access-list-index*
7. **exit**
8. **policy-map** *policy-map-name*
9. **class** *class-map-name*
10. **police rate** *units* **pps**
11. **conform-action** *action*
12. **exit**
13. **exit**
14. **control plane** [**host | transit | cef-exception**]
15. **service-policy** {**input** | **output**} *policy-map-name*
16. **exit**
17. **exit**
18. **show control-plane** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* **permit** *protocol* {**any	host** {*address*	*name*}} {**any	host** {*address*	*name*}} 例： `Device(config)# access-list 140 permit 46 any any`	プロトコルタイプによるフレームのフィルタ用アクセス リストを設定します。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* **permit** *protocol* {**tcd** | **udp**} {**any** | **host** {*source-addr* | *name*}} **eq** *port number* {**any** | **host** {*source-addr* | *name*}} **eq** *port number* 例： `Device(config)# access-list 141 permit udp any eq 1699 any eq 1698`	UDPプロトコルによるフレームのフィルタ用アクセスリストを設定し、特定のポート番号とパケットのみを適合します。
ステップ 5	**class-map** *class-map-name* 例： `Device(config)# class-map match-any MyClassMap`	クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 6	**match access-group** *access-list-index* 例： `Device(config-cmap)# match access-group 140`	アイデンティティ ポリシーに適用するアクセス グループを指定します。 有効な値の範囲は 1～2799 です。
ステップ 7	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**policy-map** *policy-map-name* 例： `Device(config)# policy-map Policy1`	サービス ポリシーを指定し、QoS 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。
ステップ 9	**class** *class-map-name* 例： `Device(config-pmap-)# class MyClassMap`	Qos ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 10	**police rate** *units* **pps** 例： `Device(config-pmap-c)# police rate 10 pps`	指定されたレートでコントロールプレーン宛てのトラフィックをポリシングします。
ステップ 11	**conform-action** *action* 例： `Device(config-pmap-c-police)# conform-action transmit`	（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するアクション指定し、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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(config-pmap-c-police)# exit`	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 モードを終了します。
ステップ 13	**exit** 例： `Device(config-pmap-)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 14	**control plane** [**host** | **transit** | **cef-exception**] 例： `Device(config)# control-plane`	デバイスのコントロールプレーンに関連付けられた属性（サービスポリシーなど）を関連付けるか変更し、コントロール プレーン コンフィギュレーション モードを開始します。
ステップ 15	**service-policy** {**input** | **output**} *policy-map-name* 例： `Device(config-cp)# service-policy input Policy1`	ポリシー マップをコントロール プレーンに適用します。
ステップ 16	**exit** 例： `Device(config-cp)# exit`	コントロール プレーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 17	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 18	**show control-plane** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**} 例： `Device# show control-plane features`	設定されたコントロールプレーン機能を表示します。

コントロール プレーン ポリシングの設定例

例：入力 Telnet トラフィックに対するコントロール プレーン ポリシングの設定

次に、コントロール プレーン上で受信される Telnet トラフィックに集約コントロール プレーン サービス用の QoS ポリシーを適用する例を示します。 送信元アドレスが 10.1.1.1 および 10.1.1.2 の信頼できるホストは Telnet パケットを制約なしでコントロール プレーンに転送します。残りすべての Telnet パケットは指定したレートでポリシングされます。

```
! Allow 10.1.1.1 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

! Allow 10.1.1.2 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet

! Rate-limit all other Telnet traffic.
Device(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Device(config)# class-map telnet-class

Device(config-cmap)# match access-group 140
Device(config-cmap)# exit
Device(config)# policy-map control-plane-in
Device(config-pmap)# class telnet-class
Device(config-pmap-c)# police 80000 conform transmit exceed drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define aggregate control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy input control-plane-in
Device(config-cp)# end
```

例：出力 ICMP トラフィックに対するコントロール プレーン ポリシングの設定

次に、コントロール プレーンから送信される Telnet トラフィックに集約コントロール プレーン サービス用の QoS ポリシーを適用する例を示します。 送信元アドレスが 10.0.0.0 および 10.0.0.1 の信頼できるネットワークは Internet Control Management Protocol（ICMP）ポート到達不能応答を制約なしで受信します。残りすべての ICMP ポート到達不能応答は廃棄されます。

```
! Allow 10.0.0.0 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.0 0.0.0.255 any port-unreachable

! Allow
10.0.0.1
 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.1 0.0.0.255 any port-unreachable

! Rate-limit all other ICMP traffic.
Device(config)# access-list 141 permit icmp any any port-unreachable
Device(config)# class-map icmp-class
```

```
Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map control-plane-out
! Drop all traffic that matches the class "icmp-class."
Device(config-pmap)# class icmp-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
! Define aggregate control plane service for the active route processor.
Device(config-cp)# service-policy output control-plane-out
Device(config-cp)# end
```

例：出力コントロール プレーン パケットのマーキング

次に、コントロール プレーンに QoS ポリシーに適用して、IPv6 precedence 6 を持つすべての出力 IPv6 エコー要求パケットをマーキングする例を示します。

```
! Match all IPv6 Echo Requests
Device(config)# ipv6 access-list coppacl-ipv6-icmp-request
Device(config-ipv6-acl)# permit icmp any any echo-request
Device(config-ipv6-acl)# exit
Device(config)# class-map match-all coppclass-ipv6-icmp-request
Device(config-cmap)# match access-group name coppacl-ipv6-icmp-request
Device(config-cmap)# exit
! Set all egress IPv6 Echo Requests with precedence 6
Device(config)# policy-map copp-policy
Device(config-pmap)# class coppclass-ipv6-icmp-request
Device(config-pmap-c)# set precedence 6
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy output copp-policy
Device(config-cp)# end
```

例：DoS 攻撃を軽減するためのコントロール プレーンの設定

次の例では、指定レートで RSVP パケットをポリシングするためにコントロール プレーン ポリシング（CoPP）を設定する方法を示し、設定された CoPP 機能を表示します。

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list 140 permit 46 any any
Device(config)# access-list 141 permit adp any eq 1699 any eq 1698
Device(config)# class-map match-any MyClassMap
Device(config-cmap)# match access-group 140
Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map Policy1
Device(config-pmap)# class MyClassMap
Device(config-pmap-c)# police rate 10 pps
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
Device(config-cp)# service-policy input Policy1
Device(config-cp)#
*Sep 14 08:07:39.898: %CP-5-FEATURE: Control-plane Policing feature enabled on Control plane
```

```
 aggregate path
Device(config-cp)#
Device(config-c p)# exit
Device(config)# exit
Device#
*Sep 14 08:09:04.154: %SYS-5-CONFIG_I: Configured from console by console
Device# show control-plane features
Total 1 features configured

Control plane aggregate path features :

-------------------------------------------------------
Control-plane Policing activated Sep 14 2012 08:0

-------------------------------------------------------
```

コントロール プレーン ポリシングのその他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『Cisco IOS Quality of Service Solutions Command Reference』
QoS 機能の概要	「Quality of Service の概要」モジュール
MQC	「MQC を使用した QoS 機能の適用」モジュール
セキュリティ機能の概要	「セキュリティの概要」モジュール

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

コントロール プレーン ポリシングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *17*：コントロール プレーン ポリシングの機能情報

機能名	リリース	機能情報
コントロール プレーン ポリシング	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2	コントロール プレーン ポリシング機能により、ユーザは、コントロール プレーン パケットのトラフィック フローを管理する Quality of Service（QoS）フィルタを設定して、偵察行為やサービス拒絶（DoS）攻撃から Cisco IOS ルータおよびスイッチを保護できます。 Cisco IOS XE Release 2.1 では、この機能は、Cisco ASR 1000 シリーズ ルータに実装されています。 Cisco IOS XE Release 2.2 では、この機能は、パケット マーキング、出力レート制限、および追加一致基準のサポートが含まれるように変更されています。 この機能により、**match protocol pppoe**、**match protocol pppoe-discovery** コマンドが導入または変更されています。

第 14 章

クラスベースのポリシング

クラスベース ポリシングでは、インターフェイスでのトラフィックの最大送受信レートを制御できます。クラスベースポリシングは、多くの場合、ネットワークの端のインターフェイスで、ネットワークを出入りするトラフィックを制限するように設定されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

クラスベース ポリシングの概要

クラスベース ポリシング機能

クラスベース ポリシングは、次のように機能します。

- ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限します。
- ATMセル損失率優先度（CLP）ビット、フレームリレー廃棄特性（DE）ビット、IP Precedence値、IP Diffservコードポイント（DSCP）値、MPLS EXP値、Quality of Service（QoS）グループを設定することによりパケットにマーク付けします。

クラスベース ポリシングでは、インターフェイスでのトラフィックの最大送受信レートを制御できます。 クラスベース ポリシング設定を含むトラフィック ポリシーをインターフェイスに適用すると、クラスベース ポリシング機能が適用されます。

クラスベース ポリシング機能は、トークン バケット メカニズムで動作します。 現在、トークン バケット アルゴリズムには、シングル トークン バケット アルゴリズムとツー トークン バケット アルゴリズムの 2 種類があります。 シングル トークン バケット システムは、**violate-action** オプションが指定されていない場合に使用されます。ツートークンバケットシステムは、**violate-action** オプションが指定されている場合に使用されます。

クラスベース ポリシングの利点

レート制限による帯域幅管理

クラスベース ポリシングでは、インターフェイスでのトラフィックの最大送受信レートを制御できます。 クラスベース ポリシングは、多くの場合、ネットワークの端のインターフェイスで、ネットワークを出入りするトラフィックを制限するように設定されます。 ほとんどのクラスベース ポリシング設定では、レートパラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

パケットのマーキング

パケットのマーキングにより、ネットワークを複数のプライオリティ レベルまたはクラス サービス（CoS）に区切ることができます。 パケットがマーキングされ、ダウンストリーム デバイスのトラフィックを識別および分類するためにこれらのマーキングが使用できます。

- クラスベース ポリシングを使用して、ネットワークに入るパケットの IP precedence または DSCP 値を設定します。 その後、ネットワーク内のネットワーキング デバイスは、調整された IP precedence 値を使用してトラフィックの処理方法を決定できます。
- クラスベース ポリシングを使用して、パケットを QoS グループに割り当てます。 ルータは QoS グループを使用して、パケットに優先順位を付ける方法を決定します。

トラフィックには、クラスベース ポリシング機能を使用せずにマークを付けることができます。クラスベースポリシングを使用せずにトラフィックにマークを付ける場合は、「ネットワーク トラフィックのマーキング」モジュールを参照してください。

クラスベース ポリシングに関する制約事項

クラスベース ポリシングは、インターフェイスまたはサブインターフェイスで設定できますが、EtherChannel インターフェイスまたはトンネル インターフェイスではサポートされません。

Cisco ASR 903 ルータに関する制約事項

- 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）はサポートされません。

クラスベース ポリシングの設定方法

トラフィック ポリシング サービス ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match ip precedence** *precedence-value*
5. **exit**
6. **policy-map** *policy-map-name*
7. **class** {*class-name* | **class-default**}
8. **police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action*
9. **exit**
10. **exit**
11. **interface** *interface-type interface-number*
12. **service-policy** {**input** | **output**} *policy-map-name*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Router(config)# class-map match-any MATCH_PREC`	作成するクラス マップの名前を指定し、QoS クラス マップ コンフィギュレーション モードを開始します。 • クラスマップは、トラフィックを差別化するために使用する条件を定義します。たとえば、クラスマップを使用して、**match** コマンドを使用して定義した一連の一致基準に基づき、音声トラフィックをデータ トラフィックから差別化できます。 （注） **match-all** または **match-any** キーワードを指定しない場合、トラフィックがそのトラフィック クラスに分類されるためには、すべての一致基準を満たさなければなりません。
ステップ 4	**match ip precedence** *precedence-value* 例： `Router(config-cmap)# match ip precedence 0`	ユーザが指定する IP precedence 値に基づいて一致するパケットをイネーブルにします。 （注） 数字の省略形（0 ～ 7）または基準名（critical、flash など）で、単一の match 文で最大 4 つの一致基準を入力できます。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map** *policy-map-name* 例： `Router(config)# policy-map POLICE-SETTING`	サービス ポリシーを指定するために 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、QoS 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。

	コマンドまたはアクション	目的
ステップ 7	**class** {*class-name* | **class-default**} 例： `Router(config-pmap)# class MATCH_PREC`	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスとして知られるクラス）を指定し、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。
ステップ 8	**police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action* 例： `Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1 violate-action drop`	指定されたバースト サイズと任意選択アクションに基づいてトラフィック ポリシングを設定します。
ステップ 9	**exit** 例： `Router(config-pmap-c)# exit`	（任意）ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**exit** 例： `Router(config-pmap)# exit`	（任意）QoS ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 11	**interface** *interface-type interface-number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • インターフェイス タイプとインターフェイス番号を入力します。
ステップ 12	**service-policy** {**input** | **output**} *policy-map-name* 例： `Router(config-if)# service-policy input POLICE-SETTING`	ポリシー マップをインターフェイスに付加します。 • **input** キーワードまたは **output** キーワードとポリシーマップ名を入力します。
ステップ 13	**end** 例： `Router(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラフィック ポリシングのモニタリングと保守

はじめる前に

（注）

手順の概要

1. **enable**
2. **show policy-map**
3. **show policy-map** *policy-map-name*
4. **show policy-map interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show policy-map** 例： `Router# show policy-map`	設定されたすべてのポリシー マップを表示します。
ステップ 3	**show policy-map** *policy-map-name* 例： `Router# show policy-map pmap`	ユーザ指定ポリシー マップを表示します。
ステップ 4	**show policy-map interface** 例： `Router# show policy-map interface`	クラスベース ポリシング機能がインターフェイスで設定されていることを確認します。機能がインターフェイスで設定されている場合 • コマンド出力はポリシング統計値を表示します。

クラスベースのトラフィック ポリシングの確認

クラスベース ポリシング機能がインターフェイスで設定されていることを確認するには、**show policy-map interface** コマンドを使用します。 機能がインターフェイスで設定されている場合、**show policy-map interface** コマンド出力はポリシング統計値を示します。

手順の概要

1. **enable**
2. **show policy-map interface**
3. **show policy-map interface** *type interface*
4. **show policy-map interface** *type interface* **service instance** *service-instance number*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show policy-map interface** 例： `Router# show policy-map interface`	クラスベース ポリシング機能がインターフェイスで設定されていることを確認します。 機能がインターフェイスで設定されている場合 • コマンド出力はポリシング統計値を表示します。
ステップ 3	**show policy-map interface** *type interface* 例： `Router# show policy-map interface GigabitEthernet 0/0/1`	特定のインターフェイスに適用されたポリシーの表示トラフィック統計情報を表示します。
ステップ 4	**show policy-map interface** *type interface* **service instance** *service-instance number* 例： `Router# show policy-map interface GigabitEthernet 0/0/1 service instance 1`	ポート チャネル下の特定のサービス インスタンスに関するポリシー マップ情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

例：クラスベースのトラフィック ポリシングの確認

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

トラブルシューティングのヒント

インターフェイス タイプをチェックします。 クラスベース ポリシングがインターフェイスでサポートされていることを確認します。クラスベース ポリシングに関する制約事項, （181 ページ）を参照してください。

クラスベース ポリシングの設定例

トラフィック ポリシングを含むサービス ポリシーの設定例

次の例では、インターフェイスから離れるすべてのパケットについて、クラスベース ポリシングは 8,000 ビット/秒の平均レート、通常バースト サイズは 1000 バイト、超過バースト サイズは 1000 バイトが設定されています。

```
class-map access-match
 match access-group 1
 exit
policy-map police-setting
 class access-match
  police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
  exit
 exit
 service-policy output police-setting
```

FastEthernet インターフェイス 1/1/1 から離れる一連のパケットについての処理は、準拠および超過トークン バケットで残っているパケットのサイズとバイト数によって異なります。 一連のパケットは、次のルールに基づいてポリシングされます。

- 前のパケットが T1 に到達し、現在のパケットが T に到達した場合、バケット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、準拠バケットに置かれます。 トークンが準拠バケットでオーバーフローになると、超過バケットにオーバーフロー 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。

（パケット間の時間（= T - T1）X ポリシング レート）/8 バイト

- 準拠バケットのバイト数がパケット（B など）の長さよりも大きい場合、パケットは準拠しており、バケットからBバイトを削除する必要があります。パケットが準拠している場合、Bバイトが準拠バケットから削除され、準拠処理が実行されます。 このシナリオでは、超過バケットには影響ありません。
- 準拠バケットのバイト数がパケット長よりも小さく、超過バケットのバイト数がパケット（B など）の長さよりも大きい場合、パケットは超過しており、B バイトがバケットから削除されます。
- 超過バケット B のバイト数が 0 未満の場合、パケットはレートに違反しているため、違反処理が実行されます。 パケットに対する処理が完了します。

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 バイトのパケットを受信すると、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、パケットは準拠しています。 パケットにより準拠処理（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）。

次のパケットが 0.25 秒後に到着すると、250 バイトが適合トークン バケットに追加され（（0.25 × 8000）/8）、適合トークン バケットには 800 バイトが残ります。 次のパケットが 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、パケットは準拠していません。

フルの 1000 バイトで始まる超過トークン バケット（超過バースト サイズで指定）に使用可能なバイトがあるかどうかがチェックされます。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、超過処理（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 X 8000)/8）。 これにより、準拠トークン バケットは 1000 バイト（準拠バケットで使用可能な最大トークン数）となり、準拠トークン バケットを 200 バイト オーバーフローします（準拠トークン バケットを容量分まで満たすために必要なのがちょうど 200 バイトであるためです）。 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 X 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。

クラスベースのトラフィック ポリシングの確認

クラスベース ポリシング機能がインターフェイスで設定されていることを確認するには、**show policy-map interface** コマンドを使用します。 機能がインターフェイスで設定されている場合、**show policy-map interface** コマンド出力はポリシング統計値を示します。

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

特定のインターフェイスに適用されているポリシーのトラフィック統計情報を表示するには、**show policy-map interface** *type nummber* コマンドを使用します。

```
Router# show policy-map interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1

  Service-policy input: TUNNEL_MARKING

    Class-map: MATCH_PREC (match-any)
      72417 packets, 25418367 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      QoS Set
        ip precedence tunnel 3
          Marker statistics: Disabled

    Class-map: MATCH_DSCP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp default (0)
      QoS Set
        ip dscp tunnel 3
          Marker statistics: Disabled

    Class-map: class-default (match-any)
      346462 packets, 28014400 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

  Service-policy output: POLICE-SETTING

    Class-map: MATCH_PREC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      police:
          cir 8000 bps, bc 1000 bytes, be 1000 bytes
        conformed 0 packets, 0 bytes; actions:
```

```
        transmit
      exceeded 0 packets, 0 bytes; actions:
        set-qos-transmit 1
      violated 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps, violate 0000 bps

  Class-map: class-default (match-any)
    31 packets, 2019 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
```

特定のインターフェイスに適用されているポリシーのトラフィック統計情報を表示するには、**show policy-map interface service instance** コマンドを使用します。

```
Router# show policy-map interface gigabitethernet 0/0/1 service instance 1
 Service-policy input: p

 Class-map: prec1 (match-all)
   0 packets, 0 bytes
   5 minute offered rate 0000 bps, drop rate 0000 bps
   Match: ip precedence 1
   police:
       cir 10000000 bps, bc 312500 bytes
     conformed 0 packets, 0 bytes; actions:
       transmit
     exceeded 0 packets, 0 bytes; actions:
       drop
     conformed 0000 bps, exceeded 0000 bps

 Class-map: class-default (match-any)
   0 packets, 0 bytes
   5 minute offered rate 0000 bps, drop rate 0000 bps
   Match: any
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
トラフィック マーキング	「ネットワーク トラフィックのマーキング」モジュール
トラフィック ポリシング	「トラフィック ポリシング」モジュール
トラフィック ポリシングとシェーピングの概念と概要	「ポリシングとシェーピングの概要」
モジュラ QoS コマンドライン インターフェイス（MQC）	「MQC を使用した QoS 機能の適用」 モジュール

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
クラスベース *Quality of Service MIB* • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2697	『*A Single Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

クラスベース ポリシングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *18*：クラスベース ポリシングの機能情報

機能名	リリース	機能情報
クラスベースのポリシング	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータ用にサポートが追加されました。 この機能により、**police** コマンドが導入または変更されました。

第 15 章

QoS パーセントベース ポリシング

QoS パーセントベース ポリシング機能を使用すると、インターフェイスで使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 ポリシングおよびトラフィック シェーピングを設定できます。この機能を使用すると、認定バースト（bc）サイズおよび超過バースト（be）サイズ（トラフィック ポリシングの設定に使用）をミリ秒（ms）単位で指定することもできます。この方法でトラフィック ポリシングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

QoS パーセントベース ポリシングの概要

QoS パーセント ベース ポリシングの利点

この機能を使用すると、インターフェイスで使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 ポリシングを設定し、バースト サイズをミリ秒単位で指定できます。 この方法でトラフィック ポリシングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。 つまり、各インターフェイスの帯域幅を再計算したり、インターフェイスのタイプごとに別のポリシー マップを設定したりする必要はありません。

QoS パーセント ベース ポリシング用のクラスおよびポリシー マップの設定

QoS：パーセントベース ポリシング機能を設定するには、トラフィック クラスを定義し、ポリシーマップを設定してから、そのポリシーマップを適切なインターフェイスにアタッチする必要があります。

MQC とは、コマンドライン インターフェイスで、トラフィック クラスの定義、トラフィック ポリシーの作成および設定（ポリシーマップ）、およびトラフィック ポリシーのインターフェイスへのアタッチが行えます。

MQC では、**class-map** コマンドは、トラフィック クラスの定義に使用されます（トラフィック クラスは、その後、トラフィック ポリシーに関連付けされます）。 トラフィック クラスの目的は、トラフィックを分類することです。

MQC は、次の 3 つのプロセスで構成されます。

- **class-map** コマンドを使用したトラフィック クラスの定義
- トラフィック クラスを 1 つまたは複数の QoS 機能と関連付けてトラフィック ポリシーを作成（**policy-map** コマンドを使用）
- **service-policy** コマンドを使用した、トラフィック ポリシーのインターフェイスへのアタッチ

トラフィック クラスには、3 つの主な要素が含まれます。名前、一連の match コマンド、そしてトラフィック クラスに **match** コマンドが複数存在する場合にこれらの **match** コマンド（match-all または match-any）の評価の仕方についての指定です。 トラフィック クラスの名前は、**class-map** コマンド ラインで付けます。たとえば、CLI でトラフィック クラスを設定するときに **class-map cisco** コマンドを入力すると、トラフィック クラスの名前は「cisco」になります。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。 パケットは、**match** コマンドで指定された基準に合っているかどうかを判断するために、チェックされます。 指定された基準に合っていれば、パケットはクラスのメンバーと見なされ、トラフィック ポリシーで設定された QoS 仕様に従って転送されます。 一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

トラフィック規制メカニズムと帯域幅のパーセンテージ

Quality of Service（QoS）では、トラフィック ポリシングとトラフィック シェーピングという 2 種類のトラフィック規制メカニズムが提供されています。トラフィック ポリサーは、通常、特定のレートに違反するトラフィックをドロップします。トラフィック シェーパーは、通常、パケットを保持するバッファを使用して過剰なトラフィックを遅延し、キューに対するデータ レートが予想より高い場合に、フローをシェーピングします。

トラフィック シェーピングとトラフィック ポリシングは連携して機能し、クラス マップで設定できます。 クラス マップは、データ パケットを特定のカテゴリ（「クラス」）に編成します。ポリシー マップ（しばしば「サービス ポリシー」とも呼ばれる）で使用すると、ユーザ定義の QoS 処理を受信できます。

この機能が導入されるまでは、トラフィック ポリシングおよびトラフィック シェーピングはインターフェイスで使用可能な帯域幅のユーザ指定の量に基づいて設定されています。ポリシーマップは、その後で特定の量の帯域幅に基づいて設定されていました。このため、各インターフェイスに別々のポリシー マップが必要とされていました。

この機能を使用すると、インターフェイスで使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 ポリシングおよびトラフィック シェーピングを設定できます。 この方法でトラフィック ポリシングおよびトラフィック シェーピングを設定すると、顧客は帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

帯域幅のパーセンテージに基づいたトラフィック ポリシングおよびトラフィック シェーピングの設定は、**police** (percent) コマンドおよび **shape** (percent) コマンドを使用して実行されます。

ミリ秒オプションのバースト サイズ

バースト パラメータ（bc および be）の目的は、パケットを徐々にドロップして、テール ドロップを防ぐことです。 十分に高いバースト値を設定すると、適切なスループットを確実に実現できます。

この機能を使用すると、トラフィック ポリシングを設定する際、認定バースト（bc）サイズおよび超過バースト（be）サイズをクラス帯域幅のミリ秒（ms）単位で指定することができます。 ミリ秒の値は、QoS：パーセントベース ポリシング機能が使用するバイト数を計算するために使用されます。

ミリ秒単位でこれらのバースト サイズを指定する場合、**police** (percent) コマンドと **shape** (percent) コマンドの **bc** キーワードと **be** キーワード（および関連付けられている引数）を使用して実行します。

QoS パーセントベース ポリシングの設定方法

パーセントベース ポリシング用のクラスおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {*class-name* **class-default**}
5. **police cir percent** *percentage* [*burst-in-ms*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percent*]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map** *policy-name* 例： `Router(config)# policy-map policy1`	作成するポリシー マップの名前を指定します。 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。 • ポリシー マップ名を入力します。
ステップ 4	**class** {*class-name* **class-default**} 例： `Router(config-pmap)# class class1`	ポリシーを設定または変更できるようにクラスを指定します。 ポリシーマップ クラス コンフィギュレーション モードを開始します。 • クラス名を入力するか、デフォルト クラス（class-default）を指定します。

	コマンドまたはアクション	目的
ステップ 5	**police cir percent** *percentage* [*burst-in-ms*] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percent*] 例： `Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40`	指定された帯域幅のパーセンテージとオプションのバースト サイズに基づいて、トラフィック ポリシングを設定します。 ポリシー マップ クラス ポリス コンフィギュレーション モードを開始します。 • 帯域幅のパーセンテージとオプションのバースト サイズを入力します。
ステップ 6	**exit** 例： `Router(config-pmap-c-police)# exit`	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 モードを終了します。

パーセントベースポリシング用のインターフェイスへのポリシーマップのアタッチ

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**]
5. **service-policy** {**input**| **output**} *policy-map-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**interface** *type number*
	
	例：
	`Router(config)#`
	`interface serial4/0/0`
		インターフェイス（サブインターフェイス）タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
		• インターフェイスのタイプ番号を入力します。
		
		（注） ネットワークのニーズにより、ポリシー マップをサブインターフェイス、ATM PVC、フレームリレー DLCI、または他のタイプのインターフェイスにアタッチする必要がある場合もあります。

ステップ 4	**pvc** [*name*] *vpi* / *vci* [**ilmi** | **qsaal** | **smds**] 例： `Router(config-if)# pvc cisco 0/16 ilmi`	（任意）ATM PVC に名前を作成するか割り当て、ATM PVC でカプセル化タイプを指定します。 ATM VC コンフィギュレーション モードを開始します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。 ATM PVC にポリシー マップをアタッチしない場合は、この手順をスキップして、パーセントベース ポリシング用のインターフェイスへのポリシーマップのアタッチに進みます。

ステップ 5	**service-policy** {**input**| **output**} *policy-map-name*
	
	例：
	`Router(config-if)#`
	`service-policy input policy1`
	
	例：
		インターフェイスの入力または出力方向にアタッチするポリシー マップの名前を指定します。
		
		（注） ポリシーマップは、入力または出力ルータで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。 ポリシー マップを適用する方向（入力または出力）とルータ（入力または出力）は、ネットワーク構成に従って変わります。 **service-policy** コマンドを使用してポリシーマップをインターフェイスに適用する場合、ネットワーク構成に適したルータおよびインターフェイスの方向を選択してください。
		
		• ポリシー マップ名を入力します。

ステップ 6	**end** 例： `Router(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了します。

パーセントベース ポリシングの設定確認

手順の概要

1. **enable**
2. **show class-map** [*class-map-name*]
3.
4. **show policy-map interface** *interface-name*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show class-map** [*class-map-name*] 例： `Router# show class-map class1`	一致基準を含めて、クラス マップに関するすべての情報が表示されます。 • クラス マップ名を入力します。
ステップ 3		

ステップ 4	**show policy-map interface** *interface-name*
	例：
	`Router#`
	`show policy-map interface`
	`serial4/0/0`
		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。
		• インターフェイス名を入力します。

ステップ 5	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

パーセントベース ポリシングのトラブルシューティングのヒント

パーセントベース ポリシングの設定確認, （199 ページ）に示すコマンドを使用すると、意図した設定を実現し、機能が正しく働いていることを確認できます。 上記の **show** コマンドの使用後に、設定が正しくない、または機能が予想どおりに働いていないと判明した場合は、次の操作を実行します。

意図したとおりに設定が行われていない場合は、次の手順を完了します。

1. **show running-config** コマンドを使用して、コマンドの出力を分析します。
2. ポリシー マップが **show running-config** コマンドの出力に表示されない場合は、**logging console** コマンドをイネーブルにします。
3. ポリシー マップをインターフェイスに再度アタッチします。

パケットが正確に一致していない場合は（たとえば、パケット カウンタが正しく増加していないなど）、次の手順を完了します。

1. **show policy-map** コマンドを実行して、コマンドの出力を分析します。
2. **show running-config** コマンドを実行して、コマンドの出力を分析します。
3. ポリシーマップがインターフェイスに接続され、認定情報速度（CIR）をインターフェイス帯域幅の割合に基づいて計算されたことを確認するには、**show policy-map interface** コマンドを使用します。

QoS パーセントベース ポリシングの設定例

帯域幅のパーセンテージに基づいたトラフィックポリシングを指定する例

次に、CIR および最大情報レート（PIR）を使用して、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)# end
```

ポリシーマップとクラスマップの設定後、ポリシーマップは次の例に示すように、インターフェイスにアタッチされます。

```
Router> enable
Router# configure terminal
```

```
Router(config-if)#

interface serial4/0/0
Router(config-if)#

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

パーセントベース ポリシングを確認する例

ここでは、**show policy-map interface** コマンドおよび **show policy-map** コマンドの出力例を示します。 これらのコマンドの出力は、ネットワーク上の機能設定の確認およびモニタに使用できます。

次は、**show policy-map** コマンドの出力例です。 このサンプル出力には、「policy1」というポリシー マップの内容が表示されています。policy 1 では、20 % の CIR に基づくトラフィック ポリシングが設定され、bc および be はミリ秒単位で指定されています。 トラフィック ポリシング設定の一部として、オプションの一致（conform）、超過（exceed）、および違反（violate）アクションが指定されています。

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
       conform-action transmit
       exceed-action drop
       violate-action drop
```

次は、**show policy-map interface** コマンドのサンプル出力です。 このサンプルには、トラフィック ポリシングがイネーブルにされている、シリアル 2/0 インターフェイスの統計情報が表示されています。 認定バースト（bc）、および超過バースト（be）がミリ秒（ms）で指定されます。

```
Router# show policy-map interface serial2/0
 Serial2/0/0
  Service-policy output: policy1 (1050)
    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
          pir 819000 bps, be 40960 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
    Class-map: class-default (match-any) (1054/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1055)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

この例では、CIR および PIR は、bps で表示され、認定バースト（bc）、および超過バースト（be）の両方が、バイトで表示されます。

CIR、PIR、bc、および be は、以下に説明する式に基づいて計算されます。

CIR 計算用の式

CIR を計算する場合は、次の式を使用します。

指定された CIR パーセンテージ（**show policy-map** コマンドの出力に示すとおり）X インターフェイスの帯域幅（BW）（ **show interfaces** コマンドの出力に示すとおり）= 合計ビット/秒単位

シリアル インターフェイス 2/0 上で、帯域幅（BW）は 2048 kbps になります。 インターフェイスの帯域幅を確認するには、**show interfaces** コマンドを使用します。 次に例を示します。

```
Router# show interfaces serial2/0/0
Serial2/0/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

次の値が CI の計算に使用されます。

20 % X 2048 kbps = 409600 bps

PIR 計算用の式

PIR を計算する場合は、次の式を使用します。

指定された PIR パーセンテージ（**show policy-map** コマンドの出力に示すとおり）X インターフェイスの帯域幅（BW）（ **show interfaces** コマンドの出力に示すとおり）= 合計ビット/秒単位

シリアル インターフェイス 2/0/0 上で、帯域幅（BW）は 2048 kbps になります。 インターフェイスの帯域幅を確認するには、**show interfaces** コマンドを使用します。 次に例を示します。

```
Router# show interfaces serial2/0
Serial2/0/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

次の値が PIR の計算に使用されます。

40 % X 2048 kbps = 819200 bps

（注） この合計と **show policy-map interface** コマンドの出力に示される合計との不一致の原因は、丸め計算、または特定のインターフェイス設定に関連する相違である可能性があります。

認定バースト（bc）計算用の式

bc を計算する場合は、次の式を使用します。

ミリ秒単位の bc（**show policy-map** コマンドに示すとおり）X ビット/秒単位の CIR = 合計バイト数

次の値が bc の計算に使用されます。

(300 ms X 409600 bps) / 8 = 15360 バイト

超過バースト（be）計算用の式

bc および be を計算する場合は、次の式を使用します。

ミリ秒単位の be（**show policy-map** コマンドに示すとおり）X ビット/秒単位の PIR = 合計バイト数

次の値が be の計算に使用されます。

400 ms X 819200 bps = 40960 バイト

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）。ポリシーマップのアタッチに関する情報を含む	「MQC を使用した QoS 機能の適用」モジュール
トラフィック シェーピングおよびトラフィック ポリシング	「ポリシングとシェーピングの概要」モジュール

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

QoS パーセントベース ポリシングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *19*：*QoS*：パーセントベース ポリシングの機能情報

機能名	リリース	機能情報
QoS：パーセントベース ポリシング	Cisco IOS XE Release 2.1	QoS：パーセントベース ポリシング機能を使用すると、インターフェイスで使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 ポリシングおよびトラフィック シェーピングを設定できます。 この機能を使用すると、認定バースト（bc）サイズおよび超過バースト（be）サイズ（トラフィック ポリシングの設定に使用）をミリ秒（ms）単位で指定することもできます。 この方法でトラフィック ポリシングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシーマップを使用できます。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 この機能により、**police (percent)**、**shape (percent)**、**show policy-map**、**show policy-map interface** コマンドが導入または変更されました。

第 16 章

2 つのレートを使用したポリシング機能

このモジュールでは、2 つのレートを使用したポリシング機能と、この機能の設定方法について説明します。

2 つのレートを使用したポリシング機能の履歴

リリース	変更内容
Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。

Cisco IOS XE ソフトウェア イメージのサポート情報の検索

プラットフォームのサポートおよび Cisco IOS XE ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、バグ検索ツールとプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

機能の概要

ATM スイッチがユーザ ネットワーク（UNI）インターフェイスのネットワーク側に設定されている場合、仮想接続の（ネットワーク内への）転送方向でセルフローをポリシングします。これらのトラフィック ポリシング メカニズムは、使用パラメータ制御（UPC）として知られています。スイッチは、受信したセルがネゴシエートされたトラフィック管理値に準拠しているかどうかを UPC によって判別し、違反セルについて次のアクションのいずれか 1 つを実行します。

- セル ヘッダー内のセル損失率優先度（CLP）ビットを変更せずにセルを渡します。
- CLP ビット値 1 でセルにタグ付けします。
- セルをドロップ（破棄）します。

SVC/SoftPVC 機能を使用すると、サービス カテゴリ、ソフト VC の宛先の終端での相手先選択接続（SVC）または終端VCに基づいて、ポリシングするトラフィックを指定することができます。

利点

レート制限による帯域幅管理

トラフィック ポリシングでは、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。トラフィック ポリシングは、多くの場合、ネットワークの端のインターフェイスで、ネットワークを出入りするトラフィックを制限するように設定されます。 ほとんどのトラフィック ポリシング設定では、レートパラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

パケットのマーキング

パケットのマーキングにより、ネットワークを複数のプライオリティ レベルまたはクラスサービス（CoS）に区切ることができます。 パケットがマーキングされ、ダウンストリーム デバイスのトラフィックを識別および分類するためにこれらのマーキングが使用できます。 ATM セル損失

率優先度（CLP）マーキングやフレームリレー廃棄特性（DE）マーキングなどでは、マーキングがトラフィックの分類に使用されます。

- トラフィック ポリシングを使用して、ネットワークに入るパケットの IP precedence または DSCP 値を設定します。 その後、ネットワーク内のネットワーキング デバイスは、調整された IP precedence 値を使用してトラフィックの処理方法を決定できます。 たとえば、重み付けランダム早期検出（WRE）機能では、IP precedence 値を使用して、パケットがドロップされる確率を決定します。
- トラフィック ポリシングを使用して、パケットを QoS グループに割り当てます。 ルータは QoS グループを使用して、ルータ内のパケットに優先順位を付ける方法を決定します。

トラフィックには、トラフィック ポリシング機能を使用せずにマークを付けることができます。 トラフィック ポリシングを使用せずにトラフィックにマークを付ける場合は、「ネットワーク トラフィックのマーキング」モジュールを参照してください。

フレームリレー フレームのパケットの優先順位付け

トラフィック ポリシング機能では、フレームリレー フレームのフレームリレー DE ビットにマーク付けできます。 フレームリレー DE ビットは 1 ビットで、0 または 1 に設定できます。 輻輳環境では、DE ビットが 1 に設定されたフレームは、DE ビットが 0 に設定されたフレームの前に破棄されます。

ATM セルのパケットの優先順位付け

トラフィック ポリシング機能では、ATM セルの ATM CLP にマーク付けできます。 ATM CLP ビットは、ATM ネットワークのパケットに優先順位を付けるために使用されます。 これにより ATM CLP ビットは 1 ビットで、0 または 1 に設定できます。 輻輳環境では、ATM CLP ビットが 1 に設定されたセルは、ATM CLP ビットが 0 に設定されたセルの前に破棄されます。

2 つのレートを使用したポリシング機能に関する制約事項

2 つのレートを使用したポリシング機能には、次のような制約事項が適用されます。

- 2 つのレートを使用したポリシング機能アクションを設定できるのは、インターフェイス、サブインターフェイス、フレームリレー データリンク接続識別子（DLCI）、ATM 相手先固定接続（PVC）だけです。
- 2 つのレートを使用したポリシング機能は EtherChannel インターフェイスまたはトンネル インターフェイスではサポートされません。

2 つのレートを使用したトラフィック ポリシング機能に関する制約事項

2 つのレートを使用したトラフィック ポリシング機能を設定するには、トラフィック クラスとサービス ポリシーを 1 つずつ作成し、作成したサービス ポリシーを指定のインターフェイスにアタッチする必要があります。

設定作業

2 つのレートを使用したポリシング機能の設定作業については、次の項を参照してください。

2 つのレートを使用したポリシング機能の設定

コマンド	目的
Router(config-pmap-c)# **police cir** cir [**bc***conform-burst*] **pir** *pir* [**be***peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]	2 つのレートを使用したトラフィック ポリシング機能に CIR と PIR の両方が使用されるように指定し、特定のレートに対して準拠、超過、違反のいずれかとしてマーキングされたパケットに適用される複数のアクションを指定します。1 つのアクションにつき 1 行を使用して、アクションを指定します。 ポリシー マップ クラス ポリス コンフィギュレーション モードを開始します。 **bc** キーワードと **be** キーワード、およびその関連する引数（それぞれ、*conform-burst* と *peak-burst*）の指定は任意です。

2 つのレートを使用したポリシング機能の設定は必須ではありませんが、**police** コマンドの構文を使用して、*action* 引数をイネーブルにしたときにパケットに対して実行するアクションを指定できます。 キーワードの選択に対応する結果アクションは表 1 に示されます。

表 *20*：*police* コマンド アクション キーワード

キーワード	結果のアクション
drop	パケットをドロップします。

キーワード	結果のアクション
set-clp-transmit	ATM セルに ATM セル損失率優先度（CLP）ビットとして 0 ～ 1 の値を設定し、ATM CLP ビットを 1 に設定してパケットを送信します。
set-dscp-transmit *new-dscp*	IP DSCP 値を設定して、その新しい IP DSCP 値でパケットを送信します。
set-frde-transmit	フレームリレーフレームにフレームリレー廃棄特性（DE）ビットとして 0 ～ 1 の値を設定し、DE ビットを 1 に設定してパケットを送信します。
set-mpls-exp-transmit	0～7 の MPLS EXP ビットを設定し、新しい MPLS EXP ビット値設定を持つパケットを送信します。
set-prec-transmit *new-prec*	IP precedence を設定して、新しい IP precedence 値設定を持つパケットを送信します。
set-qos-transmit *new-qos*	QoS グループ値を設定し、新しい QoS グループ値設定を持つパケットを送信します。
transmit	パケットをそのまま送信します。

2 つのレートを使用したポリシング機能の設定の確認

コマンド	目的
`Router#` **show policy-map interface**	インターフェイスに適用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を表示します。

トラブルシューティングのヒント

2 つのレートを使用したポリシング機能のモニタリングおよびメンテナンス

コマンド	目的
Router# **show policy-map**	設定されたすべてのポリシーマップを表示します。
Router# **show policy-map** *policy-map-name*	ユーザ指定ポリシー マップを表示します。
Router# **show policy-map interface**	インターフェイスに適用されたすべての入力および出力ポリシーの統計情報および設定を表示します。

設定例

ポリサー クラスを使用してトラフィックを制限する例

この例では、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 つのレートを使用したポリシング機能がクラスに設定されます。

```
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)# interface serial3/0/0
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 を超過するすべてのトラフィックは、ドロップされます。 バースト パラメータは 10,000 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 *policer* クラスに送信（「提供」）される例を示します。

```
Router# show policy-map interface serial3/0/0
 Serial3/0/0
  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 つのレートを使用したポリシング機能により、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。 適合とマーク付けされているパケットはそのまま送信され、超過とマーク付けされているパケットは、IP precedence 2 とマーク付けされて送信されます。 指定されたレートに違反するとマーク付けされているパケットはドロップされます。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
QoS コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
トークン バケット メカニズム	「ポリシングとシェーピングの概要」モジュール
MQC	「MQC を使用した QoS 機能の適用」モジュール
トラフィック マーキングやトラフィック ポリシングなどの QoS 機能	• 「ネットワーク トラフィックのマーキング」モジュール • 「トラフィック ポリシング」モジュール

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

2 つのレートを使用したポリシング機能の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *21*：*2* つのレートを使用したポリシング機能の機能情報

機能名	リリース	機能情報
2 つのレートを使用したポリシング機能	12.2(4)T 12.2(4)T3 12.0(26)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0 SG	この機能が導入されました。 Cisco 7500 シリーズ ルータのサポートが追加されました。 この機能は、Cisco 7200 および 7500 シリーズ ルータの Cisco IOS Release 12.0(26)S に搭載されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH に統合されました。 この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。 この機能は、Cisco IOS XE 3.1.0 SG に統合されました。