CHAPTER 32

Quality of Service の設定

（注） Catalyst 4900M および Supervisor Engine 6-E の QoS 機能は同等です。

この章では、Automatic QoS（Auto-QoS）コマンドまたは標準の QoS コマンドを使用して Catalyst 4500 シリーズ スイッチ上で Quality of Service（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。この章では、Supervisor Engine II-Plus から V-10GE まで、および Supervisor Engine 6-E での QoS サポートについて説明します。

この章の内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

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

Catalyst 4500 シリーズ スイッチでの 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、適度なタイミングで配信される可能性はどのトラフィックでも同等です。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

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 32-1 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。

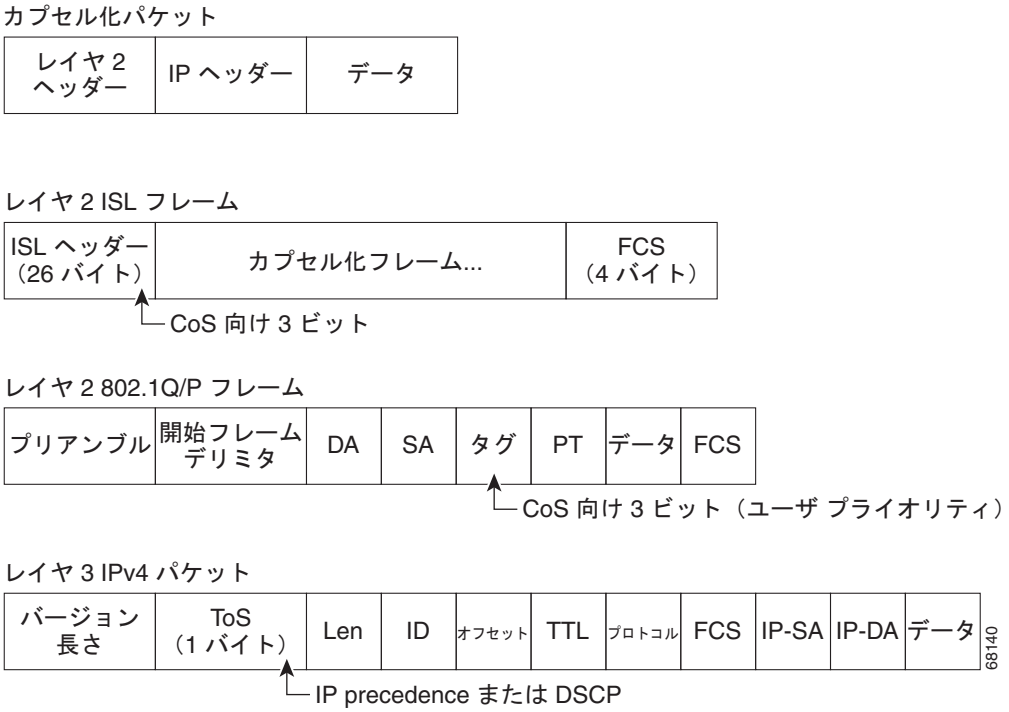
- レイヤ 3 パケットのプライオリティ ビット

  レイヤ 3 IP パケットは、IP precedence 値または Diffserv コード ポイント（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 32-1　　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*は、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 Diffserv コード ポイント（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。「DSCP マップの設定」（P.32-59）を参照してください。

（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 32-1 を参照してください。

表 32-1　IP precedence 値と DSCP 値

3 ビット IP Precedence	ToS の MSb[1] 6 ビット						6 ビット DSCP		3 ビット IP Precedence	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 32-1　IP precedence 値と DSCP 値 （続き）

3 ビット IP Precedence	ToS の MSb[1] 6 ビット						6 ビット DSCP		3 ビット IP Precedence	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。
- *スケジューリング*: レイヤ 2 フレームをキューに割り当てることです。QoS は、内部 DSCP 値（「内部 DSCP 値」（P.32-14）を参照）に基づいて、キューにフレームを割り当てます。
- *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廃棄が可能になります。

QoS の基本モデル

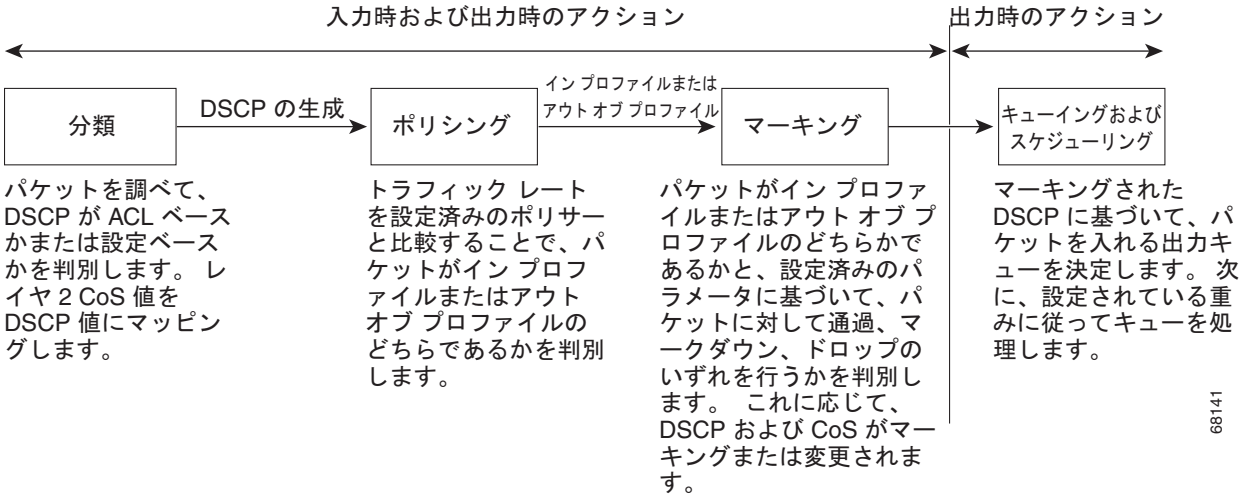
図 32-2 に、QoS の基本モデル（スイッチ QoS モデルとも呼びますが、MQC 準拠ではありません）を示します。入力インターフェイスおよび出力インターフェイスで行われるアクションには、トラフィックの分類、ポリシング、およびマーキングがあります。

- 分類は、トラフィックの種類を区別します。このプロセスによって、パケットの内部 DSCP が生成されます。内部 DSCP は、今後このパケットに対して実行されるすべての QoS アクションを表します。詳細については、「分類」（P.32-6）を参照してください。
- ポリシングは、トラフィック レートを設定済みのポリサーと比較することによって、パケットがイン プロファイルであるか、それともアウト オブ プロファイルであるかを判別します。ポリサーは、トラフィック フローが消費する帯域幅を制限します。この判別の結果が、マーカーに引き渡されます。詳細については、「ポリシングおよびマーキング」（P.32-10）を参照してください。
- マーキングは、パケットがアウト オブ プロファイルのときに行われるアクションに関してポリサーの設定情報を評価し、パケットの処置（変更なしにパケットを通過させるか、パケット内の DSCP 値をマーク ダウンするか、パケットをドロップするか）を決定します。詳細については、「ポリシングおよびマーキング」（P.32-10）を参照してください。

出力インターフェイスで行われるアクションには、キューイングおよびスケジューリングがあります。

- キューイングは、内部 DSCP を評価し、4 つの出力キューのどれにパケットを入れるかを決定します。
- スケジューリングは、出力（送信）ポートの共有およびシェーピング設定に基づいて、4 つの出力（送信）キューを処理します。共有およびシェーピング設定については、「キューイングおよびスケジューリング」（P.32-15）を参照してください。

図 32-2　QoS の基本モデル



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。QoS がスイッチ上でグローバルにイネーブルになっている場合のみ、分類はイネーブルです。デフォルトでは、QoS はグローバルにディセーブルになっているため、分類は実行されません。

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。

図 32-3 に、さまざまな分類オプションを示します。

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。

- ポート デフォルトを使用します。パケットが IP 以外のパケットである場合、デフォルトのポート DSCP 値を着信パケットに割り当てます。
- 着信フレームの CoS 値を信頼します（ポートが CoS を信頼するように設定します）。この場合、設定変更可能な CoS/DSCP マップを使用して、内部 DSCP 値を生成します。レイヤ 2 の ISL フレーム ヘッダーの場合、CoS 値は 1 バイトのユーザ フィールドの下位 3 ビットに格納されて伝達されます。レイヤ 2 802.1Q フレーム ヘッダーでは、タグ制御情報フィールドの最上位ビット 3 ビットを使用して CoS 値を伝送します。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。フレームに CoS 値が含まれていない場合は、着信フレームにデフォルトのポート CoS を割り当てます。

  Trust DSCP の設定は、IP 以外のトラフィックに対しては無意味です。ポートを Trust DSCP に設定し、IP 以外のトラフィックを受信した場合、スイッチはデフォルトのポート DSCP を割り当てます。

（注）　Catalyst 4948-10GE、Supervisor V-10GE、および Supervisor V で、.1Q タグおよび（すべての x 値に対して）Pri=x 値を指定して非 IP トラフィック（IPX など）をポート 1 から送信する場合、srcMac の変化に応じて出力インターフェイスでの送信 CoS は変化します。

ポリシー マップの「Trust DSCP」は、IP パケットにだけ機能します。非 IP パケットが「Trust DSCP」アクションのクラスによって照合されると、非 IP パケットは、別の方法で想定されるように非動作（no-OP）として「Trust DSCP」を処理するのではなく、ランダムな CoS 値で送信される可能性があります。

回避策：非 IP パケットと一致しないクラスに「Trust DSCP」が適用されるように、クラスマップの分類基準をより細かくします。IPv4 トラフィックのみと一致するクラスに「Trust DSCP」が適用されるように、一致する IP パケットと非 IP の両方と一致するクラスマップを一連のクラスマップに分類します。クラスマップ一致非 IPv4 トラフィックの場合、「trust cos」を使用できます。

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。

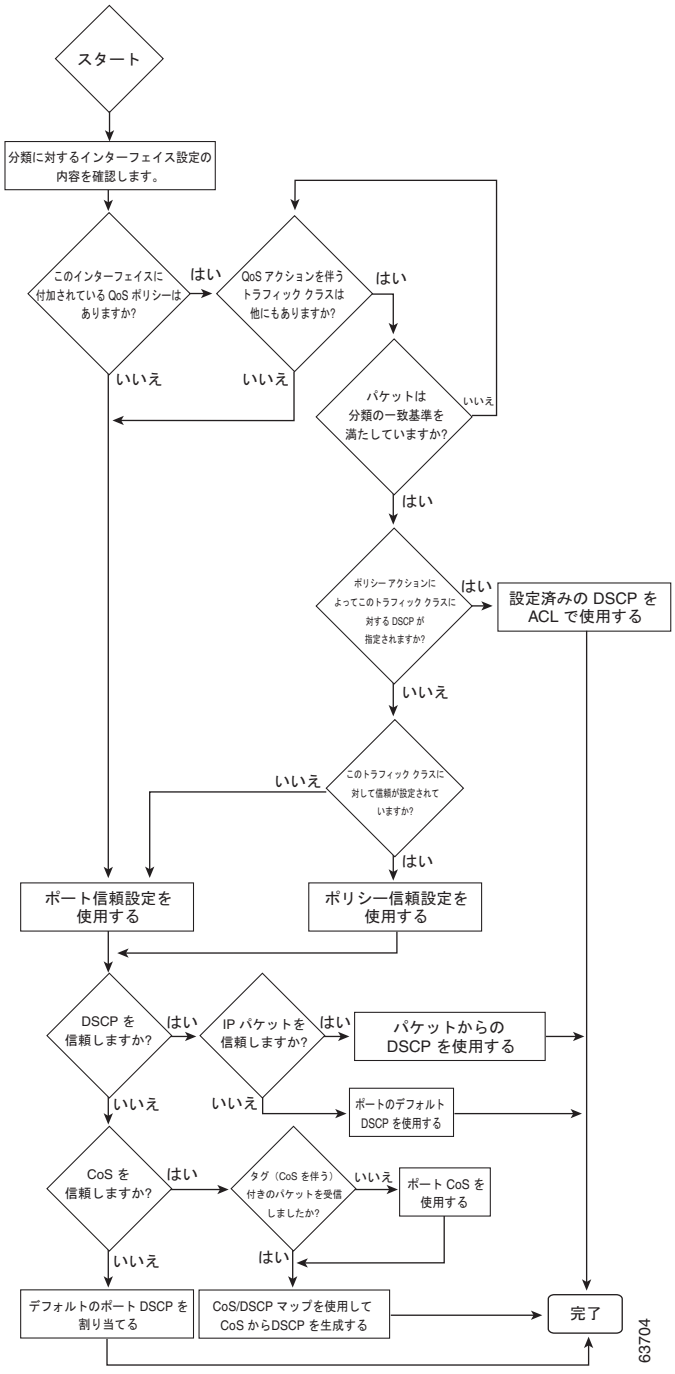
- 着信パケットの IP DSCP を信頼し（ポートを Trust DSCP に設定し）、パケットに同じ DSCP を割り当てて内部的に使用します。IETF は、1 バイトの Type of Service（ToS; タイプ オブ サービス）フィールドの最上位ビット 6 ビットを DSCP として定義しています。特定の DSCP 値が表すプライオリティは、設定可能です。DSCP 値の範囲は 0 ～ 63 です。
- 着信パケットの CoS 値（存在する場合）を信頼し、CoS/DSCP マップを使用して DSCP を生成します。
- 設定された IP 標準 ACL または拡張 ACL（IP ヘッ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。ACL を設定していない場合は、入力ポートの信頼状態に基づいてデフォルトの DSCP がパケットに割り当てられます。ACL を設定している場合は、ポリシー マップによって着信フレームに割り当てる DSCP が指定されます。

（注）　入力 QoS ポリシーが実行するマーキングに基づいてトラフィックを分類することはできません。Catalyst 4500 プラットフォームでは、入力および出力 QoS の検索が平行して実行されるため、出力 QoS ポリシーでトラフィックを分類するのに入力時にマーク付けされた DSCP 値を使用できません。

（注）　*内部 DSCP* に基づいてトラフィックを分類することはできません。*内部 DSCP* は、すべてのパケットで送信キューおよび送信 CoS 値を決定するためだけに使用される純粋な内部分類メカニズムです。

ここで説明されているマップの詳細については、「マッピング テーブル」（P.32-15）を参照してください。ポートの信頼状態の設定情報については、「インターフェイスの信頼状態の設定」（P.32-54）を参照してください。

図 32-3　分類のフローチャート



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 マップで一致（*match*）文を使用して一致基準を指定します。一致文では、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 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.32-9）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一致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 つの一致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、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、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。設定については、「QoS ポリシーの設定」（P.32-34）を参照してください。

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。アクションとしては、トラフィック クラスの CoS 値または DSCP 値を信頼すること、トラフィック クラスの特定の DSCP 値または IP precedence 値の設定、またはトラフィックの帯域幅制限の指定およびトラフィックがアウト オブ プロファイルであるときのアクションを含めることができます。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、**trust** または **set** 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べき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.32-10）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 255 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。
- ポリシー マップの信頼状態は、インターフェイスの信頼状態を上書きします。

設定については、「QoS ポリシーの設定」（P.32-34）を参照してください。

ポリシングおよびマーキング

パケットが分類され、パケットに内部 DSCP 値が割り当てられると、ポリシングおよびマーキングのプロセスが開始可能になります（図 32-4 を参照）。

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。ポリシング済み DSCP マップの詳細については、「マッピング テーブル」（P.32-15）を参照してください。

次の種類のポリサーを作成できます。

- 個別

  ポリシー マップが付加されている各ポート /VLAN に対して、QoS がポリサーで指定される帯域幅制限を一致する各トラフィック クラスに個別に適用します。ポリシー マップでこのタイプのポリサーを設定するには、ポリシー マップ クラス コンフィギュレーション モードで **police** コマンドを使用します。

- 集約

  一致するすべてのトラフィック フローに、集約ポリサーで指定される帯域幅制限が累積的に適用されます。ポリシー マップで、集約ポリサー名を指定してこのタイプのポリサーを設定するには、**police aggregate** 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。ポリサーの帯

域幅制限を指定するには、**qos aggregate-policer** 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。このようにして、集約ポリサーはポリシー マップ内にある複数のトラフィック クラスで共有されます。

- フローまたはマイクロフロー

  フローベースのポリシングでは、識別されたすべてのフローが、指定したレートに個別にポリシングされます。フローはダイナミックなので、キー識別フィールドをクラス マップで設定する必要があります。2 つのフロー一致オプション、*送信元 IP* ベース（送信元 IP アドレスが一意であるそれぞれのフローを新しいフローとして扱う）および*宛先 IP* ベース（宛先 IP アドレスが一意であるそれぞれのフローを新しいフローとして扱う）を指定できます。フローベースのポリサーの設定については、「User Based Rate Limiting の設定」（P.43）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。

- IP パケットでは、IP ペイロードの長さ（IP ヘッダーの全長フィールド）だけがポリシング演算でポリサーに使用されます。レイヤ 2 ヘッダーとトレーラーの長さは計上されていません。たとえば、64 バイトの Ethernet II IP パケットでは、46 バイトだけがポリシングに計上されます（64 バイト - 14 バイトのイーサネット ヘッダー - 4 バイトのイーサネット CRC）。

  IP 以外のパケットでは、レイヤ 2 ヘッダーに指定されたレイヤ 2 の長さは、ポリシング演算でポリサーに使用されます。IP パケットをポリシングする場合、さらにレイヤ 2 カプセル化の長さを指定するには、**qos account layer2 encapsulation** コマンドを使用します。

- デフォルトで設定されるポリサーはありません。
- 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。
- 個別ポリサーおよび集約ポリサーのポリシングは、入力インターフェイスと出力インターフェイスのどちらでも行えます。
  - Supervisor Engine V-10GE（WS-X4516-10GE）の場合は、8192 個のポリサーが入力および出力でサポートされます。
  - その他のスーパーバイザ エンジンでは、1024 個のポリサーが入力および出力でサポートされます。

（注） 入力および出力の方向で 4 個のポリサーが予約されています。

- ポリサーは、個別タイプか集約タイプにすることができます。Supervisor Engine V-10GE では、フローベース ポリサーがサポートされます。
- フロー ポリサーのポリシングは、入力レイヤ 3 インターフェイスだけで行えます。
  - Supervisor Engine V-10GE では、512 個の一意のフロー ポリサーを設定できます。

（注） 1 つのフロー ポリサーがソフトウェアによって予約されているので、511 個の一意のフロー ポリサーを定義できます。

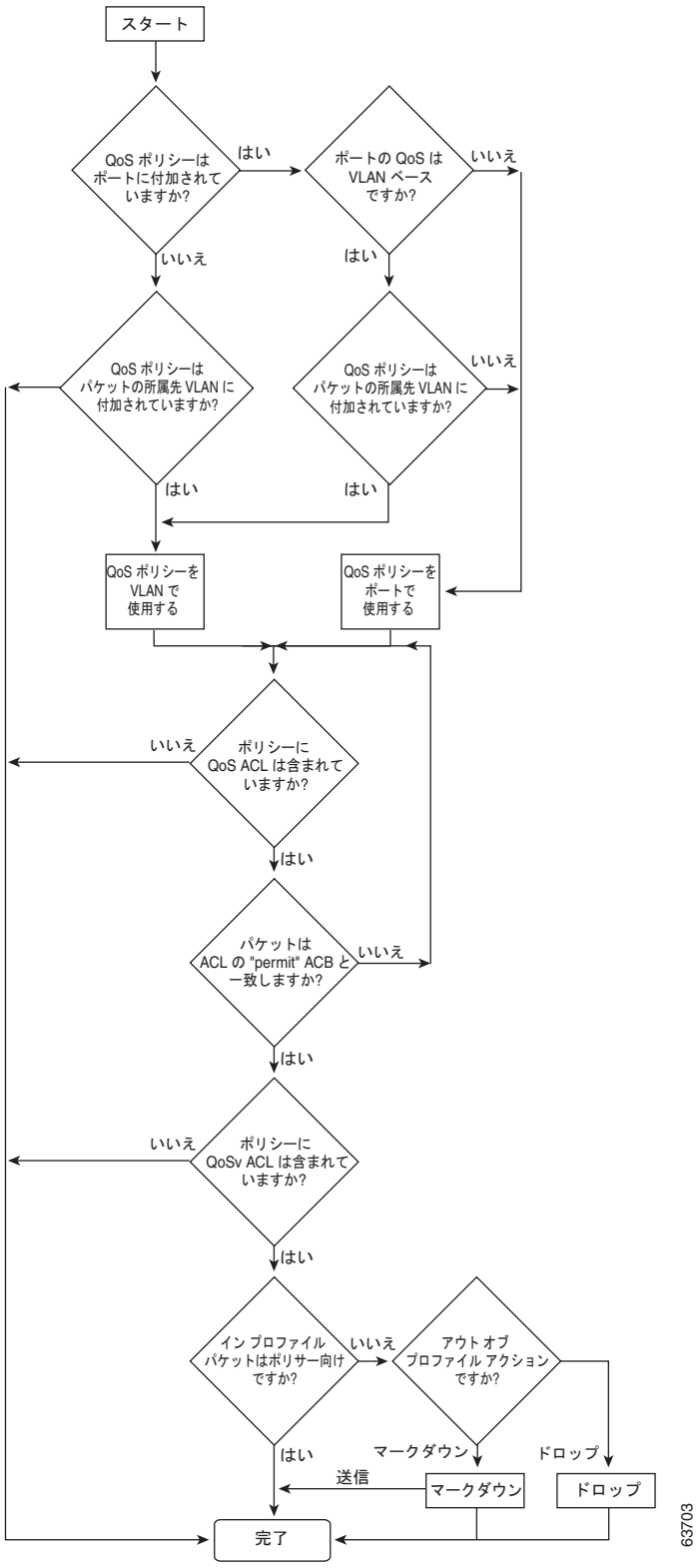
  - 100,000 より多いフローをマイクロフロー ポリシングできます。

（注） マイクロフローでは、現在のところ 2 つのフロー一致オプション（送信元 IP アドレス ベースおよび宛先 IP アドレス ベース）がサポートされます。マイクロフロー ポリシングを Netflow 統計情報収集と併用するとき、送信元 IP アドレスか宛先 IP アドレスが一致するフローの完全なフロー統計は使用できません。Netflow 統計の設定については、「NetFlow 統計情報収集機能のイネーブル化」（P.46-7）を参照してください。

- QoS を設定したインターフェイス上では、そのインターフェイス経由で送受信されるすべてのトラフィックが、インターフェイスに付加されたポリシー マップに従って、分類、ポリシング、およびマーク付けされます。ただし、インターフェイスが **qos vlan-based** コマンドによって VLAN ベース QoS を使用するように設定されている場合は、そのインターフェイス経由で送受信されるトラフィックは、パケットの所属先 VLAN に付加されたポリシー マップ（VLAN インターフェイス上に設定されている）に従って、分類、ポリシング、およびマーク付けされます。パケットの所属先 VLAN にポリシー マップが付加されていない場合には、インターフェイスに付加されたポリシー マップが使用されます。

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。設定の詳細については、「QoS ポリシーの設定」（P.32-34）および「名前付き集約ポリサーの作成」（P.32-32）を参照してください。

図 32-4　ポリシングおよびマーキングのフローチャート



内部 DSCP 値

ここでは、内部 DSCP 値について説明します。

内部 DSCP の作成元

QoS は処理中、すべてのトラフィック（IP 以外のトラフィックを含む）のプライオリティを、内部 DSCP 値で表します。QoS は、次のものに基づいて内部 DSCP 値を作成します。

- Trust CoS トラフィックの場合、受信したレイヤ 2 CoS 値または入力インターフェイスのレイヤ 2 CoS 値
- Trust DSCP トラフィックの場合、受信した DSCP 値または入力インターフェイスの DSCP 値
- 信頼されない（untrusted）トラフィックの場合、入力インターフェイスの DSCP 値

トラフィックの信頼状態は、入力インターフェイスの信頼状態です。ただし、ポリシー アクションによりトラフィック クラスに対して別の設定が行われる場合を除きます。

QoS は、設定変更可能な各種のマッピング テーブルを使用して、3 ビットの CoS から 6 ビットの内部 DSCP 値を導き出します（「DSCP マップの設定」（P.32-59）を参照）。

出力 ToS および CoS の作成元

出力 IP トラフィックについては、QoS は内部 DSCP 値から ToS バイトを作成して、出力インターフェイスに送信し、それが IP パケットに書き込まれます。**trust-dscp** および **untrusted** IP トラフィックの場合、ToS バイトには、受信した ToS バイトの元の最下位 2 ビットが含まれます。

（注）　内部 ToS 値は IP precedence 値を使用します（表 32-1（P.32-4）を参照）。

すべての出力トラフィックについて、QoS は設定変更可能なマッピング テーブルを使用して、トラフィックと対応付けられた内部 ToS 値から CoS 値を導き出します（「DSCP/CoS マップの設定」（P.32-61）を参照）。QoS は CoS 値を送信して、ISL フレームおよび 802.1Q フレームに書き込ませます。

qos trust cos コマンドを使用して *trust cos* に設定された入力インターフェイスに着信したトラフィックの場合、送信される CoS は、常に着信パケットの CoS（または、パケットをタグなしで受信した場合には、入力インターフェイスのデフォルト CoS）です。

qos trust dscp コマンドを使用してインターフェイスの信頼状態を *trust dscp* に設定していない場合、セキュリティおよび QoS ACL 分類では、常にインターフェイス DSCP が使用され、着信パケットの DSCP は使用されません。

マッピング テーブル

QoS の処理中、スイッチはすべてのトラフィック（IP 以外のトラフィックを含む）のプライオリティを、内部 DSCP 値で表します。

- 分類の際、QoS は設定変更可能なマッピング テーブルを使用して、受信した CoS から内部 DSCP（6 ビット値）を導き出します。これらのマップには、CoS/DSCP マップが含まれます。
- ポリシングの際、QoS は IP パケットまたは IP 以外のパケットに別の DSCP 値を割り当てることがあります（パケットがアウト オブ プロファイルであり、なおかつポリサーでマークダウン後の DSCP 値が指定されている場合）。この設定可能なマップは、ポリシング済み DSCP マップといいます。
- トラフィックがスケジューリング段階に達する前に、QoS は内部 DSCP を使用して、4 つの出力キューのうち 1 つを出力処理用に選択します。DSCP から出力キューへのマッピングは、**qos map dscp to tx-queue** コマンドを使用して設定します。

CoS/DSCP および DSCP/CoS マップのデフォルト値は、ネットワークに適している場合も、適していない場合もあります。

設定については、「DSCP マップの設定」（P.32-59）を参照してください。

キューイングおよびスケジューリング

各物理ポートには、4 つの送信キュー（出力キュー）があります。送信する必要がある各パケットは、いずれかの送信キューに格納されます。各送信キューは、送信キュー スケジューリング アルゴリズムに基づいて処理されます。

（DSCP のマークダウンも含めて）最終的な送信 DSCP が算出されると、送信 DSCP と送信キューのマッピング設定によって、送信キューが決定されます。パケットは、送信 DSCP から決定された送信ポートの送信キューに格納されます。送信 DSCP と送信キューのマッピングを設定するには、**qos map dscp to tx-queue** コマンドを使用します。パケットが入力ポートおよび出力ポートの QoS ポリシーおよび信頼状態の設定によって判別された IP 以外のパケットである場合、送信 DSCP は内部 DSCP 値です。

設定については、「送信キューの設定」（P.32-56）を参照してください。

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するか、パケット ヘッダーの明示的輻輳通知（ECN）ビットを設定します。

DBL は、フローをアダプティブとアグレッシブの 2 つのカテゴリに分類します。アダプティブ フローは、輻輳通知を受信するとパケット伝送レートを減らします。アグレッシブ フローは、輻輳通知に対してどのような修正措置も行いません。すべてのアクティブ フローに対して、スイッチは「buffersUsed」および「credits」という 2 つのパラメータを保持します。すべてのフローは、グローバル パラメータの「max-credits」から開始されます。credits が「aggressive-credits」（別のグローバル パラメータ）より少ないフローの場合、アグレッシブ フローと見なされ、「aggressiveBufferLimit」と呼ばれる小さなバッファ制限が指定されます。

キュー長は、パケット数によって測定されます。キュー内のパケット数により、フローに与えられるバッファ スペースのサイズが決定します。フローのキュー長が長い場合、算出値は低下します。これにより、新規着信フロー用のバッファ スペースがキュー内に確保されます。この結果、すべてのフローが、キュー内につり合いがとれた割合のパケットを置くことができます。

インターフェイスごとに 4 つの送信キューがあり、DBL はキュー単位のメカニズムであるため、DSCP 値により DBL の適用がさらに複雑になる可能性があります。

次の表に、デフォルトの DSCP と送信キューのマッピングを示します。

DSCP	送信キュー
0 ～ 15	1
16 ～ 31	2
32 ～ 48	3
49 ～ 63	4

たとえば、2 つのストリームを送信するとき、1 つのストリームは 16 の DSCP で、もう 1 つのストリームは値が 0 の場合、これらのストリームは別々のキューから送信されます。送信キュー 2 のアグレッシブ フロー（16 の DSCP を持つパケット）がリンクを飽和させる可能性があっても、0 の DSCP を持つパケットは送信キュー 1 から送信されるため、アグレッシブ フローでブロックされません。したがって、DBL がなくても、DSCP 値によって送信キュー 1、3、または 4 に配置されるパケットはアグレッシブ フローによってドロップされません。

送信キュー間のリンク帯域幅の共有

送信ポートの 4 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。送信キュー間でリンク帯域幅を共有する方法を変更するには、インターフェイス送信キュー コンフィギュレーション モードで **bandwidth** コマンドを使用します。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。

Supervisor Engine II-Plus、Supervisor Engine II-Plus TS、Supervisor Engine III、Supervisor Engine IV を使用するシステムの場合、帯域幅を設定できるのは次のポートにかぎられます。

- スーパーバイザ エンジン上のアップリンク ポート
- WS-X4306-GB GBIC モジュール上のポート
- WS-X4506-GB-T CSFP モジュール上のポート
- WS-X4232-GB-RJ モジュール上の 2 つの 1000BASE-X ポート
- WS-X4418-GB モジュール上の最初の 2 つのポート
- WS-X4412-2GB-TX モジュール上の 2 つの 1000BASE-X ポート

Supervisor Engine V を使用するシステムの場合、帯域幅はすべてのポート（10/100 FastEthernet、10/100/1000BASE-T、1000BASE-X）で設定できます。

ストリクト プライオリティ /低遅延キューイング

インターフェイス コンフィギュレーション モードで **priority high** 送信キュー コンフィギュレーション コマンドを使用し、各ポートの送信キュー 3 に高いプライオリティを設定できます。送信キュー 3 に高いプライオリティを設定した場合、送信キュー 3 のパケットは、他のキューのパケットよりも優先的にスケジューリングされます。

送信キュー 3 に高いプライオリティを設定した場合、パケットが他の送信キューよりも優先的にスケジューリングされるのは、割り当てられた帯域幅共有の設定を超えていない場合にかぎられます。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。

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。

各送信キューに最大速度を設定するには、**shape** コマンドを使用します。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、トランク 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ンク 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。

QoS およびソフトウェア処理されるパケット

Catalyst 4500 プラットフォームは、Cisco IOS ソフトウェアによって転送または生成されるパケットに、QoS マーキングまたはポリシング コンフィギュレーションを適用しません。これは、Cisco IOS がパケットを転送または生成している場合、ポートあるいは VLAN で設定された入力または出力 QoS ポリシーはパケットに適用されないためです。

ただし、Cisco IOS は生成されたコントロール パケットすべてを正しくマーク付けし、内部 IP DSCP を使用して出力送信インターフェイスで送信キューを判断します。IP パケットの場合、内部 IP DSCP は IP パケットの IP DSCP フィールドにあります。IP 以外のパケットの場合、Cisco IOS は内部でパケット プライオリティを割り当て、内部 IP DSCP 値にマッピングします。

Cisco IOS は IP precedence 値 6 をコントロール プレーン上のルーティング プロトコル パケットに割り当てます。RFC 791 での記載のとおり、「インターネットワークの制御指定は、ゲートウェイ制御発信元が使用するためだけのものです」。つまり、Cisco IOS は IP ベースのコントロール パケット（Open Shortest Path First（OSPF）、Routing Information Protocol（RIP）、Enhanced Interior Gateway Routing Protocol（EIGRP）hello、キープアライブ）をマーク付けします。ルータへの、およびルータからの Telnet パケットにも IP precedence 値 6 が与えられます。出力インターフェイスがパケットをネットワークに送信した場合、割り当てられた値はパケットとともに残ります。

レイヤ 2 制御プロトコルの場合、ソフトウェアは内部 IP DSCP を割り当てます。通常、レイヤ 2 制御プロトコル パケットは、内部 DSCP 値 48（IP precedence 値 6 に対応）が割り当てられます。

内部 IP DSCP は、送信インターフェイス上で待機状態のパケットの送信キューを特定するために使用します。キューを送信するよう DSCP を設定する方法については、「送信キューの設定」（P.56）を参照してください。

内部 IP DSCP は、トランク インターフェイス上でパケットが IEEE 802.1Q または ISL タグ付きで送信される場合、送信 CoS マーキングを決定するのにも使用します。DSCP/CoS マッピングを設定する方法については、「DSCP/CoS マップの設定」（P.61）を参照してください。

Supervisor Engine II-Plus、II+10GE、IV、V、V-10GE、4924、4948、および 4948-10GE での auto-QoS の設定

自動 QoS 機能を使用して、既存の QoS 機能の配置を容易にできます。Auto-QoS はネットワーク設計に関する予測を行うもので、それによってスイッチは、デフォルトの QoS 動作を使用せずにトラフィック フローごとに優先順位を付け、適切に出力キューを使用できます （デフォルトで自動 QoS はディセーブルになっています。スイッチでは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、単一キューでパケットを送信します）。

Auto-QoS をイネーブルにすると、入力パケット ラベルに基づいてトラフィックを自動的に分類します。スイッチは分類した結果を使用して適切な出力キューを選択します。

Auto-QoS コマンドを使用し、Cisco IP Phone と接続しているポートを識別し、アップリンクを通じて信頼できる Voice over IP（VoIP）トラフィックを受信するポートを識別します。自動 QoS は次の機能を実行します。

- IP Phone の有無を検出します。
- QoS 分類の設定
- 出力キューの設定

ここでは、スイッチ上で自動 QoS を設定する手順について説明します。

- 「生成される自動 QoS 設定」（P.32-19）
- 「コンフィギュレーションにおける自動 QoS の影響」（P.32-20）

- 「設定時の注意事項」（P.32-20）
- 「VoIP 用自動 QoS のイネーブル化」（P.32-20）

生成される自動 QoS 設定

デフォルトでは、Auto-QoS はすべてのインターフェイス上でディセーブルに設定されています。

最初のインターフェイス上で自動 QoS 機能をイネーブルにすると、次の動作が自動的に発生します。

- QoS がグローバルにイネーブルになります（**qos** グローバル コンフィギュレーション コマンド）。
- DBL がグローバルにイネーブルになります（**qos dbl** グローバル コンフィギュレーション コマンド）。
- **auto qos voip trust** 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、指定されたインターフェイスがレイヤ 2 として設定されている場合、インターフェイス上の入力分類は、パケット内で受信される CoS ラベルを信頼するように設定されます。インターフェイスがレイヤ 3 として設定されている場合は、DSCP を信頼するように設定されます （表 32-2 を参照）。
- **auto qos voip cisco-phone** 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、信頼境界機能がイネーブルになります。この機能は、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone が存在するかしないかを検出します。Cisco IP Phone が検出されたとき、インターフェイスをレイヤ 2 として設定している場合、インターフェイスの入力分類は、パケットで受信した CoS ラベルを信頼するように設定されます （インターフェイスをレイヤ 3 として設定している場合、分類は DSCP を信頼するように設定されます）。Cisco IP Phone が存在しない場合、パケットの CoS ラベルを信頼しないようにインターフェイスの入力分類が設定されます。

  信頼境界機能の詳細については、「ポート セキュリティを確保するための信頼境界機能の設定」（P.32-27）を参照してください。

auto qos voip cisco-phone または **auto qos voip trust** 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 Auto-QoS をイネーブルにすると、スイッチはトラフィック タイプと入力パケット ラベルに基づいて自動的に QoS 設定を生成し、表 32-2 に示されるコマンドをインターフェイスに適用します。

表 32-2　生成される自動 QoS 設定

説明	自動的に生成されるコマンド

スイッチが標準 QoS を自動的にイネーブルにし、DBL が CoS/DSCP マップ（着信パケット内の CoS 値を DSCP 値にマッピングします）を設定します。	`Switch(config)# qos`
	`Switch(config)# qos map cos 3 to 26`
	`Switch(config)# qos dbl`
	`Switch(config)# qos map cos 5 to 46`

スイッチが自動的に DSCP/Tx キュー マッピングを設定します。	`Switch(config)# qos map dscp 24 25 26 27 b28 29 30 31 to tx-queue 4` `Switch(config)# qos map dscp 32 33 34 35 36 37 38 39 to tx-queue 4`

スイッチが、パケットで受信される CoS/DSCP 値を信頼するように、インターフェイス上の入力分類を自動的に設定します。	`Switch(config-if)# qos trust cos`
	`or`
	`Switch(config-if)# qos trust dscp`

スイッチは、自動的に QoS サービス ポリシーを作成し、ポリシー上で DBL をイネーブルにし、インターフェイスに付加します。	`Switch(config)# policy-map autoqos-voip-policy`
	`Switch(config-pmap)# class class-default`
	`Switch(config-pmap-c)# dbl`

表 32-2　生成される自動 QoS 設定 （続き）

説明	自動的に生成されるコマンド
auto qos voip cisco-phone コマンドを入力すると、スイッチは自動的に信頼境界機能をイネーブルにします。この機能は、CDP を使用して Cisco IP Phone の有無を検出するものです。	`Switch(config-if)# qos trust device cisco-phone`

スイッチがより高いプライオリティをキュー 3 に割り当てます。キュー 3 のシェーピング制限が選択されるので、リンク速度は 33% です。共有がサポートされているポートにシェーピングを 33% として設定します。
これにより、より高いプライオリティのキューが他のキューを停止させないようになります。
	`Switch(config-if)# tx-queue 3`
	`Switch(config-if-tx-queue)# priority high`
	`Switch(config-if-tx-queue)# shape percent 33`
	`Switch(config-if-tx-queue)# bandwidth percent 33`

コンフィギュレーションにおける自動 QoS の影響

自動 QoS がイネーブルになっていると、**auto qos voip** インターフェイス コンフィギュレーション コマンドおよび生成された設定が、実行コンフィギュレーションに追加されます。

設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- このリリースでは、Cisco IP Phone の VoIP に対してだけ Auto-QoS がスイッチを設定します。
- Auto-QoS のデフォルト設定を使用する場合、Auto-QoS コマンドを入力する前にいかなる標準 QoS コマンドも設定しないでください。必要に応じて QoS 設定を微調整できますが、自動 QoS が完了した後にのみ調整することを推奨します。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。
- デフォルトでは、CDP はすべてのインターフェイス上でイネーブルになっています。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。
- レイヤ 3 インターフェイス上で **auto qos voip trust** をイネーブルにするには、ポートをレイヤ 3 に変更してから、Auto-QoS を適用し、DSCP を信頼するようにします。

VoIP 用自動 QoS のイネーブル化

VoIP 用の Auto-QoS を QoS ドメイン内でイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# debug auto qos`	（任意）Auto-QoS のデバッグをイネーブルにします。デバッグがイネーブルに設定された場合、スイッチは Auto-QoS がイネーブルまたはディセーブルに設定されると自動的に生成および適用される QoS コマンドを表示します。
ステップ 2	`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。

	コマンド	目的
ステップ 3	`Switch(config)# interface interface-id`	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、Cisco IP Phone に接続されているインターフェイス、またはネットワーク内部にある他のスイッチやルータに接続されているアップリンク インターフェイスを指定します。
ステップ 4	`Switch(config-if)# auto qos voip {cisco-phone | trust}`	Auto-QoS をイネーブルにします。 キーワードの意味は次のとおりです。 • **cisco-phone** : インターフェイスが Cisco IP Phone に接続されている場合、着信パケットの CoS ラベルは電話機が検出された場合だけ信頼されます。 • **trust** : アップリンク インターフェイスが信頼できるスイッチまたはルータに接続されていて、入力パケット内の VoIP トラフィック分類が信頼されます。
ステップ 5	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	`Switch# show auto qos interface interface-id`	入力を確認します。 このコマンドは、最初に適用された自動 QoS 設定を表示するもので、ユーザにより有効になった変更は反映されません。

インターフェイス上で Auto-QoS をディセーブルにするには、**no auto qos voip** 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。このコマンドを入力すると、スイッチは Auto-QoS 設定を、そのインターフェイスの標準 QoS デフォルト設定に変更します。このコマンドは、Auto-QoS によって実行されるグローバル コンフィギュレーションを変更しません。グローバル コンフィギュレーションは、同じ状態のままです。

次に、インターフェイス FastEthernet 1/1 に接続されているデバイスが Cisco IP Phone として検出された場合に、Auto-QoS をイネーブルにして、着信パケット内の CoS ラベルを信頼する例を示します。

```
Switch(config)# interface fastethernet1/1
Switch(config-if)# auto qos voip cisco-phone
```

次に、ギガビット イーサネット インターフェイス 1/1 に接続されたスイッチまたはルータが信頼できるデバイスの場合に、Auto-QoS をイネーブルにして、着信パケット内の CoS/DSCP ラベルを信頼する例を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip trust
```

次に、自動 QoS がイネーブルにされた場合に、自動的に生成される QoS コマンドを表示する例を示します。

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# auto qos voip cisco-phone
```

自動 QoS 情報の表示

自動 QoS 設定を表示するには、**show auto qos** [**interface** [*interface-id*]] 特権 EXEC コマンドを使用します。ユーザによる設定変更を表示するには、**show running-config** 特権 EXEC コマンドを使用します。**show auto qos** コマンド出力と **show running-config** コマンド出力を比較してユーザ定義の QoS 設定を比較できます。

auto-QoS の影響を受ける可能性のある現在の QoS の設定情報を表示するには、次のいずれかのコマンドを使用します。

- **show qos**
- **show qos map**
- **show qos interface** [*interface-id*]

これらのコマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

自動 QoS 設定例

ここでは、自動 QoS をネットワークに実装する方法について説明します（図 32-5 を参照）。

図 32-5　ネットワークでの自動 QoS の設定例

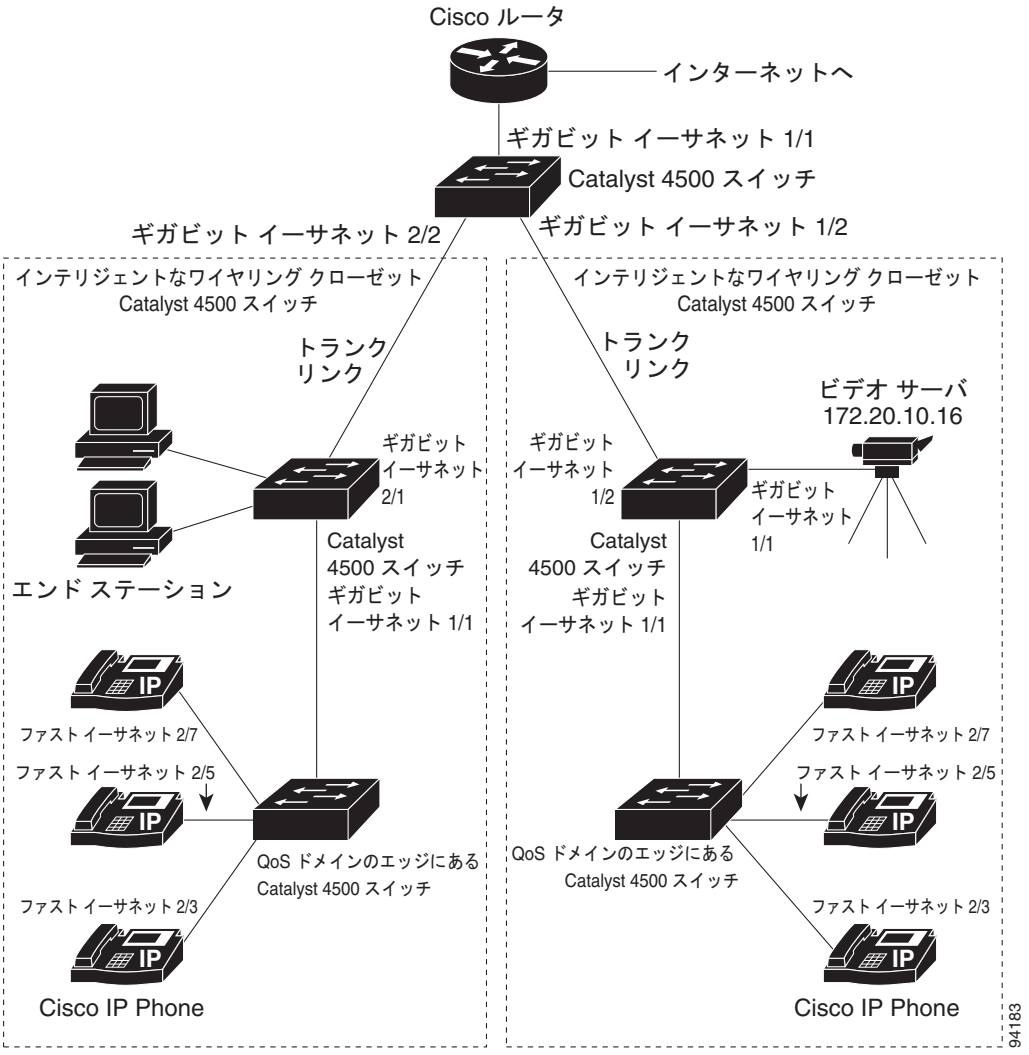


図 32-5 のインテリジェントなワイヤリング クローゼットは、Catalyst 4500 スイッチで構成されています。この例では、VoIP トラフィックを他のすべてのトラフィックよりも優先させることを目的としています。これを実行するには、ワイヤリング クローゼット内の QoS ドメインのエッジにあるスイッチ上で自動 QoS をイネーブルにします。

（注）　自動 QoS コマンドを入力する前に標準 QoS コマンドを設定しないでください。QoS 設定は微調整できますが、自動 QoS が完了した後にのみ調整することを推奨します。

VoIP トラフィックを他のすべてのトラフィックよりも優先させるために、QoS ドメインのエッジにあるスイッチを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# debug auto qos`	Auto-QoS のデバッグをイネーブルにします。デバッグをイネーブルにすると、スイッチは、自動 QoS がイネーブルである場合に自動的に生成される QoS 設定を表示します。
ステップ 2	`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 3	`Switch(config)# cdp enable`	CDP をグローバルにイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 4	`Switch(config)# interface fastethernet2/3`	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 5	`Switch(config-if)# auto qos voip cisco-phone`	インターフェイス上で Auto-QoS をイネーブルにし、インターフェイスが Cisco IP Phone に接続されていることを指定します。 着信パケット内の CoS ラベルは、IP Phone が検出された場合にだけ信頼されます。
ステップ 6	`Switch(config)# interface fastethernet2/5`	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 7	`Switch(config)# auto qos voip cisco-phone`	インターフェイス上で Auto-QoS をイネーブルにし、インターフェイスが Cisco IP Phone に接続されていることを指定します。
ステップ 8	`Switch(config)# interface fastethernet2/7`	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)# auto qos voip cisco-phone`	インターフェイス上で Auto-QoS をイネーブルにし、インターフェイスが Cisco IP Phone に接続されていることを指定します。
ステップ 10	`Switch(config)# interface gigabit1/1`	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	`Switch(config)# auto qos voip trust`	インターフェイス上で Auto-QoS をイネーブルにし、インターフェイスが信頼できるルータまたはスイッチに接続されていることを指定します。
ステップ 12	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	`Switch# show auto qos`	入力を確認します。 このコマンドは、最初に適用された自動 QoS 設定を表示するもので、ユーザによる有効な設定変更は反映されません。 Auto-QoS の影響を受ける QoS 設定に関する情報については、「自動 QoS 情報の表示」（P.32-21）を参照してください。

	コマンド	目的
ステップ 14	`Switch# show auto qos interface interface-id`	入力を確認します。 このコマンドは、最初に適用された自動 QoS 設定を表示するもので、ユーザにより有効になった変更は反映されません。
ステップ 15	`Switch# copy running-config startup-config`	**auto qos voip** インターフェイス コンフィギュレーション コマンドと生成された Auto-QoS 設定をコンフィギュレーション ファイルに保存します。

Supervisor Engine II-Plus、II+10GE、IV、V、V-10GE、4924、4948、および 4948-10GE での QoS の設定

QoS を設定する前に、次の事項を完全に理解する必要があります。

- 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

ここでは、Catalyst 4000 ファミリ スイッチ上で QoS を設定する手順について説明します。

QoS のデフォルト設定

表 32-3 に、QoS のデフォルト設定を示します。

表 32-3　QoS のデフォルト設定

機能	デフォルト値
QoS のグローバルな設定	ディセーブル
インターフェイス QoS の設定（ポート単位）	QoS がグローバルにイネーブルの場合、イネーブル
インターフェイス CoS 値	0
インターフェイス DSCP 値	0
CoS/DSCP マップ （CoS 値から設定された DSCP）	CoS 0 = DSCP　0 CoS 1 = DSCP　8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
DSCP/CoS マップ （DSCP 値から設定された CoS）	DSCP　0–7　= CoS 0 DSCP　8–15 = CoS 1 DSCP 16–23 = CoS 2 DSCP 24–31 = CoS 3 DSCP 32–39 = CoS 4 DSCP 40–47 = CoS 5 DSCP 48–55 = CoS 6 DSCP 56–63 = CoS 7
DSCP からマークダウンされた DSCP へのマッピング（ポリシング済み DSCP）	マークダウンされる DSCP 値と元の DSCP 値が同じ（マークダウンなし）
ポリサー	なし
ポリシー マップ	なし
送信キューの共有	リンク帯域幅の 1/4
送信キュー容量	ポートの送信キュー エントリの 1/4。ポートの送信キュー容量はポートのタイプによって異なり、送信キュー 1 つ当たり 240 ～ 1920 パケット
送信キューのシェーピング	なし
DCSP/ 送信キュー マップ	DSCP 0–15 キュー 1 DSCP 16–31 キュー 2 DSCP 32–47 キュー 3 DSCP 48–63 キュー 4
ハイ プライオリティ送信キュー	ディセーブル
QoS がディセーブルの場合	
インターフェイスの信頼状態	Trust DSCP
QoS がイネーブルの場合	QoS がイネーブルに設定され、その他の QoS パラメータがすべてデフォルト値である場合、送信されるすべてのトラフィックで IP DSCP が 0、レイヤ 2 CoS が 0 に設定される
インターフェイスの信頼状態	信頼できない

設定時の注意事項

QoS の設定を始める前に、次の点を理解する必要があります。

- スイッチ上に EtherChannel ポートを設定している場合、EtherChannel に QoS の分類およびポリシングを設定する必要があります。EtherChannel を形成する個々の物理ポートに、送信キューの設定が必要です。
- IP フラグメントが、Quality of Service 用にトラフィックを分類するために使用される ACL で設定された送信元および宛先に一致するが、ACL のレイヤ 4 ポート番号には一致しない場合、ACL とは引き続き一致するとされ、優先されます。意図する動作が IP フラグメントにベスト エフォートのサービスを提供する場合、次の 2 つの ACE を、トラフィックの分類に使用される ACL に追加する必要があります。

```
access-list xxx deny udp any any fragments
access-list xxx deny tcp any any fragments
```

- 設定されている IP 拡張 ACL と IP オプションのマッチングによって、QoS を強制することはできません。これらのパケットは CPU に送信され、ソフトウェアによって処理されます。IP オプションは、IP ヘッダー内のフィールドで示されます。
- スイッチが受信した制御トラフィック（スパニングツリー BPDU、ルーティング アップデート パケットなど）は、すべての入力 QoS 処理の対象になります。
- IP ルーティングがディセーブルの場合、**set** コマンドをポリシー マップで使用することはできません（デフォルトではイネーブル）。
- dot1q トンネル ポートでは、レイヤ 2 一致基準だけがタグ付きパケットに適用できます。ただし、タグなしパケットにはすべての一致基準を適用できます。
- トランク ポートでは、レイヤ 2 一致基準だけを複数の 802.1q タグを持つパケットに適用できます。

（注）　QoS は、ユニキャスト トラフィックとマルチキャスト トラフィックの両方を処理します。

QoS のグローバルなイネーブル化

QoS をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# conf terminal`	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)# qos`	スイッチ上で QoS をイネーブルにします。 QoS をグローバルにディセーブルにするには、**no qos** コマンドを使用します。
ステップ 3	`Switch(config)# 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 4	`Switch# show qos`	設定を確認します。

次に、QoS をグローバルにイネーブルにし、設定を確認する例を示します。

```
Switch# config terminal
Switch(config)# qos
Switch(config)# end
Switch#
```

```
Switch# show qos
  QoS is enabled globally

Switch#
```

ポート セキュリティを確保するための信頼境界機能の設定

通常のネットワークでは、Cisco IP Phone をスイッチ ポートに接続します（第 33 章「音声インターフェイスの設定」を参照）。通常の場合、電話機からスイッチに送信されたトラフィックは、802.1Q ヘッダーを使用するタグによってマーク付けされます。このヘッダーには VLAN 情報、およびパケットのプライオリティを決定するサービス クラス（CoS）の 3 ビット フィールドが格納されます。ほとんどの Cisco IP Phone 設定では、電話機からスイッチに送信されたトラフィックは信頼され、音声トラフィックがネットワーク内の他のタイプのトラフィックよりも適切に優先されます。**qos trust cos** 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ことにより、ポートで受信されたすべてのトラフィックの CoS ラベルを信頼するように、電話機の接続先であるスイッチ ポートを設定できます。

（注）　Cisco IOS Release 12.2(31)SG 以降では、Supervisor Engine V-10GE を使用すれば、ポートの信頼状態にかかわらずパケットの IP DSCP 値に基づいてトラフィックを分類できます。このため、Cisco IP Phone が検出されない場合でも、データ トラフィックは IP DSCP 値に基づいて分類されます。この新しい動作により、出力キュー選択が影響されることはありません。出力キュー選択はこれまでと同じく着信ポート信頼設定に基づきます。送信キューの設定については、「送信キューの設定」（P.32-56）を参照してください。

場合により、IP Phone に PC またはワークステーションを接続することもできます。この場合は、**switchport priority extend cos** 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、PC から受信したトラフィックよりも優先するように、スイッチ CLI を通して電話機を設定できます。このコマンドを使用すると、PC がハイプライオリティのデータ キューを利用しないように設定できます。

ただし、ユーザが電話機を省略して PC を直接スイッチに接続した場合、スイッチは PC によって生成された CoS ラベルを信頼し（信頼された CoS 設定のため）、ハイプライオリティ キューが誤って使用される可能性があります。信頼境界機能は、CDP を使用してスイッチ ポート上で Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出することにより、この問題を解決します。

（注）　スイッチでグローバルに、または該当するポートで CDP が稼働していない場合、信頼境界は機能しません。

ポート上に信頼境界を設定する場合、信頼がディセーブルにされます。電話機が接続されて検出されると、信頼がイネーブルになります （電話機を検出するには数分かかります）。そして、電話機が取り外され（検出されなければ）、信頼境界機能はスイッチ ポートの trusted 設定をディセーブルにし、ハイプライオリティのキューの誤使用を防ぎます。

ポート上の信頼境界をイネーブルにするには、次の作業を行います。

	コマンド	目的
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)# interface` *interface-id*	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、IP Phone に接続されているインターフェイスを指定します。 有効なインターフェイスは物理インターフェイスなどです。
ステップ 3	`Switch(config)# qos trust [cos | dscp]`	受信したトラフィックの CoS 値を信頼するように、インターフェイスを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 4	`Switch(config)# qos trust device cisco-phone`	Cisco IP Phone が信頼できるデバイスであることを指定します。 信頼境界機能と自動 QoS（**auto qos voip** インターフェイス コンフィギュレーション コマンド）を同時にイネーブルにはできません。両者は相互に排他的です。
ステップ 5	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	`Switch# show qos interface` *interface-id*	入力を確認します。
ステップ 7	`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。

信頼境界機能をディセーブルにするには、**no qos trust device cisco-phone** 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。

Dynamic Buffer Limiting のイネーブル化

（注）　Supervisor Engine 6-E は、この機能をサポートして*いません*。

Dynamic Buffer Limiting（DBL）は、Catalyst 4500 プラットフォームでのアクティブ キュー管理を提供します （詳細については、「AQM」（P.32-15）を参照してください）。

「選択的」DBL を介して、DBL アルゴリズムの対象となる（または対象とならない）フローを選択できます。特定の IP DSCP 値で、または特定の CoS 値で、DBL をグローバルにイネーブルにできます。

ここでは、次の作業について説明します。

- 「DBL のグローバルなイネーブル化」（P.32-28）
- 「DBL の選択的イネーブル化」（P.32-29）

DBL のグローバルなイネーブル化

スイッチ上で DBL をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# qos dbl`	スイッチ上で DBL をイネーブルにします。 AQM をディセーブルにするには、**no qos dbl** コマンドを使用します。

	コマンド	目的
ステップ 2	`Switch(config)# 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 3	`Switch# show qos dbl`	設定を確認します。

次に、DBL をグローバルにイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# qos dbl
Global DBL enabled
Switch(config)# end
Switch# show qos dbl
    QOS is enabled globally
    DBL is enabled globally on DSCP values:
          0-63
    DBL flow includes vlan
    DBL flow includes layer4-ports
    DBL does not use ecn to indicate congestion DBL exceed-action probability: 15% DBL max
    credits: 15 DBL aggressive credit limit: 10 DBL aggressive buffer limit: 2 packets
Switch#
```

サービス ポリシーを適用して、出力インターフェイス方向で DBL をイネーブルにできます。

```
Switch# conf terminal
Switch(config)# policy-map dbl
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# end
Switch#
00:08:12: %SYS-5-CONFIG_I: Configured from console by console
Switch# conf terminal
Switch(config)# int gig 1/2
Switch(config-if)# service-policy output dbl
Switch(config-if)# end
Switch#
```

DBL の選択的イネーブル化

DSCP 値により、IP パケット（単一またはタグなし）に対してだけ選択的に DBL を適用できます（「特定 IP DSCP 値での DBL のイネーブル化」（P.32-30）を参照）。非 IP パケットまたは二重タグ付きパケット（Q-in-Q など）に DBL を選択的に適用するには、次に説明するように CoS 値を使用する必要があります（「特定 CoS 値での DBL のイネーブル化」（P.32-31）を参照）。

次を実行できます。

- 「特定 IP DSCP 値での DBL のイネーブル化」（P.32-30）
- 「特定 CoS 値での DBL のイネーブル化」（P.32-31）

特定 IP DSCP 値での DBL のイネーブル化

DBL アクションは、送信キュー（インターフェイスごとに 4 つ）で実行されます。IP DSCP から送信キューへのマッピングを操作するには、**qos map dscp dscp-values to tx-queue queue-id** コマンドを使用します（方法については、「送信キューの設定」（P.32-56）を参照してください）。

特定の IP DSCP 値で DBL をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# [no] qos dbl dscp-based <value, value_range>`	特定の IP DSCP 値で DBL をイネーブルにします。
ステップ 2	`Switch(config)# 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 3	`Switch# show qos dbl`	設定を確認します。

次に、DSCP 値 1 ～ 10 で DBL を選択的にイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# qos dbl dscp-based 1-10
Switch(config)# end
Switch# show qos dbl
    QOS is enabled globally
    DBL is enabled globally on DSCP values:
          1-10
    DBL flow includes vlan
    DBL flow includes layer4-ports
    DBL does not use ecn to indicate congestion DBL exceed-action probability: 15%
    DBL max credits: 15
    DBL aggressive credit limit: 10
    DBL aggressive buffer limit: 2 packets
Switch#
```

次に、DSCP 値 1 ～ 10 で DBL を選択的にディセーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no qos dbl dscp-based 1-5, 7
Switch(config)# end
Switch# show qos dbl
    QOS is enabled globally
    DBL is enabled globally on DSCP values:
          6,8-10
    DBL flow includes vlan
    DBL flow includes layer4-ports
    DBL does not use ecn to indicate congestion DBL exceed-action probability: 15% DBL max
    credits: 15 DBL aggressive credit limit: 10 DBL aggressive buffer limit: 2 packets
Switch#
```

DSCP 以外のクラス属性に基づいて DBL を適用しても、引き続きポリシーマップを出力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 クラス アクションの設定」（P.32-37））。

ネットワーク ポリシーに従って値が設定されている場合、DBL がスロットリングするアグレッシブ フローの入力インターフェイスで「Trust DSCP」を設定する必要があります。

```
Interface <ingress>
  qos trust dscp
```

特定 CoS 値での DBL のイネーブル化

非 IP パケットまたは二重タグ付きパケット（たとえば、Q-in-Q）を使用するつもりであれば、CoS 値を使用して、選択的に DBL を適用する必要があります。

一重タグ付き IP パケットの場合は、次のアプローチを使用します。「特定 IP DSCP 値での DBL のイネーブル化」（P.32-30）に示すように、グローバル **qos dbl** dscp-based コマンドを指定します。

```
Interface <ingress>
  switchport mode trunk
  qos trust cos
```

非 IP パケットまたは二重タグ付きパケットの場合、次の方法を使用します。

	コマンド	目的
ステップ 1	`Switch(config)# qos dbl`	DBL をグローバルにイネーブルにします。
ステップ 2	`Switch(config)# 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 3	`Switch(config)# class-map cos`	トラフィック クラスを定義します。
ステップ 4	`Switch(config-cmap)# match cos x y`	一致基準として使用する CoS 値を指定します。
ステップ 5	`Switch(config-cmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	`Switch(config)# policy-map cos`	ユーザが指定した名前でポリシー マップを作成します。
ステップ 7	`Switch(config-pmap)# class cos`	ポリシー マップが使用するクラス マップを指定します。
ステップ 8	`Switch(config-pmap-c)# dbl`	ポリシー上で DBL をイネーブルにします。
ステップ 9	`Switch(config-pmap-c)# end`	EXEC モードに戻ります。
ステップ 10	`Switch# show policy-map cos`	設定を確認します。
ステップ 11	`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 12	`Switch(config)# interface gigabitEthernet 1/20`	設定をインターフェイスに適用します。
ステップ 13	`Switch(config-if)# service-policy output cos`	ポリシー マップをインターフェイスに付加します。
ステップ 14	`Switch# show policy-map interface`	設定を確認します。

（注）　CoS 変換の使用の詳細については、「CoS 変換の設定」（P.32-42）を参照してください。

CoS 値 2 および 3 で DBL を選択的にイネーブルにするには、次の手順を実行します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# qos dbl
Switch(config)# end
Switch# configure terminal
Switch(config)# class-map cos
Switch(config-cmap)# match cos 2 3
Switch(config-cmap)# exit
Switch(config)# policy-map cos
Switch(config-pmap)# class cos
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)# end
Switch# show policy-map cos
    Policy Map cos
      Class cos
        dbl
Switch# configure terminal
Switch(config)# interface gigabitEthernet 1/20
```

```
Switch(config-if)# service-policy output cos
Switch# show policy-map interface
 GigabitEthernet1/20

  Service-policy output: cos

    Class-map: cos (match-all)
      0 packets
      Match: cos  2  3
      dbl

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

名前付き集約ポリサーの作成

名前付き集約ポリサーを作成するには、次の作業を行います。

コマンド	目的
Switch(config)# **qos aggregate-policer** *policer_name rate burst* [[**conform-action** {**transmit** | **drop**}] [**exceed-action** {**transmit** | **drop** | **policed-dscp-transmit**}]]	名前付き集約ポリサーを作成します。

集約ポリサーは、1 つまたは複数のインターフェイスに適用できます。ただし、あるインターフェイスの入力方向と、別のインターフェイスの出力方向に同じポリサーを適用すると、スイッチング エンジン上で 2 つの異なる同等の集約ポリサーを作成したことになります。各ポリサーでは、同じポリシングパラメータが使用されます。一方のパラメータは 1 つのインターフェイスの入力トラフィックのポリシングに使用され、もう一方のパラメータは別のインターフェイスの出力トラフィックのポリシングに使用されます。集約ポリサーを複数のインターフェイスに同じ方向で適用した場合、スイッチング エンジン上に作成されるそのポリサーのインスタンスは 1 つだけです。

同様に、集約ポリサーをポートまたは VLAN に適用できます。同じ集約ポリサーをポートおよび VLAN に適用した場合、スイッチング エンジン上で 2 つの異なる同等の集約ポリサーを作成したことになります。各ポリサーは同じポリシング パラメータを使用し、1 つのポリサーは設定されたポート上のトラフィックのポリシング、もう 1 つのポリサーは設定された VLAN 上のトラフィックのポリシングを行います。集約ポリサーを複数のポートだけ、または複数の VLAN だけに適用した場合、スイッチング エンジン上に作成されるそのポリサーのインスタンスは 1 つだけです。

1 つの集約ポリサーを複数のポートおよび VLAN に異なる方向で適用した場合、実質的には、同等の 4 つの集約ポリサー（入力方向でポリサーを共有するすべてのポート用、出力方向でポリサーを共有するすべてのポート用、入力方向でポリサーを共有するすべての VLAN 用、および出力方向でポリサーを共有するすべての VLAN 用の集約ポリサー）を作成したことになります。

名前付き aggregate ポリサーを作成する場合、次の点に注意してください。

- *rate* パラメータ値の有効範囲は、次のとおりです。
  - 最小：32 Kbps（キロビット / 秒）
  - 最大：32 Gbps（ギガビット / 秒）

  「設定時の注意事項」（P.32-26）を参照してください。
- 速度（rate）はビット / 秒で入力できますが、次の簡略表記を使用することもできます。

  - k は、1,000 bps を表します。
  - m は、1,000,000 bps を表します。
  - g は、1,000,000,000 bps を表します。

（注）　小数点を使用することもできます。たとえば、1,100,000 bps の速度は、1.1m と入力できます。

- *burst* パラメータ値の有効範囲は、次のとおりです。
  - 最小：1 KB
  - 最大：512 MB
- バースト サイズ（burst）はバイトで入力できますが、次の簡略表記を使用することもできます。
  - k は、1,000 バイトを表します。
  - m は、1,000,000 バイトを表します。
  - g は、1,000,000,000 バイトを表します。

（注）　小数点を使用することもできます。たとえば、1,100,000 バイトのバーストは、1.1m と入力できます。

- 一致するイン プロファイル トラフィックに対する conform アクションを、任意で次のように指定できます。
  - デフォルトの conform アクションは、**transmit** です。
  - 一致したトラフィックをすべてドロップするには、**drop** キーワードを入力します。

（注）　**drop** を conform アクションとして設定すると、QoS は **drop** を exceed アクションとして設定します。

- CIR を超過するトラフィックについて、exceed アクションを任意で次のように指定できます。
  - デフォルトの exceed アクションは、**drop** です。
  - 一致したアウトオブプロファイル トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。
  - ポリシングをまったく行わないようにするには、**transmit** キーワードを入力して、一致したアウト オブ プロファイル トラフィックをすべて送信します。
- 名前付き集約ポリサーを削除するには、**no qos aggregate-policer** *policer_name* コマンドを使用します。

次に、10 Mbps のレート制限および 1 MB のバースト サイズを指定し、適合するトラフィックを送信して、アウト オブ プロファイル トラフィックをマークダウンする、名前付き集約ポリサーの作成例を示します。

```
Switch# config terminal
Switch(config)# qos aggregate-policer aggr-1 10000000 1000000 conform-action transmit
exceed-action policed-dscp-transmit
Switch(config)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show qos aggregate-policer aggr-1
Policer aggr-1
  Rate(bps):10000000 Normal-Burst(bytes):1000000
  conform-action:transmit exceed-action:policed-dscp-transmit
  Policymaps using this policer:
Switch#
```

QoS ポリシーの設定

ここでは、QoS ポリシーの設定について説明します。

（注）　QoS ポリシーは、ユニキャスト トラフィックおよびマルチキャスト トラフィックの両方を処理します。

QoS ポリシー設定の概要

QoS ポリシーを設定するには、トラフィック クラスを設定して、それらのトラフィック クラスに適用するポリシーを設定し、さらに、次のコマンドを使用してポリシーをインターフェイスに付加する必要があります。

- **access-list**（IP トラフィックに対して任意：**class-map** コマンドを使用して IP トラフィックをフィルタリングできます）
  - QoS では、次のアクセス リスト タイプがサポートされています。

プロトコル	番号付きアクセス リスト？	拡張アクセス リスト？	名前付きアクセス リスト？
IP	Yes： 1 ～ 99 1300 ～ 1999	Yes： 100 ～ 199 2000 ～ 2699	Yes

  - Catalyst4500 シリーズ スイッチ上の ACL については、第 39 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- **class-map**（任意）：**class-map** コマンドを使用し、トラフィックの分類基準を指定して 1 つまたは複数のトラフィック クラスを定義します（「クラス マップの設定（任意）」（P.32-35）を参照）。
- **policy-map**：各トラフィック クラスに次の項目を定義するには、**policy-map** コマンドを使用します。
  - 内部 DSCP の作成元
  - 集約または個別のポリシングおよびマーキング
- **service-policy**：**service-policy** コマンドを使用して、ポリシー マップをインターフェイスに付加します。

クラス マップの設定（任意）

ここでは、クラス マップの設定手順について説明します。

トラフィック クラスを定義し、そのクラスに属するトラフィックを識別するための一致基準を指定するには、**class-map** コンフィギュレーション コマンドを使用します。一致文には、ACL、IP precedence 値、DSCP 値などの基準を指定できます。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 1 つの一致文を入力して定義します。

クラス マップの作成

クラス マップを作成するには、次の作業を行います。

コマンド	目的
`Switch(config)# [no] class-map [match-all | match-any] class_name`	名前付きクラス マップを作成します。 クラス マップを削除するには、**no** キーワードを使用します。

クラス マップでのフィルタリングの設定

クラス マップにフィルタリングを設定するには、次のいずれかの作業を行います。

コマンド	目的
`Switch(config-cmap)# [no] match access-group {acl_index | name acl_name}`	（任意）トラフィックのフィルタリングに使用する ACL の名前を指定します。 クラス マップから文を削除するには、**no** キーワードを使用します。 **（注）** アクセス リストについては、このマニュアルでは説明しません。「QoS ポリシーの設定」（P.32-34）に記載されている **access-list** の説明を参照してください。
`Switch (config-cmap)# [no] match ip precedence ipp_value1 [ipp_value2 [ipp_valueN]]`	（任意：IP トラフィックだけ）一致基準として使用する IP precedence 値（最大 8 つ）を指定します。クラス マップから文を削除するには、**no** キーワードを使用します。
`Switch (config-cmap)# [no] match ip dscp dscp_value1 [dscp_value2 [dscp_valueN]]`	（任意：IP トラフィックだけ）一致基準として使用する DSCP 値（最大 8 つ）を指定します。クラス マップから文を削除するには、**no** キーワードを使用します。
`Switch (config-cmap)# [no] match cos value1 [value2] [value3} [value4}`	（任意：非 IPv4 トラフィックだけ）一致基準として使用する CoS 値（最大 8 つ）を指定します。クラス マップから文を削除するには、**no** キーワードを使用します。 非 IPv4 トラフィックについては、「設定時の注意事項」（P.32-20）を参照してください。

コマンド	目的
`Switch (config-cmap)# [no] match any`	（任意）すべての IP トラフィックまたは IP 以外のトラフィックを一致させます。
`Switch (config-cmap)# match flow ip {source-address | destination-address`	（任意）IP 送信元アドレスまたは宛先アドレスが一意であるそれぞれのフローを新しいフローとして扱います。

（注）　**match ip precedence** または **match ip dscp** クラス マップ コマンドを指定したクラス マップを使用する入力ポリシーまたは出力ポリシーでは、パケットを受信するポートが **trust dscp** に設定されている必要があります。設定されていない場合、IP パケット DSCP/IP precedence はトラフィックのマッチングには使用されず、受信ポートのデフォルト DSCP が使用されます。Cisco IOS Release 12.2(31)SG 以降では、Supervisor Engine V-10GE を使用すれば、ポートの信頼状態にかかわらず、パケットの IP DSCP 値に基づいてトラフィックを分類できます。

（注）　Cisco IOS Release 12.2(31) では、Catalyst 4500 シリーズ スイッチは match cos をサポートします。

（注）　Catalyst 4000 ファミリ スイッチ上のインターフェイスは、**match classmap**、**match destination-address**、**match input-interface**、**match mpls**、**match not**、**match protocol**、**match qos-group**、および **match source-address** キーワードをサポートしていません。

クラス マップの設定の確認

クラス マップの設定を確認するには、次の作業を行います。

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

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

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

次に、設定を確認する例を示します。

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

Switch#
```

次に、非 IPv4 トラフィックの CoS マッチングを設定する例を示します。ここでは、CoS 値が 5 のトラフィックをフィルタリングします。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map maptwo
Switch(config-cmap)# match cos 5
Switch(config-cmap)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show class-map maptwo
 Class Map match-all maptwo (id 1)
   Match cos 5

Switch#
```

ポリシー マップ コンフィギュレーション

1 つのインターフェイスに付加できるポリシー マップは、1 つに限られます。ポリシー マップには、一致基準およびポリサーがそれぞれ異なる 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。

ここでは、ポリシー マップの設定手順について説明します。

- 「ポリシー マップの作成」（P.32-37）
- 「ポリシー マップ クラス アクションの設定」（P.32-37）

ポリシー マップの作成

ポリシー マップを作成するには、次の作業を行います。

コマンド	目的
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。

ポリシー マップ クラス アクションの設定

ここでは、ポリシー マップ クラスのアクションを設定する手順について説明します。

- 「ポリシー マップ マーキング状態の設定」（P.32-38）
- 「ポリシー マップ クラスの信頼状態の設定」（P.32-38）
- 「ポリシー マップ クラスの DBL 状態の設定」（P.32-38）
- 「ポリシー マップ クラスのポリシングの設定」（P.32-39）
- 「名前付き集約ポリサーの使用」（P.32-39）
- 「インターフェイス別ポリサーの設定」（P.32-39）

ポリシー マップ マーキング状態の設定

ポリシー マップを設定してパケットに IP precedence または DSCP をマーク付けするには、次の作業を行います。

コマンド	目的
`Switch(config-pmap-c)# [no] set ip [precedence prec_value | dscp dscp_value]`	ポリシー マップ マーキング状態を設定します。この設定によって、後続処理のためにパケットの内部 DSCP が決定されます。 設定した値をクリアし、デフォルトに戻すには、**no** キーワードを使用します。

ポリシー マップ クラスの信頼状態の設定

ポリシー マップ クラスの信頼状態を設定するには、次の作業を行います。

コマンド	目的
`Switch(config-pmap-c)# [no] trust {cos | dscp]`	ポリシー マップ クラスの信頼状態を設定します。この設定によって、QoS が内部 DSCP 値の作成元として使用する値が選択されます（「内部 DSCP 値」（P.32-14）を参照）。 設定した値をクリアし、デフォルトに戻すには、**no** キーワードを使用します。

ポリシー マップ クラスの信頼状態を設定する際、次の点に注意してください。

- **no trust** コマンドを入力すると、入力インターフェイス上に設定されている信頼状態を使用できます（これがデフォルトです）。
- **cos** キーワードを使用すると、QoS は受信した CoS またはインターフェイス CoS に基づいて、内部 DSCP 値を設定します。
- **dscp** キーワードを使用すると、QoS は受信した DSCP を使用します。

ポリシー マップ クラスの DBL 状態の設定

ポリシー マップ クラスの DBL 状態を設定するには、次の作業を行います。

コマンド	目的
`Switch(config-pmap-c)# [no] dbl`	ポリシー マップ クラスの DBL 状態を設定します。この設定によって、トラフィック フローのキュー長を追跡します（「AQM」（P.32-15）を参照）。 DBL 値をクリアし、デフォルトに戻すには、**no** キーワードを使用します。

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

- 名前付き集約ポリサーを使用しているクラスは、機能するために同じ DBL 設定でなければなりません。

ポリシー マップ クラスのポリシングの設定

ここでは、ポリシー マップ クラスによるポリシングを設定する手順について説明します。

- 「名前付き集約ポリサーの使用」（P.32-39）
- 「インターフェイス別ポリサーの設定」（P.32-39）

名前付き集約ポリサーの使用

名前付き aggregate ポリサー（「名前付き集約ポリサーの作成」（P.32-32）を参照）を使用するには、次の作業を行います。

コマンド	目的
`Switch(config-pmap-c)# [no] police aggregate aggregate_name`	あらかじめ定義されている集約ポリサーを使用します。 ポリシー マップ クラスからポリサーを削除するには、**no** キーワードを使用します。

インターフェイス別ポリサーの設定

インターフェイス別ポリサー（「ポリシングおよびマーキング」（P.32-10）を参照）を設定するには、次の作業を行います。

コマンド	目的
`Switch(config-pmap-c)# [no] police rate burst [[conform-action {transmit | drop}] [exceed-action {transmit | drop | policed-dscp-transmit}]]`	インターフェイス別のポリサーを設定します。 ポリシー マップ クラスからポリサーを削除するには、**no** キーワードを使用します。

インターフェイス別ポリサーを設定する場合、次の点に注意してください。

- *rate* パラメータ値の有効範囲は、次のとおりです。
  - 最小値：32 Kbps（32000 と入力）
  - 最大：32 Gbps（32000000000 と入力）

（注） 「設定時の注意事項」（P.32-26）を参照してください。

- 速度（rate）はビット/秒で入力できますが、次の簡略表記を使用することもできます。
  - k は、1,000 bps を表します。
  - m は、1,000,000 bps を表します。
  - g は、1,000,000,000 bps を表します。

（注） 小数点を使用することもできます。たとえば、1,100,000 bps の速度は、1.1m と入力できます。

- *burst* パラメータ値の有効範囲は、次のとおりです。
  - 最小：1 KB
  - 最大：512 MB

- バースト サイズ（burst）はバイトで入力できますが、次の簡略表記を使用することもできます。
  - k は、1,000 バイトを表します。
  - m は、1,000,000 バイトを表します。
  - g は、1,000,000,000 バイトを表します。

（注）　小数点を使用することもできます。たとえば、1,100,000 バイトのバーストは、1.1m と入力できます。

- 一致するイン プロファイル トラフィックに対する conform アクションを、任意で次のように指定できます。
  - デフォルトの conform アクションは、**transmit** です。
  - 一致するトラフィックをすべてドロップするには、**drop** キーワードを入力します。
- 任意で、CIR を超過するトラフィックについて、一致するアウト オブ プロファイル トラフィックをすべてマークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。「ポリシング済み DSCP マップの設定」（P.32-60）を参照してください。
  - ポリシングをまったく行わないようにするには、**transmit** キーワードを入力して、一致するアウト オブ プロファイル トラフィックをすべて送信します。

次の例は、*ipp5* という名前のクラス マップを使用する、*ipp5-policy* という名前のポリシー マップを作成する方法を示しています。クラス マップ *ipp5* は、パケット優先順位を 6 に書き換えて、IP precedence 値の 5 と一致するトラフィックを集約ポリシングするように設定されています。

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

次の例は、cs2 という名前のクラス マップを使用する、cs2-policy という名前のポリシー マップを作成する方法を示しています。クラス マップ cos5 は CoS 5 で一致するように設定されており、トラフィックを集約ポリシングするように設定されています。

```
Switch(config)# class-map cs2
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit

Switch(config)# policy-map cs2-policy
Switch(config-pmap)# class cs2
police 2000000000 2000000 conform-action transmit exceed-action policed-dscp-transmit

Switch(config)# int g5/1
Switch(config-if)# service-policy input cs2-policy
Switch(config-if)# end

Switch# sh class-map cs2
 Class Map match-all cs2 (id 2)
   Match cos  5

Switch# sh policy-map cs2-policy
  Policy Map cs2-policy
    Class cs2
```

```
      police 2000000000 bps 2000000 byte conform-action transmit exceed-action
policed-dscp-transmit Switch#
```

ポリシー マップの設定の確認

ポリシー マップの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config-pmap-c)# end`	ポリシーマップ クラス コンフィギュレーション モードを終了します。 **（注）** ポリシー マップで追加クラスを作成するには、追加の **class** コマンドを入力します。
ステップ 2	`Switch# show policy-map` *policy_name*	設定を確認します。

次に、設定を確認する例を示します。

```
Switch# show policy-map ipp5-policy
show policy ipp5-policy
 Policy Map ipp5-policy
  class  ipp5
   set ip precedence 6
   dbl
police 2000000000 2000000 conform-action transmit exceed-action
policed-dscp-transmit
Switch#
```

インターフェイスへのポリシー マップの対応付け

ポリシー マップをインターフェイスに対応付けるには、次の作業を行います。

	コマンド	目的
ステップ 1	`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。
ステップ 2	`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 マップの付加を解除するには、**no** キーワードを使用します。
ステップ 3	`Switch(config-if)# 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 4	`Switch# show policy-map interface` {**vlan** *vlan_ID* | {**fastethernet** | **gigabitethernet**} *slot/interface*}	設定を確認します。

（注） IP ルーティングをグローバルにイネーブルにするまでは、インターフェイスのマーキング コマンドをイネーブルにできません。IP ルーティングがグローバルにディセーブルのときインターフェイスにサービス ポリシーを設定すると、設定は受け付けられても有効にはなりません。この場合には、「`Set command will not take effect since CEF is disabled.Please enable IP routing and CEF globally.`」というメッセージが表示され、入力を求められます。IP ルーティングをグローバルにイネーブルにするには、**ip routing** および **ip cef global** コンフィギュレーション コマンドを実行します。その後、マーキング コマンドが有効になります。

次に、ポリシー マップ *pmap1* をインターフェイス FastEthernet 5/36 に付加し、設定を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/36
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
Switch# show policy-map interface fastethernet 5/36
FastEthernet6/1

   service-policy input:p1

     class-map:c1 (match-any)
       238474 packets
       match:access-group 100
        38437 packets
       police:aggr-1
        Conform:383934 bytes Exceed:949888 bytes

    class-map:class-default (match-any)
      0 packets
      match:any
        0 packets
Switch#
```

CoS 変換の設定

（注）　Supervisor Engine 6-E は、この機能をサポートしていません。

レイヤ 2 VPN を提供するサービス プロバイダーは、サービス プロバイダーの VLAN を示す外部タグとカスタマーの VLAN を示す内部タグを持つ二重タグ トラフィックまたは Q-in-Q トラフィックを伝送します。外部タグの CoS に基づいて、SP ネットワーク内で、差別化したサービス レベルを提供できます。

dot1q トンネル ポートで CoS 変換を使用すると、プロバイダーのコア ネットワークに入る dot1q トンネル パケットの外部タグの CoS 値を、カスタマーの VLAN タグの CoS から導き出すことができます。その結果、プロバイダーはカスタマーの QoS セマンティックスをネットワーク内で保つことができます。

CoS 変換は、特定の着信 CoS 値に一致させ、一致したパケットに関連付けられている内部 DSCP を指定するようにユーザが明示的に設定することによって実現されます。この内部 DSCP は、スイッチからの送信時に DSCP/CoS マッピングを通じて CoS に変換されます。外部 VLAN タグにはこの CoS 値がマーク付けされます。

このプロセス中に内部タグの CoS が保存され、サービス プロバイダーのネットワーク内で伝送されます。

次に、ポリシー マップがカスタマーの VLAN ID と CoS 値をネットワーク内で保つ例を示します。

```
Class Map match-any c0
   Match cos  0

 Class Map match-any c1
   Match cos  1

 Class Map match-any c2
   Match cos  2
```

```
 Class Map match-any c3
   Match cos  3

 Class Map match-any c4
   Match cos  4

 Class Map match-any c5
   Match cos  5

 Class Map match-any c6
   Match cos  6

 Class Map match-any c7
   Match cos  7

Policy Map cos_mutation
    Class c0
      set dscp default

    Class c1
      set dscp cs1

    Class c2
      set dscp cs2

    Class c3
      set dscp cs3

    Class c4
      set dscp cs4

    Class c5
      set dscp cs5

    Class c6
      set dscp cs6

    Class c7
      set dscp cs7


interface GigabitEthernet5/1
 switchport access vlan 100

 switchport mode dot1q-tunnel
 service-policy input cos_mutation
```

User Based Rate Limiting の設定

User Based Rate Limiting（UBRL）ではマイクロフロー ポリシング機能が採用され、トラフィック フローがダイナミックに学習されて、それぞれの一意のフローが個別レートにレート制限されます。UBRL は、内蔵 NetFlow がサポートされている Supervisor Engine V-10GE で使用できます。UBRL は、送信元または宛先フロー マスクを持つルーテッド インターフェイス上の入力トラフィックに適用できます。最大 85,000 の個別フローおよび 511 の異なるレートをサポートできます。UBRL は通常、ユーザ単位のきめ細かいレート制限メカニズムが必要な環境（ユーザ単位の発信トラフィック レートがユーザ単位の着信トラフィック レートと異なる場合など）で使用されます。

（注）　デフォルトでは、UBRL はルーティングされた IP トラフィックだけをポリシングします。スイッチングされる IP トラフィックをポリシングするには、**ip flow ingress layer2-switched** グローバル コマンドを使用します。ただし、レイヤ 3 インターフェイス上に UBRL 設定を残す必要があります。UBRL 設定と **ip flow ingress layer2-switched** グローバル コマンドを使用すると、VLAN 間フローをポリシングすることもできます（「スイッチド/ブリッジド IP フローの設定」（P.46-8）を参照してください）。**ip flow ingress** コマンドを入力する必要はありません。

フローは 5 タプルとして定義されます（IP 送信元アドレス、IP 宛先アドレス、IP ヘッド プロトコル フィールド、レイヤ 4 送信元ポート、宛先ポート）。フローベース ポリサーでは、フローごとにトラフィックをポリシングできます。フローはダイナミックなので、クラス マップで識別値が必要です。

source-address キーワードを使用して **match flow** コマンドを指定すると、送信元アドレスが一意であるそれぞれのフローは、新しいフローとして扱われます。**destination-address** キーワードを使用して **match flow** コマンドを指定すると、宛先アドレスが一意であるそれぞれのフローは、新しいフローとして扱われます。ポリシー マップによって使用されるクラス マップは、フロー オプションが設定されている場合、フローベース ポリシー マップとして扱われます。**match flow** コマンドを、**ip destination-address ip protocol L4 source-address L4 destination-address** キーワードを指定して使用すると、一意の IP 送信元、IP 宛先、IP プロトコル、レイヤ 4 送信元、および宛先アドレスを含む各フローは、新しいフローとして扱われます。

（注）　マイクロフローは、Supervisor Engine V-10GE だけでサポートされます。

フローベース クラス マップとポリシー マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# class-map match-all class_name`	名前付きクラス マップを作成します。
ステップ 2	`Switch(config-cmap)# match flow ip {source-address | ip destination-address ip protocol L4 source-address L4 destination-address | destination-address}`	フローのキーフィールドを指定します。
ステップ 3	`Switch(config-cmap)# end`	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 4	`Switch# show class-map class-name`	設定を確認します。

例

例 1

次に、送信元アドレスに関連付けられたフローベース クラス マップを作成する例を示します。

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip {source-address [ip destination_address ip protocol L4
source-address L4 destination address]}
Switch(config-cmap)# end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow  ip source-address
```

例 2

次に、宛先アドレスに関連付けられたフローベース クラス マップを作成する例を示します。

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# end
Switch#

Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow  ip destination-address
```

例 3

ファスト イーサネット インターフェイス 6/1 上で、送信元アドレス 192.168.10.20 および 192.168.10.21 を持つアクティブなフローが 2 つ存在すると仮定します。次の例では、それぞれのフローを 1 Mbps に維持し、9000 バイトのバースト値を許可する方法を示します。

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address
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 fa6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory

Switch# show policy-map interface
FastEthernet6/1

 Service-policy input: p1

   Class-map: c1 (match-all)
     15432182 packets
     Match: flow  ip source-address
     police: Per-interface
       Conform: 64995654 bytes Exceed: 2376965424 bytes

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

例 4

インターフェイス FastEthernet 6/1 に 2 つのアクティブなフローがあり、宛先アドレスが 192.168.20.20 と 192.168.20.21 であるとします。次の例では、それぞれのフローを 1 Mbps に維持し、9000 バイトのバースト値を許可する方法を示します。

```
Switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip destination-address
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 fa6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory

Switch# show policy-map interface
 FastEthernet6/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      2965072 packets
      Match: flow  ip destination-address
      police: Per-interface
        Conform: 6105636 bytes Exceed: 476652528 bytes

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

例 5

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。

```
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。

（注） **match flow ip source-address|destination-address** コマンドを使用する場合、これら 2 つのフローは同じ送信元および宛先アドレスを持つため、1 つのフローに統合されます。

```
Switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol l4
source-port l4 destination-port
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
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1

class-map c1
```

```
   match flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port
!
 policy-map p1
    class c1
       police 1000000 bps 9000 byte conform-action transmit exceed-action drop
!
interface FastEthernet 6/1
  service-policy input p1

Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port

Switch# show policy-map p1
  Policy Map p1
    Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop

Switch# show policy-map interface
 FastEthernet6/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      15432182 packets
      Match: flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port
      police: Per-interface
        Conform: 64995654 bytes Exceed: 2376965424 bytes


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

階層型ポリサーの設定

（注） 階層型ポリサーは、Supervisor Engine V-10GE 上だけでサポートされます。

フロー ポリサーを既存ポリサーと結合し、2 つのポリシング レートをインターフェイスで作成できます。たとえばデュアル ポリシングを使用すると、特定インターフェイスのすべての着信トラフィック レートを 50 Mbps に制限し、このトラフィックの一部であるそれぞれのフローのレートを 2 Mbps に制限できます。

階層型ポリサーは、**service-policy** ポリシーマップ コンフィギュレーション コマンドで設定できます。ポリシー マップで使用されるクラス マップが、フローベース一致基準（**match flow ip source-address** など）と一致する場合、ポリシー マップは *フローベース*と呼ばれます。それぞれの子ポリシー マップは、親のすべての match access-group コマンドを継承します。

（注） *フローベース* ポリシー マップだけを子ポリシー マップとして設定できます。親ポリシー マップをフローベース ポリシー マップにすることはできません。子ポリシー マップと親ポリシー マップの両方で、クラスマップ設定に **match-all** が含まれている必要があります。

個別ポリサーか集約ポリサーの子としてフローベース ポリシー マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# policy-map` *policy_name*	個別ポリシー マップ名か集約ポリシー マップ名を指定します。
ステップ 2	`Switch(config-pmap)# class` *class_name*	このポリシー マップのクラスマップ名を指定します。
ステップ 3	`Switch(config-flow-cache)# service-policy` *service_policy_name*	フローベース ポリシー マップの名前を指定します。

（注）　親が集約ポリサー、子がマイクロフロー ポリサーである階層型ポリサー設定では、子のマイクロフロー ポリサーに一致するパケットはイン プロファイルであるパケットだけを報告します（つまり、ポリシング レートを一致させます）。ポリシング レートを超過するパケットは、クラスマップ パケット一致統計情報では報告されません。

次の例は、階層型ポリシー マップの作成方法を示しています。名前が *aggregate-policy* であるポリシー マップには、名前が *aggregate-class* であるクラス マップが含まれます。名前が *flow-policy* であるフローベース ポリシー マップは、子ポリシー マップとしてこのポリシー マップに付加されます。

```
Switch# config terminal
Switch(config)# policy-map aggregate-policy
Switch(config-pmap)# class aggregate-class
Switch(config-pmap-c)# service-policy flow-policy
Switch(config-pmap-c)# end
Switch#
```

次の例では、IP アドレス範囲が 101.237.0.0 ～ 101.237.255.255 であるトラフィックが 50 Mbps にポリシングされます。101.237.10.0 ～ 101.237.10.255 の範囲のフローは、2 Mbps の速度で個別にポリシングされます。このトラフィックは、集約ポリサーとその他のフローベース ポリサーという 2 つのポリサーを通過します。

次の例は、このシナリオの設定を示しています。

```
class-map match-all flow-class
 match flow ip source-address
 match access-group 20
!
class-map match-all aggregate-class
 match access-group 10
!
policy-map flow-policy
 class flow-class
   police 2000000 bps 10000 byte conform-action transmit exceed-action drop
!
policy-map aggregate-policy
 class aggregate-class
   police 50000000 bps 40000 byte conform-action transmit exceed-action drop
  service-policy flow-policy
!
access-list 10 permit 101.237.0.0 0.0.255.255
access-list 20 permit 0.0.10.0 255.255.0.255
```

次に、設定を確認する例を示します。

```
Switch# show policy-map flow-policy
```

```
 Policy Map flow-policy
   Class flow-class
     police 2000000 bps 10000 byte conform-action transmit exceed-action drop
Switch# show policy-map aggregate-policy
 Policy Map aggregate-policy
   Class aggregate-class
     police 50000000 bps 40000 byte conform-action transmit exceed-action drop
     service-policy flow-policy

Switch# show policy-map interface
FastEthernet6/1
 Service-policy input: aggregate-policy

   Class-map: aggregate-class (match-all)
     132537 packets
     Match: access-group 10
     police: Per-interface
       Conform: 3627000 bytes Exceed: 0 bytes

     Service-policy : flow-policy

       Class-map: flow-class (match-all)
         8867 packets
         Match: access-group 20
         Match: flow  ip source-address
         police: Per-interface
       Conform: 1649262 bytes Exceed: 59601096 bytes

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

   Class-map: class-default (match-any)
     5 packets
     Match: any        5 packets
```

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 フォン）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。

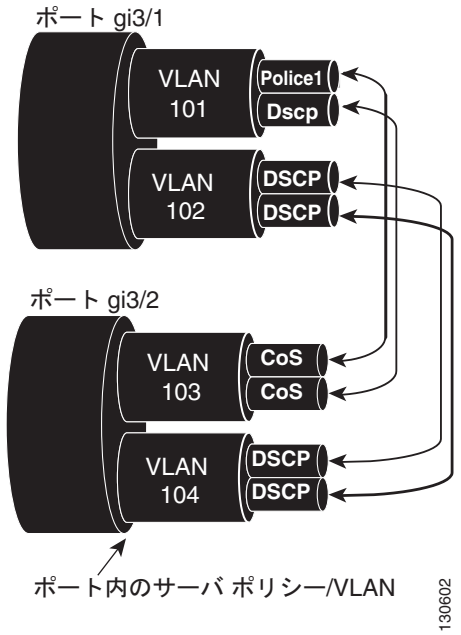
per-Port per-VLAN QoS を設定するには、次の作業を行います。

	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 32-6 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、入力および出力ポリシング、DSCP の信頼、またはデータよりも音声パケットへの優先制御で構成されます。

図 32-6　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: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes
```

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: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

 GigabitEthernet6/1 vlan 300

  Service-policy output: p2

    Class-map: class-default (match-any)
```

```
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

GigabitEthernet6/1 vlan 301

 Service-policy output: p2

   Class-map: class-default (match-any)
     0 packets
     Match: any
       0 packets
     police: Per-interface
       Conform: 0 bytes Exceed: 0 bytes

GigabitEthernet6/1 vlan 400

 Service-policy input: p1

   Class-map: class-default (match-any)
     0 packets
     Match: any
       0 packets
     police: Per-interface
       Conform: 0 bytes Exceed: 0 bytes
```

インターフェイス上での QoS のイネーブル化またはディセーブル化

qos インターフェイス コマンドを使用すると、設定されている QoS 機能が再びイネーブルになります。**qos** インターフェイス コマンドは、インターフェイスのキュー設定に影響しません。

インターフェイスからのトラフィックに対して QoS 機能をイネーブルまたはディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# **interface** {**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。
ステップ 2	Switch(config-if)# [**no**] **qos**	インターフェイス上で QoS をイネーブルにします。 インターフェイス上で QoS をディセーブルにするには、**no** キーワードを使用します。
ステップ 3	Switch(config-if)# **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 4	Switch# **show qos interface**	設定を確認します。

次に、インターフェイス VLAN 5 上で QoS をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface vlan 5
Switch(config-if)# no qos
Switch(config-if)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show qos | begin QoS is disabled
  QoS is disabled on the following interfaces:
    Vl5
<...Output Truncated...>
Switch#
```

レイヤ 2 インターフェイス上での VLAN ベース QoS の設定

デフォルトでは、QoS は物理インターフェイスに付加されたポリシー マップを使用します。レイヤ 2 インターフェイスについては、VLAN に付加されたポリシー マップを使用するように QoS を設定できます （「インターフェイスへのポリシー マップの対応付け」（P.32-41）を参照）。

レイヤ 2 インターフェイス上で VLAN ベースの 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**} *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)# [**no**] **qos vlan-based**	レイヤ 2 インターフェイス上で VLAN ベースの QoS を設定します。 インターフェイス上で VLAN ベース QoS をディセーブルにするには、**no** キーワードを使用します。
ステップ 3	Switch(config-if)# **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 4	Switch# **show qos**	設定を確認します。

（注）　レイヤ 2 インターフェイスに入力 QoS ポリシーが付加されていない場合、ポートが VLAN ベースで設定されていなくても、（パケットが着信する）VLAN に付加された入力 QoS ポリシーがあればそれが使用されます。このデフォルトが望ましくない場合には、レイヤ 2 インターフェイスにプレースホルダの入力 QoS ポリシーを対応付けます。同様に、レイヤ 2 インターフェイスに出力 QoS ポリシーが付加されていない場合、ポートが VLAN ベースで設定されていなくても、（パケットを送信する）VLAN に付加された出力 QoS ポリシーがあればそれが使用されます。このデフォルトが望ましくない場合には、レイヤ 2 インターフェイスにプレースホルダの出力 QoS ポリシーを付加します。

次に、インターフェイス FastEthernet 5/42 で VLAN ベースの QoS を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/42
Switch(config-if)# qos vlan-based
Switch(config-if)# end
```

次に、設定を確認する例を示します。

```
Switch# show qos | begin QoS is vlan-based
QoS is vlan-based on the following interfaces:
    Fa5/42
Switch#
```

（注）　レイヤ 2 インターフェイスに VLAN ベース QoS が設定されている場合に、QoS ポリシーがない VLAN のポートにパケットが着信すると、ポートに付加された QoS ポリシーがある場合はそれが使用されます。これは、入力および出力 QoS ポリシーの両方に適用されます。

インターフェイスの信頼状態の設定

このコマンドは、インターフェイスの信頼状態を設定します。デフォルトでは、すべてのインターフェイスは信頼できません。

インターフェイスの信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`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。
ステップ 2	`Switch(config-if)# [no] qos trust [dscp | cos]`	インターフェイスの信頼状態を設定します。 設定した値をクリアし、デフォルトに戻すには、**no** キーワードを使用します。
ステップ 3	`Switch(config-if)# 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 4	`Switch# show qos`	設定を確認します。

インターフェイスの信頼状態を設定する際、次の点に注意してください。

- インターフェイスの状態を untrusted に戻すには、**no qos trust** コマンドを使用します。
- **qos trust cos** コマンドを使用して *trust cos* に設定された入力インターフェイスに着信したトラフィックの場合、送信される CoS は、常に着信パケットの CoS（または、パケットをタグなしで受信した場合には、入力インターフェイスのデフォルト CoS）です。
- **qos trust dscp** コマンドを使用してインターフェイスの信頼状態を *trust dscp* に設定していない場合、セキュリティおよび QoS ACL 分類では、常にインターフェイス DSCP が使用され、着信パケットの DSCP は使用されません。
- Cisco IOS Release 12.2(31)SG 以降では、Supervisor Engine V-10GE を使用すれば、ポートの信頼状態にかかわらずパケットの IP DSCP 値に基づいてパケットを分類できます。パケット送信キューイングはこの動作による影響を受けません。送信キューの詳細については、「送信キューの設定」（P.32-56）を参照してください。

次に、**trust cos** キーワードを使用してインターフェイス GigabitEthernet 1/1 を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# qos trust cos
Switch(config-if)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show qos interface gigabitethernet 1/1 | include trust
  Trust state: trust COS
Switch#
```

インターフェイスの CoS 値の設定

QoS は、trusted として設定された入力インターフェイスからのタグなしフレーム、および untrusted として設定された入力インターフェイスからのすべてのフレームに、このコマンドで指定された CoS 値を割り当てます。

入力インターフェイスの CoS 値を設定するには、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**} *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)# [**no**] **qos cos** *default_cos*	入力インターフェイスの CoS 値を設定します。 設定した値をクリアし、デフォルトに戻すには、**no** キーワードを使用します。
ステップ 3	Switch(config-if)# **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 4	Switch# **show qos interface** {**fastethernet** | **gigabitethernet**} *slot/interface*	設定を確認します。

次に、インターフェイス FastEthernet 5/24 にデフォルトとして CoS 5 を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/24
Switch(config-if)# qos cos 5
Switch(config-if)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show qos interface fastethernet 5/24 | include Default COS
  Default COS is 5
Switch#
```

インターフェイスの DSCP 値の設定

QoS は、trust dscp に設定されたインターフェイスで受信した非 IPv4 フレーム、および untrusted として設定されたインターフェイスで受信したすべてのフレームに、このコマンドで指定された DSCP 値を割り当てます。

入力インターフェイスの DSCP 値を設定するには、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**} *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)# [**no**] **qos dscp** *default_dscp*	入力インターフェイスの DSCP 値を設定します。 設定した値をクリアし、デフォルトに戻すには、**no** キーワードを使用します。
ステップ 3	Switch(config-if)# **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 4	Switch# **show qos interface** {**fastethernet** | **gigabitethernet**} *slot/interface*	設定を確認します。

次に、インターフェイス FastEthernet 5/24 のデフォルトとして DSCP 5 を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/24
```

```
Switch(config-if)# qos dscp 5
Switch(config-if)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show qos interface fastethernet 6/1
QoS is enabled globally
Port QoS is enabled
  Port Trust State:CoS
  Default DSCP:0 Default CoS:0

  Tx-Queue    Bandwidth     ShapeRate     Priority    QueueSize
                (bps)         (bps)                   (packets)
    1         31250000      disabled      N/A         240
    2         31250000      disabled      N/A         240
    3         31250000      disabled      normal      240
    4         31250000      disabled      N/A         240
Switch#
```

送信キューの設定

ここでは、送信キューを設定する手順について説明します。

- 「DSCP 値から特定の送信キューへのマッピング」（P.32-56）
- 「送信キュー間での帯域幅の割り当て」（P.32-57）
- 「送信キューのトラフィック シェーピングの設定」（P.32-58）
- 「ハイ プライオリティ送信キューの設定」（P.32-58）

ネットワークと QoS ソリューションの複雑さによっては、次に挙げる手順のすべてを実行する必要があります。ただし、最初に次の質問に答えてください。

- 各キューへの（DSCP 値による）パケットの割り当て
- 特定のポートでの送信キューと他のキューとの相対的なサイズ
- 各キューへの使用可能な帯域幅の割り当て
- 各送信キューの最大速度、および各送信キューから送信できる最大バースト トラフィック

インターフェイスの QoS 状態に関係なく、スイッチではすべての送信キューはイネーブルです。DSCP 値はデフォルトで信頼されているため、スイッチは DSCP に基づいて適切な送信キューを使用してマッピングします。このキュー選択は、内部 DSCP から送信キューへのマッピング テーブルに基づきます。

DSCP 値から特定の送信キューへのマッピング

DSCP 値を送信キューにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# [**no**] **qos map dscp** ***dscp-values*** **to tx-queue** ***queue-id***	DSCP 値を送信キューにマッピングします。*dscp-list* には、最大 8 つの DSCP 値を指定できます。*queue-id* の範囲は、1 ～ 4 です。 送信キューから DSCP 値を削除するには、**no qos map dscp to tx-queue** コマンドを使用します。
ステップ 2	Switch(config)# **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 3	Switch# **show qos maps dscp tx-queues**	設定を確認します。

次に、送信キュー 2 に DSCP 値をマッピングする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# qos map dscp 50 to tx-queue 2
Switch(config)# end
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show qos maps dscp tx-queue
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 :d2  0  1  2  3  4  5  6  7  8  9
-----------------------------------
0 :   02 02 02 01 01 01 01 01 01 01
1 :   01 01 01 01 01 01 02 02 02 02
2 :   02 02 02 02 02 02 02 02 02 02
3 :   02 02 03 03 03 03 03 03 03 03
4 :   03 03 03 03 03 03 03 03 04 04
5 :   04 04 04 04 04 04 04 04 04 04
6 :   04 04 04 04
Switch#
```

送信キュー間での帯域幅の割り当て

送信キューの帯域幅を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# **interface gigabitethernet** *slot/interface*	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)# **tx-queue** ***queue_id***	設定する送信キューを選択します。
ステップ 3	Switch(config-if-tx-queue)# [**no**] [**bandwidth** *rate* | **percent** *percent*]	送信キューの帯域幅レートを設定します。 送信キューの帯域幅の比率をデフォルト値に戻すには、**no** キーワードを使用します。
ステップ 4	Switch(config-if-tx-queue)# **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 5	Switch# **show qos interface**	設定を確認します。

帯域幅レートは、インターフェイスによって異なります。

帯域幅を設定できるのは、次のインターフェイスにかぎられます。

- Supervisor Engine III（WS-X4014）上のアップリンク ポート
- WS-X4306-GB モジュール上のポート

- WS-X4232-GB-RJ モジュール上の 2 つの 1000BASE-X ポート
- WS-X4418-GB モジュール上の最初の 2 つのポート
- WS-X4412-2GB-TX モジュール上の 2 つの 1000BASE-X ポート

次に、送信キュー 2 に 1 Mbps の帯域幅を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# tx-queue 2
Switch(config-if-tx-queue)#bandwidth 1000000
Switch(config-if-tx-queue)# end
Switch#
```

送信キューのトラフィック シェーピングの設定

送信キューから送信されるパケットが指定の最大速度を超えないように設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# interface {fastethernet | gigabitethernet} slot/interface`	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)# tx-queue queue_id`	設定する送信キューを選択します。
ステップ 3	`Switch(config-if-tx-queue)# [no] [shape rate | percent percent]`	送信キューの送信レートを設定します。 送信キューの最大速度を削除するには、**no** キーワードを使用します。
ステップ 4	`Switch(config-if-tx-queue)# 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 5	`Switch# show qos interface`	設定を確認します。

次に、送信キュー 2 のシェープ レートを 1 Mbps に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if-tx-queue)# tx-queue 2
Switch(config-if-tx-queue)# shape 1000000
Switch(config-if-tx-queue)# end
Switch#
```

ハイ プライオリティ送信キューの設定

送信キュー 3 をハイ プライオリティに設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch(config)# interface {fastethernet | gigabitethernet} slot/interface`	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)# tx-queue 3`	設定する送信キュー 3 を選択します。
ステップ 3	`Switch(config-if)# [no] priority high`	この送信キューをハイ プライオリティに設定します。 送信キューのプライオリティをクリアするには、**no** キーワードを使用します。

	コマンド	目的
ステップ 4	`Switch(config-if)# 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 5	`Switch# show qos interface`	設定を確認します。

次に、送信キュー 3 をハイ プライオリティに設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet 1/1
Switch(config-if-tx-queue)# tx-queue 3
Switch(config-if-tx-queue)# priority high
Switch(config-if)# end
Switch#
```

DSCP マップの設定

ここでは、DSCP マップを設定する方法について説明します。内容は次のとおりです。

- 「CoS/DSCP マップの設定」（P.32-59）
- 「ポリシング済み DSCP マップの設定」（P.32-60）
- 「DSCP/CoS マップの設定」（P.32-61）

マップはいずれもグローバルに定義され、すべてのポートに適用されます。

CoS/DSCP マップの設定

CoS/DSCP マップを使用して、着信パケットの CoS 値を、QoS がトラフィックのプライオリティを表すために内部使用する DSCP 値にマッピングします。

表 32-4 に、デフォルトの CoS/DSCP マップを示します。

表 32-4　デフォルトの CoS/DSCP マップ

CoS 値	0	1	2	3	4	5	6	7
DSCP の値	0	8	16	24	32	40	48	56

これらの値が使用しているネットワークに適さない場合は、値を変更する必要があります。

CoS/DSCP マップを変更するには、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)# qos map cos` *cos1 ... cos8* `to dscp` *dscp*	CoS/DSCP マップを変更します。 *cos1...cos8* には、最大 8 つの CoS を入力できます。指定できる値の範囲は 0 ～ 7 です。各 CoS 値はスペースで区切ります。 *dscp* の範囲は 0 ～ 63 です。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	`Switch# show qos maps cos-dscp`	入力を確認します。
ステップ 5	`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。

次の例では、CoS 0 の入力 CoS/DSCP マッピングを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# qos map cos 0 to dscp 20
Switch(config)# end
Switch# show qos maps cos dscp

CoS-DSCP Mapping Table:
CoS:  0   1  2  3  4  5  6  7
---------------------------------
DSCP: 20  8 16 24 32 40 48 56
Switch(config)#
```

（注）　デフォルトのマップに戻すには、**no qos cos to dscp** 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。

次の例では、CoS/DSCP マッピング テーブル全体をクリアする方法を示します。

```
Switch(config)# no qos map cos to dscp
Switch(config)#
```

ポリシング済み DSCP マップの設定

ポリシングおよびマーキング アクションによって得られる新しい値に DSCP 値をマークダウンするには、ポリシング済み DSCP マップを使用します。

デフォルトのポリシング設定 DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

CoS/DSCP マップを変更するには、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)# qos map dscp policed` *dscp-list* **to dscp** *mark-down-dscp*	ポリシング済み DSCP マップを変更します。 • *dscp-list* には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *mark-down-dscp* には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Switch# show qos maps dscp policed`	入力を確認します。
ステップ 5	`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。

デフォルトのマップに戻すには、**no qos dscp policed** 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、DSCP 50 ～ 57 を、マークダウンされる DSCP 値 0 にマッピングする例を示します。

```
Switch# configure terminal
Switch(config)# qos map dscp policed 50 51 52 53 54 55 56 57 to dscp 0
Switch(config)# end
Switch# show qos maps dscp policed
Policed-dscp map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    00 00 00 00 00 00 00 00 58 59
      6 :    60 61 62 63
```

（注） 前述のポリシング済み DSCP マップでは、マークダウンされた DSCP 値がマトリクスの本体に示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点にある値が、マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

DSCP/CoS マップの設定

DSCP/CoS マップは、CoS 値を生成する目的で使用します。

表 32-5 に、デフォルトの DSCP/CoS マップを示します。

表 32-5　デフォルトの DSCP/CoS マップ

DSCP の値	0 ～ 7	8 ～ 15	16 ～ 23	24 ～ 31	32 ～ 39	40 ～ 47	48 ～ 55	56 ～ 63
CoS 値	0	1	2	3	4	5	6	7

これらの値がネットワークに適さない場合は、値を変更する必要があります。

DSCP/CoS マップを変更するには、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)# [no] qos map dscp` *dscp-list* `to cos` *cos*	DSCP/CoS マップを変更します。 • *dscp-list* には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *cos* には、一連の DSCP 値を対応させる CoS 値を 1 つだけ入力します。 DSCP の範囲は 0 ～ 63、CoS の範囲は 0 ～ 7 です。 デフォルトのマップに戻すには、**no qos dscp to cos** 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。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	`Switch# show qos maps dscp to cos`	入力を確認します。
ステップ 5	`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。

次に、DSCP 値 0、8、16、24、32、40、48、および 50 を CoS 値 0 にマッピングして、マップを表示する例を示します。

```
Switch# configure terminal
Switch(config)# qos map dscp 0 8 16 24 32 40 48 50 to cos 0
Switch(config)# end
Switch# show qos maps dscp cos
Dscp-cos map:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 01
      1 :    01 01 01 01 01 01 00 02 02 02
      2 :    02 02 02 02 00 03 03 03 03 03
      3 :    03 03 00 04 04 04 04 04 04 04
      4 :    00 05 05 05 05 05 05 05 00 06
      5 :    00 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

（注） 前述の DSCP/CoS マップでは、CoS 値がマトリクスの本体に示されています。d1 列は DSCP の最上位桁、d2 行は DSCP の最下位桁を示します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

レイヤ 2 制御パケット QoS のイネーブル化

（注） レイヤ 2 制御パケット QoS は、Supervisor Engine 6-E ではサポートされて*いません*。

この機能では、大量の制御パケットの入力による高 CPU 利用率の問題を解決します。問題の解決は、制御したいプロトコル（QoS CAM にインストール済み）に対応する QoS スタティック エントリを無効にすることで行われます。

解決法では、ハードウェアは、レイヤ 2 制御トラフィックに一致するユーザ定義サービス ポリシーに対応するアクションを適用します。この制御モードは、デフォルト モードが既存のモードであるため、CLI を介して展開できます。

必須レイヤ 2 パケットに一致するようにポリシーを設定し、希望するレベルにポリシングする必要があります。レイヤ 2 制御パケットは、基本的に宛先 MAC アドレスで識別されます。この機能が、そのパケット タイプでイネーブルになっていると、目的の制御パケットに一致する MACL およびそれらの MACL に一致する対応クラスマップがまだ存在しない場合、自動生成されます。

制御パケットのポリシングを行うには、ポリシーマップでこれらのクラスマップを使用する必要があるだけです。その後他のポリシーマップと同様に、ポート単位、VLAN 単位、またはポート単位/VLAN 単位でポリシーマップを適用できます。

レイヤ 2 制御パケット QoS をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# interface t`	コンフィギュレーション モードに入ります。
ステップ 2	`Switch(config)# qos control-packets [bpdu-range | cdp-vtp | sstp]`	レイヤ 2 制御ポリシングをイネーブルにします。 この機能をイネーブルにするパケット タイプを指定できます。 デフォルトでは、すべてのパケット タイプが選択されます。

	コマンド	目的
ステップ 3	`Switch(config)# 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 4	`Switch# show run | inc qos control-packets`	設定を確認します。

次の表では、この機能で影響を受けるパケット タイプを一覧にします。

表 32-6　パケット タイプと作用対象のアドレス範囲

機能がイネーブルになるパケット タイプ	動作するアドレス範囲
BPDU 範囲	0180.C200.0000 BPDU 0180.C200.0002 OAM, LACP 0180.C200.0003 Eapol
CDP-VTP	0100.0CCC.CCCC
SSTP	0100.0CCC.CCCD

次に、レイヤ 2 制御パケット QoS を CDP-VTP パケットに設定する例を示します。

```
Switch# config terminal
Switch(config)# qos control-packets cdp-vtp
Switch(config)# end
Switch# show run | inc qos control-packets
qos control-packets cdp-vtp
```

すべてのパケット タイプでこの機能がイネーブルになっているとき、**show running** コマンドの出力には、**qos control-packets** 文字列が表示されます。

```
Switch# show running | inc qos control-packets
qos control-packets
```

ここで、SSTP パケットに対してこの機能をディセーブルにしている場合、次の出力が表示されます。

```
Switch# show running | inc qos control-packets
qos control-packets bpdu-range
qos control-packets cdp-vtp
```

show running コマンドおよび一般的な関連コマンドで、目的の制御パケットをキャプチャ、ドロップ、およびポリシングする、MACL およびユーザ設定ポリシーのステータスを確認できます。

この機能をディセーブルにするには、**no qos control-packets [bpdu-range | cdp-vtp | sstp]** コマンドを実行します。たとえば、CDP-VTP パケットで機能をディセーブルにするには、**no qos control-packets cdp-vtp** コマンドを実行します。

（注） 指定したプロトコルタイプに対してこの機能の設定を解除すると、そのプロトコルタイプを処理するユーザ設定ポリシーは、ただちに無効な状態になります。TCAM リソースを保存するには、MACL およびクラスマップ（自動生成またはユーザ定義）とともにポリシーも削除します。

（注） インターフェイスがダウン ステートの場合、TCAM リソースは消費されません。

次の表に、対応パケット タイプで機能がイネーブルになっているときに作成されるクラスマップを示します。

表 32-7　パケット タイプおよび自動生成 MACL/クラスマップ

パケット タイプ	自動生成 MACL/クラスマップ
BPDU 範囲	mac access-list extended system-control-packet-bpdu-range permit any 0180.c200.0000 0000.0000.000c class-map match-any system-control-packet-bpdu-range match access-group name system-control-packet-bpdu-range
SSTP	mac access-list extended system-control-packet-sstp permit any host 0100.0ccc.cccd class-map match-any system-control-packet-sstp match access-group name system-control-packet-sstp
CDP-VTP	mac access-list extended system-control-packet-cdp-vtp permit any host 0100.0ccc.cccc class-map match-any system-control-packet-cdp-vtp match access-group name system-control-packet-cdp-vtp

次に、MACL およびポリサー設定を適用する例を示します。
BPDU 範囲パケット：

- BPDU 範囲でこの機能をイネーブルにします。

```
qos control-packets bpdu-range
```

- 対応 MACL/クラスマップを作成します（自動的に実行）。

```
mac access-list extended system-control-packet-bpdu-range
    permit any 0180.C200.0000 0000.0000.000C

class-map match-any system-control-packet-bpdu-range
    match access-group name system-control-packet-bpdu-range
```

- ポリシーマップを作成し、目的のインターフェイス/VLAN に付加します。

```
policy-map police-bpdu
  class system-control-packet-bpdu-range
    police 32000 bps 1000 byte conform-action transmit exceed-action drop

interface GigabitEthernet 1/1
      switchport trunk encapsulation dot1q
      switchport mode trunk
      vlan-range 100
          service-policy input police_bpdu
```

システムが生成したクラスマップおよび MACL を変更しないでください。変更すると、スイッチがリロードを行うとき、または実行コンフィギュレーションをファイルから更新するとき、予期せぬ動作になることがあります。

これらのシステム生成クラスマップまたは MACL を調整または変更する必要がある場合、ユーザ定義クラスマップおよび MACL を作成する必要があります。次に、作成した新しいユーザ定義 MACL/クラスマップを使用して、目的のポリシングを実行します。

（注）　ユーザ定義クラスマップ名をプレフィックス **system-control-packet-** で始める必要がある点だけが唯一の制限事項です。クラスマップが **system-control-packet-** で始まらない場合、特定のスーパーバイザ エンジンでは、設定された QoS アクションが実行されないことがあります。

（注）　ユーザ定義 MACL に使用する名前には、制限事項はありません。

たとえば、次に挙げる名前は、制御パケットをポリシングする、有効なユーザ定義クラスマップ名です。

```
system-control-packet-bpdu1
system-control-packet-control-packet
system-control-packet-bla
```

たとえば、EAPOL、OAM、または BPDU パケットに異なるクラスマップを定義する予定である場合、自動生成クラスマップの system-control-packet-bpdu-range はすべてのパケットに一致するため、ユーザ定義 MACL/クラスマップ（前述の例）の作成が役立ちます。

```
mac access-list extended system-control-packet-bpdu
   permit any 0180.c200.0000
class-map match-any system-control-packet-bpdu
   match access-group name system-control-packet-bpdu

mac access-list extended system-control-packet-eapol
   permit any 0180.c200.0003
class-map match-any system-control-packet-eapol
   match access-group name system-control-packet-eapol

mac access-list extended system-control-packet-oam
   permit any 0180.c200.0002
class-map match-any system-control-packet-oam
   match access-group name system-control-packet-oam
```

次にこれらのクラスマップを使用して、共通ポリサーを system-control-packet-bpdu-range に適用する代わりに、各パケットに異なるポリサーを定義できます。

使用上のガイドライン

この機能がイネーブルになっているとき、ポートおよび VLAN に適用された既存のポリシーは、制御したいレイヤ 2 制御パケットが偶発的に希望しない QoS アクションの対象になることがなく、この機能がスイッチ上で設定された他のポリシーから影響を受けることがないというポリシーであることを確認する必要があります。

前述の制御パケットで QoS をイネーブルにする前に、新規および既存のポリシーを調べて編集し、選択した制御パケットに一致するポリシーマップの分類子が正しい順番で定義および設定されていることを確認する必要があります。同じポリシーマップ内の後半に出現する別の分類子のアクションで意図しない結果になることを避けるため、制御パケットに一致する分類子をポリシーマップの冒頭に配置する必要があります。

クラス class-default に関連付けられたアクションの場合、動作はスーパーバイザ エンジンのタイプによって異なります。

- 内蔵 NetFlow がサポートされている Supervisor Engine V-10GE

  class-default に関連付けられたアクションは、一致しない制御パケットには適用されず、control-packet クラスマップがそれよりも前に制御パケットを取得していない場合、デフォルトの許可アクションは適用されません。system-control-packet- で始まるクラスマップを使用するポリサーに関連付けられたアクションだけが、制御パケットに適用されます。

- 他のすべてのスーパーバイザ エンジン

  class-default に関連付けられたアクションは、一致しない制御パケットに適用されます。

（注） 内蔵 NetFlow がサポートされている Supervisor Engine V-10GE では、これらのタイプのパケットでマイクロフロー統計は使用できません。

（注） BPDU 範囲でこの機能がイネーブルになっている場合、最初の 802.1X 認証フェーズが完了した後でだけ EAPOL パケットをポリシングできます。

（注） フォワーディング スパニングツリー ステートになっているポートでポート セキュリティがイネーブルになっているとき、レイヤ 2 制御パケットはそのポート上でポリシングできません。

機能の相互作用

個々のフローのユーザ設定ポリシーを適用したあと、CPU への集約フローをレート制限するために、レイヤ 2 *の上位に* CoPP ポリシーを設定します。その場合、基本的に CoPP は、ユーザ定義ポリシーによりポート単位/VLAN 単位ベースですでに入力側でフィルタされたパケットの出力側でさらにレート制限を行って、CPU のための別レベルの保護を提供します。CoPP は、ポート上にユーザ定義ポリシーが適用されている間は、第 2 レベルの防御となり、VLAN は第 1 レベルの防御になります。

たとえば、ポリシーマップマッチングおよびギガビット イーサネット インターフェイス 1/1 から送信される BPDU 範囲トラフィックのポリシングを設定する場合、VLAN 1 は次のようになります。

```
policy-map police_bpdu_1
      class system-control-packet-bpdu-range
  police 32000 bps 1000 byte conform-action transmit exceed-action drop

   interface GigabitEthernet1/1
      switchport trunk encapsulation dot1q
      switchport mode trunk
      vlan-range 1
      service-policy input police_bpdu_1
```

さらに、ギガビット イーサネット インターフェイス 1/2 VLAN 2 で 2 番めを設定すると、BPUD 範囲パケットのマッチングおよびポリシングは次のようになります。

```
policy-map police_bpdu_2
      class system-control-packet-bpdu-range
  police 34000 bps 1000 byte conform-action transmit exceed-action drop

   interface GigabitEthernet1/2
      switchport trunk encapsulation dot1q
      switchport mode trunk
      vlan-range 2
```

```
      service-policy input police_bpdu_2
```

CoPP は次のように設定します。

```
policy-map system-cpp-policy
      class system-cpp-bpdu-range
  police 50000 bps 1000 byte conform-action transmit exceed-action drop
```

次の点に注意してください。

- インターフェイス 1/1、VLAN 1 では、BPDU 範囲パケットは、police_bpdu_1 に従って毎秒 32000 ビットのレートでポリシングされます。
- インターフェイス 1/2、VLAN 2 では、BPDU 範囲パケットは、police_bpdu_2 に従って毎秒 34000 ビットのレートでポリシングされます。
- 集約フローは、毎秒 50000 ビットのレートで CPU ポートの CoPP からポリシングされます。

また、ポートまたは VLAN のグループに適用された名前付き集約ポリサーを使用して、ポリサー リソースの消費を減らすこともできます。

（注）　フォワーディング スパニングツリー ステートになっているポートでポート セキュリティがイネーブルになっているとき、レイヤ 2 制御パケットはそのポート上でポリシングできません。

Supervisor Engine 6-E での auto-QoS の設定

Supervisor Engine II-Plus から V-10GE までの Auto-QoS とは異なり、Supervisor Engine 6-E の Auto-QoS 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、Supervisor Engine 6-E のスイッチ上のインターフェイスに適用された Auto-QoS は、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を設定することを意味します。

クラスマップは次のとおりです。

```
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-Cos
  match cos  5
class-map match-all AutoQos-VoIP-Control-QosGroup24
  match qos-group 24
class-map match-all AutoQos-VoIP-Control-QosGroup26
  match qos-group 26
class-map match-all AutoQos-VoIP-Bearer-QosGroup
  match qos-group 46
class-map match-all AutoQos-VoIP-Bearer-Dscp
  match  dscp ef
class-map match-all AutoQos-VoIP-Control-Cos
  match cos  3
```

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。

ポリシー マップは次のとおりです。

```
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
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-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
```

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。

Supervisor Engine 6-E に採用されているスイッチでの Auto-QoS の呼び出しでは、Supervisor Engine II-Plus から V-10GE までで使用されるのと同じコンフィギュレーション コマンドを使用します。

スイッチ間接続の場合、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。

Supervisor Engine 6-E での QoS の設定

（注） Catalyst 4900M および Supervisor Engine 6-E の QoS 機能は同等です。

（注） HQoS は Supervisor Engine 6-E ではサポートされていません。

次の内容について説明します。

- 「MQC ベースの QoS の設定」（P.32-69）
- 「概要」（P.32-70）
- 「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」（P.32-71）
- 「プラットフォーム ハードウェアの機能」（P.32-72）
- 「QoS サービス ポリシーを適用するための前提条件」（P.32-72）
- 「QoS サービス ポリシーの適用に関する制約事項」（P.32-72）
- 「分類」（P.32-73）
- 「ポリシング」（P.32-73）
- 「ネットワーク トラフィックのマーキング」（P.32-74）
- 「シェーピング、共有（帯域幅）、プライオリティ キューイング、および DBL」（P.32-81）

MQC ベースの QoS の設定

Cisco IOS Release 12.2(40)SG 以降、Catalyst 4500 シリーズ スイッチは、Supervisor Engine 6-E を使用して QoS の 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 ポリシーには、各トラフィック クラスに実行する QoS ポリシー アクションを定義します。
- 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 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」を参照してください。

概要

Supervisor Engine 6-E は、QoS の導入のベスト エフォートと DiffServ タイプをサポートします（RFC 2597、2598、2474、2475 によって DiffServ 標準が定義されます）。上位 Supervisor Engine 6-E QoS モデルは、次のとおりです。

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。

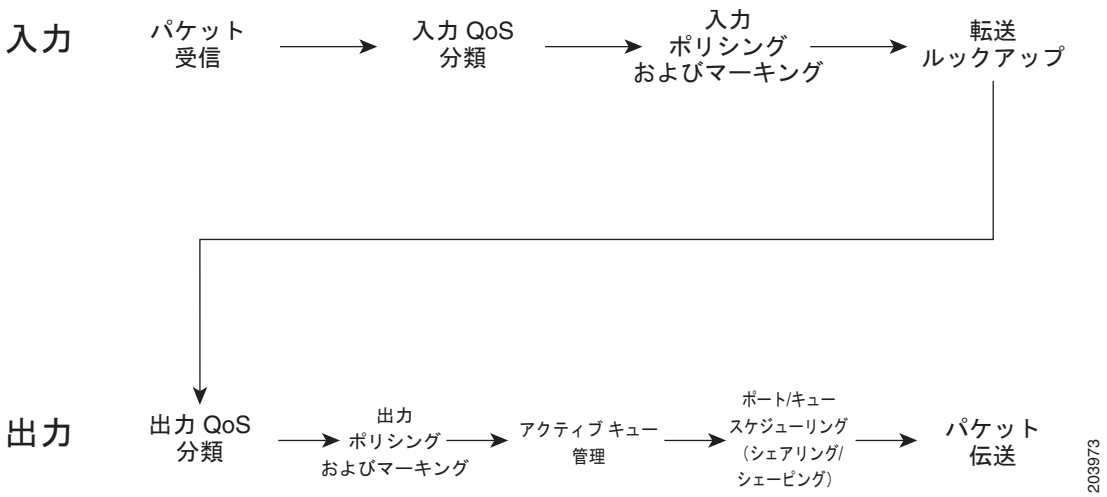
ステップ 5　出力分類に応じて、パケットがポリシングされ、そのプライオリティが任意で（*再）マークされます*。さらに、パケットの送信キューがトラフィック クラスによって決定されます。

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。

図 32-7 に、Supervisor Engine 6-E の高レベル モデルを示します。

図 32-7　QoS パケット処理



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、Supervisor Engine 6-E でサポートされるさまざまな分類基準およびアクションのまとめを示します。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 destination-address mac	宛先 MAC アドレスを一致条件として使用します。
match source-address mac	送信元 MAC アドレスを一致基準として使用します。
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。
service-policy	一致基準として使用するトラフィック ポリシーの名前を指定します（トラフィック ポリシーを互いにネストさせるため（階層型トラフィック ポリシー））。最大で 2 つのレベルがサポートされます。

サポートされる分類アクション	説明
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 Diffserv コード ポイント（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	後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	4 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。

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、ポートの数に応じて固定です。最大値の制限はありません。
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。

（注）　ポリシーの SVI への関連付けはサポートされていません。

分類

Supervisor Engine 6-E 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。入力で実行されるパケット 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、Supervisor Engine 6-E は分類リソース共有もサポートします。

デフォルトで、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が適用されている場合は、ACL エントリが Supervisor Engine 6-E 上で共有されます。CAM エントリが共有されている場合でも、QoS アクションはターゲットごとに異なります。

次に例を示します。

```
    class-map c1
      match ip any

Policy Map p1
    class ipp5
      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、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。

ポリシング

Supervisor Engine 6-E 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

  Supervisor Engine 6-E 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、Supervisor Engine 6-E 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。

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の詳細については、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/products/ps6350/products_configuration_guide_book09186a0080435d50.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 マーキングは同時にはサポートされません。
- 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。
- PVQoS ポリシーのあるポート チャネルを削除すると、スイッチはクラッシュします。

  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 Quality of Service（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

トラフィック 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 Diffserv コード ポイント（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。

次の属性を設定および変更できます。

- 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 32-8　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 precendence	パケット ヘッダーの precendence 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 32-8 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.32-37）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.32-41）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 マップは多対一型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 マップはトラフィック属性について to-from 関係を確立し、属性に加える変更を定義します。つまり、属性は、ある値から（from）別の値に（to）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 32-9　to-from 関係を確立できるトラフィック属性

「to」属性	「from」属性
Precedence	CoS、QoS グループ、DSCP、Precedence
DSCP	CoS、QoS グループ、DSCP、Precendence
CoS	DSCP、QoS グループ、CoS、Precedence

次に、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）の例を示します。

```
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 コンフィギュレーション」（P.32-37）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.32-41）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。

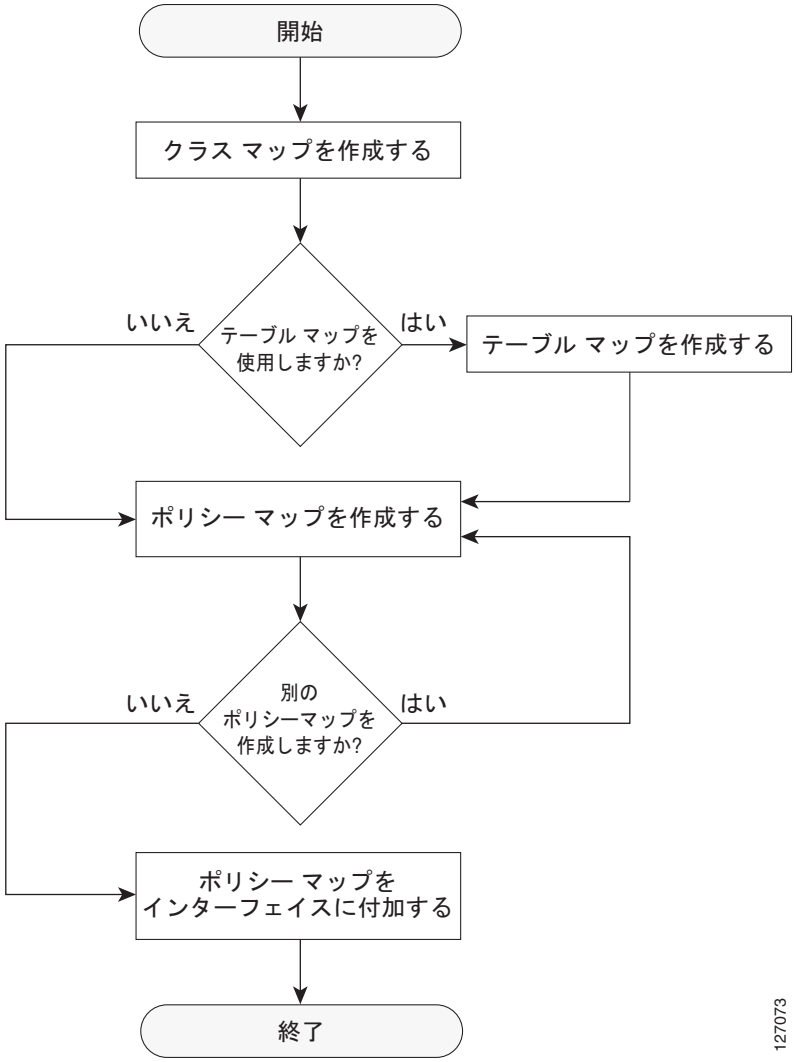
分類ベース：この場合、クラスに一致するすべてのトラフィックは、明示的方法またはテーブル マップ ベースの方法のいずれかを使用してマーク付けされます。この方法は、*無条件*マーキングと呼ばれます。

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 マーキングの手順フローチャート

図 32-8 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 32-8　トラフィック マーキングの手順フローチャート



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

Supervisor Engine 6-E は、トラフィックのクラスに一致するパケットの複数の QoS 属性をマーク付けできます。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するとき、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付けするマルチリージョン（conform/exceed/violate）は、サポートされ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

Supervisor Engine 6-E は、パケットを送信、マークダウン、ドロップするポリサー アクションだけでなく、COS および DSCP/Precedence フィールドでのマーキング アクションの種類を各エントリが指定する、128 エントリのマーキング アクション テーブルを提供します。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。128 の一意のマーキング アクションまたは 32 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、Supervisor Engine 6-E 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

次の手順を実行します。

- クラス マップ（*ipp5*）とポリシー マップを作成します。（「QoS ポリシーの設定」（P.32-34）を参照）。
- マーキング アクションを設定します （「ポリシー マップ クラス アクションの設定」（P.32-37）を参照）。

（注）　Supervisor Engine 6-E では、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 32-8（P.32-76）および表 32-9（P.32-77）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。
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.32-74）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 キューイング、および DBL

Supervisor Engine 6-E は、送信キューの選択にあたり、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。

Supervisor Engine 6-E ハードウェアは、ポートごとに 4 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 Supervisor Engine 6-E には、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 4 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 4 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。

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、サポートされていません。シャーシとラインカードの種類に基づいて、ポート上の 4 つのキューすべてが同じキュー 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。

Supervisor Engine 6-E は、約 1.5 % 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 ポリシーにクラスレベルの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。 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 kbps* | **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。 帯域幅は、Kbps またはパーセンテージで指定できます。 • *cir-bps* の場合、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。 • *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 policy-map** 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 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。

Supervisor Engine 6-E は、約 1.5 % 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。 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輻輳が発生している場合に、ポリシー マップに属するクラスに設定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 policy-map** コンフィギュレーション コマンドを使用します。デフォルトの帯域幅に戻すには、**no bandwidth 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、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

Supervisor Engine 6-E では、ポート上の伝送キューを 1 つだけ、*完全優先*（低遅延キューまたは LLQ）として設定できます。

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。Supervisor Engine 6-E 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。

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。

	コマンド	目的
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。 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設定します。 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 policy-map** 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
```

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）　Supervisor Engine 6-E 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。 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 policy-map** 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 class** 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

伝送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。

階層ポリシー

論理 QoS セマンティックスをサポートするには、階層ポリシーのサポートが必要です。次に、さまざまな動作を実現するために階層ポリシーを設定する方法について説明します。

例 1

次の例では、特定のキューに送信されるトラフィックのサブセットをポリシングまたはマーキングし、デフォルト キューの残りのトラフィックをポリシングまたはマーキングしていることを前提とします。

```
Policy-map queue-policy
   class queue-class
     shape <...>
     bandwidth <...>
service-policy police-and-mark-traffic-class-1

   class queue2-class
     set <...>
     police <...>
service-policy police-and-mark-traffic-class-2

   class class-default
     set <...>
     police <...>
…

policy-map police-and-mark-traffic-class-1
   class traffic-class-1
     set <...>
     police <...>
```

例 2

次の例では、すべてのトラフィックが集約でポリシングまたはマーキングされ、同じキューイング分類ポリシーが使用されることを前提とします。MQC セマンティックスのように、クラスでキューイングアクションを使用しない場合、「class-default」はトラフィックのそのクラスのキューとして機能します。

```
Policy-map queue-policy
   class queue1-class
     shape <...>
     bandwidth <...>

   class queue8-class
     shape <...>
     bandwidth <...>

class queue8-class
     shape <...>
     bandwidth <...>
policy-map port-level-policy
class traffic-class-1
     set <...>
     police <...>
…
class traffic-class-n
     set <...>
     police <...>

class class-default
service-policy police-and-mark-traffic-class-2
```

例 1 と異なり、例 2 は、キューイングを設定する一般的な方法です。

例 3

次に、特定のポートをサブレートにシェーピングし、キューイングまたはポリシングのポリシーを適用する例を示します。

（注） Supervisor Engine 6-E では、ポート シェーピングはサポート*されません*。

この設定モデルでは、次の手順を実行します。

ステップ 1　ポリシングまたはマーキングのポリシー アクション（最下位子ポリシー）の設定。

ステップ 2　ステップ 1（中間の子ポリシー）の設定として各キューのキューイング アクションおよびパケットのポリシングまたはマーキングの設定。

ステップ 3　ポート レベルのシェーピング（親ポリシー）の設定。

ポリシーの設定は次のようになります。

```
Policy-map port-level-policy
   class class-default
     shape percent 100
service-policy queuing-policy
```

```
Policy-map queuing-policy
   class queue1-class
     shape <...>
     bandwidth <...>
service-policy police-and-mark-traffic-class-1

...
class class-default
     shape <...>
     bandwidth <...>
service-policy police-and-mark-traffic-class-default

Policy-map police-and-mark-traffic-class-1
   class traffic-class-1
     shape <...>
     police <...>
...
```

ポリシーの関連付け

Supervisor Engine 6-E 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。

詳細については、次のリンクを参照してください。

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a0080435d50.html

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。

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、ユーザが出力 VLAN ベース ポリシングおよびマーキングを設定すると、ポートの選択的キューイングを入力した場合、このパケットの両方のポリシーからのアクションが適用されます。

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。

Supervisor Engine 6-E 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.32-91）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。