QoS の設定

QoS の設定

このマニュアルでは、Cisco IE-3X00 および ESS3300 スイッチプラットフォーム上で、モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）コマンドを使用して Quality of Service（QoS）を設定する方法について説明します。QoS を使用すると、特定のトラフィックを他のトラフィックタイプよりも優先的に処理できます。QoS が設定されていない場合、パケットの内容やサイズに関係なく、各パケットにベストエフォート型サービスが提供されます。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。MQC では、特定のトラフィックストリームの優先順位付けまたは制限を行うための総合的な階層型設定のフレームワークを提供します。

モジュラ QoS CLI

MQC により、ユーザはトラフィック ポリシーを作成し、それらをインターフェイスに適用できます。1 つのトラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の QoS 機能が含まれます。トラフィックの分類には、トラフィック クラスを使用します。また、トラフィック ポリシーの QoS 機能により、分類されたトラフィックの処理方法を決定します。

MQC を設定する手順は、次のとおりです。

手順 1：**トラフィック クラスを定義します。**

class-map [match-all | match-any] class-map-name グローバル コンフィギュレーション コマンドを使用して、トラフィッククラスを定義し、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。トラフィッククラスは、名前、設定済み match コマンドの評価方法の指示（クラスマップで複数の match コマンドが設定されている場合）、および一連の match コマンドの 3 つの要素で構成されます。

- class-map コマンドラインで、トラフィッククラスの名前を指定し、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。

- class-map match-any または class-map match-all を入力することにより、次の match コマンドを評価するためのキーワードを任意で指定できます。match-any を指定した場合、評価されるトラフィックは指定の基準のいずれか 1 つに一致する必要があります。match-all を指定した場合、評価されるトラフィックは指定の基準のすべてに一致する必要があります。match-all クラスマップには、1 つの match 文しか含めることができませんが、match-any クラスマップには複数の match 文を含めることができます。

match-all または match-any を入力しない場合、デフォルトは match-all になります。

- パケット分類のための基準を指定するには、match クラスマップ コンフィギュレーション コマンドを使用します。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。

手順 2：**トラフィック ポリシーを作成し、1 つまたは複数の QoS 機能にトラフィック クラスを関連付けます。**

policy-map policy-map-name グローバル コンフィギュレーション コマンドを使用して、トラフィックポリシーを作成し、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。トラフィック ポリシーでは、QoS 機能を定義して、指定されたトラフィック クラスに関連付けます。トラフィックポリシーは、名前、トラフィッククラス（class ポリシーマップ コンフィギュレーション コマンドにより指定される）、およびそのクラスで設定された QoS ポリシーの 3 つの要素で構成されます。

- policy-map コマンドラインで、トラフィックポリシーの名前を指定し、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。
- ポリシーマップ コンフィギュレーション モードで、指定のポリシーに対するトラフィックの分類で使用されるトラフィック クラス名を入力して、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。
- ポリシーマップ クラス コンフィギュレーション モードで、QoS 機能を開始すると、分類されたトラフィックに適用できます。たとえば、入力ポリシーマップに、set、police、または police aggregate コマンドを使用したり、出力ポリシーマップに、bandwidth、priority、queue-limit、または shape average コマンドを使用できます。

（注） パケットは、トラフィック ポリシー内のいずれかのトラフィック クラスだけに一致します。パケットがトラフィック ポリシー内の複数のトラフィック クラスに一致する場合、ポリシーで定義された最初のトラフィック クラスが使用されます。パケットに複数の一致基準を設定するには、単一のトラフィック ポリシーに複数のトラフィック クラスを関連付けます。

手順 3：**インターフェイスにトラフィック ポリシーを付加します。**

service-policy インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスで送受信されるパケット用にポリシーマップをインターフェイスに付加できます。トラフィック ポリシーの特性を着信または発信パケットに適用するかどうかを指定する必要があり

ます。たとえば、service-policy output class1 インターフェイス コンフィギュレーション コマンドを入力すると、class1 という名前のトラフィックポリシーのすべての特性が、指定されたインターフェイスに付加されます。指定されたインターフェイスから発信されるすべてのパケットは、class1 という名前のトラフィックポリシーで指定された基準に従って評価されます。

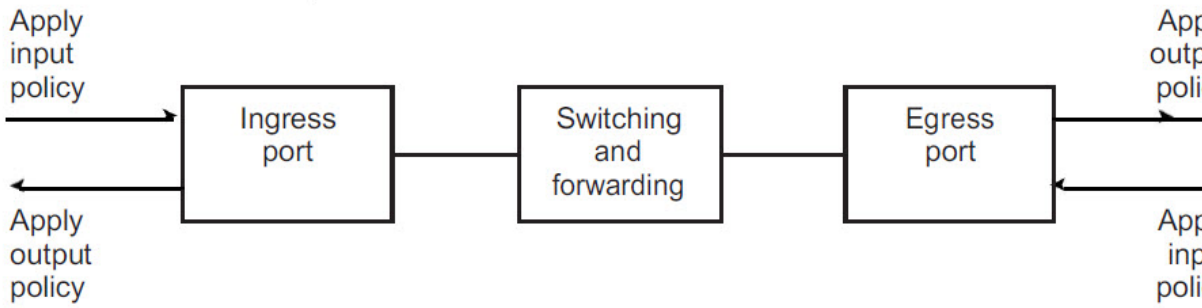
（注） インターフェイスに付加されたポリシーマップを削除するために、no policy-map コンフィギュレーション コマンドまたは no policy-map policy-map-name グローバル コンフィギュレーション コマンドを入力すると、ポリシーマップが分離されて削除されます。

入力ポリシーおよび出力ポリシー

ポリシーマップは、入力ポリシーマップまたは出力ポリシーマップのいずれかになり、スイッチでパケットが送受信される際に、インターフェイスに適用されたサービス ポリシーによって付加されます。入力ポリシーマップは、受信されたトラフィック上でポリシングおよびマーキングを実行します。ポリシングされたパケットが最大許容レートを超過している場合、廃棄されるか、またはプライオリティが低くなります（マーク ダウン）。出力ポリシー マップは、スイッチから発信されるトラフィック上でスケジューリングおよびキューイングを実行します。

入力ポリシーと出力ポリシーは、基本構造は同じですが規制する特性が異なります。最大 200 のポリシー マップを定義できます。

図 *1*：入力ポリシーおよび出力ポリシーの関係



入力ポリシー マップ

入力ポリシーマップの分類基準には、CoS、DSCP、またはアクセスコントロールリスト（ACL）の照合が含まれます。入力ポリシーマップでは、次のいずれかのアクションを実行できます。

- CoS、DSCP の設定またはマーキング
- ポリシング

クラスの class-default は、ポリシーマップで他のいずれのクラスとも明示的に一致しない任意のトラフィックに対して、ポリシーマップで使用されます。入力ポリシーマップでは、

bandwidth、queue-limit、priority、および shape average などのキューイングおよびスケジューリングキーワードはサポートされていません。

入力ポリシーマップの最大クラス数は 11 + class-default です。入力ポリシーには、最大 11 のクラスを設定できます。

出力ポリシー マップ

出力ポリシー マップの分類基準には、CoS または DSCP の照合が含まれます。出力ポリシーマップでは、次のいずれかのアクションを実行できます。

- キューイング（queue-limit）
- スケジューリング（bandwidth、priority、shape average）

出力ポリシー マップでは、アクセス グループのマッチングをサポートしません。

出力ポリシーは、マーキングまたはポリシングをサポートしません（ポリシングのあるプライオリティの場合は除く）。スイッチ上では、出力パケットのマーキングは実行されません（出力ポリシーには set コマンドが含まれません）。

クラスの *class-default* は、ポリシーマップで他のいずれのクラスとも明示的に一致しない任意のトラフィックに対して、ポリシーマップで使用されます。出力ポートには最大 8 つのキューがあるため、出力ポリシーマップには最大 8 つのクラスを設定できます（class-defalt を含む）。

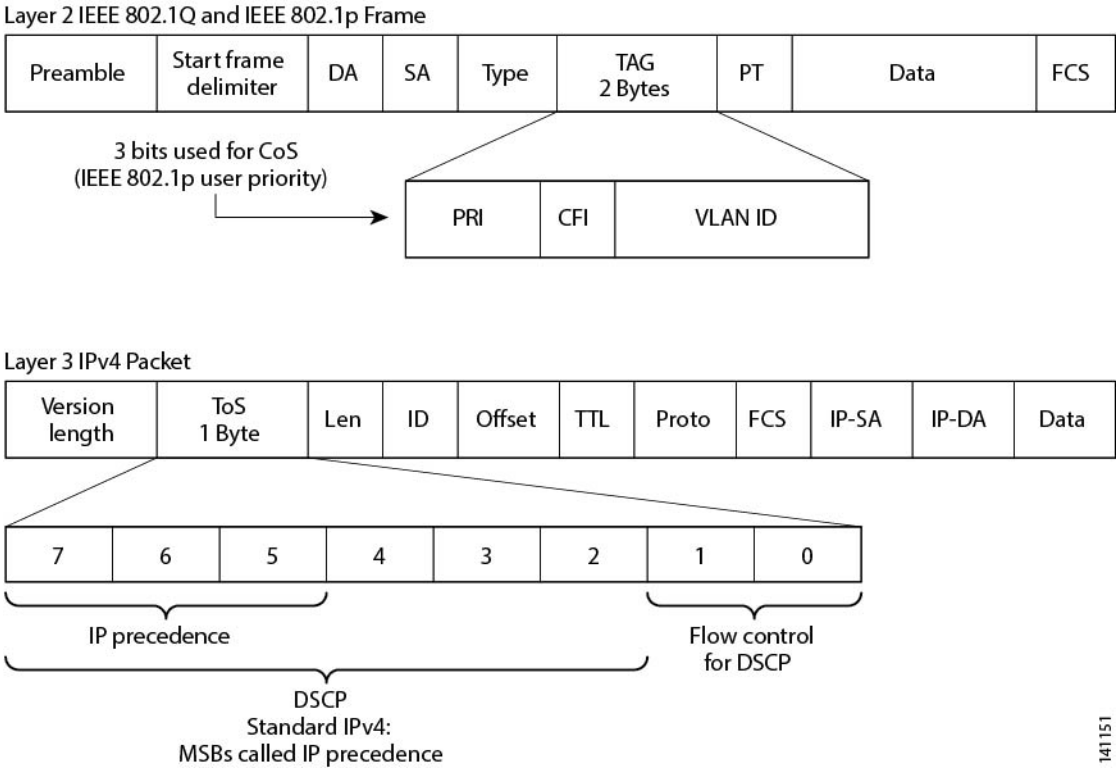
スイッチ上の任意のポートまたはすべてのポートに、出力ポリシーマップを付加できます。スイッチは各ポートに固有の出力ポリシーマップの設定および付加をサポートしています。ただし、これらの出力ポリシー マップには、それぞれ固有のキュー制限を 3 つしか設定できません。これら 3 つの固有のキュー制限設定は、スイッチ上にあるポート数に応じた数の出力ポリシーマップに含まれます。帯域幅、プライオリティ、またはシェーピングの設定には制限はありません。

分類

分類では、パケットヘッダーのフィールドを検査して、トラフィックの種類を区別します。スイッチはパケットを受信すると、ヘッダーを検査して、すべての主要なパケットフィールドを識別します。パケットは、ACL、DSCP、または CoS に基づいて分類できます。

- レイヤ 2 の IEEE 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN（仮想 LAN）のトラフィックを除き、すべてのトラフィックが 802.1Q フレームに収められます。レイヤ 2 802.1Q フレームヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット（ユーザプライオリティビット）で CoS 値を、下位 12 ビットで VLAN ID 値を伝達します。他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。
- レイヤ 2 CoS 値の範囲は 0 ～ 7 です。
- IPv4 パケットと IPv6 パケットの両方が DSCP 値を伝送できます。QoS では、DSCP 値のみを使用できます。
- IPv6 パケットを分類するには、DSCP で match を使用します。

図 *2:* フレームおよびパケットにおける *QoS* 分類レイヤ



ここでは、分類に関するその他の情報について説明します。

クラス マップ （5 ページ）

match コマンド （6 ページ）

レイヤ 2 CoS に基づく分類 （10 ページ）

IP DSCP に基づく分類 （6 ページ）

分類の比較 （7 ページ）

QoS ACL に基づく分類 （9 ページ）

クラス マップ

前述のとおり、MQC クラスマップを使用して、特定のトラフィック フロー（またはクラス）に名前を付けて、他のすべてのトラフィックと区別します。クラス マップでは、特定のトラフィック フローとの比較を行い、さらにそれを分類するために使用する基準を定義します。複数のトラフィック タイプを分類する場合は、別のクラス マップを作成し、異なる名前を使用できます。クラスマップ名を指定して class-map コマンドを入力すると、クラスマップ コンフィギュレーション モードが開始されます。このモードで、match クラスマップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。パケットはクラスマップ基準に照合されてから、ポリシー マップで指定された関連アクションが実行されます。

分類では、複数の基準に照合できます。class map match-any class-map name グローバル コンフィギュレーション コマンドを使用すると、リストされた基準のいずれかを使用する分類を定義できます。

（注） match-all または match-any を入力しない場合、デフォルトは match-all になります。match-all クラス マップでは、複数の分類基準（match 文）を設定できません。一致条件を含まないクラスマップは、デフォルトで match-all となります。

match コマンド

パケットの分類に使用される内容の種類を設定するには、match クラスマップ コンフィギュレーション コマンドを使用して、分類基準を指定します。設定された基準に一致するパケットは、特定のクラスに属し、指定されたポリシーに従って転送されます。たとえば、CoS 値および IP DSCP 値で match class-map コマンドを使用できます。これらの値は、パケット上でマーキングと呼ばれます。アクセスグループを照合することもできます。

- 入力ポリシーマップでは、ポリシーマップとクラスマップを混在させて、同じポリシーマップ内で IP パケットと非 IP パケットを分類することはできません。
- 出力ポリシーマップでは、2 つのクラスマップに同じ一致基準を設定できません。たとえば、2 つの異なるクラスマップで同じ DSCP 値に一致するクラスを定義することはできません。

次に、クラスマップ example を作成して、リストされた基準のいずれかに一致するクラスを定義する例を示します。この例では、DSCP 値 が 32 または 40 のパケットが受信された場合、このパケットはクラス マップにより識別（分類）されます。

```
Switch(config)# class-map match-any example
Switch(config-cmap)# match ip dscp 32
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit
```

IP DSCP に基づく分類

IP DSCP 値に基づいて IPv4 トラフィックを分類し、match ip dscp クラスマップ コンフィギュレーション コマンドを入力する場合、次のいくつかの分類オプションがあります。

- 特定の DSCP 値（0 ～ 63）の入力
- IP precedence 値および DSCP 値 0 に対応するデフォルト サービスの使用。デフォルトの Per Hop Behavior（PHB）は通常、ベストエフォート サービスです。
- DSCP 値をバイナリ形式で入力する、保証型転送（AF）の使用。AF では、輻輳が発生し、トラフィックが最大許容レートを超過していない場合に、パケットの特定のクラスが転送される相対的な確率を設定します。AF per-hop behavior により、IP パケットが異なる 4 つの AF クラス（AF11 ～ 13、AF21 ～ 23、AF31 ～ 33、および AF41 ～ 43）で配信されます。各 AF クラスには、特定のバッファ スペース容量および廃棄確立が割り当てられ、DSCP 番号がバイナリ形式で指定されます。輻輳が発生すると、パケットの廃棄優先順位

により、クラス内のパケットの相対的な重要性が決定されます。AF41 では、パケットがネットワークの端から端へ転送される確立が最も高くなります。

- 1 ～ 7 の範囲の Class Selector（CS ; クラス セレクタ）サービス値の入力（パケットの ToS フィールドの IP precedence ビットに対応）
- 急送型転送（EF）の使用による低遅延パスの指定。これは、DSCP 値 46 に対応します。EF サービスでは、プライオリティ キューイングを使用して、プライオリティの低いトラフィック クラスをプリエンプトします。

次に、使用可能な分類オプションを表示します。

```
Switch(config-cmap)# match ip dscp ?
<0-63> Differentiated services codepoint value
af11 Match packets with AF11 dscp (001010)
af12 Match packets with AF12 dscp (001100)
af13 Match packets with AF13 dscp (001110)
af21 Match packets with AF21 dscp (010010)
af22 Match packets with AF22 dscp (010100)
af23 Match packets with AF23 dscp (010110)
af31 Match packets with AF31 dscp (011010)
af32 Match packets with AF32 dscp (011100)
af33 Match packets with AF33 dscp (011110)
af41 Match packets with AF41 dscp (100010)
af42 Match packets with AF42 dscp (100100)
af43 Match packets with AF43 dscp (100110)
cs1 Match packets with CS1(precedence 1) dscp (001000)
cs2 Match packets with CS2(precedence 2) dscp (010000)
cs3 Match packets with CS3(precedence 3) dscp (011000)
cs4 Match packets with CS4(precedence 4) dscp (100000)
cs5 Match packets with CS5(precedence 5) dscp (101000)
cs6 Match packets with CS6(precedence 6) dscp (110000)
cs7 Match packets with CS7(precedence 7) dscp (111000)
default Match packets with default dscp (000000)
ef Match packets with EF dscp (101110)
```

DSCP のプライオリティ設定の詳細については、RFC-2597（AF PHB）、RFC-2598（EF）、または RFC-2475（DSCP）を参照してください。

分類の比較

表 1 : 一般的なトラフィック分類 （7 ページ）に、一般的なトラフィックタイプに推奨される IP DSCP 値、IP precedence 値、および CoS 値を示します。

表 *1* : 一般的なトラフィック分類

トラフィック タイプ	ホップ単位の DSCP	DSCP（10 進数）	IP プレシデンス	CoS
音声ベアラ：プライオリティキュー、または最高のサービスウェイトおよび最低の廃棄プライオリティを持つキューのトラフィック	EF	46	5	5

トラフィック タイプ	ホップ単位の DSCP	DSCP（10 進数）	IP プレシデンス	QoS
音声制御：音声ゲートウェイまたは音声アプリケーションサーバからの、コールセットアップに関連したシグナリング トラフィック	AF31	26	3	3
ビデオ会議：ほとんどのネットワークで、IP 上でのビデオ会議には、損失、遅延、および遅延の種類に関して Voice over IP（VoIP）トラフィックと同様な要件があります。	AF41	34	4	4
ストリーミング ビデオ：損失、遅延、および遅延の種類に関して高い耐性を持つ、比較的高い帯域幅のアプリケーション。通常、E メールおよび Web 参照のような日常的なバックグラウンド アプリケーションよりも重要と見なされます。	AF13	18	1	1
ミッション クリティカル データ（ゴールドデータ）：企業の業務上重要な、遅延に影響されやすいアプリケーション	-	-	-	-
	-	-	-	-
レベル 1	AF21	18	2	2
レベル 2	AF22	20	2	2
レベル 3	AF23	22	2	2
重要度が低いデータ（シルバーデータ）：クリティカルではないが、比較的重要なデータ	-	-	-	-
	-	-	-	-
レベル 1	AF11	10	1	1
レベル 2	AF12	12	1	1
レベル 3	AF13	14	1	1
ベストエフォートデータ（ブロンズデータ）：重要度に関係なく、デフォルト 0 0 0 のすべての非対話型トラフィックを含むその他のトラフィック	デフォルト	0	0	0
ベストエフォートデータよりも重要でないデータ：クリティカルでなく、優先度が低い、帯域幅を消費するデータ トラフィック。これは、最初に廃棄されるトラフィック タイプです。	-	-	-	-
		-	-	-
		-	-	-
レベル 1		2	0	0
レベル 2		4	0	0
レベル 3		6	0	0

QoS ACL に基づく分類

パケットは、入力ポリシー マップで ACL 検索に基づいても分類されます。ACL 検索に基づいて分類する場合は、まず IPv4、IPv6、または MAC ACL を作成します。クラスマップを設定し、match access-group {*acl-number* | *acl name*} クラスマップ コンフィギュレーション コマンドを使用して、ポリシーマップにクラスマップを付加します。

すべての ACL における ACE の最大数は 256 です。これには、入力サービスポリシーおよび暗黙のルールで設定されたマーキングアクションルールが含まれます。

（注） 出力ポリシー マップには、match access-group を設定できません。

IP 標準、IP 拡張、またはレイヤ 2 MAC ACL を使用すると、同じ特性（クラス）を持つパケットのグループを定義できます。レイヤ 3 およびレイヤ 4 パラメータに基づいて IP トラフィックを分類する IP ACL を設定するには、access-list グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 パラメータに基づいて IP および 非 IP トラフィックを分類するレイヤ 2 MAC ACL を設定するには、mac access-list extended グローバル コンフィギュレーション コマンドを使用します。

（注） IP フラグメントを設定済みの IP 拡張 ACL に照合して、QoS を実行できません。IP フラグメントはベストエフォート型として送信されます。IP フラグメントは IP ヘッダーのフィールドで示されます。

match access-group コマンドでは、許可アクションが含まれる ACL だけを使用できます。拒否アクションが含まれる ACL は、QoS ポリシーで照合されません。

（注） 入力ポリシー マップのクラスごとに 1 つのアクセス グループだけがサポートされます。

次の例では、ポリシーマップのクラスマップが音声、データ、およびビデオトラフィックの一致基準を指定して、ポリシーマップが各トラフィックタイプの入力ポリシングに対するアクションを設定します。

```
Switch(config)# policy-map policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action transmit
Switch(config-pmap-c)# exceed-action set-cos-transmit 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-1 data
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# exit
```

レイヤ 2 CoS に基づく分類

match コマンドを使用することにより、CoS 値（0 ～ 7 の範囲）に基づいてレイヤ 2 トラフィックを分類できます。

Note:match cos コマンドは、レイヤ 2 802.1Q トランクポートでのみサポートされます。

次に、CoS 値 5 に一致するクラス マップを作成する例を示します。

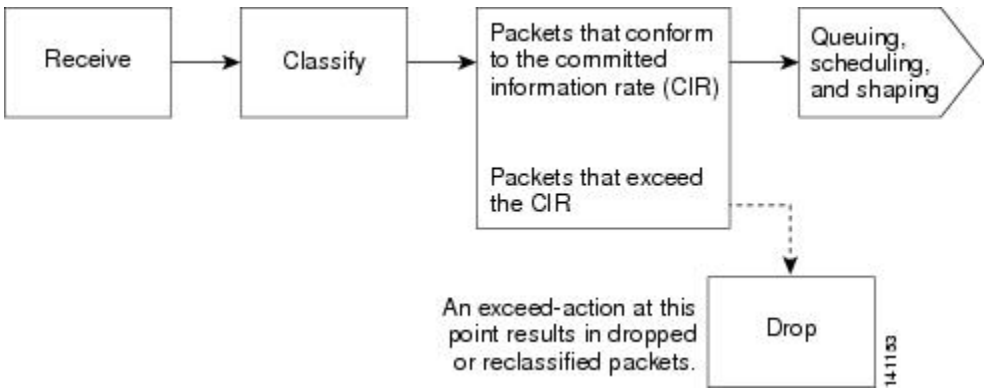
```
Switch(config)# class-map premium
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

ポリシング

パケットが分類されたあとに示されるポリシングを使用して、トラフィッククラスを規制できます。ポリシング機能では、特定のトラフィック フローで使用可能な帯域幅量を制限するか、または任意のトラフィック タイプが過剰な帯域幅およびシステム リソースを使用しないようにします。ポリサーは、ポリサーおよびトラフィック クラスの設定プロファイルと着信トラフィックのレートを比較することにより、パケットを適合または不適合として識別します。許容平均レートまたはバーストレートを超過するパケットは、不適合または非適合となります。これらのパケットは、ポリサーの設定に応じて、廃棄されるかまたは変更（追加処理用にマーキング）されます。

ポリシングは、主に受信インターフェイス上で使用されます。ポリサーを含むポリシーマップは、入力サービス ポリシーに限り付加できます。ポリシングは出力ポリシーマップでは許可されません。

図 *3:* 分類されたパケットのポリシング



個別のポリシング

個別のポリシングは、入力ポリシーマップにだけ適用されます。ポリシーマップ コンフィギュレーション モードで、class コマンドのあとにクラスマップ名を入力して、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。

シスコ産業用イーサネットスイッチは、個別ポリシングまたは集約ポリシングについて 1-rate、2-color 入力ポリシングおよび 2-rate、3-color のポリシングをサポートします。

（注） 入力ポリシーの「set」と「police」には 2 つの制限があります。

- set と police は、単一クラス内の単一ポリシーで一緒にサポートされません。ただし、これらのアクションを異なるクラスに適用する場合は、サポートされる設定です。
- Asic は、ポリシング設定ごとの単一マーキングアクションを制限します。IE3X00 では現在、この単一のマーキングアクションは黄色パケットにのみ使用できます。

1-rate、2-color ポリシングについては、police ポリシーマップ クラス コンフィギュレーション コマンドを使用して、ポリサー、トラフィックの認定速度制限、トラフィックの認定バースト サイズ制限、または制限未満（conform-action）および制限を越える（exceed-action）トラフィックに対して実行するアクションを定義します。バースト サイズ（bc）を指定しない場合は、システムにより適切なバースト サイズ値が算出されます。算出された値は、ほとんどのアプリケーションに適しています。

最初のトークン バケットを更新するため、認定情報レート（CIR）の設定を含む、2-rate ポリサーを設定する場合、2 番目のトークン バケットが更新される最大情報レート（PIR）も設定します。PIR を設定しない場合、ポリサーは標準 1-rate、2-color ポリサーです。

2-rate、3-color ポリシングについては、指定の CIR および PIR に適合するパケット（conform-action）、PIR には適合するが CIR には適合しないパケット（exceed-action）、および PIR 値を超えるパケット（violate-action）で実行するアクションを任意に設定できます。

- PIR に等しい CIR 値を設定している場合、CIR 以下のトラフィック レート速度は適合範囲内です。CIR を超えるトラフィックは違反範囲に入ります。
- PIR を CIR よりも大きな値に設定すると、CIR を下回るトラフィック レートは適合になります。CIR を超過し、PIR 以下のトラフィック レートは超過になります。PIR を超過するトラフィック レートは違反になります。
- PIR を設定しない場合、ポリサーは 1-rate、2-color ポリサーとして設定されます。

バースト サイズの設定が低すぎると、バースト トラフィックがある状況でスループットが低下する場合があります。バースト サイズの設定が高すぎると、トラフィック レートが高くなりすぎる場合があります。

（注） スイッチでは、show policy-map interface 特権 EXEC コマンド出力で conform、exceed、および violate の各クラスのバイトレベル統計情報がバイトカウンタでサポートされています。

ポリシーマップを有効にするには、service-policy input インターフェイス コンフィギュレーション コマンドを使用し、ポリシーマップを物理ポートに付加します。ポリシングは、受信トラフィックでだけ行われるため、ポリサーは入力サービス ポリシーにだけ付加できます。

conform-action および exceed-action ポリシーマップ クラス コンフィギュレーション コマンド、または conform-action および exceed-action ポリシーマップ クラス ポリシング コンフィギュレー

ションコマンドを使用すると、パケットが指定のトラフィックレートに適合または超過する場合に実行するアクションを指定できます。

適合アクションとは、変更なしでパケットを送信するか、パケットをドロップすることです。超過アクションとは、パケットを廃棄すること、パケットを変更しないで送信すること、新しい CoS 値、DSCP 値、または IP DSCP 値を設定することです。

conform-action、exceed-action、および violate-action ポリシーマップ クラス コンフィギュレーション コマンド、または conform-action、exceed-action、および violate-action 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 コマンドを使用すると、パケットが指定のトラフィックレートに適合または超過する場合に実行するアクションを指定できます。

各サービス クラスで複数の適合アクションおよび超過アクションを同時に設定できます。各サービスクラスで複数の適合アクション、超過アクション、および違反アクションを同時に設定できます。

クラスで複数の動作を設定する場合、ポリシーマップ クラスポリシング コンフィギュレーションモードで複数の適合または超過の各アクションのエントリ適合、超過、または違反の各アクションのエントリを入力する必要があります（次の例を参照）。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 500000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-cos-transmit 2
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

マーキング

入力ポリシー マップでパケット マーキングを使用すると、特定のクラスに属するトラフィックの属性を設定または変更できます。ネットワーク トラフィックがクラス内に組み込まれたあとで、マーキングを使用して、特定のトラフィック タイプを識別して固有の処理を行います。たとえば、クラスの CoS 値を変更したり、特定のトラフィックタイプの IP DSCP 値を設定できます。その後、これらの新しく設定された値を使用して、トラフィックの処理方法を決定します。

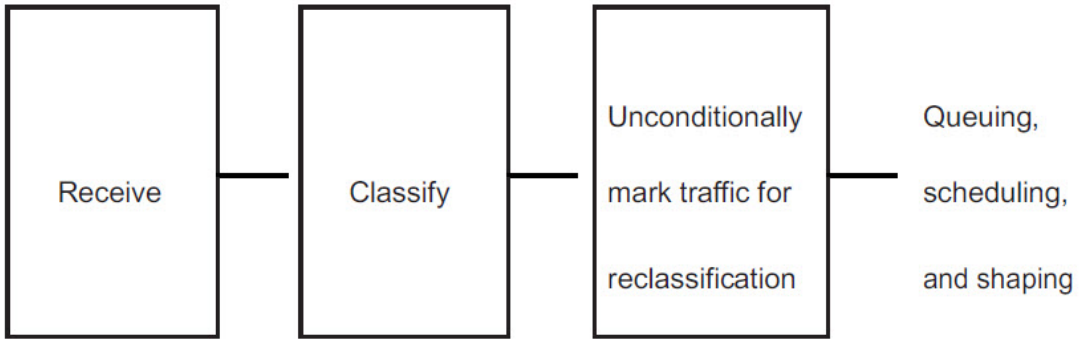
トラフィック マーキングは通常、入力ポートの特定のトラフィック タイプで実行されます。マーキング アクションにより、CoS、DSCP、または precedence ビットは、設定に応じて書き換えられるか、またはそのまま変更されません。これにより、QoS ドメインで使用されるポリシーに従って、パケットのプライオリティが高くなるかまたは低くなります。そのため、他の QoS 機能ではマーキング情報を使用して、パケットの相対的および絶対的な重要性を判断できます。マーキング機能では、ポリシング機能から取得した情報または分類機能から直接取得した情報を使用できます。

ポリシーマップで、すべてのサポート対象の QoS マーキング（CoS、IP DSCP）に対して set コマンドを使用することにより、トラフィックを指定およびマーキングできます。set コマンドにより、特定クラスに一致するパケットは無条件にマーキングされます。その後、インターフェイスにポリシー マップを入力ポリシー マップとして付加します。

同一アクションに対してパケットの DSCP、precedence、および CoS マーキングを変更するアクションを同時に設定できます。

次の図に、トラフィックのマーキングの手順を示します。

図 *4:* 分類されたトラフィックのマーキング



次に、ポリシーマップを使用してパケットをマーキングする例を示します。最初のマーキング（set コマンド）は、クラス AF31 ～ AF33 によって一致しなかったすべてのトラフィックを照合する QoS デフォルトクラスマップに適用され、すべてのトラフィックの IP DSCP 値を 1 に設定します。2 番目のマーキングは、クラス AF31 ～ AF33 のトラフィックの IP DSCP を 3 に設定します。

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

輻輳管理およびスケジューリング

Cisco Modular QoS CLI（MQC）は、発信トラフィック フローを制御する関連メカニズムをいくつか備えています。これらのメカニズムは、出力ポリシーマップに実装され、出力トラフィック キューを制御します。

輻輳管理機能で、パケットがインターフェイスに送信される順番を、これらのパケットに割り当てられた優先順位を基に決定することで輻輳をコントロールできます。輻輳管理は、キューを作成し、そのキューにパケットの分類に基づいてパケットを割り当て、キューにあるパケットの送信をスケジューリングする必要があります。

異なるスケジューリング メカニズムを使用すると、他のトラフィックを均等に処理しながら、特定のトラフィック クラスに保証された帯域幅を割り当てることができます。特定のトラフィッ

ク クラスで消費される最大帯域幅を制限して、低遅延キューの遅延の影響を受けやすいトラフィックが他のキューよりも先に送信されるように保証できます。

スイッチでは、次のスケジューリング メカニズムをサポートします。

トラフィック シェーピング

平均レート シェーピングを設定するには、shape average ポリシーマップ クラス コマンドを使用します。このコマンドは、特定のクラスの最大帯域幅を設定します。キューの帯域幅は、ポートでさらに使用できる帯域幅があってもこの値に制限されます。このコマンドにより、割合またはターゲットビットレート値でシェーピング平均を設定できます。

CBWFQ

bandwidth ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、特定のクラスに割り当てられる帯域幅を制御できます。最小帯域幅は、総帯域幅もしくは残りの帯域幅との割合で指定できます。

このコマンドは、次の帯域幅設定をサポートしています。

- 帯域幅の割合：特定のクラスに最小帯域幅を割り当てるには、bandwidth percent ポリシーマップ クラス コマンドを使用します。合計が 100 % を超えることはできません。合計が 100% 未満である場合は、残りの帯域幅がすべての帯域幅キューで均等に分割されます。
- 残存帯域幅：指定されたキューでの未使用帯域幅の共有率を作成するには、bandwidth remaining ポリシーマップ クラス コマンドを使用します。未使用帯域幅は、これら指定されたキューにより、設定で指定されている比率で使用されます。このコマンドは、priority コマンドがポリシー内の特定のキューでも使用される場合に使用します。

プライオリティ キューイングまたはクラスベース プライオリティ キューイング

priority ポリシーマップ クラス コンフィギュレーション コマンドを使用して、他のトラフィックタイプよりも優先されるトラフィックタイプを指定します。他のトラフィックキュー間で、既知の残存帯域幅に絶対優先を指定できます。

- 完全プライオリティを設定するには、priority ポリシーマップ クラス コンフィギュレーション コマンドだけを使用して、プライオリティキューを設定します。その他のトラフィック クラスには、bandwidth remaining percent ポリシーマップ クラス コンフィギュレーション コマンドを使用して、必要な比率で余剰の帯域幅を割り当てます。
- 無条件のポリシングを含むプライオリティを設定するには、priority ポリシーマップ クラス コンフィギュレーション コマンドおよび police ポリシーマップ クラス コンフィギュレーション コマンドを使用して、プライオリティキューを無条件にレート制限します。この場合、他のトラフィッククラスは、要件に応じて shape average により設定できます。

トラフィック シェーピング

トラフィック シェーピングは、トラフィック ポリシングと同様のトラフィック制御メカニズムです。入力ポリシー マップでトラフィック ポリシングが使用されている場合、トラフィッ

クシェーピングはインターフェイスからトラフィックを発信するときに実行されます。スイッチは、インターフェイスから発信されるトラフィックのクラスにはクラスベースシェーピングを、およびインターフェイスから発信されるすべてのトラフィックにはポートシェーピングを適用できます。トラフィック シェーピングのキュー設定により、キューの最大帯域幅および Peak Information Rate（PIR）が設定されます。

シェーピングにはバッファが関連付けられており、十分なトークンがないパケットがすぐにドロップされずにバッファされます。シェーピングされるトラフィックのサブセットで使用可能なバッファ数は制限され、さまざまな要因に基づいて計算されます。

（注） シェーピングと優先順位は、出力ポリシーマップの同じクラス内では設定できません。ただし、シェーピングと帯域幅は一緒に設定できます。

クラスベースのシェーピング

クラスベースシェーピングは、shape average ポリシーマップ クラス コンフィギュレーション コマンドを使用して、データ伝送速度（bps）を制限し、トラフィッククラスの認定情報速度（CIR）に使用します。スイッチは、送信側のポートごとに 8 つのキューをサポートします。8 番目のキューは常に、クラス class-default、未分類トラフィック用のデフォルトキューです。

```
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

Class-Based Weighted Fair Queuing：クラスベース WFQ

CBWFQ を設定することにより、ポートで使用可能な総帯域幅の一部を割り当てて、キューの相対的優先順位を設定できます。**bandwidth** ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、トラフィッククラスの出力帯域幅を総帯域幅に対するパーセンテージ、または残りの帯域幅に対するパーセンテージで設定できます。

- bandwidth ポリシーマップ クラス コンフィギュレーション コマンドを使用して、トラフィッククラスを総帯域幅に対するパーセンテージで設定する場合、これはそのトラフィッククラスの最小帯域幅保証（CIR）を表します。つまり、トラフィック クラスは最低でもコマンドにより指定された帯域幅を取得しますが、その帯域幅に制限されるわけではありません。ポート上の余剰の帯域幅はすべて、CIR レートの設定と同じ比率で各クラスに割り当てられます。

出力ポリシーマップの別のクラスで完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合、帯域幅を総帯域幅に対するパーセンテージで設定できません。

- bandwidth ポリシーマップ クラス コンフィギュレーション コマンドを使用して、トラフィッククラスを残りの帯域幅に対するパーセンテージで設定する場合、これはクラスに割り当てられるポートの余剰帯域幅の一部を表しています。つまり、ポート上に余剰の帯域幅が

ある場合、およびこのトラフィック クラスに最小帯域幅保証がない場合にだけ、クラスに帯域幅が割り当てられます。

出力ポリシーマップの別のクラスに完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合にだけ、帯域幅を残りの帯域幅に対するパーセンテージで設定できます。

（注） 出力ポリシー マップ内の同一のクラスには、帯域幅とトラフィック シェーピング（shape average）またはプライオリティ キューイング（priority）を設定できません。

（注） クラスのCIR帯域幅を総帯域幅に対するパーセンテージで設定する場合、ポリシーマップ内のすべてのクラスのCIRの処理後に残った余剰な帯域幅すべては、CIRレートと同じ比率でクラス間に配分されます。クラスのCIRレートが0に設定されている場合、このクラスはどの余剰帯域幅に対しても不適格となるため、帯域幅を取得できません。

プライオリティ キューイング

priority ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、特定のトラフィッククラスで優先処理が行われるよう保証できます。完全プライオリティ キューイングを使用すると、プライオリティ キューは常に処理されます。キュー内のすべてのパケットは、キューが空になるまでスケジューリングされ、送信されます。プライオリティ キューイングにより、関連付けられたクラスのトラフィックは、他のキューのパケットよりも先に送信されます。

（注） **priority** コマンドを使用する際は注意してください。完全プライオリティ キューイングを過剰に使用すると、他のキューで輻輳が発生する場合があります。

スイッチでは、完全プライオリティ キューイングまたはポリシーマップ クラス サブモード コマンドと併用されるプライオリティをサポートしています。

完全プライオリティキューイング（ポリシングなしのプライオリティ）では、トラフィッククラスを低遅延キューに割り当てて、このクラスのパケットの遅延確率が最小になるよう保証します。完全プライオリティ キューイングが設定されている場合、プライオリティ キューは空になるまで継続的に処理され、他のキューのパケットは処理されない場合もあります。

プライオリティ キューイングには、次の制限事項があります。

- priorityコマンドは、スイッチ上で付加されたすべての出力ポリシーの単一の一意のクラスに関連付けできます。
- 同一クラスでは、プライオリティとその他のスケジューリングアクション（shape averageまたはbandwidth）を設定できません。

• 出力ポリシーマップの class-default にはプライオリティキューイングを設定できません。

次に、クラス out-class1 を完全プライオリティキューとして設定し、このクラスのすべてのパケットが他のトラフィッククラスより先に送信される例を示します。他のトラフィックキューでは、out-class2 は残りの帯域幅の 50%、out-class3 は残りの帯域幅の 20% を取得するように設定されます。クラス class-default は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

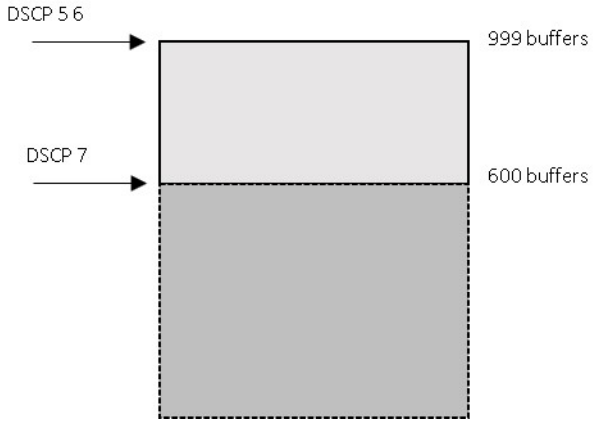
輻輳回避およびキューイング

輻輳回避では、テールドロップなどのアルゴリズムを使用して、キューイングおよびスケジューリング ステージを開始するパケット数を制御して、輻輳およびネットワークのボトルネックを回避します。キュー サイズの制限は、キューのパケット マーキングに応じて設定されます。スイッチを通過するパケットごとに、特定のキューおよびしきい値が割り当てられます。たとえば、特定の DSCP 値または CoS 値は特定の出力キューおよびしきい値にマッピングされます。テールドロップのキューの最大しきい値をパケット数として指定できます。

輻輳回避は、パケットがエンキューされるプライオリティキューを選択し、個々のキューにテールドロップメカニズムを実装します。テールドロップメカニズムは、パケットに関連付けられたドロップ優先順位、バッファ占有レベル、および設定されたしきい値を使用して、パケットを廃棄するかどうかを決定します。

次の図は、最大深度が 999 バッファのキューでのテールドロップ動作の例を示しています。キューごとに 2 つのドロップしきい値が許可されます。キューの最大バッファ数は 999 です。600 バッファは、クラス「class_dscp_low」に一致する分類子のサブセットである DSCP 7 のみのしきい値設定です。キューの最大値のデフォルト設定は 1000 バッファです。最大キュー制限は小さくすることができます。

キューが輻輳し、600 以上のバッファで満たされると、新しいパケットが DSCP 7 でマークされて到着し、フレームは 600 のバッファ制限しきい値の対象になります。600 バッファのしきい値を超過するため、フレームはテールドロップされます。



この例の CLI を次に示します。

```
class-map match-any class_dscp_low
match dscp 5  6  7

policy-map p1
class class_dscp_low
  bandwidth percent 50
  queue-limit 999
  queue-limit dscp 7 600
```

キュー制限の設定

テールドロップは、ポリシーマップ クラス サブ モードで **queue-limit** コマンドを使用すると設定されます。このコマンドにより、特定のトラフィック クラスに関連するキューサイズ（バッファ サイズ）が調整されます。しきい値は、バッファ数（各バッファは 256 バイトの固定単位）またはトラフィッククラスのパーセンテージとして設定します。キュー制限を設定することにより、対応するトラフィックの輻輳発生時の廃棄しきい値が確立されます。

（注） ポリシーマップ クラス サブ モードで **queue-limit** コマンドを使用してキューサイズを設定する場合は、まずスケジューリングアクション（bandwidth、shape average または priority）を設定する必要があります。唯一の例外は、出力ポリシーマップの class-default のキュー制限を設定する場合です。

スイッチは、すべての出力ポリシーマップにおいてそれぞれ固有のキュー制限設定を最大 3 つまでサポートしています。出力ポリシーマップの任意のキュー定義内で、最大 2 つのしきい値を定義できます。1 つ目はキューの最大値です。デフォルトのキュー深度は 1000 バッファです。2 つ目は分類子のサブセット（COS または DSCP）のしきい値です。ただし、複数のポリシーマップで同じキュー制限を共有できます。2 つのポリシーマップがキュー制限の設定を共有する場合、両方のポリシーマップのクラスで、すべてのしきい値が同じでなければなりません。

スイッチ上の複数の出力ポリシーマップで同じキュー制限値を使用できます。ただし、クラスのキュー制限値の 1 つを変更すると、新たな固有のキュー制限設定が作成されます。インターフェイスに付加できる出力ポリシーマップの固有のキュー制限設定は、どの時点でも 3 つだけ

です。4 つめのキュー制限が設定された出力ポリシー マップを付加しようとすると、次のエラー メッセージが表示されます。

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit configurations
 exceeded.
```

（注） 出力ポリシーマップでクラスにキュー制限を設定する場合、他のすべての出力ポリシーマップでは、クラスに対して同一の一致基準を使用する必要があります。キュー制限のしきい値に限り、異なる値を設定できます。たとえば、ポリシーマップ PM1 の dscp 30 および dscp 50 に、class A のキュー制限のしきい値が設定されていて、ポリシーマップ PM2 で class A のキュー制限を設定する場合、dscp 30 および dscp 50 を一致基準として使用する必要があります。dscp 20 および dscp 40 は、使用できません。別のしきい値を設定できますが、これにより、新たなキュー制限設定が作成されます。

デフォルトでは、バッファスペースの総容量は、すべてのポートおよび各ポートのすべてのキューで均等に配分されます。これは、大部分のアプリケーションに適合します。遅延の影響を受けやすいトラフィックのキューサイズを削減したり、またはバースト性のあるトラフィックのキュー サイズを増加させたりできます。

（注） queue-limit コマンドを使用して、クラスのキューしきい値を設定する場合、しきい値は、キューの最大しきい値以下にする必要があります。

キュー制限を設定する場合、指定できるバッファ数の範囲は 16 の倍数で、32 ～ 999 です。この場合、各バッファは 256 バイトの単位となります。

（注） 最適なパフォーマンスを実現するため、キュー制限でバッファ数を 272 以下に設定することを推奨します。

キューの帯域幅とキュー サイズ（キュー制限）は、別々に設定されます。相互依存はしません。帯域幅およびキュー制限を設定する場合、送信されるトラフィック タイプを考慮する必要があります。

- キュー制限を大きくすると、パケットを損失することなくバーストトラフィックに対応できますが、遅延は増えます。
- キュー制限を小さくすると、遅延は減りますが、バーストトラフィックより安定したトラフィックフローに適しています。
- 通常、キュー制限を非常に小さくするのは、プライオリティキューイングを最適化する際です。プライオリティキューイングされるトラフィックの場合、通常少しのパケットに対応するだけのバッファサイズが必要です。通常、大きなキューサイズは遅延を増加させるため、必要ではありません。高いプライオリティの遅延の影響を受けやすいパケットには、相対的に大きな帯域幅および相対的に小さなキュー サイズを設定します。

これらの制限事項は、WTD 修飾子に適用されます。

- queue-limit コマンドを使用した場合、WTD 修飾子（cos、dscp）に 1 つのしきい値のみ設定できます。ただし、これらのしきい値にマッピングできる修飾子の数に制限はありません。修飾子を指定しないでqueue-limitコマンドを使用することにより、最大キューを設定する 2 番目のしきい値を設定できます。
- queue-limit コマンドの WTD 修飾子は、関連するクラスマップの少なくとも 1 つの一致基準と同じである必要があります。

スイッチポート数に応じた数の出力ポリシーマップを設定および付加できますが、一意のキュー制限は2つしか設定できません。他の出力ポリシーマップが同じキュー制限およびクラス設定を使用する場合、帯域幅パーセンテージが異なる場合でも、キュー制限設定は同じであると見なされます。

QoS のデフォルト設定

ポリシーマップ、クラスマップ、またはポリサーは設定されていません。出力ポートでは、すべてのトラフィックがCoSおよびDSCP値に基づいてプロファイルインデックスが割り当てられたキューに送られます。

パケットは変更されません（パケット内のCoSおよびDSCP値は変更されません）。トラフィックはパススルーモードでスイッチングされ、書き換えられずにポリシングを伴わないベストエフォート型として分類されます。

制約事項と制限

- QoS を設定できるのは物理ポートのみです。
- QoSが設定されたポートでは、そのポートを通じて受信されるすべてのトラフィックは、ポートに付加された入力ポリシーマップに従って分類、ポリシング、およびマーキングが行われます。QoS が設定されたトランク ポートでは、そのポートを通じて受信されるすべての VLAN 内トラフィックは、ポートに付加されたポリシー マップに従って分類、ポリシング、およびマーキングが行われます。
- QOS は論理ポート（EtherChannel）ではサポートされません。
- スイッチで受信された制御トラフィック（スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。
- CDP、LLDP、STP などのすべての制御パケットは、出力ポートのキュー 6 から転送するようにマークされます。したがって、追加のパケットはポートカウンタ統計に含まれます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。

- 新しいポリシーをインターフェイスに付加しようとし、これによりポリサーインスタンスの数が 1024 -（スイッチ上のインターフェイス数 + 1）より多い数になる場合、エラーメッセージを受信し、設定は失敗します。

次の表は、QoS のサポートと設定に関する制限をまとめたものです。

機能	制約/制限
QoS グループ	未サポート
階層型 QoS（HQoS）	未サポート
クラスマップ	• match-all クラス マップには、1 つの分類基準（match 文）しか指定できませんが、match-any クラス マップには複数の match 文を指定できます。 • match cos コマンドは、レイヤ 2 802.1Q トランク ポートでだけサポートされます。 • 入力ポリシーマップでは、同一ポリシーマップまたはクラスマップ内に IP 分類（match ip dscp、IP ACL の match access-group）と非 IP 分類（match cos、または MAC ACL の match access-group）を設定できません。 • 出力ポリシー マップでは、異なるクラス マップで同じ分類基準（つまり、同じ match 修飾子および match 値）を使用できません。 • スイッチ上のクラス マップの最大数は、1024 です。
ポリシーマップ内のクラスマップ数	入力ポリシーの場合は11+クラスデフォルト、出力ポリシーの場合は 7 + クラスデフォルト。

機能	制約/制限

QoS の ACL	• EQ ポートの比較演算子は、以下に示す制限の対象にはなりません。EQ ポート比較演算子は、ACL 内の ACE の制限に達するまで、すべての ACE で使用できます。
	• EQ 以外のポート比較アクションは、LT、GT、および NEQ です。これら 3 つのタイプのポート比較演算子には制限があります。これらのタイプのポート比較演算子の合計 16 個（TCP トラフィックに適用される 8 個の比較演算子および UDP トラフィックに適用される 8 個の比較演算子）をスイッチでグローバルに使用できます。
	• TCP/UDP 送信元/宛先ポートでは、range、lt、gt、neq 操作を含む IPv4 ACL がサポートされます。各範囲ルールは、2 ポートの比較演算子を使用します。
	  • ポートごとの比較オプションごとに使用されるポート比較演算子の数。Range：TCP/UDP ports - 2 の範囲
	  • LT：port # - 1 「より小さい」
	  • GT：port # - 1「より大きい」
	  • NEQ：port # - 1「と等しくない」
	• 拡張ヘッダーとフローラベルが一致する IPv6 ACL はサポートされていません。
	• オブジェクトグループおよび宛先オプションに一致する IPv6 ACL はサポートされていません。
	• IPv4 ACL での TTL ベース照合はサポートされません。
	• IPv4 ACL での IP オプションベース照合はサポートされません。
	• アクセスグループは VLAN ID で照合できません。

ポリシーマップ内の ACE 数	256（ポリシー内のすべてのクラス間）。
複数の一致基準ですべて一致	未サポート
さまざまなタイプのアクセスグループでのクラスマップ照合	ポリシーマップ内では、アクセスグループのタイプが異なる場合、クラスマップ照合はサポートされていません。すべてのクラスマップは、同じタイプのアクセスグループ（mac、ipv4、または ipv6）で照合する必要があります。

機能	制約/制限
入力ポリシーの **set** と **police**	• set と police は、単一クラス内の単一ポリシーで一緒にサポートされません。ただし、これらのアクションを異なるクラスに適用する場合は、サポートされる設定です。 • Asic は、ポリシング設定ごとの単一マーキングアクションを制限します。IE3x00 では現在、この単一のマーキングアクションは黄色パケットにのみ使用できます。
個別のポリサー	• ポリシングは、入力ポリシー マップ上でだけサポートされます。 • スイッチ上では、最大 200 のポリサーがサポートされます • ポリシングは入力ポートでのみサポートされます。 • スイッチ上のポリサー インスタンスの数は 1024 - （インターフェイス数 + 1）です。 • スイッチは、最大 200 のポリサープロファイルをサポートします。 • violate-action を設定しない場合、デフォルトで違反クラスが exceed-action と同じアクションに割り当てられます。
bandwidth qos-reference *(value)*	このインターフェイスレベルの QOS コマンドはサポートされていません。
ポリサーおよびマーキング	入力方向でのみサポートされます。
キューイングおよびスケジューリング（帯域幅、シェーパー、優先順位、キュー制限）	出力方向でのみサポートされます。
出力ポリシーマップ	出力ポリシーマップのクラスマップがアクセスグループで一致しません。

（注） 制約事項と制限事項の詳細については、上記の表に記載されている機能の説明についてのセクションを参照してください。

QoS の設定

QoS を設定する前に、制約事項と制限 （20 ページ）を確認してください。また、次の内容を理解しておいてください。

- 使用するアプリケーションのタイプおよびネットワークのトラフィックパターン
- トラフィックの特性およびネットワークのニーズ。バースト性の高いトラフィックかどうかの判別。音声およびビデオストリーム用の帯域幅確保の必要性
- ネットワークの帯域幅要件および速度
- ネットワーク上の輻輳発生箇所

次に、着信トラフィックの分類、ポリシングおよびマーキング方法と発信トラフィックのスケジューリングおよびキューイング方法について説明します。

ネットワーク設定に応じて、次の作業を 1 つまたは複数実行する必要があります。

- CoS および DSCP を使用したトラフィックの分類 （24 ページ）
- ACL を使用したトラフィックの分類 （25 ページ）
- IP 拡張 ACL の作成 （27 ページ）
- レイヤ 2 MAC ACL の作成 （29 ページ）
- クラス マップを使用したトラフィック クラスの定義 （31 ページ）
- トラフィック ポリシーのインターフェイスへの適用 （33 ページ）
- 入力ポリシー マップの設定 （34 ページ）
- 個別のポリシングを含む入力ポリシー マップの設定 （35 ページ）
- マーキングを含む入力ポリシー マップの設定 （42 ページ）
- 出力ポリシー マップの設定 （44 ページ）
- CBWFQ を含む出力ポリシー マップの設定 （45 ページ）
- ポート シェーピングを含む出力ポリシー マップの設定 （47 ページ）
- クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定 （48 ページ）
- WTD を含む出力ポリシー マップの設定 （51 ページ）

CoS および DSCP を使用したトラフィックの分類

次に、クラスマップ example を作成して、リストされた基準のいずれかに一致するクラスを定義する例を示します。この例では、DSCP 値 が 32 または 40 のパケットが受信された場合、このパケットはクラス マップにより識別（分類）されます。

```
Switch(config)# class-map match-any example
Switch(config-cmap)# match ip dscp 32
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit
```

次の例では、CoS 値が 2 のパケットを照合するクラスを定義します。

```
switch(config)# class-map class-cos
switch (config-cmap)# match cos 2
switch (config-cmap) # exit
```

ACL を使用したトラフィックの分類

IP トラフィックは、IP 標準または IP 拡張 Access Control List（ACL；アクセスコントロールリスト）を使用して分類できます。レイヤ 2 MAC ACL を使用すると、IP および非 IP トラフィックを分類できます。

すべての ACL においてアクセス コントロール エントリ（ACE）の最大数は 256 です。これには、入力サービスポリシーおよび暗黙のルールで設定されたマーキングアクションルールが含まれます。

TCP/UDP 送信元/宛先ポートでは、range、lt、gt、neq 操作を含む IPv4 ACL がサポートされます。各範囲ルールは、2 ポートの比較演算子を使用します。ポート比較オプションごとに使用されるポート比較演算子の数は次のとおりです。

- Range：TCP/UDP ports—2 の範囲
- LT：port #—1 「より小さい」
- GT：port #—1「より大きい」
- NEQ：port #—1「と等しくない」

これらのポート比較演算子の使用方法については、制約事項と制限 （20 ページ）を参照してください。

IP 標準 ACL の作成

IP トラフィック用に IP 標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

（注） 次のステップ 2 またはステップ 3 から選択します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**access-list** *access-list-number* **permit** *source [source-wildcard]*	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。有効範囲は 1 ～ 99 および 1300 ～ 1999 です。 • QoS ポリシーの一致基準として使用される ACL には、必ずキーワード permit を使用します。QoS ポリシーは、キーワード deny を使用する ACL には一致しません。 • source には、パケットの送信元となるネットワークまたはホストを指定します。any キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。
ステップ 3	**ip access-list standard** *name*	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。名前には、1 ～ 99 の番号を使用できます。 アクセスリスト コンフィギュレーション モードで、permit source *[source-wildcard]* を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

アクセス リストを削除するには、no access-list access-list-number グローバル コンフィギュレーション コマンドを使用します。

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。ネットワークアドレスのホスト部分にワイルドカードビットが適用されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
```

IP 拡張 ACL の作成

IP トラフィック用に IP 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**access-list** *access-list-number* **permit** *protocol {source source-wildcard destination destination-wildcard}* **precedence** *precedence]* **tos** *tos* **dscp** *dscp*	IP 拡張 ACL を作成します。必要な回数だけ、この手順を繰り返します。 （注） **dscp** 値を入力した場合、**tos** または **precedence** は入力できません。**dscp** を入力しない場合は、**tos** と **precedence** 値の両方を入力できます。 • *access-list-number* には、アクセス リスト番号を入力します。有効範囲は 100 ～ 199 および 2000 ～ 2699 です。 • QoS ポリシーの一致基準として使用される ACL には、必ずキーワード permit を使用します。QoS ポリシーは、deny ACL に一致しません。 • source には、パケットの送信元となるネットワークまたはホストを指定します。any キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 • *protocol* には、IP プロトコルの名前または番号を入力します。使用可能なプロトコルキーワードのリストを表示するには、DSCP 値でなく疑問符（?）を使用します。すべてのインターネット プロトコル（ICMP、TCP、UDP を含む）と一致させる場合は、ip を入力します。 • *source* はパケットの送信元であるネットワークまたはホストの番号です。 • *source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 • *destination* はパケットの宛先となるネットワークまたはホストの番号です。

	コマンドまたはアクション	目的
		• *destination-wildcard* は、ワイルドカードビットを宛先アドレスに適用します。 source、destination、wildcards は、次のように指定できます。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード any。 • 単一のホスト 0.0.0.0 を表すキーワード host。 その他のキーワードは任意で、意味は次のとおりです。 • precedence：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、routine（0）、priority（1）、immediate（2）、flash（3）、flash-override（4）、critical（5）、internet（6）、network（7）です。 • tos：パケットを 0 ～ 15 の番号または名前で指定するサービスタイプレベルと一致させる場合に入力します。指定できる値は、normal（0）、max-reliability（2）、max-throughput（4）、min-delay（8）です。 • dscp：0 ～ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符（?）を使用すると、使用可能な値のリストが表示されます。
ステップ 3	**ip access-list extended** *name*	名前を使用して拡張IPv4アクセスリストを定義し、アクセス リスト コンフィギュレーション モードを開始します。名前には、100 ～ 199 の番号を使用できます。 アクセスリストコンフィギュレーションモードで、前ステップで定義した permit *protocol {source-wildcard destination destination-wildcard}* precedence *precedence* tos *tos* dscp *dscp* を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists**	入力内容を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

アクセス リストを削除するには、no access-list access-list-number グローバル コンフィギュレーション コマンドを使用します。

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IP トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、アクセスリスト 103 を作成し、class1 という名前のクラスマップを設定する例を示します。class1 にはアクセス リスト 103 という一致条件が 1 つ設定されています。これは、任意のホストから任意の宛先へのトラフィックを許可し、特定の送信元/宛先ポートが指定された range、lt、gt 演算子を含みます。

```
Switch(config)# access-list 103 permit udp any any lt 102
Switch(config)# access-list 103 permit tcp any any gt 1024
Switch(config)# access-list 103 permit tcp any any range 5555 5560
Switch(config)# access-list 103 permit udp any any range 2327 2499

Switch(config)# class-map match-any class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)#exit

Switch(config)# policy-map child policy-1
Switch(config-pmap)# class 143
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
```

レイヤ 2 MAC ACL の作成

非 IP トラフィック用にレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**mac access-list extended** *name*	リストの名前を指定して、レイヤ 2 MAC ACL を作成し、拡張 MAC ACL 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	**permit** *{host src-MAC-addr mask | any | host dst-MAC-addr | dst-MAC-addr mask}[type mask]*	QoS ポリシーの一致基準として使用される ACL には、必ずキーワード permit を使用します。 • *src-MAC-addr* には、パケットの送信元となるホストの MAC アドレスを指定します。MAC アドレスは、16 進表記（H.H.H）で、source 0.0.0、source-wildcard ffff.ffff.ffff にキーワード any を使用したり、source 0.0.0 にキーワード host を使用して指定できます。 • *mask* では、無視するビット位置に 1 を入力することによって、ワイルドカードビットを指定します。 • *dst-MAC-addr* には、パケットの宛先となるホストの MAC アドレスを指定します。MAC アドレスは、16 進表記（H.H.H）で、source 0.0.0、source-wildcard ffff.ffff.ffff にキーワード any を使用したり、source 0.0.0 にキーワード host を使用して指定できます。 •（任意）*type mask* には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。*type* の範囲は 0 ～ 65535 です。通常は 16 進数で指定します。*mask* では、一致をテストする前に Ethertype に適用される don’t care ビットを入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*access-list-number* | *access-list-name*]	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

アクセス リストを削除するには、no mac access-list extended access-list-name グローバル コンフィギュレーション コマンドを入力します。

次に、2 つの許可（permit）ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示します。最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、

MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。2 番めのステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-macl)# exit
```

クラス マップを使用したトラフィック クラスの定義

個々のトラフィック フロー（またはクラス）を他のすべてのトラフィックから分離して名前を付けるには、class-map グローバル コンフィギュレーション コマンドを使用します。クラス マップが、特定のトラフィック フローとの照合を行い、さらにそれを分類するために使用する基準を定義します。match ステートメントには、ACL、CoS 値、DSCP 値などの条件を指定できます。一致基準は、クラスマップ コンフィギュレーション モードで入力される 1 つまたは複数の match ステートメントで定義されます。

クラス マップの設定を行うときは、次の注意事項に従ってください。

- match-all クラスマップには、1 つの分類基準（match 文）しか指定できませんが、match-any クラス マップには複数の match 文を指定できます。
- match cos コマンドは、レイヤ 2 802.1Q トランク ポートでだけサポートされます。
- 入力ポリシーマップでは、同一ポリシーマップまたはクラスマップ内に IP 分類（match ip dscp、IP ACL の match access-group）と非 IP 分類（match cos、または MAC ACL の match access-group）を設定できません。
- 出力ポリシー マップでは、異なるクラス マップで同じ分類基準（つまり、同じ match 修飾子および match 値）を使用できません。
- スイッチ上のクラス マップの最大数は、1024 です。

非 IP トラフィック用にレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**class-map [match-all | match-any]** *class-map-name*	クラスマップを作成し、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。デフォルトでは、クラス マップは定義されていません。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合

	コマンドまたはアクション	目的
		は、クラスマップ内のすべての一致条件と一致する必要があります。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • class-map-name には、クラス マップ名を指定します。 一致文が指定されない場合、デフォルトは match-all になります。 （注） match-all クラス マップでは、複数の分類基準（match 文）を設定できません。
ステップ 3	**match** {**access-group** *acl-index-or-name* | **cos** *cos-list* | **ip dscp** *dscp-list*}	トラフィックを分類するための一致条件を定義します。デフォルトでは、一致条件は定義されていません。 各クラスマップでサポートされる一致タイプおよび ACL は、それぞれ 1 つだけです。 • access-group *acl-index-or-name* を指定する場合は、ACL の番号または名前を指定します。アクセス グループの照合は、入力ポリシー マップでだけサポートされます。 • cos *cos-list* を指定する場合は、1 行に最大 4 つの CoS 値のリストを入力して、着信パケットと照合します。各値はスペースで区切ります。5 つ以上の CoS 値を照合する場合は、複数の *cos-list* 行を入力できます。指定できる範囲は 0 ～ 7 です。 • ip dscp *dscp-list* を指定する場合は、着信パケットと照合する最大 8 つの IPv4 DSCP 値を入力します。各値はスペースで区切ります。9 つ以上の DSCP 値を照合する場合は、複数の *dscp-list* 行を入力できます。指定できる数値範囲は 0 ～ 63 です。DSCP 値は、他の形式でも設定できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show class-map**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

既存のクラスマップまたは一致基準を削除するには、該当するコマンドの **no** 形式を使用します。

次に、アクセスリスト 103 を作成し、class1 という名前のクラスマップを設定する例を示します。class1 にはアクセス リスト 103 という一致条件が 1 つ設定されています。このクラス マップによって、任意のホストから任意の宛先へのトラフィック（DSCP 値は 10）が許可されます。

```
Switch(config)# access-list 103 permit any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

次に、DSCP 値が 10、11、および 12 である着信トラフィックと照合する、class2 という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map match-any class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

トラフィック ポリシーのインターフェイスへの適用

service-policy インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスにトラフィックポリシーを付加し、ポリシーが適用される方向（着信トラフィックの入力ポリシーマップ、または発信トラフィックの出力ポリシーマップ）を指定します。入力ポリシー マップおよび出力ポリシー マップは、別々の QoS 機能をサポートします。

サービス ポリシーは、物理ポートにだけ付加できます。ポートごとに、入力ポリシー マップおよび出力ポリシー マップをそれぞれ 1 つだけ付加できます。

（注） no policy-map コンフィギュレーション コマンドまたは no policy-map policy-map-name グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシーマップを削除する場合、ポリシーマップが消去されているインターフェイスの一覧を示す警告メッセージが表示されます。ポリシー マップは消去および削除されます。

次に例を示します。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet1/17
```

ポートに ポリシー マップを付加するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**interface** *interface-id*	ポリシー マップを適用するポートを指定し、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。指定できるインターフェイスは、物理ポートです。
ステップ 3	**service-policy {input | output}** *policy-map-name*	ポリシーマップの名前、およびそれが入力ポリシーマップか出力ポリシーマップのいずれかを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show policy-map interface** *[interface-id]*	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

次のタスク

ポリシー マップとポートの関連付けを解除するには、no service-policy {input | output} policy-map-name インターフェイス コンフィギュレーション コマンドを使用します。

入力ポリシー マップの設定

ポリシー マップでは、動作の実行対象トラフィック クラスおよびそのアクションを指定します。トラフィック クラスの一致基準に一致しないすべてのトラフィックは、デフォルト クラスに属します。スイッチに着信するトラフィックは、入力ポリシー マップにより規制されます。入力ポリシーマップでは、CoS、DSCP、または ACL を照合して、個別のポリシング、集約ポリシング、または CoS 値、DSCP 値へのマーキングを設定できます。

入力ポリシー マップの設定を行うときは、次の注意事項に従ってください。

- 1 つのポートに付加できる入力ポリシー マップは 1 つに限られます。
- スイッチ上に設定されるポリシー マップの最大数は 193 です。
- スイッチで設定可能なポリサープロファイルの合計数は 193 です。
- 各入力ポリシーマップの最大クラス数は、7 + class-default です。
- スイッチに付加できる入力ポリシー マップ数は、ハードウェア リソースのアベイラビリティにより制限されます。いずれかのハードウェア リソースの制限を超過する原因となる入力ポリシー マップを付加しようとすると、設定エラーになります。

- service-policy input インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに単一レベルのポリシーマップを付加すると、インターフェイスからポリシーを消去せずに、ポリシーを変更できます。分類基準、クラス、またはアクションの追加または削除、もしくは設定されたアクション（ポリサー、レート、マッピング、マーキングなど）のパラメータの変更を行えます。
- 802.1Q トンネル ポート上でトラフィックを分類するには、MAC ACL に基づくレイヤ 2 分類を含む入力ポリシー マップだけが使用できます。CoS または VLAN ID に基づくレイヤ 3 分類またはレイヤ 2 分類を含む入力ポリシーマップは、トンネルポート上でサポートされません。
- 入力ポリシーマップは、スケジューリングまたはキューイングではなく、ポリシングおよびマーキングをサポートします。入力ポリシーマップでは、bandwidth、priority、queue-limit、または shape average を設定できません。

次に、異なるタイプの入力ポリシー マップの設定方法を説明します。

個別のポリシングを含む入力ポリシー マップの設定

トラフィックの認定速度制限、認定バーストサイズ制限、およびトラフィッククラスの動作を定義するには、police ポリシーマップ クラス コンフィギュレーション コマンドを使用して、個別のポリサーを設定します。

個別のポリサーを設定する場合は、次の注意事項に従ってください。

- ポリシングは、入力ポリシー マップ上でだけサポートされます。
- スイッチ上では、最大 200 のポリサーがサポートされます
- ポリシングは入力ポートでのみサポートされます。
- スイッチ上のポリサー インスタンスの数は 1024 -（インターフェイス数 + 1）です。スイッチは、最大 200 のポリサープロファイルをサポートします。
- violate-action を設定しない場合、デフォルトで違反クラスが exceed-action と同じアクションに割り当てられます。

クラス マップの設定を行うときは、次の注意事項に従ってください。

- match-all クラス マップには、1 つの分類基準（match 文）しか指定できませんが、match-any クラス マップには複数の match 文を指定できます。
- match cos コマンドは、レイヤ 2 802.1Q トランク ポートでだけサポートされます。
- 入力ポリシーマップでは、同一ポリシーマップまたはクラスマップ内に IP 分類（match ip dscp、IP ACL の match access-group）と非 IP 分類（match cos、または MAC ACL の match access-group）を設定できません。
- 出力ポリシー マップでは、異なるクラス マップで同じ分類基準（つまり、同じ match 修飾子および match 値）を使用できません。
- スイッチ上のクラス マップの最大数は、1024 です。

（注） 次の手順で、ステップ 5、6、または 7 を実行します。また、ステップ 8 またはステップ 9 を実行します。

個別のポリシングを含む入力ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**policy-map** *policy-map-name*	ポリシーマップ名を入力することによってポリシーマップを作成し、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。デフォルトでは、クラス マップは定義されていません。
ステップ 3	**class** *{class-map-name | class-default}*	クラスマップ名またはすべての未分類のパケットを照合する class-default を入力して、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。 クラスマップ名を入力する場合は、class-map グローバル コンフィギュレーション コマンドを使用してクラスマップを作成済みである必要があります。
ステップ 4	**police** {*rate-bps* | **cir** *cir-bps*} [*burst-bytes* |**bc** *burst-bytes*]	トラフィック クラスのポリサーを定義します。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。指定できる範囲は 64000 ～ 1000000000 です。 • cir *cir-bps* には、設定情報レート（CIR）を bps で指定します。指定できる範囲は 64000 ～ 1000000000 です。 • *burst-bytes*（任意）には、標準バーストサイズをバイト単位で指定します。指定できる範囲は 64000 ～ 1000000000 です。 • bc *burst-bytes*（任意）には、適合バースト（bc）または許容バーストバイト数を指定します。指定できる範囲は 64000 ～ 100000000 です。

	コマンドまたはアクション	目的
ステップ 5	**conform-action [drop | transmit]**	（任意）CIR に適合するパケットで実行するアクションを入力します。
ステップ 6	**exceed-action cos** {*cos_value* | **cos** [**table**] | **dscp** [**table**]}	（任意）CIR に適合するパケットで実行するアクションを入力します。 • cos *cos_value* には、分類されたトラフィックに割り当てる新しい CoS 値を入力します。指定できる範囲は 0 ～ 7 です。
ステップ 7	**exceed-action [ip] dscp** {*dscp_value* | **cos** [**table**] | **dscp** [**table**]}	（任意）CIR に適合するパケットで実行するアクションを入力します。 • [ip] dscp *dscp_value* を指定する場合は、分類されたトラフィックに割り当てる新しい DSACP 値を入力します。指定できる範囲は 0 ～ 63 です。 （注） police コマンドのあとに、単一の exceed-action をコマンドストリングの一部として入力できます。または、police コマンドのあとに Enter キーを押して、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でき、ここで複数のアクションを入力できるようになります。ポリシーマップクラスポリシング コンフィギュレーション モードでは、実行するアクションを入力する必要があります。 （注） コマンドのキーワードとして、exceed-action drop を明示的に設定する場合は、ポリシーマップクラスポリシングコンフィギュレーションモードを開始し、no exceed-action drop コマンドを入力して以前に設定された超過アクションを削除する必要があります。
ステップ 8	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 9	**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。

	コマンドまたはアクション	目的
ステップ 10	**interface** *interface-id*	ポリシーを付加するインターフェイスで、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。 .
ステップ 11	**service-policy input** *policy-map-name*	入力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。
ステップ 12	**end**	特権 EXEC モードを終了します。
ステップ 13	**show policy-map** *[policy-map-name* [**class** *class-map-name*]]	入力内容を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

no policy-map コンフィギュレーション コマンドまたは no policy-map policy-map-name グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシーマップを削除する場合、ポリシーマップが消去されているインターフェイスの一覧を示す警告メッセージが表示されます。ポリシー マップは消去および削除されます。次に例を示します。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet1/17
```

クラスで複数の動作を設定する場合、ポリシーマップ クラス ポリシング コンフィギュレーション モードで複数の適合または超過の各アクションのエントリ適合、超過、または違反の各アクションのエントリを入力する必要があります（次の例を参照）。

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 500000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-cos-transmit 2
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

個別の 2-rate、3-color ポリシングを含む入力ポリシーマップの設定

個別の 2-rate、3-color ポリシングを含む入力ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

（注） 次の手順で、ステップ 5、6、または 7 を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**policy-map** *policy-map-name*	ポリシーマップ名を入力することによってポリシーマップを作成し、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。デフォルトでは、クラス マップは定義されていません。
ステップ 3	**class** {*class-map-name* | **class-default**}	クラスマップ名またはすべての未分類のパケットを照合する class-default を入力して、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。 クラスマップ名を入力する場合は、class-map グローバル コンフィギュレーション コマンドを使用してクラスマップを作成済みである必要があります。
ステップ 4	**police**{*rate-bps* | **cir** {*cir-bps*} [*burst-bytes*] [**bc** [*conform-burst*] [**pir** *pir-bps* [**be** *peak-burst*]]	トラフィックのクラスの1つまたは2つのレート、認定情報レート（CIR）および最大情報レート（PIR）を使用してポリサーを定義します。デフォルトでは、ポリサーは定義されていません。 • *rate-bps* には、平均トラフィックレートをビット/秒（bps）で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • cir *cir-bps* には、bc トークンバケットが更新される CIR を bps で指定します。指定できる範囲は 8000 ～ 1000000000 です。 • *burst-bytes*（任意）には、標準バーストサイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • bc *burst-bytes*（任意）には、適合バースト（bc）または許容バーストバイト数を指定します。指定できる範囲は 64000 ～ 100000000 です。 •（任意）bc *conform-burst* には、ポリシングの bc トークンバケットで使用される認定バーストを指定します。指定できる範囲は、8000 ～ 1000000 バイトです。 •（任意）pir *pir-bps* には、ポリシングの be トークンバケットが更新される最大情報レートを指

	コマンドまたはアクション	目的
		定します。指定できる範囲は、8000 ～ 1000000000 b/s です。pir *pir-bps* を入力しない場合、ポリサーは 1-rate、2-color ポリサーとして設定されます。 • be *peak-burst* には、be トークンバケットで使用するピークバーストサイズを指定します。指定できる範囲は 8000 ～ 1000000 バイトです。デフォルト値は、ユーザ設定に基づき内部で計算されます。
ステップ 5	**conform-action [drop | transmit]**	（任意）CIR に適合するパケットで実行するアクションを入力します。
ステップ 6	**exceed-action [drop | set-cos-transmit** {*cos_value* | [**cos**]} | **set-dscp-transmit** {*dscp_value* | [**dscp**]}	
ステップ 7	**violate-action [drop | transmit]**	
ステップ 8	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 9	**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 10	**interface** *interface-id*	ポリシーを付加するインターフェイスで、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。 .
ステップ 11	**service-policy input** *policy-map-name*	入力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。
ステップ 12	**end**	特権 EXEC モードを終了します。
ステップ 13	**show policy-map** [*policy-map-name* | **interface**]	入力内容を確認します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

既存のポリシーマップ、クラスマップ、またはポリサーを削除するには、該当するコマンドの no 形式を使用します。

次に、ポリシーマップ コンフィギュレーション モードを使用して 2-rate、3-color ポリシングを設定する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit exceed-action
 set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

次に、ポリシーマップ クラス ポリシング コンフィギュレーション モードで同じ設定を作成する例を示します。

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

次に、CoS 値が 4 のトラフィック分類を作成して、ポリシーマップを作成し、入力ポートに付加する例を示します。平均トラフィック レートは、10000000 b/s に制限され、バースト サイズは 10000 バイトです。

```
Switch(config)# class-map video-class
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police cir 10000000 bc 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit
```

次に、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 モードを使用して、複数の超過アクションを設定する例を示します。このポリシー マップでは、CIR を 23000 bps に、適合バースト サイズを 10000 バイトに設定します。このポリシーマップには、適合アクションおよび超過アクション（DSCP 用およびレイヤ 2 CoS 用）が含まれます。

```
Switch(config)# class-map cos-set-1
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 48
Switch(config-pmap-c-police)# exceed-action set-cos-transmit 5
Switch(config-pmap-c-police)# exit
```

```
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy input map1
Switch(config-if)# exit
```

マーキングを含む入力ポリシー マップの設定

特定のクラスに属するトラフィックの属性を設定または変更するには、set ポリシーマップ クラス コンフィギュレーション コマンドを使用します。

トラフィックをマーキングする入力ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**policy-map** *policy-map-name*	ポリシーマップ名を入力することによってポリシーマップを作成し、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 3	**class** {*class-map-name* | **class-default}**	クラスマップ名またはすべての未分類のパケットを照合する class-default を入力して、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。クラスマップ名を入力する場合は、class-map グローバル コンフィギュレーション コマンドを使用してクラスマップを作成済みである必要があります。
ステップ 4	次のいずれかを選択してください。 • **set cos** {*cos_value*} • **set [ip] dscp** *dscp_value*	パケットに新しい値を設定して、トラフィックにマーキングします。 • cos *cos_value* には、分類されたトラフィックに割り当てる新しい CoS 値を入力します。指定できる範囲は 0 ～ 7 です。 • [ip] dscp *dscp_value* を指定する場合は、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。
ステップ 5	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 6	**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。

	コマンドまたはアクション	目的
ステップ 7	**interface** *interface-id*	ポリシーを付加するインターフェイスで、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。
ステップ 8	**service-policy input** *policy-map-name*	入力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	入力内容を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

ポリシーマップを削除する場合、または割り当てられたCoS値またはDSCP値を削除する場合は、該当するコマンドの no 形式を使用します。

次に、ポリシーマップを使用してパケットをマーキングする例を示します。最初のマーキング（set コマンド）は、クラス AF31 ～ AF33 によって一致しなかったすべてのトラフィックを照合する QoS デフォルトクラスマップに適用され、すべてのトラフィックの IP DSCP 値を 1 に設定します。2 番目のマーキングは、クラス AF31 ～ AF33 のトラフィックの IP DSCP を 3 に設定します。

```
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface Gi1/3
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

次の例では、ポリシーマップのクラスマップが音声、データ、およびビデオトラフィックの一致基準を指定して、ポリシーマップが各トラフィックタイプの入力ポリシングに対するアクションを設定します。

```
Switch(config)# policy-map policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action transmit
Switch(config-pmap-c)# exceed-action set-cos-transmit 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-1 data
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
```

```
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# exit
```

出力ポリシー マップの設定

出力ポリシーマップは、スイッチから発信されるパケットの輻輳回避、キューイング、およびスケジューリングを管理するのに使用します。スイッチには、4 つの出力キューがあり、そのキュー トラフィックを制御するには、出力ポリシー マップを使用します。これらのキューでは、シェーピング、キュー制限、および帯域幅を設定します。高いプライオリティ（クラスベース プライオリティ キューイング）を使用できます。クラスベース プライオリティ キューイングにポリシング付きプライオリティが設定されている場合以外は、ポリシングは出力ポリシーマップでサポートされません。出力ポリシーマップの分類基準は、CoS または DSCP の照合です。

物理ポートに出力ポリシー マップを設定する際は、次の注意事項に従ってください。

- 出力ポリシーマップには、最大 8 つのクラス（クラス class-default を含む）を含めることができます。
- 出力ポリシーマップのクラスマップは、アクセスグループを使用できません。
- 出力ポリシーマップごとに各クラスで異なるアクションを設定できますが、すべての出力ポリシー マップで同じクラス設定を使用する必要があります。
- 出力ポリシーマップのクラス class-default にはクラスベース プライオリティ キューイングを設定できません。
- 出力ポリシー マップでは、プライオリティ キューイングが設定されていない限り、クラスのデフォルトには、ポート上の未設定の帯域幅に等しい最小帯域幅保証を受信します。
- 設定済みアクションのパラメータ（レート、パーセンテージなど）だけを変更したり、またはインターフェイスにポリシーマップが付加されている場合にクラスマップの分類基準を追加、削除する場合は、まず service-policy インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスに出力ポリシーマップを付加します。クラスまたはアクションを追加、削除するには、すべてのインターフェイスからポリシーマップを消去して、変更し、再度インターフェイスに付加する必要があります。

ポリシーマップで 3 つのクラスが必要となる予定がある場合は、その時点では 3 つすべてを使用しないときでも、ポリシーマップの作成時に 3 つのクラスを定義する必要があります。インターフェイスにポリシー マップを付加したあとで、ポリシー マップにクラスを追加できません。

- ポート帯域幅に依存する出力ポリシーマップが適用されている場合、固定ポート速度で動作するようにインターフェイスを設定することを推奨します。ポート速度を修正し、速度の自動ネゴシエーションを削除するには、interface level コマンドを使用します。デュプレックスのネゴシエーションを終了できます。速度の自動ネゴシエーションが設定されているポートで出力ポリシーマップが設定されていて、その速度が出力ポリシーマップを無効にする値に自動ネゴシエーションされた場合、ポートは error-disabled ステートになります。

- 1 つのポートに付加できる出力ポリシー マップは、1 つに限られます。
- スイッチ上に設定されるポリシー マップの最大数は 256 です。

ここでは、異なるタイプの出力ポリシー マップの設定について説明します。

CBWFQ を含む出力ポリシー マップの設定

クラスベース均等化キューイング（CBWFQ）を設定するには、bandwidth ポリシーマップ クラス コンフィギュレーション コマンドを使用します。CBWFQ では、ポートで使用可能な総帯域幅の一部を割り当てることにより、キューの相対的な優先順位を設定します。

CBWFQ の設定時は、次の注意事項に従ってください。

ポート帯域幅に依存する出力ポリシーマップが適用されている場合、固定ポート速度で動作するようにインターフェイスを設定することを推奨します。ポート速度を修正し、速度の自動ネゴシエーションを削除するには、interface level コマンドを使用します。デュプレックスのネゴシエーションを終了できます。速度の自動ネゴシエーションが設定されているポートで出力ポリシーマップが設定されていて、その速度が出力ポリシーマップを無効にする値に自動ネゴシエーションされた場合、ポートは error-disabled ステートになります。

最小帯域幅をビットレートまたはパーセンテージで指定することにより、CBWFQ を使用してトラフィック クラスに割り当てられる帯域幅を制御するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**policy-map** *policy-map-name*	ポリシーマップ名を入力することによってポリシーマップを作成し、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 3	**class** *{class-map-name* | **class-default}**	子クラスマップ名またはすべての未分類のパケットを照合する class-default を入力して、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。
ステップ 4	**bandwidth** *{rate* | **percent** *value* | **remaining** *value}*	ポリシー マップ クラスに出力帯域幅制限を設定します。 • 帯域幅を kps で設定するには、rate を入力します。指定できる範囲は 64000 ～ 1000000000 です。

	コマンドまたはアクション	目的
		• 総帯域幅のパーセンテージとして帯域幅を設定するには、percent value を入力します。指定できる範囲は 1 ～ 100% です。 • 残りの帯域幅のパーセンテージとして帯域幅を設定するには、remaining percent value を入力します。指定できる範囲は 1 ～ 100% です。このキーワードは、出力ポリシー マップ内の他のクラスに完全プライオリティ（ポリシングなしのプライオリティ）が設定されている場合に限り有効です。 出力ポリシー内の各帯域幅設定では、同一の単位（絶対レートまたはパーセンテージ）を指定する必要があります。合計保証帯域幅は、使用可能な合計レートを超過できません。
ステップ 5	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 6	**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 7	**interface** *interface-id*	ポリシーを付加するインターフェイスで、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。
ステップ 8	**service-policy output** *policy-map-name*	出力インターフェイスにポリシーマップ（ステップ 2 で作成）を付加します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	入力内容を確認します。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

作成された出力ポリシー マップを、出力ポートに付加します。

既存のポリシー マップ、クラス マップ、または帯域幅設定を削除するには、該当するコマンドの no 形式を使用します。

Note：no policy-map コンフィギュレーション コマンドまたは no policy-map policy-map-name グローバル コンフィギュレーション コマンドを入力して、インターフェイスに付加されたポリシーマップを削除する場合、ポリシーマップが消去されているインターフェイスの一覧を示す

警告メッセージが表示されます。ポリシーマップは消去および削除されます。次に例を示します。

```
Warning: Detaching Policy test1 from Interface GigabitEthernet1/17
```

次に、クラス マップで定義されたトラフィック クラスに、使用可能な合計帯域幅の 25% を割り当てて、キューの優先順位を設定する例を示します。

```
Switch(config)# policy-map gold_policy
Switch(config-pmap)# class out_class-1
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# service-policy output gold_policy
Switch(config-if)# exit
```

ポート シェーピングを含む出力ポリシー マップの設定

ポート シェーピングは、インターフェイスから発信されるすべてのトラフィックに適用されます。shape average コマンドによりポートの最大帯域幅が指定されている場合は、クラスのデフォルトだけを使用するポリシーマップを使用します。

ポート シェーピングを使用して、トラフィック クラスの最大許容平均速度を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**policy-map** *policy-map-name*	ポリシーマップ名を入力することによってポリシーマップを作成し、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 3	**class class-default**	デフォルト クラスのポリシーマップ 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 4	**shape average** *target bps*	平均クラスベース シェーピング速度を指定します。target bps には、平均ビットレートを bps で指定します。指定できる範囲は 64000 ～ 1000000000 です。
ステップ 5	**interface** *interface-id*	ポリシーを付加するインターフェイスで、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。
ステップ 6	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。

	コマンドまたはアクション	目的
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	入力内容を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

既存の階層型ポリシーマップ、ポートシェーピングの設定を削除したり、または階層型ポリシーマップからポリシーマップを削除するには、該当するコマンドの no 形式を使用します。

次に、前述の例で設定された out-policy ポリシー マップに基づいて割り当てられ、ポートを 900 Mbps にシェーピングする階層型ポリシー マップを設定して、ポート シェーピングを設定する例を示します。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

クラスベース プライオリティ キューイングを含む出力ポリシー マップの設定

priority ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、特定のトラフィッククラスで優先処理が行われるよう保証できます。完全プライオリティ キューイングの場合、プライオリティ キューは常に処理されます。キュー内のすべてのパケットは、キューが空になるまでスケジューリングされ、送信されます。プライオリティ キューを過剰に使用すると、他のキューのパケットが遅延して、不必要な輻輳が発生する可能性があります。

完全プライオリティ キューイング（ポリシングなしのプライオリティ）または無条件のプライオリティ ポリサー（ポリシングありのプライオリティ）を設定できます。プライオリティ キューイングの設定時は、次の注意事項に従ってください。

- priority コマンドは、スイッチ上で付加されたすべての出力ポリシーの単一の一意のクラスに関連付けられます。
- トラフィッククラスをプライオリティ キューとして設定する場合、同一クラスのその他のキューイング アクションとして設定できるのは、police および queue-limit だけです。同一クラスのプライオリティ キューを使用して、bandwidth または shape average を設定できません。
- priority コマンドは、出力ポリシーマップの class-default に関連付けられません。

- トラフィッククラスにポリシングなしのプライオリティキューイングを設定する場合、余剰の帯域幅を割り当てるには、bandwidth remaining percent ポリシーマップ クラス コンフィギュレーション コマンドを使用して、他のキューで共有を設定するしかありません。このコマンドは、割り当てられた帯域幅を保証しませんが、分散レートは保証されます。

完全プライオリティ キューを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**class-map** *class-map-name*	3 つの出力キューのクラスを作成します。各クラスの一致条件での分類を開始します。
ステップ 3	**policy-map** *policy-map-name*	ポリシーマップ名を入力することによってポリシーマップを作成し、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 4	**class** *class-map-name*	プライオリティクラスの名前（class-map グローバル コンフィギュレーション コマンドを使用して作成）を入力して、プライオリティクラスでポリシーマップ 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	**priority**	このクラスに完全スケジューリング プライオリティを設定します。 （注） priority コマンドに関連付けられるのは、スイッチ上の 1 つの一意のクラスマップだけです。その他のキューイングアクション（bandwidth または shape average）と、プライオリティを同時に設定できません。
ステップ 6	**exit**	プライオリティ クラスのポリシーマップ 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	**class** *class-map-name*	非プライオリティ クラスの名前を入力して、そのクラスのポリシーマップ 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 8	**bandwidth remaining percent** *value*	ポリシー マップ クラスの出力帯域幅制限を、残りの帯域幅のパーセンテージとして設定します。指定できる範囲は 1 ～ 100% です。

	コマンドまたはアクション	目的
ステップ 9	**exit**	クラスのポリシーマップ 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**	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 11	**interface** *interface-id*	ポリシーを付加するインターフェイスで、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。
ステップ 12	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 3 で作成）を付加します。
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show policy-map**	入力内容を確認します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

作成された出力ポリシー マップを、出力ポートに付加します。

既存のポリシーマップまたはクラスマップの削除、プライオリティクラスの完全プライオリティキューイングまたは他のクラスへの帯域幅設定の解除を行うには、該当するコマンドの no 形式を使用します。

次に、クラス out-class1 を完全プライオリティキューとして設定し、このクラスのすべてのパケットが他のトラフィッククラスより先に送信される例を示します。他のトラフィックキューでは、out-class2 は残りの帯域幅の 50%、out-class3 は残りの帯域幅の 20% を取得するように設定されます。クラス class-default は、保証なしで、残りの 30% を取得します。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

WTD を含む出力ポリシー マップの設定

WTD では、トラフィック クラスに関連付けられたキュー サイズ（バッファ サイズ）を調整します。WTD は、queue-limit ポリシーマップ クラス コンフィギュレーション コマンドにより設定されます。

WTD を設定する場合は、次の注意事項に従ってください。

- queue-limit コマンドによる WTD の設定は、最初にスケジュールアクション（bandwidth、shape average、または priority など）を設定する場合にだけサポートされます。class-default で queue-limit を設定する場合は、例外です。
- ポート数に応じた数の出力ポリシーマップを設定および付加できますが、インターフェースへの出力ポリシーマップに一度に付加できる一意のキュー制限の設定は、3 つのみです。複数の出力ポリシーマップで同じキュー制限設定を使用できます。クラスのキュー制限値の 1 つを変更すると、新たな固有のキュー制限設定が作成されます。
- 出力ポリシーマップでクラスにキュー制限を設定する場合、他のすべての出力ポリシーマップでは、クラスに対して同一の一致基準を使用する必要があります。キュー制限のしきい値に限り、異なる値を設定できます。たとえば、ポリシーマップ PM1 の dscp 30 および dscp 50 に、class A のキュー制限のしきい値が設定されていて、ポリシーマップ PM2 で class A のキュー制限を設定する場合、dscp 30 および dscp 50 を修飾子として使用する必要があります。dscp 20 および dscp 40 は、使用できません。別のしきい値を設定できますが、これにより、新たなキュー制限設定が作成されます。
- queue-limit コマンドを使用して、クラスのキューしきい値を設定する場合、修飾子を設定せずに WTD しきい値をキューの制限しきい値以下にする必要があります。修飾子なしで設定されたキュー サイズは、修飾子を使用して設定されたいずれのキュー サイズよりも大きくする必要があります。
- queue-limit コマンドでは、WTD 修飾子（cos、dscp）に一意のしきい値を 1 つのみ設定できます。ただし、これらのしきい値にマッピングできる修飾子の数に制限はありません。修飾子を指定しないで queue-limit コマンドを使用することにより、最大キューを設定する 2 番目の一意のしきい値を設定できます。
- 出力ポリシーマップで一意のクラスにキュー制限を設定した場合、他のすべての出力ポリシーマップでは、修飾子タイプおよび修飾値に同じ形式を使用する必要があります。キュー制限しきい値だけ、異なる値を設定できます。たとえば、ポリシーマップ 1 の dscp 30 および dscp 50 に、クラス A のキュー制限のしきい値を設定して、ポリシーマップ 2 でクラス A のキュー制限を設定する場合、dscp 30 および dscp 50 を修飾子として使用する必要があります。dscp 20 および dscp 40 は、使用できません。別のしきい値を設定できますが、これにより、新しいキュー制限設定が作成されます。

WTD を使用してトラフィック クラスのキュー サイズを調整するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**policy-map** *policy-map-name*	ポリシーマップ名を入力することによってポリシーマップを作成し、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 3	**class** {*class-map-name* | **class-default**}	デフォルトクラスのポリシーマップ 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 4	**bandwidth** {*rate* | **percent** *value* | **remaining percent** *value*}	トラフィック クラスのスケジューリング アクションを設定します。
ステップ 5	**queue-limit** [**cos** *value* | **dscp** *value*] *number-of-packets* [**packets**]	トラフィック クラスのキューサイズを指定します。 • （任意）cos value には、CoS 値を指定します。範囲は 0 ～ 7 です。 • （任意）dscp value には、DSCP 値を指定します。指定できる範囲は 0 ～ 63 です。 • number-of-packets には、WTD の最小しきい値を設定します。指定できる範囲は、16 の倍数で 16 ～ 544 です。この場合、各パケットは 256 バイトの固定単位になります。 （注） 最適なパフォーマンスを実現するため、キュー制限を 272 以下に設定することを推奨します。 値は、デフォルトでパケットに指定されますが、キーワード packets は任意です。 （注） 複数の出力ポリシー マップで同じキュー制限設定を使用できます。ただし、これらのポリシー マップには、固有のキュー制限を 3 つしか設定できません。
ステップ 6	**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 7	**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。

	コマンドまたはアクション	目的
ステップ 8	**interface** *interface-id*	ポリシーを付加するインターフェイスで、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。
ステップ 9	**service-policy output** *policy-map-name*	出力インターフェイスにポリシー マップ（ステップ 2 で作成）を付加します。 （注） 4 つめのキュー制限設定を含む出力ポリシー マップを付加しようとすると、エラー メッセージが表示され、付加は許可されません。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]	入力内容を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次のタスク

作成された出力ポリシー マップを、出力ポートに付加します。

既存のポリシーマップ、クラスマップ、または WTD 設定を削除するには、該当するコマンドの no 形式を使用します。

次に、指定された帯域幅およびキュー サイズが設定されたポリシー マップの例を示します。DSCP 30 ではないトラフィックには、112 パケットのキュー制限が割り当てられます。DSCP 値が 30 のトラフィックには、48 パケットのキュー制限が割り当てられます。クラストラフィックに属していないすべてのトラフィックは、class-default に分類され、使用可能な合計帯域幅の 10% が、256 パケットのラージキューサイズで設定されます。

```
Switch(config)# policy-map gold-policy
Switch(config-pmap)# class traffic
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# queue-limit dscp 30 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 256
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# service-policy output gold-policy
Switch(config-if)# exit
```

次に、class A が DSCP 値およびポリシー マップ、PM1 に一致するよう設定する例を示します。30、40、50、および 60 の DSCP 値は、112 パケットの最大しきい値にマッピングされます。

```
Switch(config)# class-map match-any classA
Switch(config-cmap)# match ip dscp 30 40 50 60
Switch(config-cmap)# exit
Switch(config)# policy-map PM1
Switch(config-pmap)# class classA
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# service-policy output PM1
Switch(config-if)# exit
```

次に、out-class1、out-class2、out-class3、および class-default がそれぞれ最低 40、20、10、および 10% のトラフィック帯域幅を取得するように、帯域幅およびキュー制限を設定する例を示します。対応するキューサイズは、48、32、16、および 272（256 バイト）パケットに設定されます。

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

QoS 情報の表示

QoS 情報を表示するには、 表に示す特権 EXEC コマンドを 1 つまたは複数組み合わせて使用します。

ここでは、次の内容について説明します。

- QoS 統計情報 （55 ページ）
- 制約事項と制限 （20 ページ）

標準 QoS 情報を表示するためのコマンド

コマンド	目的
show class-map [class-map-name]	すべてのクラス マップまたは指定されたクラス マップの QoS クラスマップ情報を表示します。
show policer aggregate [aggregate-policer-name]	すべての集約ポリサーまたは指定された集約ポリサーの情報を表示します。
show policy-map [policy-map-name | interface [interface-id] [input | output] [class class-name]]	指定されたポリシー マップ名、インターフェイス、入力/出力ポリシー マップ、またはポリシー マップ クラスの QoS ポリシー マップ情報を表示します。
show running-config	設定済みのクラス マップ、ポリシー マップ、テーブル マップ、および集約ポリサーを表示します。

インターフェイス上の両方向で完全パス QoS をテストするには、ethernet loopback facility インターフェイス コンフィギュレーション コマンドを入力してイーサネット ターミナル ループバックを設定できます。ターミナル ループバック モードでは、ポートは、リンクがアップに見える状態になりますが、実際はリンクはダウンになっており、パケットは送信されません。ポートの設定変更は、ループバックされているトラフィックに即座に影響を与えます。

QoS 統計情報

QoS 入力および出力ポリシー マップの統計情報を表示する方法は、いくつかあります。

入力ポリシーマップの場合、**show policy-map interface [interface-id]** 特権 EXEC コマンドを使用してクラス単位、ポリサー単位の適合および超過統計情報を表示できます。ポリサーの適合統計情報は設定済みポリサープロファイルに適合するパケット数で、ポリサーの超過統計情報は設定済みポリサープロファイルを超過したパケット数です。スイッチでは、クラス単位の分類統計情報をサポートしませんが、クラスの回線速度でポリシングを設定することによりこれらの統計情報を決定できます。この場合、設定済みポリサープロファイルを超過するパケットはありません。また、ポリサーの適合統計情報はクラスの分類統計情報に等しくなります。

出力ポリシーマップの場合、**show policy-map interface [interface-id]** コマンドを使用して、指定されたクラスに一致する合計パケット数を示すクラス単位の分類統計情報を表示できます。このカウントには、指定のクラスで送信および廃棄された合計パケット数も含まれます。クラス単位のテール ドロップ統計情報を表示する場合も、同じコマンドが使用できます。

キューおよびパケット処理の詳細については、CLI コマンド **show platform hardware qos asic 0 port [port id]** を使用してください。

ポート ID は、CLI **show platform pm port-map** から取得できます。

例：

```
Switch#show platform pm port-map
interface gid gpn asic slot unit gpn-idb
------------------------------------------
Te1/1 1 1 0/25 1 1 Yes
Te1/2 2 2 0/27 1 2 Yes
Gi1/3 3 3 0/2 1 3 Yes
```

```
Gi1/4 4 4 0/3 1 4 Yes
Gi1/5 5 5 0/0 1 5 Yes
Gi1/6 6 6 0/1 1 6 Yes
Gi1/7 7 7 0/6 1 7 Yes
Gi1/8 8 8 0/7 1 8 Yes
Gi1/9 9 9 0/4 1 9 Yes
Gi1/10 10 10 0/5 1 10 Yes
Gi2/1 11 11 0/10 2 1 Yes
Gi2/2 12 12 0/11 2 2 Yes
Gi2/3 13 13 0/8 2 3 Yes
Gi2/4 14 14 0/9 2 4 Yes
Gi2/5 15 15 0/14 2 5 Yes
Gi2/6 16 16 0/15 2 6 Yes
Gi2/7 17 17 0/12 2 7 Yes
Gi2/8 18 18 0/13 2 8 Yes
Gi2/9 19 19 0/18 2 9 Yes
Gi2/10 20 20 0/19 2 10 Yes
Gi2/11 21 21 0/16 2 11 Yes
Gi2/12 22 22 0/17 2 12 Yes
Gi2/13 23 23 0/22 2 13 Yes
Gi2/14 24 24 0/23 2 14 Yes
Gi2/15 25 25 0/20 2 15 Yes
Gi2/16 26 26 0/21 2 16 Yes
Switch#
```

```
Switch#show platform hardware qos asic 0 port 1
Dumping QoS settings for port 1Port | Trust | Modify | Modify | Default | Default| Mode
 | DSCP | UP | QosProfile | UP---- |------ | ------ | ------ | ---------- | -------1 |
L2+L3 | No | No | 65 | 0Queue[0]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0
Thresh[2]:22 Drops[2]:0Queue[1]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
 Drops[2]:0Queue[2]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
Drops[2]:0Queue[3]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
Drops[2]:0Queue[4]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
Drops[2]:0Queue[5]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:68
Drops[2]:99932Queue[6]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:196
Drops[2]:99932Queue[7]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:104455
Drops[2]:0
Dumping Ingress QoS stats 0

class [0]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0

class [1]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0

class [2]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0

class [3]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0

class [4]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0
```

```
class [5]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0

class [6]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0

class [7]:    in_class_policer:
    redCntr_packets 0
    yellowCntr_packets 0
    greenCntr_packets 0
Switch#
```

翻訳について
このドキュメントは、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。