CHAPTER 40

Quality of Service の設定

この章では、標準の Quality of Service（QoS）コマンドまたは自動 QoS（auto-QoS）コマンドのいずれかを使用して、Catalyst 4500 シリーズ スイッチ上で QoS を設定する方法について説明します。ここでは、VLAN だけでなくさまざまな種類のインターフェイス（アクセス、レイヤ 2 トランク、レイヤ 3 ルーティング、EtherChannel）での QoS 設定を指定する方法を説明します。また、所定のインターフェイスの異なる VLAN 上で異なる QoS（per-Port per-VLAN QoS（PVQoS））を設定する方法についても説明します。

スイッチは、Modular QoS CLI（*MQC*）と呼ばれる QoS コンフィギュレーション モデルをサポートします。QoS が設定されているスーパーバイザ エンジンの該当する設定セクションを参照してください。MQC の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.3*』の「Modular Quality of Service Command-Line Interface」の項を参照してください。

この章で説明する内容は、次のとおりです。

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で Cisco IOS コマンド リファレンスと関連資料を参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

QoS の概要

ネットワークは通常、*ベスト エフォート型*の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、正しいタイミングで配信される可能性も同じです。輻輳が発生すると、ドロップされる可能性はすべてのトラフィックで同じです。

QoS は、ネットワーク トラフィック（ユニキャストおよびマルチキャスト）を選択して、トラフィックの相対的な重要度に従ってプライオリティを与え、プライオリティ ベースの処理を実行して、輻輳を回避します。QoS はさらに、ネットワーク トラフィックが使用する帯域幅を制限します。QoS を実装すると、ネットワーク パフォーマンスが予測可能になり、帯域幅をより効率的に利用できます。

ここでは、次の内容について説明します。

プライオリティ

QoS の実装は、DiffServ アーキテクチャに基づきます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。この分類は、IP パケット ヘッダーで伝送され、現在ほとんど使用されていない IP タイプ オブ サービス（ToS）フィールドの 6 ビットを使用して分類（クラス）情報が伝送されます。分類情報はレイヤ 2 フレームでも伝達できます。レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて説明します（図 40-1 を参照）。

- レイヤ 2 フレーム内のプライオリティ値：

  レイヤ 2 の ISL（スイッチ間リンク）フレーム ヘッダーには、下位 3 ビットで IEEE 802.1p サービス クラス（CoS）値を伝達する 1 バイトのユーザ フィールドがあります。レイヤ 2 ISL トランクとして設定されたインターフェイス上では、すべてのトラフィックが ISL フレームを使用します。

  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 値が伝達されます。レイヤ 2 802.1Q トランクとして設定されたインターフェイスでは、ネイティブ VLAN 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。

  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（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

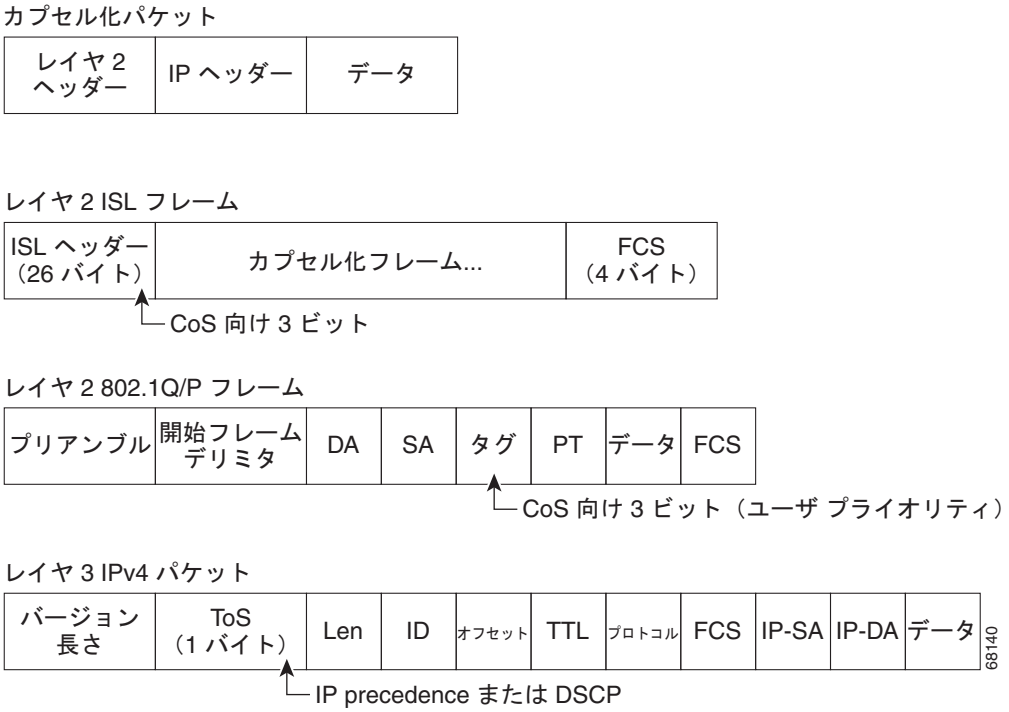
- レイヤ 3 パケットのプライオリティ ビット：

  レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point（DSCP）値のいずれかを伝送できます。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値も使用できます。

  IP precedence 値の範囲は 0 ～ 7 です。

  DSCP 値の範囲は 0 ～ 63 です。

図 40-1　　フレームおよびパケットにおける QoS 分類レイヤ



インターネット上のすべてのスイッチおよびルータはクラス情報に基づき、同じクラス情報を持ったパケットに対しては転送上、同じ取り扱いを行い、クラス情報が異なるパケットに対しては異なった取り扱いを行います。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンド ホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳しい検証は、コア スイッチおよびルータが過負荷にならないように、ネットワーク エッジに近い位置で行われることが前提になります。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のあるホップ単位動作をさせることによって、エンドツーエンドの QoS ソリューションを構築できます。

ネットワークに QoS を実装する作業は、インターネットワーキング装置が提供する QoS 機能、ネットワーク上のトラフィック タイプおよびトラフィック パターン、着信トラフィックおよび発信トラフィックに対して適用すべき制御の粒度に応じて、簡単なものにも複雑なものにもなります。

QoS の用語

QoS 機能についての説明では、次の用語が使用されます。

- *パケット*：レイヤ 3 でトラフィックを伝送します。
- *フレーム*：レイヤ 2 でトラフィックを伝送します。レイヤ 2 フレームは、レイヤ 3 パケットを伝送します。
- *ラベル*：レイヤ 3 パケットおよびレイヤ 2 フレームで伝送されるプライオリティ値です。
  - レイヤ 2 CoS 値：範囲は 0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

    レイヤ 2 ISL フレーム ヘッダーには、1 バイトのユーザ フィールド（LSB 3 ビットで IEEE 802.1p CoS 値を伝送）があります。

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、MSB 3 ビット（ユーザ プライオリティ ビット）で CoS 値が伝送されます。

その他のフレーム タイプでは、レイヤ 2 CoS 値は伝送されません。

（注）　レイヤ 2 ISL トランクとして設定されたインターフェイスでは、すべてのトラフィックが ISL フレームに収められます。レイヤ 2 802.1Q トランクとして設定されたインターフェイスでは、ネイティブ VLAN のトラフィックを除き、すべてのトラフィックが 802.1 Q フレームに収められます。

- レイヤ 3 IP precedence 値：IPv4 の仕様では、1 バイトの ToS フィールドの MSB 3 ビットを IP precedence と定義しています。IP precedence 値の範囲は 0（低プライオリティ）～ 7（高プライオリティ）です。
- レイヤ 3 DSCP 値：Internet Engineering Tasks Force（IETF; インターネット技術特別調査委員会）は、1 バイトの IP ToS フィールドのうち MSB 6 ビットを DSCP と定義しています。特定の DSCP 値で表される PHB は設定可能です。DSCP 値の範囲は 0 ～ 63 です。

（注）　レイヤ 3 の IP パケットは、IP precedence 値または DSCP 値のいずれかを伝送します。DSCP 値は IP precedence 値と下位互換性があるので、QoS ではどちらの値でも使用できます。表 40-1 を参照してください。

表 40-1　IP precedence 値と DSCP 値

3 ビット IP 優先順位	ToS の MSb[1] 6 ビット						6 ビット DSCP		3 ビット IP 優先順位	ToS の MSb[1] 6 ビット						6 ビット DSCP
	8	7	6	5	4	3				8	7	6	5	4	3	
0	0	0	0	0	0	0	0		4	1	0	0	0	0	0	32
	0	0	0	0	0	1	1			1	0	0	0	0	1	33
	0	0	0	0	1	0	2			1	0	0	0	1	0	34
	0	0	0	0	1	1	3			1	0	0	0	1	1	35
	0	0	0	1	0	0	4			1	0	0	1	0	0	36
	0	0	0	1	0	1	5			1	0	0	1	0	1	37
	0	0	0	1	1	0	6			1	0	0	1	1	0	38
	0	0	0	1	1	1	7			1	0	0	1	1	1	39
1	0	0	1	0	0	0	8		5	1	0	1	0	0	0	40
	0	0	1	0	0	1	9			1	0	1	0	0	1	41
	0	0	1	0	1	0	10			1	0	1	0	1	0	42
	0	0	1	0	1	1	11			1	0	1	0	1	1	43
	0	0	1	1	0	0	12			1	0	1	1	0	0	44
	0	0	1	1	0	1	13			1	0	1	1	0	1	45
	0	0	1	1	1	0	14			1	0	1	1	1	0	46
	0	0	1	1	1	1	15			1	0	1	1	1	1	47

表 40-1　IP precedence 値と DSCP 値 （続き）

3 ビット IP 優先順位	ToS の MSb[1] 6 ビット						6 ビット DSCP		3 ビット IP 優先順位	ToS の MSb[1] 6 ビット						6 ビット DSCP
	8	7	6	5	4	3				8	7	6	5	4	3	
2	0	1	0	0	0	0	16		6	1	1	0	0	0	0	48
	0	1	0	0	0	1	17			1	1	0	0	0	1	49
	0	1	0	0	1	0	18			1	1	0	0	1	0	50
	0	1	0	0	1	1	19			1	1	0	0	1	1	51
	0	1	0	1	0	0	20			1	1	0	1	0	0	52
	0	1	0	1	0	1	21			1	1	0	1	0	1	53
	0	1	0	1	1	0	22			1	1	0	1	1	0	54
	0	1	0	1	1	1	23			1	1	0	1	1	1	55
3	0	1	1	0	0	0	24		7	1	1	1	0	0	0	56
	0	1	1	0	0	1	25			1	1	1	0	0	1	57
	0	1	1	0	1	0	26			1	1	1	0	1	0	58
	0	1	1	0	1	1	27			1	1	1	0	1	1	59
	0	1	1	1	0	0	28			1	1	1	1	0	0	60
	0	1	1	1	0	1	29			1	1	1	1	0	1	61
	0	1	1	1	1	0	30			1	1	1	1	1	0	62
	0	1	1	1	1	1	31			1	1	1	1	1	1	63

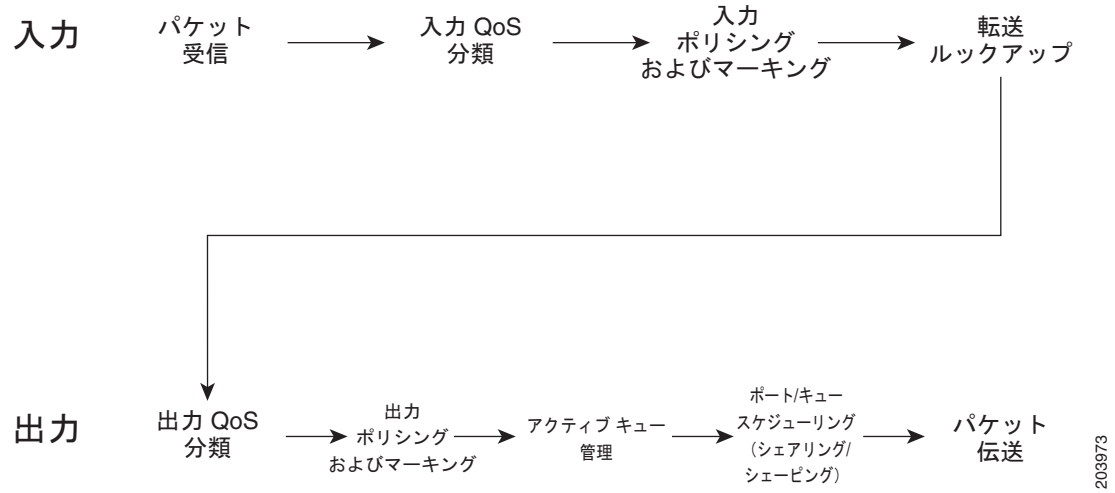
1. MSb = Most Significant bit（最上位ビット）

- *分類* : マーク付けするトラフィックを選択することです。
- *マーキング*: RFC 2475 に従い、レイヤ 3 の DSCP 値をパケットに設定する処理です。このマニュアルでは、マーキングの定義を拡大して、レイヤ 2 CoS 値の設定までを含めています。
- *ポリシング*: トラフィック フローが使用する帯域幅を制限する処理です。ポリシングによって、トラフィックのマーキングまたはドロップが可能になります。

QoS の基本モデル

図 40-2 では、QoS 機能の概要フローについて説明します。

図 40-2　QoS パケット処理



QoS モデルは次のように実行されます。

ステップ 1　着信パケットは、（さまざまなパケット フィールド、受信ポートや VLAN に基づいて）トラフィック クラスに属するように分類されます。

ステップ 2　プライオリティの低いパケットがドロップされる、またはパケット フィールド（DSCP および CoS）に低いプライオリティでマークされるように、トラフィック クラスに応じて、パケットのレート制限/ポリシングが設定され、そのプライオリティが任意でマークされます（通常はネットワークのエッジ）。

ステップ 3　パケットがマークされたら、転送用に*検索*されます。このアクションでは、送信ポートとパケットを送信する VLAN が取得されます。

ステップ 4　パケットは、発信ポートまたは VLAN に基づいて出力方向で分類されます。分類では、入力 QoS によってパケット マーキングを考慮します。

ステップ 5　出力分類に応じて、パケットがポリシングされ、そのプライオリティが任意で（*再*）*マークされます*。さらに、パケットの送信キューがトラフィック クラスによって決定されます。

ステップ 6　送信キューのステートが Active Queue Management（AQM; アクティブ キュー管理）アルゴリズムとドロップしきい値設定を介して動的にモニタされ、そのパケットをドロップするか、送信用にキューに入れるかが決定されます。

ステップ 7　伝送に適格である場合、パケットは送信キューに入れられます。送信キューが、出力 QoS 分類基準に基づいて選択されます。選択されたキューは、遅延と帯域幅に応じた振る舞いをします。

分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。分類は、QoS ポリシー マップをインターフェイスに対応付けると有効になります。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。

IP 以外のトラフィックについては、次の分類オプションがあります。

- 着信フレームの VLAN タグの CoS 値がパケットを分類するために使用されます。
- フレームに CoS 値が含まれない場合、ポートのデフォルト CoS 値（「0」）が分類に使用されます。

レイヤ 2 ヘッダーのフィールドを検査する設定済み MAC ACL に基づいて分類を実行します。

IP トラフィックについては、次の分類オプションがあります。

- 着信パケットの IP DSCP または IP precedence が分類に使用されます。DSCP 値の範囲は 0 ～ 63 です。
- 設定された IP 標準 Access Control List（ACL; アクセス コントロール リスト）または拡張 ACL（IP ヘッダーの各種のフィールドを検証する）に基づいて、分類を実行します。

QoS ACL に基づく分類

QoS のパケット分類は、複数の一致基準を使用して行うことができ、指定された一致基準をパケットがすべて満たしている必要があるか、または少なくとも 1 つの一致基準を満たしていればよいかを指定できます。QoS 分類基準を定義するには、クラス マップで *match* 文を使用して一致基準を指定します。「match」文では、マッチングの対象になるパケットのフィールドを指定することも、IP 標準 ACL または IP 拡張 ACL または MAC ACL を使用することもできます。詳細については、「クラス マップおよびポリシー マップに基づく分類」（P.40-8）を参照してください。

すべての一致基準に一致するようにクラス マップを設定した場合、パケットがクラス マップ内のすべての match 文を満たしていないと、QoS アクションは実行されません。パケットがクラス マップの一致基準を 1 つでも満たさない場合、そのパケットについて QoS アクションは実行されません。

最低 1 つの一致基準に一致するようにクラス マップを設定した場合、パケットがクラス マップ内の少なくとも 1 つの match 文を満たしていれば、QoS アクションが実行されます。パケットがクラス マップの一致基準をどれも満たしていない場合、そのパケットについて QoS アクションは実行されません。

（注）　IP 標準 ACL および IP 拡張 ACL を使用する場合、QoS コンテキストでは、ACL の中の許可（permit）ACE と拒否（deny）ACE の意味は多少異なります。

- 「permit」を指定している ACE を検出し、なおかつパケットがそれを満たしている場合、そのパケットは QoS 分類の一致基準に「一致した」ことになります。
- 「deny」を指定している ACE を検出し、なおかつパケットがそれを満たしている場合、そのパケットは QoS 分類の一致基準に「一致しない」ことになります。
- 一致する許可（permit）アクションが検出されないまま、すべての ACE の検証が終わった場合、そのパケットは QoS 分類の基準に「一致しない」ことになります。

（注）　アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

クラス マップを使用してトラフィック クラスを定義したあとで、トラフィック クラスに対する QoS アクションを定義するポリシーを作成できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、クラスを集約的に分類する（たとえば、DSCP を割り当てる）コマンド、またはクラスをレート制限するコマンドを組み込めます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP トラフィックを分類するための IP ACL を実装するには、**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。

match-all キーワードを指定してクラスマップを作成した場合、一致基準として IP と MAC ACL の両方を含めることはできません。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）を、他のすべてのトラフィックから切り離して名前を付けるためのメカニズムです。クラス マップは、特定のトラフィック フローを分類する目的で使用する一致基準を定義します。基準としては、ACL で定義されるアクセス グループとのマッチング、または特定の DSCP 値、IP precedence 値、または L2 CoS 値のリストとのマッチングを指定できます。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 マップの基準に関するパケットのマッチングが終わったあとで、ポリシー マップを使用して QoS アクションを指定できます。

ポリシー マップは、各トラフィック クラスに対する QoS アクションを指定します。アクションには、特定の CoS、DSCP、または IP precedence 値の設定が含まれる場合があります。この設定によって、指定されたレートにトラフィックをポリシングし、トラフィックの帯域幅制限を指定し、指定されたレートにトラフィックをシェーピングします。ポリシー マップを有効にするには、インターフェイスにポリシー マップを付加する必要があります。

クラス マップを作成するには、**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。**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、トラフィックの一致基準を定義します。

ポリシー マップは、**policy-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し、名前を付けます。このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。このモードでは、**police**, **bandwidth**、または **shape** ポリシー マップ コンフィギュレーション コマンドおよびポリシー 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、特定のトラフィック クラスに対して実行するアクションを指定します。ポリシー マップを有効にするには、**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、ポリシー マップをインターフェイスに付加します。

ポリシー マップには、ポリサーを定義するコマンド（トラフィックの帯域幅制限）および制限を超過した場合に実行するアクションを含めることもできます。詳細については、「ポリシングおよびマーキング」（P.40-8）を参照してください。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに、最大 254 のクラス文を指定できます。
- 1 つのポリシー マップで異なるクラスを指定できます。

ポリシングおよびマーキング

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「*アウト オブ プロファイル*」または「*不適合*」になります。各ポリサーは、イン プロファイルまたはアウト オブ プロファイル パケットに対して実行するアクションを指定します。これらのアクション（マーカーによって実行される）では、パケットを変更せずにそのまま通過させること、パケットをドロップすること、または、設定変更可能なポリシング済み DSCP マップから得られる新しい DSCP 値にパケットをマークダウンすることが可能です。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 **police** コマンドを使用して、ポリシー マップ内のポリサーを設定できます。ポリシング済み DSCP マップの詳細については、「キューイングおよびスケジューリング」（P.40-9）を参照してください。

ポリシングおよびポリサーを設定する場合、次の点に注意してください。

- ポリサーは、ポリサー レートを計算するときに、レイヤ 2 ヘッダー長だけを考慮に入れます。これに対し、シェーパーはレート計算でヘッダー長と IPG を考慮に入れます。
- Cisco IOS Release 15.0(2) SG/IOS XE 3.2.0 以降、Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、Catalyst 4948E/Supervisor Engine 7-E は、**qos account layer-all encapsulation** コマンドをサポートします。このコマンドは、ポリシング機能で 20 バイトのレイヤ 1 ヘッダー（12 バイトのプリアンブル + 8 バイト IPG）とレイヤ 2 ヘッダーを考慮に入れます。
- 設定できるのは、平均レート パラメータおよび認定バースト パラメータだけです。
- ポリシー マップおよびポリシング アクションを設定したあと、**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、入力インターフェイスまたは出力インターフェイスにポリシーを付加します。
- 2 レート 3 カラー（2r3c）ポリサーの場合は、違反アクションが明示的に指定されていなければ、超過アクションが違反アクションとして使用されます。

キューイングおよびスケジューリング

Catalyst 4500 シリーズ スイッチは、ポートごとに 8 つの送信キューをサポートします。パケットをポートから転送する決定が下されると、出力 QoS 分類によって、パケットを入れる送信キューが決定されます。

出力ポリシーが、1 つまたは複数のトラフィックのクラスに対する 1 つまたは複数のキューイング関連アクションでポートに付加されるとき、キューが割り当てられます。1 つのポートにはキューが 8 つしかないため、キューイング アクションを伴うトラフィック クラスは最大で 8 つです（予約クラスの *class-default* を含む）。キュー アクションを持たないトラフィックのクラスは、キューイングなしクラスと呼ばれます。キューイングなしのクラス トラフィックは、*class-default* に対応するキューを使用します。

AQM

Active Queue Management（AQM）は、バッファ オーバーフローが発生する前に輻輳に関して通知する先行型の手法です。AQM は、Dynamic Buffer Limiting（DBL）を使用して実行されます。DBL はスイッチ内の各トラフィックのキュー長を追跡します。フローのキュー長が制限を超えると、DBL はパケットをドロップします。

送信キュー間のリンク帯域幅の共有

送信ポートの 8 つの送信キューは、その送信ポートで使用できるリンク帯域幅を共有します。クラス モードで **policy-map class** コンフィギュレーション コマンドの **bandwidth** コマンドを使用して、送信キュー間で個別に共有されるリンク帯域幅を設定できます。

このコマンドを使用して、各送信キューに最低限保証される帯域幅を指定します。

デフォルトでは、すべてのキューがラウンド ロビン方式でスケジューリングされています。

ストリクト プライオリティ /低遅延キューイング

完全プライオリティ（低遅延キューまたは LLQ と呼ばれます）としてのみ、ポートで 1 つの送信キューを設定できます。

LLQ では、トラフィック クラスに対して完全プライオリティ キューイングが提供されます。これにより、他のキューのパケットの前に、音声など遅延の影響を受けやすいデータを送信できます。プライオリティ キューは、空になるまでまたはシェーピング レートを下回るまで、最初に処理されます。クラ

スレベル ポリシーごとのプライオリティ キューの宛先にできるのは、1 つのトラフィック ストリームだけです。トラフィック クラスのプライオリティ キューをイネーブルにするには、クラス モードで **priority policy-map class** 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 シェーピング

トラフィック シェーピングは、トラフィックが設定上の最大送信速度に従うように、発信トラフィックの速度を制御する能力を提供します。ある制限に適合するトラフィックを、ダウンストリーム トラフィックの速度要件を満たすようにシェーピングし、データ速度の不一致を解消できます。

クラス モードで **policy-map class** コンフィギュレーション コマンドの **shape** コマンドを使用して、各送信キューは、最大速度で送信するように設定できます。

この設定により、トラフィックの最大速度を指定できます。設定されたシェープ レートを超過するトラフィックは、キューに格納されたあと、設定された速度で送信されます。バースト トラフィックによってキューの容量を超過した場合には、設定されたシェープ レートを維持するために、パケットがドロップされます。

パケットの変更

QoS を設定するには、パケットの分類、ポリシング、キューイングを行います。このプロセス中に、次のようにパケットが変更されることがあります。

- IP パケットの場合、分類によって、パケットに DSCP が割り当てられます。ただし、この段階でパケットは変更されません。割り当てられた DSCP が伝送されるだけです。その理由は、QoS の分類と ACL の検索が並行して実行され、ACL によってパケットの拒否とロギングが指示される場合があるためです。この状況では、パケットは元の DSCP 付きで CPU に転送され、CPU で再び ACL ソフトウェアによって処理されます。
- IP 以外のパケットの場合、分類によってパケットに内部 DSCP が割り当てられますが、非 IP パケットに DSCP はないので、上書きは行われません。代わりに、内部 DSCP がキューイングおよびスケジューリング決定の両方で使用され、さらにパケットが ISL または 802.1Q トランク ポートのいずれかで送信される場合、タグへの CoS プライオリティ値の書き込みに使用されます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます（これらのパケットが不適合で、ポリサーがマークダウン DSCP を指定している場合）。この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。IP パケットの場合、あとの段階でパケットの変更が行われます。

PVQoS

PVQoS により、トラフィック ポート上の個別の VLAN に差別化された QoS が提供されます。この機能により、サービス プロバイダーはビジネスまたは住宅への各トラフィック ポートの個々の VLAN ベース サービスをレート制限できるようになります。企業の Voice over IP（VoIP）環境で、攻撃者が IP Phone になりすましている場合でも、この機能を使用して音声 VLAN をレート制限できます。ポート単位 /VLAN 単位サービス ポリシーは、入力トラフィックまたは出力トラフィックのいずれかに別々に適用できます。設定の詳細については、「PVQoS のイネーブル化」（P.40-36）を参照してください。

フロー ベースの QoS

（注）　この項を読む前に、この章の Flexible Netflow（第 62 章「Flexible NetFlow の設定」）および QoS 実装の設定に精通している必要があります。

フロー ベース QoS は、動的にトラフィック フローを学習するために、マイクロフロー ポリシングとマーキング機能をイネーブルにします。また、固有な各フローを個々のレートに制限します。フローベース QoS は、内蔵 NetFlow ハードウェアを搭載した Catalyst 4500 シリーズ スイッチで使用可能です。これは、Flexible Netflow（FNF）を使用して定義されたフロー マスクを使用して、スイッチド インターフェイスとルーテッド インターフェイスの両方で、着信トラフィックに適用できます。これは、ハードウェアで最大 100,000 の個々のフローと、最大 512 の固有なポリサー設定をサポートします。フローベース QoS は、ユーザ単位の細かいレート制限が必要な環境でよく使用されます。たとえば、フロー単位の発信トラフィックと着信トラフィックのレートが異なる場合です。フロー ベース QoS は、User Based Rate Limiting（UBRL）とも呼ばれます。

*フロー*は、FNF フロー レコード内のキー フィールドで定義されたものとプロパティが同じパケットのストリームとして定義されます。パケットのキー フィールド内の値が既存のフローに対して一意の場合に、新しいフローが作成されます。

フローベース QoS ポリシーには、FNF フロー レコードに対して照合する 1 つ以上のクラス マップが含まれています。このようなクラス マップは、その中で指定されたすべての一致基準を満たす **match-all** として設定する必要があります。フローベース QoS ポリシーが QoS ターゲットに対応付けられている場合は、最初に、ターゲット上の入力トラフィックがクラス マップ内で指定された分類ルールに基づいて分類されます。 分類子に FNF フロー レコードがある場合、FNF フロー レコードで指定したキー フィールドは、フローを作成するために、分類されたトラフィックに適用されます（フローがまだ存在しない場合）。 その後で、対応するポリシー アクション（ポリシングとマーキング）がこれらの個別のフローに適用されます。フローベース ポリサー（*マイクロフロー ポリサー*とも呼ばれる）はフローごとにレートを制限します。フローは動的に作成され、非アクティブ フローは定期的にドロップされます。

フローベース QoS ポリシーは、ポート（P）、VLAN（V）、ポート単位/VLAN 単位（PV）、EtherChannel などの QoS ターゲットに対応付けることができますが、入力方向に限定されます。

FNF のイネーブル化方法については、「フローベース QoS ポリシーの適用」（P.40-42）を参照してください。

QoS ポリシーのメタデータの使用

Cisco IOS Release IOS XE 3.3.0 SG（15.1(1) SG）以降、メタデータ フィルタでクラス マップを設定できます。このようなクラスを含む QoS ポリシーは、*メタデータ ベース QoS ポリシー*または*パラメータ化された QoS* ポリシーと呼びます。これは、個々のフローの 5 タプルおよび適用可能な QoS アクションではなく、わかりやすい直感的なメタデータ属性に基づいてフローを分類できます。

ソフトウェアは、次の目的で MSI および MSI プロキシなどのメカニズムを使用します。

- フローの識別
- ネットワーク エッジで受信したトラフィックからのメタデータ情報の収集
- オンパス RSVP シグナリング メカニズムで、フロー パス上のすべてのネットワーク要素に RSVP メッセージ ホップバイホップを使用して、メタデータ情報を生成し、転送します。

Cisco Medianet メタデータ設定の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/mdata/configuration/15-2mt/mdata-15-2-book.html

メタデータ コマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios-xml/ios/qos/command/qos-cr-book.html

制約事項

次の制約事項は、Catalyst 4500 シリーズ スイッチのメタデータ ベース QoS ポリシーの使用に適用されます。

- 入力方向のターゲットだけに対応付けることができます。
- 物理ポートおよび EtherChannel だけに対応付けることができます。VLAN、ポート VLAN、および SVI インターフェイスに対応付けることはできません。
- ポリシーには、複数のメタデータベースの分類子を割り当てることができます。
- クラスマップには、match-all、match-any セマンティクスで 1 つ以上のメタデータ フィルタを割り当てることができます。
- メタデータのクラスに対応するポリシー アクションは、集約トラフィックに適用されます。ただし、メタデータのフィルタが Flexible NetFlow レコードのフィルタとともに設定されている場合、ポリシー アクションは、個々のフロー（ポリサーなど）に適用されます。

  ポリシー アクション セマンティクスに関するフローごとの QoS ポリシーの項を参照してください。
- メタデータ フィルタに関連付けられているフローがない場合、拒否 ACE で暗黙 ACL が設定されます。
- 同じメタデータの QoS ポリシーが複数のインターフェイスに適用される場合、ポリシーは、インターフェイスごとに個別の TCAM エントリのハードウェアにインストールされます。TCAM エントリは、インターフェイスと共有されません。
- 新しいフローがメタデータ フィルタと関連付けられると、新しい一連の TCAM エントリがインストールされます。これには、以前に検出された他の既存のフローとともに、新しいフローが含まれます。

統計情報

- 同じメタデータ ポリシー インターフェイスはハードウェアの TCAM リソースを共有しませんが、**show policy-map interface** *ifname* コマンドで観察されるメタデータ フィルタ統計情報は、それが共有されたかのように、レポートされます。
- メタデータ フィルタの統計情報だけを入手できます。個々 のフロー統計情報は入手できません。

例

次に、メタデータ フィルタを使用する 2 つのクラスのメタデータ ベース QoS ポリシーを示します。

```
class-map c1
 match application telepresence-media

class-map c2
 match access-group name mysubnet

class-map match-any c3
 match application webex-video
 match application webex-audio

policy-map p1
 class c1
  police cir 10m
```

```
class c2
 set dscp cs1
 police cir 2m
class c3
 police cir 5m
```

QoS の設定

（注）　HQoS は Catalyst 4500 シリーズ スイッチではサポートされません。

次の内容について説明します。

MQC ベースの QoS の設定

（注）　Starting with Cisco IOS Release 12.2(40)SG 以降、Supervisor Engine 6-E または Supervisor Engine 6L-E を備えた Catalyst 4900M、Catalyst 4948E、または Catalyst 4500 シリーズ スイッチは、QoS の MQC モデルを使用します。Cisco IOS Release 15.0(1)XO 以降、Supervisor Engine を使用している Catalyst 4500 シリーズ スイッチは、MQC モデルを採用しています。

QoS を適用するには、次の作業を完了できる CLI 構造であるモジュラ QoS コマンドライン インターフェイス（MQC）を使用します。

- トラフィック クラスの定義に使用される一致基準を指定します。
- トラフィック ポリシー（ポリシー マップ）を作成します。トラフィック ポリシーにより、各トラフィック クラスに実行する QoS ポリシー アクションが定義されます。
- ポリシー マップで指定されたポリシー アクションをインターフェイス、VLAN、またはポートおよび VLAN に適用します。

MQC についての詳細は、『*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.3*』の「Modular Quality of Service Command-Line Interface」を参照してください。

（注）　デフォルトで、着信トラフィックは信頼できると見なされます。インターフェイスで*信頼境界*機能がイネーブルの場合だけ、ポートを非信頼モードにすることができます。このモードでは、スイッチは IP パケットの DSCP 値とイーサネット フレーム上にある VLAN タグの Cos 値を「0」とマークします。

プラットフォームでサポートされる分類基準および QoS 機能

次の表に、Catalyst 4500 シリーズ スイッチでサポートされているさまざまな分類基準とアクションの概要を示します。詳細については、『*Catalyst 4500 Series Switch Command Reference*』を参照してください。

サポートされる分類アクション	説明
match access-group	指定した ACL をベースにクラス マップに対して一致基準を設定します。
match any	すべてのパケットに対して適切に一致する基準となる、クラス マップの一致基準を設定します。
match cos	レイヤ 2 サービス クラス（CoS）マーキングに基づいてパケットを照合します。
match [ip] dscp	特定の IP DiffServ コード ポイント（DSCP）値を一致条件として識別します。1 つの match 文に最大 8 つの DSCP 値を含めることができます。
match [ip] precedence	IP precedence 値を一致基準として識別します。
match protocol	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
match qos-group	特定の QoS グループ値を一致基準として識別します。出力方向でだけ適用されます。
サポートされる QoS 機能	**説明**
police	トラフィック ポリシングを設定します。
police（割合）	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
police（2 つのレート）	認定情報レート（CIR）と最大情報レート（PIR）の 2 つのレートを使用したトラフィック ポリシングを設定します。
set cos	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。
set dscp	IPv4 の ToS バイトまたは IPv6 パケットのトラフィック クラス バイトで DSCP 値を設定して、パケットにマークを付けます。
set precedence	パケット ヘッダーに precedence 値を設定します。
set qos-group	あとでパケットを分類するために使用できる QoS グループ ID を設定します。
table map support	別のパケット フィールドに基づいてパケット フィールドに無条件にマーク付けします。
priority	ポリシー マップに属するトラフィックのクラスにプライオリティを与えます。
shape	指定したアルゴリズムに従って、指示されたビット レートまでトラフィックをシェーピングします。
bandwidth	8 つのキューそれぞれに、保障されている最小帯域幅を提供します。
dbl	Dynamic Buffer Limiting です。
queue-limit	送信キューが保持できるパケットの最大数を指定します。

プラットフォーム ハードウェアの機能

QoS アクション	サポートされるエントリ数
分類	64k 入力および 64k 出力分類エントリがサポートされます。 1 つのポリシーでは、最大 24k ACL を使用できます。
ポリシング	16K ポリサーがサポートされています。ポリサーは、2k のブロックの指定方向に割り当てられます。たとえば、2k ポリサーを入力に、14k ポリサーを出力に、それぞれ使用できます。単一レート ポリサーは、1 つのポリサー エントリを使用します。Single Rate Three Color Marker（srTCM）（RFC 2697）および Two Rate Three Color Marker（trTCM）（RFC 2698）は、2 つのポリサー エントリを使用します。
マーキング	CoS および DSCP/Precedence は、それぞれが 512 エントリをサポートできる 2 つのマーキング テーブルを介してサポートされます。各方向にそれぞれ別個のテーブルがあります。
キューイング	キュー サイズは、シャーシおよびラインカードのタイプに応じてポートごとに設定可能な最大エントリ数で設定されます。
DBL	設定されたすべてのクラスマップで DBL アクションをイネーブルにできます。

QoS サービス ポリシーを適用するための前提条件

スイッチ QoS モデルとは異なり、さまざまなターゲットで QoS をイネーブルにするための前提条件はありません。サービス ポリシーを適用すれば QoS がイネーブルになり、そのポリシーの適用を解除すると、ターゲット上で QoS がディセーブルになります。

QoS サービス ポリシーの適用に関する制約事項

インターフェイス、VLAN、またはポートおよび VLAN 上で、トラフィック マーキングを設定できます。インターフェイスは、レイヤ 2 アクセス ポート、レイヤ 2 スイッチ トランク、レイヤ 3 ルーテッド ポート、または EtherChannnel が考えられます。ポリシーは、*vlan configuration* モードを使用して VLAN に付加されます。

QoS サービス ポリシーの VLAN および EtherChannel への適用については、「ポリシーの関連付け」（P.40-39）を参照してください。

分類

スーパーバイザ エンジンは、レイヤ 2、IP、および IPv6 パケットの分類をサポートします。入力に対して実行される ARP パケット マーキングは出力方向で照合できます。前述の表では、すべての機能が一覧になっています。デフォルトでは、スイッチは分類リソース共有もサポートします。同様に、ポート、VLAN、またはポート単位/VLAN 単位ターゲットに同じポリシーを対応付けると、QoS アクションは各ターゲットで一意ですが、ACL エントリは共有されます。

次に例を示します。

```
    class-map c1
      match ip dscp 50

Policy Map p1
    class c1
      police rate 1 m burst 200000
```

ポリシーマップ p1 がインターフェイス Gig 1/1 および Gig 1/2 に適用されている場合、1 つの CAM エントリ（IP パケットに一致する 1 つの ACE）が使用されますが、2 つのポリサー（ターゲットごとに 1 つずつ）が割り当てられます。したがって、dscp 50 を伴うすべての IP パケットがインターフェイス Gig 1/1 上で 1 Mbps にポリシングされ、インターフェイス Gig 1/2 上のパケットも 1 Mbps にポリシングされます。

（注）　Cisco IOS Release 12.2(46)SG では、**match protocol arp** コマンドを実行できます。詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』を参照してください。

分類統計

スーパーバイザ エンジンは、パケット ベースの分類統計情報と TCAM リソース共有だけをサポートします。ポリシー マップが複数のターゲットに適用されている場合は、**show policy-map interface** コマンドによって、インターフェイスに依存しない集約分類統計が表示されます。

（注）　インターフェイス単位のポリシー マップ統計を取得するには、インターフェイスごとに一意のポリシー マップ名を設定する必要があります。

ポリシー マップがポート チャネル メンバー ポートに対応付けられている場合は、分類統計が表示されません。

ポリシー マップの設定

1 つのインターフェイスに対応付けできるポリシー マップは、1 つに限られます。ポリシー マップには、一致基準とアクションがそれぞれ異なる 1 つまたは複数のポリシー マップ クラスを含めることができます。

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

ポリシー マップの作成

ポリシー マップを作成するには、次のコマンドを入力します。

コマンド	目的
`Switch(config)# [no] policy-map policy_name`	ユーザが指定した名前でポリシー マップを作成します。 ポリシー マップを削除するには、**no** キーワードを使用します。

インターフェイスへのポリシー マップの対応付け

ポリシー マップを作成するには、次のコマンドを入力します。

コマンド	目的
Switch(config)# **interface** {vlan *vlan_ID* | {**fastethernet** | **gigabitethernet**} *slot/interface* | Port-channel *number*}	設定するインターフェイスを選択します。
Switch(config-if)# [**no**] **service-policy input** *policy_map_name*	ポリシー マップをインターフェイスの入力方向に対応付けます。インターフェイスからポリシー マップの対応付けを解除するには、no キーワードを使用します。
Switch(config-if)# **end**	コンフィギュレーション モードを終了します。
Switch# show policy-map interface {vlan *vlan_ID* | {**fastethernet** | **gigabitethernet**} slot/interface}	設定を確認します。

ポリシング

スーパバイザ エンジンは、次の動作モードでポリサーをサポートします。

- Single Rate Policer Two Color Marker

  この種類のポリサーは、CIR と通常バーストでだけ設定され、conform アクションと exceed アクションだけがあります。

  これは、Supervisor Engine II-Plus から V-10GE ベース システムでサポートされる唯一の形式です。

- srTCM（RFC 2697）
- trTCM（RFC 2698）
- Color Blind Mode

  設定済みポリサー レートの 0.75% のポリシング精度。

  エンジンは、16384（16 × 1024、16K）単一レート、単一バースト ポリサーをサポートします。16K ポリサーは、2K ポリサーのバンク 8 個で編成されています。ポリサー バンクは、QoS 設定に従い、ソフトウェアによって動的に割り当てられます（入力または出力ポリサー バンク）。したがって、16K ポリサーは、次のように動的にソフトウェアで分割されます。

  - 0 入力ポリサーと 16K 出力ポリサー
  - 2K 入力ポリサーと 14K 出力ポリサー
  - 4K 入力ポリサーと 12K 出力ポリサー
  - 6K 入力ポリサーと 10K 出力ポリサー
  - 8K 入力ポリサーと 8K 出力ポリサー
  - 10K 入力ポリサーと 6K 出力ポリサー
  - 12K 入力ポリサーと 4K 出力ポリサー
  - 14K 入力ポリサーと 2K 出力ポリサー
  - 16K 入力ポリサーと 0 出力ポリサー

これらの数値は、単一レートおよびバースト パラメータをサポートするハードウェア内の個々のポリサー エントリを表します。この数値に基づき、スイッチは、次の数のポリサーをサポートします。

- 単一バースト付き 16K 単一レート ポリサー（Two Color Marker）
- 8K srTCM

- 8K trTCM

これらのポリサーは、2K ポリサー バンクの塊で、入力と力の間で分割されます。さまざまなタイプのポリサーは、すべてシステム内に共存できます。ただし、ポリサーの特定タイプ（srTCM、trTCM など）は、128 個のポリサーのブロックとして設定可能です。

（注）　2 つのポリサーが内部で使用するために予約されています。

ポリシングの実装方法

Catalyst 4500 シリーズ スイッチにポリシング機能を実装する方法については、次のリンク先で Cisco IOS マニュアルを参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpolsh.html

プラットフォームの制約事項

プラットフォームの制約事項は、次のとおりです。

- マルチポリサー アクションを指定できます（CoS および IP DSCP の設定がサポートされています）。
- 無条件マーキングとポリサー ベース マーキングが同じフィールド（cos、dscp、または precedence）上に存在する場合は、ポリサー ベース マーキングが優先されます。
- ポリサー ベースのサービスポリシーがポートと VLAN の両方に付加されている場合、ポートベースのポリシングがデフォルトで優先されます。特定の VLAN ポリシーを指定ポートで優先させるには、ポート単位 /VLAN 単位ポリシーを設定する必要があります。
- ポート単位、VLAN 単位 QoS ポリシーがあるポートチャネルは、削除しないでください。

  回避策：ポート チャネルを削除する前に、次の作業を実行します。

  1. 存在する場合は PVQoS ポリシーを削除します。
  2. **no vlan-range** コマンドを使用して、ポート チャネル上の VLAN 設定を削除します。

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ク付けにより、特定のクラスまたはカテゴリに属するトラフィック（つまりパケット）の属性を設定または変更できます。ネットワーク トラフィックの分類とともに使用すると、ネットワーク トラフィックのマーク付けは、ネットワーク上で多くの QoS 機能をイネーブルにする基礎となります。ここでは、ネットワーク トラフィックのマーク付けのための概念的情報と設定作業を説明します。

内容

ネットワーク トラフィックのマーキングに関する情報

ネットワーク トラフィックにマーキングするには、次の概念を理解する必要があります。

ネットワーク トラフィックにマーキングする目的

トラフィック マーキングは、特定のトラフィック タイプを識別して個別に処理し、ネットワーク トラフィックを異なるカテゴリに分割するために使用されます。

トラフィックの分類によってネットワーク トラフィックをクラスに構成した後は、トラフィック マーキングによって、特定のクラスに属するトラフィックの値（属性）にマーキング（つまり、設定または変更）できます。たとえば、あるクラスのサービス クラス（CoS）値を 2 から 1 に変更し、別のクラスの Differentiated Services Code Point（DSCP）値を 3 から 2 に変更できます。ここでは、これらの値は属性またはマーキング フィールドと呼ばれています。

設定および変更できる属性は、次のとおりです。

- タグ付きイーサネット フレームの CoS 値
- IPv4 の ToS バイトでの DSCP/Precedence 値
- QoS グループ識別番号（ID）
- IPv6 のトラフィック クラス バイトでの DSCP/Precedence 値

ネットワーク トラフィックにマーキングする利点

トラフィック マーキングによって、ネットワーク上のトラフィックの属性を微調整できます。より細かく調整できるようになったことで、特別な処理が必要なトラフィックを分離し、それによって最適なアプリケーション パフォーマンスの実現に役立ちます。

トラフィック マーキングを使用すると、ネットワーク トラフィックの属性を設定する方法に基づいて、トラフィックの処理方法を決定できます。また、その属性に基づいて、次のようにネットワーク トラフィックを複数のプライオリティ レベルまたはサービス クラスに分類できます。

- 多くの場合、トラフィック マーキングは、ネットワークに着信するトラフィックの IP precedence または IP DSCP 値の設定に使用されます。ネットワーク内のネットワーキング デバイスは、新しくマーキングされた 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、音声トラフィックには特定の IP Precedence または DSCP でマーク付けし、そのマーキングのすべてのパケットをキューに入れるように完全優先を設定できます。この場合、マーキングは完全プライオリティ キューのトラフィックを識別するために使用されます。
- トラフィック マーキングは、クラスベースの QoS 機能（一部、制約事項があるものの、ポリシー マップ クラス コンフィギュレーション モードで使用可能な機能）のトラフィックを識別するために使用できます。
- トラフィック マーキングは、スイッチ内の QoS グループにトラフィックを割り当てるために使用できます。スイッチは QoS グループを使用し、送信用にトラフィックのプライオリティを設定する方法を決定します。一般的に、QoS グループ値は次の 2 つの理由のいずれかに使用されます。

- 広い範囲のトラフィック クラスを利用する場合。QoS グループ値には、DSCP に類似する、64 の異なる個別マーキングがあります。
- precedence 値または DSCP 値の変更は推奨されません。

トラフィック属性にマーキングする 2 つの方式

（注）　ここでは、*ポリサー ベース*のマーキングとは異なる*無条件*マーキングを説明します。無条件マーキングは、分類にだけ基づきます。

方法 1：無条件明示的マーキング（set コマンドを使用）

ポリシー マップで設定された set コマンドを使用して、変更するトラフィック属性を指定します。次の表に、使用可能な set コマンドと対応する属性を示します。set コマンドの詳細については、『*Catalyst 4500 Series Switch Command Reference*』を参照してください。

表 40-2　　set コマンドおよび適用可能なパケット タイプ

set コマンド	トラフィック属性	パケット タイプ
set cos	発信トラフィックのレイヤ 2 CoS 値	イーサネット IPv4、IPv6
set dscp	ToS バイトの DSCP 値	IPv4、IPv6
set precedence	パケット ヘッダーの precedence 値	IPv4、IPv6
set qos-group	QoS グループ ID	イーサネット、IPv4、IPv6

個別の **set** コマンドを使用している場合、それらの set コマンドはポリシー マップで指定されます。次に、表 40-2 に一覧になっている set コマンドの 1 つで設定されたポリシー マップの例を示します。

この設定例では、**set cos** コマンドがポリシー マップ（policy1）で設定され、CoS 属性をマーク付けしています。

```
enable
configure terminal
policy map p1
    class class1
      set cos 3
end
```

ポリシー マップの設定については、「ポリシー マップの作成」（P.40-16）を参照してください。

最後の作業として、ポリシー マップをインターフェイスに適用します。ポリシー マップをインターフェイスに適用する方法については、「インターフェイスへのポリシー マップの対応付け」（P.40-16）を参照してください。

方法 2：無条件テーブルマップベース マーキング

トラフィック属性のマーキングに使用できるテーブル マップを作成します。テーブル マップは 2 方向の変換表の一種で、トラフィック属性を別の属性にマッピングしたリストです。テーブル マップは、多対 1 タイプの変換およびマッピング スキームをサポートします。テーブル マップでは、トラフィック属性の to-from 関係を確立し、属性に行われた変更を定義します。つまり属性は、別の値から取得された 1 つの値に設定されます。値は、変更される特定の属性に基づいています。たとえば、Precedence 属性は 0 ～ 7 の数値に、一方 DSCP 属性は 0 ～ 63 の数値にそれぞれ設定できます。

次に、テーブル マップの設定例を示します。

```
table-map table-map1
map from 0 to 1
map from 2 to 3
```

```
exit
```

次の表に、テーブル マップを使用して to-from 関係を確立できるトラフィック属性の一覧を示します。

表 40-3　to-from 関係を確立できるトラフィック属性

to 属性	from 属性
優先順位	CoS、QoS グループ、DSCP、Precedence
DSCP	CoS、QoS グループ、DSCP、Precedence
CoS	DSCP、QoS グループ、CoS、Precedence

次の例では、以前に作成したテーブル マップ（table-map1）を使用するように設定されたポリシー マップ（policy2）を示します。

```
Policy map policy
    class class-default
      set cos dscp table table-map
exit
```

この例では、テーブル マップの定義に従って、CoS 属性と DSCP 属性の間にマッピング関係が作成されました。

テーブル マップを使用するためのポリシー マップの設定の詳細については、「ポリシー マップの設定」（P.40-16）を参照してください。

最後の作業として、ポリシー マップをインターフェイスに適用します。ポリシー マップをインターフェイスに適用する方法については、「インターフェイスへのポリシー マップの対応付け」（P.40-16）を参照してください。

アクション ドライバのマーク付け

マーキング アクションは、2 つの QoS 処理手順のうちの 1 つに基づいてトリガーされます。

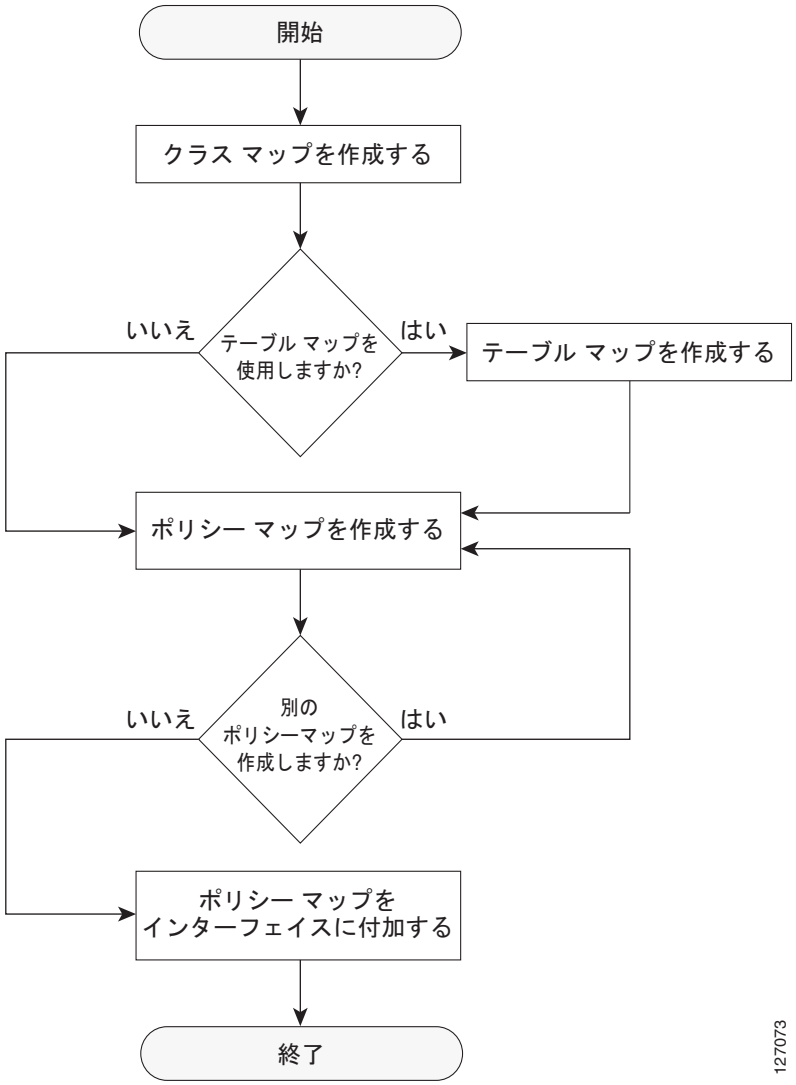
分類ベース：この場合、クラスに一致するすべてのトラフィックは、明示的方法またはテーブル マップ ベースの方法のいずれかを使用してマーク付けされます。この方法は、*無条件*マーキングと呼ばれます。

ポリサー結果ベース：この場合、トラフィックのクラスは、パケットで使用可能なポリサー結果（conform/exceed/violate）に基づいて、別にマーキングされます。この方法は、*条件付き*マーキングと呼ばれます。

トラフィック マーキング手順のフローチャート

図 40-3 に、トラフィック マーキングを設定する手順を示します。

図 40-3　トラフィック マーキング手順のフローチャート



ネットワーク トラフィック マーキングに関する制約事項

パケット マーキング アクションには、次の制約事項が適用されます。

- QoS グループは、入力方向でだけマーク付けでき、無条件明示的マーキングだけをサポートします。
- 明示的マーキングは、ポリサーベース マーキングに対してだけサポートされます。

マルチ属性マーキングのサポート

スーパーバイザ エンジンは、トラフィック クラスと一致するパケットの複数の QoS 属性をマークできます。たとえば、DSCP、CoS、および QoS グループは、明示的マーキングまたはテーブルマップベース マーキングのいずれかを使用して、すべて一緒に設定できます。

（注）　複数フィールドまたはポリサーベース マルチフィールドの無条件明示的マーキングを使用している場合は、ToS または CoS マーキング テーブルで設定可能なテーブルマップ数をマークするマルチリージョン（conform/exceed/violate）が、サポートされている最大数より少なくなります。

マーキング用のハードウェア機能

各エントリが、パケットを送信 / マークダウン / ドロップするために、CoS および DSCP/Precedence フィールドのマーキング アクション、およびポリサー アクションのタイプを指定している場合、Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、および Supervisor Engine 6L-E は、128 エントリのマーキング アクションを提供します（Supervisor Engine 7-E は、256 エントリのマーキング アクションを提供します）。

このテーブルは、入力および出力の各方向でサポートされます。このテーブルは、無条件マーキングとポリサーベース マーキングの両方に使用されます。256 の一意のマーキング アクションまたは 64 の一意のポリサーベース アクション、またはこの 2 つの組み合わせをサポートするために使用可能です。

各マーキング フィールド（CoS および DSCP）のために、スーパーバイザ エンジンは、各方向に 512 エントリのマーキング テーブルを提供します。これらのテーブルは、スイッチ QoS モデルをサポートするスーパーバイザ エンジンで使用可能なマッピング テーブルに類似しています。ただし、ユーザが設定する複数の固有マッピング テーブルを保持する機能を持ちます。

たとえば、ToS マーキング テーブルは、DSCP/Precedence フィールド マーキングを提供し、次のいずれかとして使用できます。

- それぞれが 64 の DSCP または QoS グループ値を他の DSCP にマッピングする 8 つの異なるテーブルマップ
- それぞれが 8 つの CoS（16 の CoS および CFi）値を入力（出力）方向の DSCP にマッピングする 64（32）の異なるテーブルマップ
- 上記 2 種類のテーブルマップの組み合わせ

512 エントリの CoS マーキング テーブルでは、同様のマッピングが使用可能です。

ポリシー マップ マーキング アクションの設定

ここでは、ネットワーク トラフィックに無条件マーキング アクションを確立する方法を説明します。

前提条件として、クラス マップ（*ipp5*）とポリシー マップを作成します （「ポリシー マップの設定」（P.40-16）を参照）。

（注）　マーキング アクション コマンド オプションが拡張されています（表 40-2（P.40-20）および表 40-3（P.40-21）を参照）。

テーブルマップベース無条件マーキングの設定

テーブルマップ ベースの無条件マーキングを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# table-map name`	テーブルマップを設定します。

	コマンド	目的
ステップ 3	Switch(config-tablemap)# **map from** *from_value* ***to*** *to_value*	*from_value* から *to_value* へのマップを作成します。
ステップ 4	Switch(config-tablemap)# **exit**	テーブルマップ コンフィギュレーション モードを終了します。
ステップ 5	Switch(config)# **policy-map** *name*	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 6	Switch(config-p)# **class** name	QoS アクションのクラスを選択します。
ステップ 7	Switch(config-p-c)# **set cos** | **dscp** | **prec cos** | **dscp** | **prec** | **qos-group** [**table** *name*]	暗黙の、または明示的テーブルマップに基づいて、マーキング アクションを選択します。
ステップ 8	Switch(config-p-c)# **end**	コンフィギュレーション モードを終了します。
ステップ 9	Switch# **show policy-map *name***	ポリシーマップの設定を確認します。
ステップ 10	Switch# **show table-map name**	テーブルマップの設定を確認します。

次に、テーブルマップを使用してマーキング アクションをイネーブルにする例を示します。

```
Switch(config)# table-map dscp2Cos
Switch(config-tablemap)# map from 8 to 1
Switch(config-tablemap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class ipp5
Switch(config-pmap-c)# set cos dscp table dscp2Cos
Switch(config-pmap-c)# end
Switch# show policy-map p1

Policy Map p1
    Class ipp5
      set cos dscp table dscp2Qos

Switch# show table-map dscp2Cos

 Table Map dscp2Cos
    from 8 to 1
    default copy
```

ポリサー結果ベースの条件付きマーキングの設定

ポリサー結果ベースの条件付きマーキングを設定するには、単一レートまたはデュアル レート ポリサーを設定します。「ポリシングの実装方法」（P.40-18）を参照してください。

次に、各ポリサー リージョンの明示的アクションで Two Rate Three Color ポリサーを設定する例を示します。

```
Switch# configure terminal
Switch(config-pmap-c)# policer cir percent 20 pir percent 30
Switch(config-pmap-c-policer)# conform-action set-cos-transmit 3 set-dscp-transmit 10
Switch(config-pmap-c-policer)# exceed-action set-cos-transmit 4 set-dscp-transmit 20
Switch(config-pmap-c-policer)# violate action drop
Switch# show policy-map p1

  Policy Map police
    Class ipp5
     police cir percent 20 pir percent 30
       conform-action set-cos-transmit 3
       conform-action set-dscp-transmit af11
       exceed-action set-cos-transmit 4
       exceed-action set-dscp-transmit af22
       violate-action drop
```

マーキング統計

マーキング統計では、*マーク付けされた*パケット数を示します。

無条件マーキングの場合、*分類エントリ*は、マーク付けされたパケットにあるフィールドを代わりに示すマーキング アクション テーブルのエントリを示します。したがって、分類統計はそれ自身で無条件マーキング統計を示します。

ポリサーを使用する条件付きマーキングでは、ポリサーがパケット レート ポリサーである場合、ポリサーは異なるポリシング結果のバイト統計だけを提供するため、マーク付けされたパケット数は判別できません。

シェーピング、共有（帯域幅）、プライオリティ キュー、キュー制限、および DBL

Catalyst 4500 シリーズ スイッチは、送信キューを選択するための分類ベース（クラス ベース）モードをサポートします。このモードでは、送信キューは、出力 QoS 分類検索に基づいて選択されます。

（注） 出力キューだけがサポートされます。

スーパーバイザ エンジンは、ポートごとに 8 つの送信キューをサポートします。パケットをポートから転送することが決定されると、出力 QoS 分類により、パケットが入れられる必要がある送信キューが決定されます。

デフォルトで、ポートにサービス ポリシーが関連付けられていない場合、帯域幅や優先順位付けの類に関する保証のない 2 つのキュー（制御パケット キューとデフォルト キュー）があります。唯一の例外は、制御トラフィックに多少の最小リンク帯域幅が与えられるように、システム生成制御パケットが制御パケット キューに入れられることです。

出力ポリシーが、1 つまたは複数のトラフィックのクラスに対する 1 つまたは複数のキューイング関連アクションでポートに付加されるとき、キューが割り当てられます。ポートごとに 8 つのキューしかないので、キューイング アクションを持つトラフィック クラスは最大でも 8 つ（予約クラス、class-default を含む）となります。キュー アクションを持たないトラフィックのクラスは、*キューイングなし*クラスと呼ばれます。キューイングなしのクラス トラフィックは、最終的にクラス class-default に対応するキューを使用します。

キューイング ポリシー（キューイング アクションを伴うポリシー）が対応付けられている場合は、制御パケット キューが削除され、制御パケットが分類ごとに関連キューに入れられます。出力 QoS クラスは、IP Precedence 6 および 7 トラフィックと一致するように設定し、帯域幅保証を設定する必要があります。

キューのダイナミックなサイズ変更（キュー制限クラスマップ アクション）は、**queue-limit** コマンドを使用することでサポートされています。シャーシとラインカードの種類に基づいて、ポート上の 8 つのキューすべては、同じキュー サイズで設定されます。

シェーピング

シェーピングにより、キューにあるアウト オブ プロファイル パケットを遅延させて指定のプロファイルに適合させることができます。シェーピングは、ポリシングとは異なります。ポリシングは、設定したしきい値を超えたパケットをドロップしますが、シェーピングは、パケットを*バッファし*、トラフィックを指定のしきい値内に保ちます。シェーピングでは、トラフィックの処理がポリシングよりも*滑らかに*行われます。**policy-map** 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 クラスの平均レート トラフィック シェーピングをイネーブルにします。

スーパーバイザ エンジンは、約 ± 0.75% の精度で 32 Kbps ～ 10 Gbps の範囲のシェーピングをサポートします。

キューイング クラスが明示的シェーピング設定を使用せずに設定されているとき、キュー シェーピングはリンク レートに設定されます。

サービス ポリシー内でクラスレベル シェーピングを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# policy-map` *policy-map-name*	ポリシーマップ名を入力してポリシー 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、ポリシー マップは定義されていません。
ステップ 3	`Switch(config-pmap)# class` *class-name*	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	`Switch(config-pmap-class)# shape average` {*cir-bps* [*optional_postfix*] | `percent` *percent*}	平均レート トラフィック シェーピングをイネーブルにします。 シャーピング レートは絶対値またはパーセンテージで指定できます。 • *cir-bps* [*optional_postfix*] に対して、シェーピング レートを bps 単位で指定します。範囲は 32,000 ～ 10,000,000,000 bps です。オプションの接尾辞（K、M、G）を入力します。 • *percent* の場合、トラフィックのクラスをシェーピングするリンク レートのパーセンテージを指定します。指定できる範囲は 1 ～ 100 です。 デフォルト設定では、平均レート トラフィック シェーピングはディセーブルになっています。
ステップ 5	`Switch(config-pmap-class)# 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	`Switch(config-pmap)# 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	`Switch(config)# interface` *interface-id*	物理ポートを指定し、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。
ステップ 8	`Switch(config-interface)# service-policy output` *policy-map-name*	ポリシーマップ名を指定し、物理インターフェイスに適用します。
ステップ 9	`Switch(config-interface)# end`	特権 EXEC モードに戻ります。
ステップ 10	`Switch# show policy-map [`*policy-map-name* `[class` *class-map-name*`]]` **or** `Switch# show policy-map interface` *interface-id*	入力を確認します。
ステップ 11	`Switch# 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。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラスを削除するには、**no class class-name** ポリシー マップ コンフィギュレーション コマンドを使用します。平均レート トラフィック シェーピングをディセーブルにするには、**no shape average policy-map** クラス コンフィギュレーション コマンドを使用します。

次に、クラスレベル、平均レート シェーピングを設定する例を示します。ここでは、トラフィック クラス class1 をデータ伝送レート 256 Kbps に制限します。

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch#

Switch# show policy-map policy1
  Policy Map policy1
    Class class1
       shape average 256000
```

次に、queuing-class トラフィックについて、クラスレベル、平均シェーピング パーセンテージを、リンク帯域幅の 32% に設定する例を示します。

```
Switch# configure terminal
Switch(config)# policy-map queuing-policy
Switch(config-pmap)# class queuing-class
Switch(config-pmap-c)# shape average percent 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output queuing-policy1
Switch(config-if)# end
Switch #

Switch# show policy-map queuing-policy
  Policy Map queuing-policy
    Class queuing-class
       Average Rate Traffic Shaping
       cir 32%
```

共有（帯域幅）

トラフィックのクラスに割り当てられた帯域幅は、輻輳中にクラスに対して保証される最小帯域幅です。送信キュー シェーピングは、出力リンク帯域幅が指定ポートの複数キューで共有されるプロセスです。

スーパーバイザ エンジンは、約 ± 0.75% の精度で 32 Kbps ～ 10 Gbps の範囲の共有をサポートします。すべてのキューイング クラスにわたる設定帯域幅の合計は、リンク帯域幅を超えないようにしてください。

サービス ポリシーにクラスレベル帯域幅アクションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# policy-map` *policy-map-name*	ポリシーマップ名を入力してポリシー 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、ポリシー マップは定義されていません。
ステップ 3	`Switch(config-pmap)# class` *class-name*	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	`Switch(config-pmap-class)# bandwidth` {*bandwidth-kbps* | **percent** *percent*}	スイッチにトラフィックの輻輳があるとき、このポリシー マップに属するクラスに提供される最小帯域幅を指定します。スイッチが輻輳していない場合、クラスは **bandwidth** コマンドで指定した以上の帯域幅が与えられます。 デフォルト設定では、帯域幅は指定されていません。 帯域幅は、Kbps またはパーセンテージで指定できます。 ・*bandwidth-kbps* では、クラスに割り当てられる帯域幅を Kbps で指定します。指定できる範囲は 32 ～ 10000000 です。 ・*percent* では、クラスに割り当てられる使用可能帯域幅のパーセンテージを指定します。指定できる範囲は 1 ～ 100 です。 すべてのクラス帯域幅を Kbps またはパーセンテージ（混在は不可）で指定します。
ステップ 5	`Switch(config-pmap-class)# 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	`Switch(config-pmap)# 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	`Switch(config)# interface` *interface-id*	物理ポートを指定し、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。
ステップ 8	`Switch(config-interface)#` **service-policy output** *policy-map-name*	ポリシーマップ名を指定し、物理インターフェイスに適用します。
ステップ 9	`Switch(config-interface)# end`	特権 EXEC モードに戻ります。
ステップ 10	`Switch# show policy-map` [*policy-map-name* **[class** *class-map-name*]] **or** `Switch# show policy-map interface` *interface-id*	入力を確認します。
ステップ 11	`Switch# 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。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラスを削除するには、**no class class-name** ポリシー マップ コンフィギュレーション コマンドを使用します。デフォルト帯域幅に戻すには、**no 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。

次に、prec1、prec2、および prec3 という 3 つのクラスに対して、policy11 という名前のクラスレベル ポリシー マップを作成する例を示します。これらのクラスのポリシーでは、最初のクラスのキューに 30%、2 番めのクラスのキューに 20%、3 番めのクラスのキューに 10% の使用可能帯域幅が、それぞれ割り当てられます。

```
Switch # configure terminal
Switch(config)# policy-map policy11
Switch(config-pmap)# class prec1
Switch(config-pmap-c)# bandwidth percent 30
Switch(config-pmap-c)# exit
Switch(config-pmap)# class prec2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class prec3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy11
Switch(config-if)# end
Switch #

Switch# show policy-map policy11
  Policy Map policy11
    Class prec1
      bandwidth percent 30
    Class prec2
      bandwidth percent 20
    Class prec3
      bandwidth percent 10
```

次に、prec1、prec2、および prec3 という 3 つのクラスに対して、policy11 という名前のクラスレベル ポリシー マップを作成する例を示します。これらのクラスのポリシーでは、最初のクラスのキューに 300 Mbps、2 番めのクラスのキューに 200 Mbps、3 番めのクラスのキューに 100 Mbps の使用可能帯域幅が、それぞれ割り当てられます。

```
Switch # configure terminal
Switch(config)# policy-map policy11
Switch(config-pmap)# class prec1
Switch(config-pmap-c)# bandwidth 300000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class prec2
Switch(config-pmap-c)# bandwidth 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class prec3
Switch(config-pmap-c)# bandwidth 100000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy11
Switch(config-if)# end
Switch #

Switch# show policy-map policy11
  Policy Map policy11
    Class prec1
      bandwidth 300000 (kbps)
    Class prec2
      bandwidth 200000 (kbps)
    Class prec3
      bandwidth 100000 (kbps)
```

キューで最小帯域幅が保証されないために、キューイング クラスが明示的共有 / 帯域幅設定を使用せずに設定されている場合、ハードウェア キューはポート上の未割り当て帯域幅の共有を取得するようにプログラミングされます。以下の例を参照してください。

新しいキューに対して帯域幅が残っていない場合、または明示的共有 / 帯域幅設定を持たないすべてのキューの最小設定可能レート（32 Kbps）を満たすのに未割り当て帯域幅が十分でない場合、ポリシーの関連付けは拒否されます。

たとえば、次のような 2 つのキューがあるとします。

```
policy-map queue-policy
   class q1
     bandwidth percent 10

   class q2
     bandwidth percent 20
```

そのキューの帯域幅割り当ては次のようになります。

```
q1 = 10%
           q2 = 20%
class-default = 70%
```

同様に、もう 1 つのキューイング クラス（q3 とします）が明示的帯域幅なしで（たとえば、shape コマンドだけで）追加されると、帯域幅割り当ては次のようになります。

```
q1 = 10%
           q2 = 20%
           q3 = min(35%, q3-shape-rate)
class-default = max(35%, (100 - (q1 + q2 + q3 )))
```

プライオリティ キューイング

完全プライオリティ（低遅延キューまたは LLQ と呼ばれます）としてのみ、ポートで 1 つの送信キューを設定できます。

LLQ では、トラフィック クラスに対して完全プライオリティ キューイングが提供されます。これにより、他のキューのパケットの*前に*、音声など遅延の影響を受けやすいデータを送信できます。プライオリティ キューは、空になるまでまたはシェーピング レートを下回るまで、最初に処理されます。クラスレベル ポリシーごとのプライオリティ キューの宛先にできるのは、1 つのトラフィック ストリームだけです。トラフィック クラスのプライオリティ キューをイネーブルにするには、クラス モードで **priority policy-map class** コンフィギュレーション コマンドを使用します。

LLQ は、レート制限されていない限り、他のキューを停止させることがあります。スーパーバイザ エンジンは、キューが*輻輳*すると（キュー長に基づく）、2 パラメータ ポリサー（レート、バースト）が有効になる*条件付きポリシング*をサポートしません。ただし、完全プライオリティ キューに入れられたパケットのレート制限のための無条件ポリサーの適用はサポートします。

プライオリティ キューがポリシー マップの 1 つのクラスで設定されている場合、*bandwidth remaining* だけが他のクラスに受け入れられ、その他のクラスのための最小帯域幅は、プライオリティ キューの使用後に残されている残りの帯域幅から保証されます。プライオリティ キューがポリサーで設定されている場合は、*bandwidth* と *bandwidth remaining* のどちらも他のクラスに受け付けられます。

（注） すべてのクラスに対して、*bandwidth* または *bandwidth remaining* を使用してください。1 つのポリシー マップ内で 1 つのクラスに *bandwidth* を適用して、別のクラスに *bandwidth remaining* を適用することはできません。

サービス ポリシーにクラスレベル プライオリティ キューイングを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# **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	Switch(config)# **policy-map** *policy-map-name*	ポリシーマップ名を入力してポリシー 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、ポリシー マップは定義されていません。
ステップ 3	Switch(config-pmap)# **class** *class-name*	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	Switch(config-pmap-class)# **priority**	完全プライオリティ キューをイネーブルにし、トラフィックのクラスにプライオリティを与えます。 デフォルト設定では、完全プライオリティ キューイングはディセーブルになっています。
ステップ 5	Switch(config-pmap-class)# **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	Switch(config-pmap)# **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	Switch(config)# **interface** *interface-id*	物理ポートを指定し、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。
ステップ 8	Switch(config-interface)# **service-policy output** *policy-map-name*	ポリシーマップ名を指定し、物理インターフェイスに適用します。
ステップ 9	Switch(config-interface)# **end**	特権 EXEC モードに戻ります。
ステップ 10	Switch# **show policy-map** [*policy-map-name* [**class** *class-map-name*]] **or** Switch# **show policy-map interface** *interface-id*	入力を確認します。
ステップ 11	Switch# **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。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラスを削除するには、**no class class-name** ポリシー マップ コンフィギュレーション コマンドを使用します。プライオリティ キューをディセーブルにするには、**no priority** ***policy-map class*** コンフィギュレーション コマンドを使用します。

次に、policy1 というクラスレベル ポリシーを設定する例を示します。class 1 は、プライオリティ キューとして設定され、空になるまで最初に処理されます。

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch #
```

```
Switch# show policy-map policy1
  Policy Map policy1
    Class class1
      priority
```

キュー制限

クラスベース キューが物理ポートでインスタンス化される際に、デフォルト サイズで設定されます。このサイズは、このトラフィック クラスに属するパケットがキューイング可能なキュー エントリの数を表します。スケジューラは、キュー シェーピング、帯域幅、およびプライオリティ設定に基づいて、すでに送信可能なキューからパケットを移動します。

キュー制限は、指定時間内のキュー内にあるパケットの最大数を指定します。キューが一杯になった場合に、後続のパケットをキューイングしようとするとテール ドロップになります。ただし、DBL がキューでイネーブルである場合は、キューが一杯になっていなくても DBL アルゴリズムに基づいてパケットが確率的にドロップされます。

帯域幅、シェーピング、またはプライオリティなどのキュー スケジューリングがすでに設定されている場合だけ、**queue-limit** コマンドをクラスの下に設定できます。この要件の例外は、クラスデフォルト クラス上でスタンドアロン **queue-limit** コマンドをサポートしている場合です。

キュー メモリ

割り当て可能なキュー エントリの数は、16 ～ 8184 の範囲内の 8 の倍数です。クラスベース キューが物理ポートでインスタンス化される際に、デフォルトのエントリ数が与えられます。このデフォルト キュー サイズは、シャーシ内のスロット数と、各スロットの前面パネル ポート数に基づいています。

Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、および Supervisor Engine 6L-E には、512（524,288 K）のキュー エントリがあります。そのうち、システムは、空いているリザーブ プールで 100 K（102,400）キュー エントリを予約します。残りの 412 K（421,88）のうち、ドロップ ポートに 8184 エントリが提供され、CPU ポートに 11704 エントリが割り当てられます。Supervisor Engine 7-E には、1M（1,048,576）のキュー エントリがあり、そのうち 100K（102,400）のキュー エントリが空きリザーブ プールに保留されています。残りのキュー エントリのうち、ドロップ ポートに 8184 エントリが割り当てられ、再循環ポートに 24576 エントリが割り当てられ、CPU ポートに 8656 エントリが割り当てられています。

残りのエントリは、シャーシ内のスロットに均等に分割されます。冗長シャーシ内では、このエントリ分配のために 2 つのスーパーバイザ スロットが 1 つとして扱われます。各スロット内では、そのスロットにあるラインカード上に存在する前面パネルのポート間でキュー エントリの数が均等に分割されます。

インターフェイス上にあるキュー エントリのユーザ設定が専用割り当て分を越えた場合、システムが空いているリザーブ プールを活用して設定に対応しようとします。空いているリザーブ プールからのエントリは、先着順でインターフェイスに割り当てられます。

サーバ ポリシーの関連付け

キューイング アクションのある QoS サービス ポリシーが設定されているものの、明示的に queue-limit コマンドが物理インターフェイスの出方向に添付されていない場合、クラスベースの各キューはその物理ポートの専用割り当て分から同数のキュー エントリを取得します。queue-limit コマンドを使用してキューに明示的にサイズが指定されている場合、スイッチはインターフェイスの専用割り当てから全エントリを割り当てようとします。必要なエントリ数がインターフェイスの専用割り当て分を越える場合、スイッチは空いているリザーブからエントリを割り当てようとします。

キューに関連付けられたキュー エントリは常に連続している必要があります。この要件により、スイッチ間で共有されている 512K のキューエントリにフラグメンテーションが発生する可能性があります。たとえば、あるインターフェイスで専用割り当て分のキュー エントリが十分ない場合、そのキューを設定するために空いているリザーブ分を使用することになります。この場合、他のポートやスロットと共有できないため、専用割り当て分のキュー エントリは未使用のままになります。

インターフェイスに関連付けられている QoS サービスポリシーが削除された場合、空いているリザーブ分から取得したキュー エントリは空いているリザーブ プールに戻されます。インターフェイス キューイング コンフィギュレーションは、2 つのキュー（デフォルトのシェーピング、帯域幅、サイズを持つクラスデフォルトおよび制御パケット キュー）に戻ります。制御パケットキューはサイズ 16 で設定されていて、デフォルト キューはインターフェイスの専用割り当て分に基づいて可能な最大サイズに設定されています。

キュー割り当て障害

キュー メモリのフラグメンテーションや十分な空いているリザーブ エントリがないために、スイッチがインターフェイス上の 1 つまたは複数のキューで必要な明示的キュー サイズを満たすことができない場合があります。このシナリオでは、スイッチはエラー メッセージをログして、ユーザに障害を通知します。QoS サービス ポリシーはインターフェイス上に設定されたままになります。QoS サービス ポリシーを削除し、スイッチ上の他のポートで、空いているリザーブ分からキュー エントリの現在の利用率を調査することで、エラーを修復することができます。

サービス ポリシーにクラスレベル queue-limit を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# policy-map` *policy-map-name*	ポリシーマップ名を入力してポリシー 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、ポリシー マップは定義されていません。
ステップ 3	`Switch(config-pmap)# class` *class-name*	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	`Switch(config-pmap-class)# shape average` {*cir-bps* [*optional_postfix*] | **percent** *percent*}	平均レート トラフィック シェーピングをイネーブルにします。 シャーピング レートは絶対値またはパーセンテージで指定できます。 • *cir-bps* [*optional_postfix*] に対して、シェーピング レートを bps 単位で指定します。範囲は 32,000 ～ 10,000,000,000 bps です。オプションの接尾辞（K、M、G）を入力します。 • *percent* の場合、トラフィックのクラスをシェーピングするリンク レートのパーセンテージを指定します。指定できる範囲は 1 ～ 100 です。 デフォルト設定では、平均レート トラフィック シェーピングはディセーブルになっています。
ステップ 5	`Switch(config-pmap-class)# queue-limit` *number-of-packets*	パケット内の明示的なキュー サイズを提示します。サイズは 8 の倍数で、16 ～ 8184 の範囲にする必要があります。
ステップ 6	`Switch(config-pmap-class)# 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 7	`Switch(config-pmap)# 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	目的
ステップ 8	Switch(config)# **interface** *interface-id*	物理ポートを指定し、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。
ステップ 9	Switch(config-interface)# **service-policy output** *policy-map-name*	ポリシーマップ名を指定し、物理インターフェイスに適用します。
ステップ 10	Switch(config-interface)# **end**	特権 EXEC モードに戻ります。
ステップ 11	Switch# **show policy-map** [*policy-map-name* **[class** *class-map-name*]] **or** Switch# **show policy-map interface** *interface-id*	入力を確認します。
ステップ 12	Switch# **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。

明示的キュー サイズを削除するには、ポリシーマップ内のクラスで **no queue-limit** コマンドを使用します。

次に、明示的な **queue-limit** コマンドを使用してクラスベースのキューを設定する例を示します。ここでは、トラフィック クラス class1 をキュー サイズ 4048 に制限します。

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# queue-limit 4048
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch#

Switch# show policy-map policy1
  Policy Map policy1
    Class class1
       shape average 256000
       queue-limit 4048
Switch#
```

DBL を経由した AQM

AQM は、パケットをポートの送信キューに入れる前の、トラフィック フローのバッファ制御を提供します。この機能は、共有メモリ スイッチで非常に役立ち、特定のフローによるスイッチ パケット メモリの占有が行われないようにします。

（注） スーパーバイザ エンジンは、DBL 経由のアクティブ スイッチ バッファ管理をサポートします。

トラフィックのデフォルト クラス（クラス class-default）を除き、他のキューイング アクションが少なくとも 1 つ設定されている場合にだけ DBL アクションを設定できます。

サービス ポリシーのシェーピングとともにクラスレベル DBL アクションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Switch# **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	Switch(config)# **policy-map** *policy-map-name*	ポリシーマップ名を入力してポリシー 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、ポリシー マップは定義されていません。
ステップ 3	Switch(config-pmap)# **class** *class-name*	トラフィック ポリシーを作成または変更するクラスの名前を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルト設定では、トラフィック クラスは定義されていません。
ステップ 4	Switch(config-pmap-class)# **shape average** *cir-bps*	平均レート トラフィック シェーピングをイネーブルにします。 トラフィックがシェーピングされるビット レートである CIR を bps で指定します。指定できる範囲は 32000 ～ 10000000000 bps です。 デフォルト設定では、平均レート トラフィック シェーピングはディセーブルになっています。
ステップ 5	Switch(config-pmap-class)# **dbl**	トラフィックのこのクラスに関連付けられたキューで DBL をイネーブルにします。
ステップ 6	Switch(config-pmap-class)# **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 7	Switch(config-pmap)# **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 8	Switch(config)# **interface** *interface-id*	物理ポートを指定し、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。
ステップ 9	Switch(config-interface)# **service-policy output** *policy-map-name*	ポリシーマップ名を指定し、物理インターフェイスに適用します。
ステップ 10	Switch(config-interface)# **end**	特権 EXEC モードに戻ります。
ステップ 11	Switch# **show policy-map** [*policy-map-name* **[class** *class-map-name*]] **or** Switch# **show policy-map interface** *interface-id*	入力を確認します。
ステップ 12	Switch# **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。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラスを削除するには、**no class class-name** ポリシー マップ コンフィギュレーション コマンドを使用します。関連付けられたキューで DBL をディセーブルにするには、**no dbl** policy-map *c*lass コンフィギュレーション コマンドを使用します。

次に、クラスレベルの DBL アクションを平均レート シェーピングとともに設定する例を示します。トラフィッククラス *class1* に関連付けられたキューで DBL をイネーブルにします。

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch#

Switch# show policy-map policy1
  Policy Map policy1
    Class class1
       shape average 256000
     dbl
```

送信キューの統計

送信キューの統計情報を表示するには、**show policy-map interface** コマンドを使用します。

```
Switch# show policy-map interface gigabitEthernet 1/1
 GigabitEthernet1/1

  Service-policy output: queuing-policy

    Class-map: queuing-class (match-all)
      1833956 packets
      Match: cos  1
      Queueing
      (total drops)  1006239
      (bytes output) 56284756
      shape (average) cir 320000000, bc 1280000, be 1280000
      target shape rate 320000000

    Class-map: class-default (match-any)
      1 packets
      Match: any

      (total drops)  0
      (bytes output) 2104
```

PVQoS のイネーブル化

PVQoS 機能を使用すれば、指定したインターフェイス上の複数の VLAN 上で複数の QoS 設定を指定できます。通常、この機能は、トランク ポートや音声 VLAN（シスコ製 IP 電話機）ポートなどの複数の VLAN に属しているポート上で使用します。

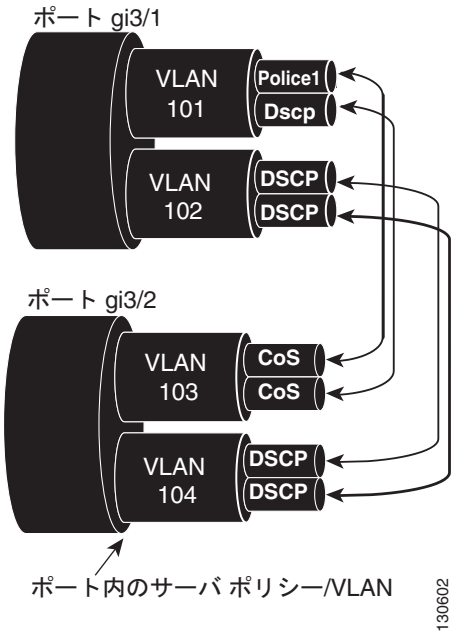
per-Port per-VLAN QoS を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# interface {fastethernet | gigabitethernet | tengigabitethernet} slot/interface | Port-channel number`	設定するインターフェイスを選択します。
ステップ 2	`Switch(config-if)# vlan-range vlan_range`	関連する VLAN を指定します。
ステップ 3	`Switch(config-if-vlan-range)# service-policy {input | output} policy-map`	ポリシーマップおよび方向を指定します。
ステップ 4	`Switch(config-if-vlan-range)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 5	`Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	`Switch# show policy-map interface interface_name`	設定を確認します。

例 1

図 40-4 に、PVQoS 構成のトポロジ例を示します。トランク ポート gi3/1 は、複数の VLAN（101 および 102）で構成されています。ポート内部には、独自のサービス ポリシーを VLAN 単位で作成できます。このポリシーは、ハードウェアで実行され、入出力ポリシングまたはデータを上回る音声パケットの優先処理で構成されます。

図 40-4　　ポート単位/VLAN 単位トポロジ



次のコンフィギュレーション ファイルでは、ポート GigabitEthernet 3/1 に適用されるポリシーマップ P31_QOS を使用して、VLAN 単位で入力および出力ポリシングを実行する方法について示しています。

```
ip access-list 101 permit ip host 1.2.2.2 any
ip access-list 103 permit ip any any
Class-map match-all RT

match ip access-group 101
Class-map Match all PD

match ip access-group 103
Policy-map P31_QoS

Class RT


Police 200m 16k conform transmit exceed drop

Class PD


Police 100m 16k conform transmit exceed drop

Interface Gigabit 3/1
Switchport
Switchport trunk encapsulation dot1q
Switchport trunk allowed vlan 101-102
    Vlan range 101
```

```
        Service-policy input P31_QoS
        Service-policy output P31_QoS
    Vlan range 102
        Service-policy input P32_QoS
        Service-policy output P32_QoS
```

例 2

たとえば、ギガビット イーサネット インターフェイス 6/1 がトランク ポートで、VLAN 20、300 ～ 301、および 400 に属しているとします。次に、VLAN 20 と VLAN 400 内のトラフィックにポリシー マップ p1 を、VLAN 300 ～ 301 内のトラフィックにポリシー マップ p2 を適用する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# vlan-range 20,400
Switch(config-if-vlan-range)# service-policy input p1
Switch(config-if-vlan-range)# exit
Switch(config-if)# vlan-range 300-301
Switch(config-if-vlan-range)# service-policy output p2
Switch(config-if-vlan-range)# end
Switch#
```

例 3

次に、ギガビット イーサネット インターフェイス 6/1 上で設定された VLAN 20 のポリシー マップ統計情報を表示する例を示します。

```
Switch# show policy-map interface gigabitEthernet 6/1 vlan 20

 GigabitEthernet6/1 vlan 20

  Service-policy input: p1

    Class-map: c1 (match-all)
      0 packets
      Match: cos  1
      Match: access-group 100
      police:
          cir 100000000 bps, bc 3125000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps

    Class-map: class-default (match-any)
      0 packets
      Match: any
```

例 4

次に、インターフェイス GigabitEthernet 6/1 上で設定されたすべての VLAN のポリシーマップの統計情報を表示する例を示します。

```
Switch# show policy-map interface gigabitEthernet 6/1

 GigabitEthernet6/1 vlan 20

  Service-policy input: p1

    Class-map: c1 (match-all)
      0 packets
```

```
      Match: cos  1
      Match: access-group 100
      police:
          cir 100000000 bps, bc 3125000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps

    Class-map: class-default (match-any)
      0 packets
      Match: any

GigabitEthernet6/1 vlan 300

 Service-policy output: p2

    Class-map: c1 (match-all)
      0 packets
      Match: cos  1
      Match: access-group 100
      QoS Set
        dscp 50
      police:
          cir 200000000 bps, bc 6250000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps

    Class-map: class-default (match-any)
      0 packets
      Match: any

GigabitEthernet6/1 vlan 301

 Service-policy output: p2

    Class-map: c1 (match-all)
      0 packets
      Match: cos  1
      Match: access-group 100
      QoS Set
        dscp 50
      police:
          cir 200000000 bps, bc 6250000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
```

ポリシーの関連付け

スーパーバイザ エンジンは、ポート単位/VLAN 単位ポリシーをサポートします。関連付けられたポリシーは、インターフェイス、VLAN、および指定ポートの特定 VLAN にそれぞれ付加されます。

ポリシーは、さまざまなオブジェクトに関連付けることができます。次の表に、オブジェクトと許可されているアクションを示します。

表 40-1　QoS ポリシーの関連付けの表

オブジェクト	アクション
物理ポート	ポリシング、マーキング、および キューイング
VLAN	ポリシングおよびマーキング
ポートと VLAN（PV）	ポリシングおよびマーキング
EtherChannel	ポリシングおよびマーキング
EtherChannel メンバ ポート	キューイング

QoS アクションの制約事項

- 異なるターゲット上で指定した方向に同じアクションを複数回実行することはできません。つまり、入力方向のポートと VLAN の両方でパケットをポリシングすることはできません。ただし、入力ポートと出力 VLAN 上ではポリシングできます。
- キューイング アクションは、物理ポートの出力方向でだけ許可されます。
- ポリサーなどのパーセンテージ ベース アクションは、VLAN、ポートと VLAN（PV）、および EtherChannel 上で設定することができません。
- ポート チャネルまたは VLAN の設定に持たせることができるのは、ポリシングまたはマーキング アクションだけです。キューイング アクションを持たせることはできません。

QoS ポリシーのプライオリティ

- ポートおよび VLAN 上のポリシーが、競合アクション（ポートと VLAN の両方でのポリシングまたはマーキング アクションなど）で設定されている場合、ポート ポリシーが取得されます。
- 指定ポートの VLAN 上でのポリシーが上書きされる必要がある場合、ユーザは PV ポリシーを設定できます。

QoS ポリシーの統合

適用可能ポリシーは、指定方向の指定パケットに適用されます。たとえば、出力 VLAN ベース ポリシングおよびマーキングを設定し、さらにそのポートでの選択的キューイングを設定すると、このパケットに対し、両方のポリシーからのアクションが適用されます。

EtherChannel では、ポリシーマップに関して次の制限事項があります。

- EtherChannel レベルでは、ポリシング アクションとマーキング アクションだけがサポートされます。
- 物理メンバ ポート レベルでは、キューイング アクションだけがサポートされます。

パケットは、EtherChannel ポリシーによってマーキングできます（dscp フィールドまたは cos フィールド）。物理メンバ ポート ポリシーで dscp フィールドまたは cos フィールドに基づいた分類を使用している場合、それはマーキングされた（変更された）値に基づいている必要があります。正しい動作を確保するために、EtherChannel には次の制限事項があります。

物理メンバ ポートのポリシーマップの分類基準は、以下のいずれか 1 つのフィールドだけに基づいていなければなりません。

- dscp
- precedence
- cos

- 任意の非マーキング フィールド（dscp にも cos にも基づかない分類）

物理メンバ ポートのポリシーマップの分類基準は、フィールドの組み合わせにはできません。この制限事項により、EtherChannel ポリシーが dscp または cos をマーキングしている場合に、マーキングされた（変更された）値に基づく分類を確実にハードウェアに実装できます。

（注）　物理メンバ ポート上でのポリシー マップに関する分類基準は、新しいタイプのフィールドを追加するように変更することができません。

Auto-QoS は EtherChannel でもそのメンバ ポートでもサポートされていません。Auto-QoS で設定されている物理ポートは、物理ポートのメンバになることはできません。

ソフトウェア QoS

最高レベルには、スイッチからローカルで送信された（制御プロトコル パケット、ping、Telnet など）2 種類のトラフィックがあります。この 2 種類とは、高プライオリティ トラフィック（通常は、OSPF Hello や STP などの制御プロトコル パケット）と低プライオリティ パケット（他のすべてのパケット タイプ）です。

ローカルで送信されたパケットの QoS 処理は、2 つの種類で異なります。

スーパーバイザ エンジンには、ソフトウェア パスで処理されたパケットに QoS を適用する方法が用意されています。ソフトウェアでこの QoS 処理を受けるパケットは、ソフトウェア スイッチド パケットとソフトウェア生成パケットの 2 種類に分類できます。

受信時には、ソフトウェア スイッチド パケットは、パケットを代わりに別のインターフェイスから送信する CPU に送信されます。そういったパケットの場合、入力ソフトウェア QoS は入力マーキングを提供し、出力ソフトウェア QoS は出力マーキングとキュー選択を提供します。

ソフトウェア生成パケットは、スイッチによりローカルで送信されたパケットです。これらのパケットに適用された出力ソフトウェア QoS 処理のタイプは、ソフトウェア スイッチド パケットに適用されたタイプと同じです。これら 2 つの処理タイプの唯一の違いは、ソフトウェア スイッチド パケットが、出力分類を目的として、パケットの入力マーキングを考慮する点です。

高プライオリティ パケット

高プライオリティ パケットは、次のいずれかとしてマーク付けされます。

- PAK_PRIORITY を使用して内部的に
- IP Precedence 6 を使用して（IP パケット用）
- CoS 6 を使用して（VLAN タグ付きパケット用）

これらのパケットは、次のように動作します。

- これらのパケットは、出力サービス ポリシーのように設定されたポリシング、AQM、ドロップしきい値（またはパケットをドロップすることができる機能）が原因でドロップされることはありません。ただし、ハードウェア リソースの制約（パケット バッファ、キューが満杯など）が原因でドロップされることはあります。
- これらのパケットは、ポートまたは VLAN である出力サービス ポリシーのマーキング設定に従って、分類およびマーク付けされます（「ポリシーの関連付け」（P.40-39）を参照）。
- これらの高プライオリティ パケットは、次の基準に従って出力ポートのキューに入れられます。
  - ポートに出力キューイング ポリシーがない場合、パケットは、デフォルト キューとは別に設定され、5% のリンク帯域幅が予約されている制御パケット キューに入れられます。

– ポートに出力キューイング ポリシーがある場合、そのパケットに適用可能な分類基準に基づいてキューが選択されます。

低プライオリティ パケット

高プライオリティ（前述）と見なされないパケットは、*重要ではない*と見なされます。これらのパケットには、ローカルで送信された ping、Telnet、およびその他のプロトコル パケットが含まれます。これらのパケットは、指定の伝送ポートを通過する他のパケットと同様に（出力分類、マーキングおよびキューイングを含む）、処理されます。

フローベース QoS ポリシーの適用

フロー ベース QoS は、動的にトラフィック フローを学習するために、マイクロフロー ポリシングとマーキング機能をイネーブルにします。また、固有な各フローを個々のレートに制限します。フローベース QoS は、内蔵 NetFlow ハードウェア サポートで使用可能です。

詳細については、「フロー ベースの QoS」（P.40-11）を参照してください。

次に、フローベース QoS ポリシーを QoS ターゲットに適用する手順を示します。

ステップ 1　一意のフローを識別するキー フィールドを指定して、FNF フロー レコードを作成します。FNF モニタに関連付けられた任意の FNF フロー レコードを使用することができます。

ステップ 2　一致基準のセットを指定するためのクラス マップを作成します。ステップ 1 で作成した FNF フロー レコードを **match flow record** コマンドを使用して、クラス マップ一致基準に含めます。その後で、**class-map match-all** *class_name* を使用して、すべての一致基準と一致するようにクラス マップを設定します。

ステップ 3　ポリシー マップを作成して、ステップ 2 で作成したクラス マップに関連付けるアクションを定義します。

ステップ 4　ポリシーを 1 つ以上の QoS ターゲットに対応付けます。

例

次に、フローベース QoS ポリシーを設定して、個々のフローにマイクロフロー ポリサーを適用する例を示します。

例 1

この例では、サブネット 192.168.10.* 上に複数のユーザ（送信元 IP アドレスで識別される）が存在することを前提とします。 下のコンフィギュレーションは、マクロ ポリシングを使用して、送信元アドレスが 192.168.10.* の範囲内のユーザ単位トラフィックに制限するフローベース QoS ポリシーの設定方法を示しています。マイクロフロー ポリサーは、CIR が 1Mbps に、「適合アクション」が transmit に、「超過アクション」が drop に設定されます。

ステップ 1：指定された送信元アドレスとトラフィックが一致するように ACL を定義します。

```
Switch(config)# ip access-list extended UserGroup1
Switch(config-ext-nacl)# permit ip 192.168.10.0 0.0.0.255 any
Switch(config-ext-nacl)# exit
Switch(config)#
```

ステップ 2：送信元アドレスをキーとして使用してフローを作成するためのフロー レコードを定義します。

```
Switch(config)# flow record r1
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# exit
Switch(config)#
```

ステップ 3：UserGroup1 に対して一致するようにクラス マップを設定し、フロー作成用のフロー レコード定義を指定します。

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match access-group name UserGroup1
Switch(config-cmap)# match flow record r1
Switch(config-cmap)# exit
Switch(config)#
```

ステップ 4：一致するトラフィックに関するマイクロフロー ポリシング アクションでフローベース QoS ポリシー マップを設定します。

```
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police cir 1m
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

ステップ 5：フロー QoS ポリシーをインターフェイスに対応付けます。

```
Switch(config)# interface gigabitEthernet3/1
Switch(config-if)# service-policy input p1
Switch(config-if)#
```

ポリシー マップ設定とインターフェイス固有のポリシー マップ統計情報を表示するには、**show** コマンド（この章のポリシーとマーキングに関するセクションを参照）を使用します。

例 2

この例では、サブネットの 192.168.10.* と 172.20.55.* 上に複数のユーザ（送信元 IP アドレスで識別される）が存在することを前提とします。最初にすべきことは、192 ネットワークから任意の宛先に送信されるすべての TCP トラフィックに対して、常に、500Kbps の CIR と 650Kbps の PIR でポリシングすることです。**exceed action** キーワードは、dscp 値を 32 に下げます。次にすべきことは、172 ネットワークから送信されるユーザ単位のトラフィックを 2Mbps の CIR でポリシングして、トラフィックの dscp 値を無条件に 10 にすることです。

ステップ 1：指定された送信元アドレスとトラフィックが一致するように ACL を定義します。

```
Switch(config)# ip access-list extended UserGroup1
Switch(config-ext-nacl)# permit ip 19 2.168.10.0 0.0.0.255 any
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended UserGroup2
Switch(config-ext-nacl)# permit ip 172.20.55.0 0.0.0.255 any
Switch(config-ext-nacl)# exit
Switch(config)#
```

ステップ 2：送信元アドレスをキーとして使用してフローを作成するためのフロー レコードを定義します。

```
Switch(config)# flow record r1
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
```

```
Switch(config-flow-record)# match transport tcp source-port
Switch(config-flow-record)# match transport tcp destination-port
Switch(config-flow-record)# exit
Switch(config)# flow record r2
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# exit
Switch(config)#
```

ステップ 3：UserGroup1 に対して一致するようにクラス マップを設定し、フロー作成用のフロー レコード定義を指定します。

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match access-group name UserGroup1
Switch(config-cmap)# match flow record r1
Switch(config-cmap)# exit
Switch(config)# class-map match-all c2
Switch(config-cmap)# match access-group name UserGroup2
Switch(config-cmap)# match flow record r2
Switch(config-cmap)# exit
Switch(config)#
```

ステップ 4：一致するトラフィックに関するマイクロフロー ポリシング アクションでフローベース QoS ポリシー マップを設定します。

```
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police cir 500k pir 650k
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 32
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# class c2
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police cir 2m
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

ステップ 5：フロー QoS ポリシーをインターフェイスに対応付けます。

```
Switch(config)# interface gigabitEthernet3/1
Switch(config-if)# service-policy input p1
Switch(config-if)# exit
```

ポリシー マップ設定とインターフェイス固有のポリシー マップ統計情報を表示するには、QoS セクションで説明した show コマンドを使用します。

例 3

ファスト イーサネット インターフェイス 6/1 上に 2 つのアクティブ フローが存在するとします。

表 40-2

SrcIp	DStIp	IPProt	SrcL4Port	DstL4Port
192.168.10.10	192.168.20.20	20	6789	81
192.168.10.10	192.168.20.20	20	6789	21

次の設定では、各フローが、許可可能な 9,000 のバースト値を使用して 1,000,000 bps にポリシングされます。

```
Switch(config)# flow record r1
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match transport tcp source-port
Switch(config-flow-record)# match transport tcp destination-port
Switch(config-flow-record)# match transport udp source-port
Switch(config-flow-record)# match transport udp destination-port
Switch(config-flow-record)# exit
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow record r1
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
```

設定時の注意事項

フローベース QoS ポリシーの作成、設定、変更、削除と、フローベース QoS ポリシーのサポートされているターゲットへの対応付け（および対応付け解除）に関する一般的なガイドラインは、QoS セクションで説明したものと同じです。 以降の説明と制限が、フローベース QoS ポリシーに適用されます。

- クラス マップには複数の match 文を含めることができますが、1 つのクラス マップで指定できる FNF フロー レコードは 1 つだけです。
- フロー レコードにキー フィールドが含まれていない場合は、クラス マップ内で使用することができません。非キー フィールドをフロー レコード内に含めることができます。ただし、すべてが非キー フィールドの場合はマイクロフロー QoS で無視されます。 キー フィールドのみがフロー作成に使用されます。
- FNF フロー レコードがいずれかのクラス マップで参照されている場合は、そのフロー レコードを変更することができません。フロー レコードを変更するには、すべてのクラス マップから削除してください。
- FNF フロー レコードを含むクラス マップは、**match-all** として設定する必要があります。クラス マップでヒットするトラフィックは、クラス マップ内のすべての一致基準を満たす必要があります。
- ポリシーには複数のクラスを含めることができ、クラス マップごとに同じ FNF フロー レコードを含めることも、別々の FNF フロー レコードを含めることもできます。
- フローベース QoS ポリシーと FNF モニタの両方を同時に同じターゲットに適用することはできません。
- インターフェイス モードがスイッチポートからルーテッド ポートにまたはその逆に変更された場合は、そのポートに対応付けられたすべてのフロー QoS ポリシーがモード変更後も適用されたままになります。
- pv4、ipv6、およびデータリンクの 3 種類の FNF フロー レコードがあります。データリンク フロー レコードは、ipv4 および ipv6 フロー レコードと相互排他的です。データリンク フロー レコードを含むクラス マップは、ipv4 または ipv6 フロー レコードを含むクラス マップと同じポリシー内で共存させることができません。逆も同じです。

- クラス マップの class-default は編集することができません。また、一致フロー レコードを使用して設定することもできません。代わりに、match any フィルタとフロー レコードを使用するクラス マップとフロー レコードを使用して、ポリシーを設定できます。
- トラフィックは、クラス マップがポリシー内で定義されたときと同じ順序で分類されます。そのため、FNF フロー レコードがクラス マップ内の唯一の match 文の場合は、分類基準がフロー レコードで識別されるすべてのパケット タイプと一致します。つまり、同じポリシー内で同じトラフィック タイプと一致するクラス マップは冗長であり、決してヒットすることがありません。
- フロー レコードを含むクラス マップに関連付けられたポリサーは*マイクロフロー ポリサー*と呼ばれます。マイクロフロー ポリサーの CIR レートと PIR レートは、% キーワードで設定することができません。
- 同じポリシー内のフロー レコードには、別のクラス マップから作成され、フローが一意で区別できることを保証する適切なキー フィールドを含める必要があります。そうでない場合は、別のクラス マップから生成されたフローと区別できません。このような場合は、ハードウェア内で最初のフローを生成したクラス マップに対応するポリシー アクションが適用され、その結果は必ずしも予想どおりになるとは限りません。
- 別々の QoS ターゲット上で受信されたトラフィックからのフローは、それらのターゲットに同じポリシーが適用されている場合でも、区別されます。
- フローが 5 秒を超えて非アクティブだった場合はドロップされます。5 秒より長くフローと一致するトラフィックは存在しません。
- フローがドロップされると、そのフローに関連付けられたポリサー ステート情報も削除されます。新しいフローが作成されると、そのフローのポリサー インスタンスが再初期化されます。
- フローベース QoS ポリシーによって作成されたフローは、ハードウェアにしか存在せず、エクスポートすることができません（FNF モニタと同様）。
- フローベース QoS ポリシーによって作成されたフローに関するフロー単位統計情報は入手できません。
- クラス マップ統計情報には、分類基準と一致するパケット数が表示されます。個別のフロー統計情報は表示されません。
- ポリサー統計情報には、個々のフローの集約ポリサー統計情報が表示されます。
- ハードウェアによって生成されたフローに関する情報は入手できないため、QoS ポリシー マップに関連付けられた show コマンドに表示されません。クラス マップとポリサー統計情報のみが **show policy-map** コマンドの出力に表示されます。

CoS 変換の設定

CoS リフレクションおよび CoS 変換は、Supervisor Engine 6-E および Catalyst 4900M でサポートされます。次に、CoS リフレクションを適用する方法の例を示します。

トラフィックが VLAN 10 および CoS 1、2、... のインターフェイス ギガビット 2/5 に到達すると仮定します。外部タグの VLAN 11 と C-tag からコピーされた CoS（C-tag は VLAN 10 および COS 1、2、...）とともに、インターフェイス ギガビット 2/6 からトラフィックを出力させます。

```
class-map match-all c2

  match cos  2

class-map match-all c1

  match cos  1

!
```

```
policy-map my
class c1
   set cos 1
class c2
  set cos 2

interface GigabitEthernet2/5
switchport mode trunk
switchport vlan mapping 10 dot1q-tunnel 11
spanning-tree bpdufilter enable
service-policy input my
!
interface GigabitEthernet2/6
switchport mode trunk
```

システム キューの制限の設定

（注）　この機能は、Cisco IOS Release 15.0(2) SG1 以降および Cisco IOS XE Release 3.2.1SG だけで使用できます。

hw-module system max-queue-limit コマンドを使用すると、Catalyst 4500 シリーズ スイッチでは、すべてのインターフェイスのキュー制限があるポリシーを適用する代わりに、すべてのインターフェイスのキュー制限をグローバルに変更できます。

キュー制限をグローバルに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# hw-module system max-queue-limit` *max-queue-limit*	すべてのインターフェイスのキュー制限をグローバルに設定します。 有効値の範囲は 1024 ～ 8184 です。値は 8 の倍数にする必要があります。

	コマンド	目的
ステップ 3	`Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	`Switch# reload`	スタンドアロン スーパーバイザ エンジンをリロードします。
	or	
	`Switch# redundancy reload shelf`	SSO モードで冗長スーパーバイザ エンジンをリロードします。
	`Switch# redundancy force-switchover`	RPR モードで冗長スーパーバイザ エンジンをリロードします。 このコマンドの後に、redundancy force-switchover をもう一度実行する必要があります。

これはグローバル コンフィギュレーション コマンドです。ポート単位、クラス単位の **queue-limit** コマンドで、これをオーバーライドできます。

スタンドアロン スーパーバイザ エンジンでは、このコマンドを適用した後に、エンジンをリブートする必要があります。

SSO モードの冗長スーパーバイザでは、両方のスーパーバイザに対して、**redundancy reload shelf** コマンドを入力し、強制的にリブートする必要があります。RPR モードの冗長スーパーバイザでは、両方のスーパーバイザにシステム キュー制限を適用するために、2 回連続してスイッチ オーバーを実行する必要があります。

次に、スタンドアロンのスーパーバイザ エンジンで、グローバルにキュー制限を 1024 に設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# hw-module system max-queue-limit 1024
Switch(config)# exit
Switch# reload  (for standalone supervisors)
Switch# redundancy reload shelf (for reduandancy supervisors in SSO mode)
or
Switch# redundancy force-switchover (followed by another redundancy force-switchover, for
reduandancy supervisors in RPR mode)
```

auto-QoS の設定

（注） auto-QoS は、VLAN または EtherChannel インターフェイスには適用できません。

（注） CDP をサポートするデバイスに接続されたポート上に auto-QoS ポリシーがある場合、そのポートは自動的に信頼されます。ただし、デバイスが CDP をサポートしない場合（レガシー Digital Media Player など）、QoS の信頼は手動で適用する必要があります。

Catalyst 4500 シリーズ スイッチは MQC モデルを採用しています。これは、特定のグローバル コンフィギュレーション（qos や qos dbl など）を使用する代わりに、スイッチ上のインターフェイスに適用された auto-QoS によって、いくつかのグローバル クラス マップおよびポリシー マップが設定されることを意味します。

auto-QoS はトラフィックを照合し、各一致パケットを qos-group に割り当てます。これにより、出力ポリシー マップは、プライオリティ キューを含む特定のキューに、特定の qos-group を配置できます。

着信と発信の両方向で QoS が必要です。着信時に、スイッチ ポートは、パケットの DSCP を信頼する必要があります（デフォルトで実行されます）。発信時に、スイッチ ポートは、音声パケットに「front of line」プライオリティを付与する必要があります。音声が発信キューの他のパケットの後ろで待機して、遅延が長くなりすぎる場合、パケットの受信時間の範囲外となるため、エンド ホストは、そのパケットをドロップします。

（注）　QoS は、2 車線の道路に例えることができます。そのため、一方向で動作する場合、他の方向では動作しません。

- 定義する必要がある 7 のポリシー マップがあります（5 つの入力と 2 つの出力）。
- AutoQos-4.0-Input-Policy
- AutoQos-VoIP-Input-Cos-Policy
- AutoQos-VoIP-Input-Dscp-Policy
- AutoQos-4.0-Cisco-Phone-Input-Policy
- AutoQos-4.0-Output-Policy
- AutoQos-4.0-Cisco-Softphone-Input-Policy
- AutoQos-VoIP-Output-Policy

すべてのポートで、COS の問題は、ネイティブ VLAN 上のパケットがゼロとしてマークされることです。

入力の照合に使用されるクラス マップは次のとおりです。

```
!for control traffic between the phone and the callmanager
!and phone to phone [Bearer] DSCP matching
!Note: Control traffic can be either AF31 or CS3.So, we match to both values and assign
them to different qos-groups when matching DSCP and only a single group when matching COS.

class-map match-all AutoQos-VoIP-Control-Dscp26
  match  dscp af31
class-map match-all AutoQos-VoIP-Control-Dscp24
  match  dscp cs3
class-map match-all AutoQos-VoIP-Bearer-Dscp
  match  dscp ef

!for control traffic and phone to phone [Bearer] COS matching
!Note: Both CS3 and AF31 control traffic maps to COS 3

class-map match-all AutoQos-VoIP-Control-Cos
  match cos  3
class-map match-all AutoQos-VoIP-Bearer-Cos
  match cos  5

!for control traffic between the softphonephone and the callmanager
!and softphone  to softphonephone [Bearer] DSCP matching
Class Map match-all AutoQos-4.0-Multimedia-Conf-Classify (id 36)
   Match access-group name AutoQos-4.0-ACL-Multimedia-Conf
Class Map match-all AutoQos-4.0-Signaling-Classify (id 2)
   Match access-group name AutoQos-4.0-ACL-Signaling
Class Map match-all AutoQos-4.0-Transaction-Classify (id 18)
   Match access-group name AutoQos-4.0-ACL-Transactional-Data
Class Map match-all AutoQos-4.0-Bulk-Data-Classify (id 29)
   Match access-group name AutoQos-4.0-ACL-Bulk-Data
Class Map match-all AutoQos-4.0-Scavenger-Classify (id 1)
   Match access-group name AutoQos-4.0-ACL-Scavenger
```

```
!for untrueted interfaces
class-map match-all AutoQos-4.0-Multimedia-Conf-Classify
           match access-group name AutoQos-4.0-ACL-Multimedia-Conf
   class-map match-all AutoQos-4.0-Signaling-Classify
     match access-group name AutoQos-4.0-ACL-Signaling
   class-map match-all AutoQos-4.0-Transaction-Classify
     match access-group name AutoQos-4.0-ACL-Transactional-Data
   class-map match-all AutoQos-4.0-Bulk-Data-Classify
     match access-group name AutoQos-4.0-ACL-Bulk-Data
   class-map match-all AutoQos-4.0-Scavenger-Classify
     match access-group name AutoQos-4.0-ACL-Scavenger
         class-map match-all AutoQos-4.0-Default-Classify
     match access-group name AutoQos-4.0-ACL-Default

!for interfaces with video devices
class-map match-any AutoQos-4.0-VoIP
      match dscp ef
      match cos 5
    class-map match-all AutoQos-4.0-Broadcast-Vid
      match dscp cs5
    class-map match-all AutoQos-4.0-Realtime-Interact
      match dscp cs4
    class-map match-all AutoQos-4.0-Network-Ctrl
      match dscp cs7
    class-map match-all AutoQos-4.0-Internetwork-Ctrl
      match dscp cs6
    class-map match-any AutoQos-4.0-Signaling
      match dscp cs3
      match cos 3
    class-map match-all AutoQos-4.0-Network-Mgmt
      match dscp cs2
    class-map match-any AutoQos-4.0-Multimedia-Conf
      match dscp af41
      match dscp af42
      match dscp af43
   class-map match-any AutoQos-4.0-Multimedia-Stream
      match dscp af31
      match dscp af32
      match dscp af33
    class-map match-any AutoQos-4.0-Transaction-Data
      match dscp af21
      match dscp af22
      match dscp af23
    class-map match-any AutoQos-4.0-Bulk-Data
      match dscp af11
      match dscp af12
      match dscp af13
    class-map match-all AutoQos-4.0-Scavenger
      match dscp cs1
```

クラス マップの目的は、制御トラフィックとデータ（ベアラ）音声トラフィックがレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスを特定することです。

DSCP と COS が発信ポリシー マップで使用される割り当て済み qos-group に設定される場合、2 つの入力ポリシー マップ（1 つは DSCP 照合用、もう 1 つは CoS 照合用）は、次のとおりです。

```
policy-map AutoQos-VoIP-Input-Dscp-Policy
  class AutoQos-VoIP-Bearer-Dscp
   set qos-group 46
  class AutoQos-VoIP-Control-Dscp26
   set qos-group 26
  class AutoQos-VoIP-Control-Dscp24
   set qos-group 24
```

```
!Note: For COS, Control traffic only has a single COS value of 3 (versus DSCP which has 2
values to match).So, only 2 class-maps instead of 3 like above.

policy-map AutoQos-VoIP-Input-Cos-Policy
  class AutoQos-VoIP-Bearer-Cos
   set qos-group 46
  class AutoQos-VoIP-Control-Cos
   set qos-group 24

Policy Map AutoQos-4.0-Input-Policy
    Class AutoQos-4.0-VoIP
      set qos-group 32
    Class AutoQos-4.0-Broadcast-Vid
      set qos-group 32
    Class AutoQos-4.0-Realtime-Interact
      set qos-group 32
    Class AutoQos-4.0-Network-Ctrl
      set qos-group 16
    Class AutoQos-4.0-Internetwork-Ctrl
      set qos-group 16
    Class AutoQos-4.0-Signaling
      set qos-group 16
    Class AutoQos-4.0-Network-Mgmt
      set qos-group 16
    Class AutoQos-4.0-Multimedia-Conf
      set qos-group 34
    Class AutoQos-4.0-Multimedia-Stream
      set qos-group 26
    Class AutoQos-4.0-Transaction-Data
      set qos-group 18
    Class AutoQos-4.0-Bulk-Data
      set qos-group 10
    Class AutoQos-4.0-Scavenger
      set qos-group 8


  Policy Map AutoQos-4.0-Cisco-Phone-Input-Policy
    Class AutoQos-4.0-VoIP-Data-Cos
      set dscp ef
      set qos-group 32
     police cir 128000 bc 8000
       conform-action transmit
       exceed-action set-dscp-transmit cs1
       exceed-action set-cos-transmit 1
    Class AutoQos-4.0-VoIP-Signal-Cos
      set dscp cs3
      set qos-group 16
     police cir 32000 bc 8000
       conform-action transmit
       exceed-action set-dscp-transmit cs1
       exceed-action set-cos-transmit 1
    Class AutoQos-4.0-Default-Classify
      set dscp default
      set cos 0
     police cir 10000000 bc 8000
       conform-action transmit
       exceed-action set-dscp-transmit cs1
       exceed-action set-cos-transmit 1

Policy Map AutoQos-4.0-Cisco-Softphone-Input-Policy
    Class AutoQos-4.0-VoIP-Data
      set dscp ef
      set cos 5
      set qos-group 32
```

```
    police cir 128000 bc 8000
      conform-action transmit
      exceed-action set-dscp-transmit cs1
      exceed-action set-cos-transmit 1
  Class AutoQos-4.0-VoIP-Signal
    set dscp cs3
    set cos 3
    set qos-group 16
   police cir 32000 bc 8000
     conform-action transmit
     exceed-action set-dscp-transmit cs1
     exceed-action set-cos-transmit 1
  Class AutoQos-4.0-Multimedia-Conf-Classify
    set dscp af41
    set cos 4
    set qos-group 34
   police cir 5000000 bc 8000
     conform-action transmit
     exceed-action drop
  Class AutoQos-4.0-Signaling-Classify
    set dscp cs3
    set cos 3
    set qos-group 16
   police cir 32000 bc 8000
     conform-action transmit
     exceed-action drop
  Class AutoQos-4.0-Transaction-Classify
    set dscp af21
    set cos 2
    set qos-group 18
   police cir 10000000 bc 8000
     conform-action transmit
     exceed-action set-dscp-transmit cs1
     exceed-action set-cos-transmit 1
  Class AutoQos-4.0-Bulk-Data-Classify
    set dscp af11
    set cos 1
    set qos-group 10
   police cir 10000000 bc 8000
     conform-action transmit
     exceed-action set-dscp-transmit cs1
     exceed-action set-cos-transmit 1
  Class AutoQos-4.0-Scavenger-Classify
    set dscp cs1
    set cos 1
    set qos-group 8
   police cir 10000000 bc 8000
     conform-action transmit
     exceed-action drop
  Class AutoQos-4.0-Default-Classify
    set dscp default
    set cos 0

Policy Map AutoQos-4.0-Classify-Input-Policy
  Class AutoQos-4.0-Multimedia-Conf-Classify
    set dscp af41
    set cos 4
    set qos-group 34
  Class AutoQos-4.0-Signaling-Classify
    set dscp cs3
    set cos 3
    set qos-group 16
  Class AutoQos-4.0-Transaction-Classify
    set dscp af21
```

```
      set cos 2
      set qos-group 18
    Class AutoQos-4.0-Bulk-Data-Classify
      set dscp af11
      set cos 1
      set qos-group 10
    Class AutoQos-4.0-Scavenger-Classify
      set dscp cs1
      set cos 1
      set qos-group 8
    Class AutoQos-4.0-Default-Classify
      set dscp default
      set cos 0
```

出力の照合に使用されるクラス マップは次のとおりです。

```
!Since we assigned matched traffic to a qos-group on input,
!we only need to match the qos-group on output

!Note: Any other traffic not matched on input and assigned to a qos-group goes into the
class-default queue

!for control traffic (CS3 and AF31)
class-map match-all AutoQos-VoIP-Control-QosGroup24
  match qos-group 24
class-map match-all AutoQos-VoIP-Control-QosGroup26
  match qos-group 26

!For phone to phone (Bearer EF) traffic
class-map match-all AutoQos-VoIP-Bearer-QosGroup
  match qos-group 46

!For softphone
Class Map match-any AutoQos-4.0-Scavenger-Queue (id 24)
   Match qos-group 8
   Match   dscp cs1 (8)
Class Map match-all AutoQos-4.0-Priority-Queue (id 3)
   match qos-group 32
Class Map match-all AutoQos-4.0-Control-Mgmt-Queue (id 28)
   Match qos-group 16
Class Map match-all AutoQos-4.0-Multimedia-Conf-Queue (id 10)
   Match qos-group 34
Class Map match-all AutoQos-4.0-Multimedia-Stream-Queue (id 5)
   Match qos-group 26
Class Map match-all AutoQos-4.0-Trans-Data-Queue (id 30)
   Match qos-group 18
Class Map match-all AutoQos-4.0-Bulk-Data-Queue (id 17)
   Match qos-group 10
!These classes are required by all SRND4 clis
class-map match-all AutoQos-4.0-Priority-Queue
      match qos-group 32
    class-map match-all AutoQos-4.0-Control-Mgmt-Queue
      match qos-group 16
    class-map match-all AutoQos-4.0-Multimedia-Conf-Queue
      match qos-group 34
    class-map match-all AutoQos-4.0-Multimedia-Stream-Queue
      match qos-group 26
    class-map match-all AutoQos-4.0-Trans-Data-Queue
      match qos-group 18
    class-map match-all AutoQos-4.0-Bulk-Data-Queue
            match qos-group 10
    class-map match-any AutoQos-4.0-Scavenger-Queue
      match qos-group 8
      match dscp cs1
```

出力ポリシー マップは、次のとおりです。

```
!Each class maps to a different qos-group with
!class-default taking any traffic not assigned to a qos-group

!Note: in this example, the outbound policy map drops voice packets when the priority
queue exceeds 33% utilization of the link.Each deployment must establish their own upper
bound for voice packets.

policy-map AutoQos-VoIP-Output-Policy
  class AutoQos-VoIP-Bearer-QosGroup
   set dscp ef
   set cos 5
   priority
   police cir percent 33
  class AutoQos-VoIP-Control-QosGroup26
   set dscp af31
   set cos 3
   bandwidth remaining percent 5
  class AutoQos-VoIP-Control-QosGroup24
   set dscp cs3
   set cos 3
   bandwidth remaining percent 5
  class class-default
   dbl
```

（注） デフォルトの CoS と DSCP または dscp と cos のマッピングはありません。値は、トランクに対して明示的に設定する必要があります。

```
Policy Map AutoQos-4.0-Output-Policy
    Class AutoQos-4.0-Scavenger-Queue
      bandwidth remaining percent 1
    Class AutoQos-4.0-Priority-Queue
      priority
     police cir percent 30 bc 33 ms
       conform-action transmit
       exceed-action drop
    Class AutoQos-4.0-Control-Mgmt-Queue
      bandwidth remaining percent 10
    Class AutoQos-4.0-Multimedia-Conf-Queue
      bandwidth remaining percent 10
    Class AutoQos-4.0-Multimedia-Stream-Queue
      bandwidth remaining percent 10
    Class AutoQos-4.0-Trans-Data-Queue
      bandwidth remaining percent 10
      dbl
    Class AutoQos-4.0-Bulk-Data-Queue
      bandwidth remaining percent 4
      dbl
    Class class-default
      bandwidth remaining percent 25
      dbl
```

3 つのポリシー マップは次のように定義されます。

- policy-map AutoQos-VoIP-Input-Dscp-Policy

  このポリシー マップは、Auto-QoS がポート上で設定されるとき、レイヤ 3 インターフェイス（ネイバー スイッチへのアップリンク接続など）に入力サービス ポリシーとして適用されます。

- policy-map AutoQos-VoIP-Input-Cos-Policy

このポリシー マップは、アップリンク接続または Cisco IP Phone にフックされたポートのいずれかの、レイヤ 2 インターフェイスに入力サービス ポリシーとして適用されます。

- policy-map AutoQos-VoIP-Output-Policy

  このポリシー マップは、Auto-QoS が設定されている任意のポートの出力ポリシーとして適用され、トラフィックが音声データか制御トラフィックかに従ってポート上で出力トラフィックを管理するポリシーを確立します。

入力ポリシー マップの目的は、音声データまたは制御トラフィック識別し、マーク付けしながらスイッチを通過させることです。出力ポリシー マップは、入力時に発生するマーク付けでパケットに一致させ、帯域幅、ポリシングまたはプライオリティ キューイングなどの出力パラメータを適用します。

スイッチ対スイッチの接続の場合、インターフェイス上での入力および出力サービス ポリシーの適用には、**[no] auto qos voip trust** コマンドが使用されます。

```
service-policy input AutoQos-VoIP-Input-Cos-Policy
```

または

```
service-policy input AutoQos-VoIP-Input-Dscp-Policy
```

および

```
service-policy output AutoQos-VoIP-Output-Policy
```

入力ポリシーの選択は、ポートがレイヤ 2 かレイヤ 3 かに依存します。レイヤ 2 の場合、ポリシーは、受信したパケットの Cos 設定を信頼します。レイヤ 3 ポートの場合、パケットに含まれる DSCP 値に依存します。

電話接続ポートの場合、ポートへの次のサービス ポリシーの適用には、**[no] auto qos voice cisco-phone** コマンドが使用されます。

```
qos trust device cisco-phone

service-policy input AutoQos-VoIP-Input-Cos-Policy
```

および

```
service-policy output AutoQos-VoIP-Output-Policy
```

ここでは、Cisco IP Phone を認識する信頼境界が確立され、電話からのパケットの CoS 設定を信頼します。Cisco IP Phone が検出されない場合、CoS フィールドは無視され、パケットは音声トラフィックとして分類されません。Cisco Phone が検出されると、パケット内の CoS 値に基づいて入力パケットにマークが付けられます。このマーキングは、出力で適切なトラフィック分類と処理のために使用されます。

auto qos srnd4 : 新しい auto qos コマンドがインターフェイスで設定されたときに生成され、新しい設定を生成するためにレガシー CLI から移行します。この CLI は、移行時に、1 つ以上のインターフェイスでレガシー auto-QoS がイネーブルになっている場合にだけ、グローバル設定を生成します。

auto qos video : 信頼できないインターフェイスの QoS 設定を生成します。これは、信頼できないデスクトップおよびデバイスからのトラフィックを分類し、それに従ってマークを付けるためのサービスポリシーを組み込んでいます。

auto qos void cisco-softphone : Cisco IP SoftPhone アプリケーションを実行している PC に接続されたインターフェイスの QoS 設定を生成し、このようなインターフェイスから生じたポリシング トラフィックとしてマークを付けます。この CLI で設定されたポートは、信頼できないと見なされます。

auto qos classify : 信頼できないインターフェイスの QoS 設定を生成します。これは、信頼できないデスクトップまたはデバイスから生じるトラフィックを分類し、それに従ってマークを付けるためのサービスポリシーを適用します。生成されたサービス ポリシーは、ポリシングされません。