CHAPTER 30

# Quality of Service の設定

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 QoS を設定する方法について説明します。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）を設定する方法についても説明します。

この章の内容は、次のとおりです。



（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、『*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/univercd/cc/td/doc/product/software/ios124/124cr/index.htm

## 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るため、正しい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。輻輳が発生した場合にドロップされる可能性についても、すべてのトラフィックで同等です。

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

ここでは、次の内容について説明します。

# プライオリティ

QoS の実装は、DiffServ アーキテクチャに基づきます。これは、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）による規格です。このアーキテクチャでは、ネットワークの入口で各パケットを分類すると規定されています。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 Type of Service（ToS; タイプ オブ サービス）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。分類は、レイヤ 2 フレームで伝送される場合もあります。レイヤ 2 フレームまたはレイヤ 3 パケットのこのような特殊ビットについては、図 30-1 を参照してください。

- レイヤ 2 フレーム内のプライオリティ値：

  レイヤ 2 の Inter-Switch Link（ISL; スイッチ間リンク）フレーム ヘッダーには、1 バイトのユーザ フィールドがあり、最下位ビット 3 ビットで IEEE 802.1p Class of Service（CoS; サービス クラス）値が伝送されます。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、最上位ビット 3 ビット（ユーザ プライオリティ ビットと呼ばれる）で CoS 値が伝送されます。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。

  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。

  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。

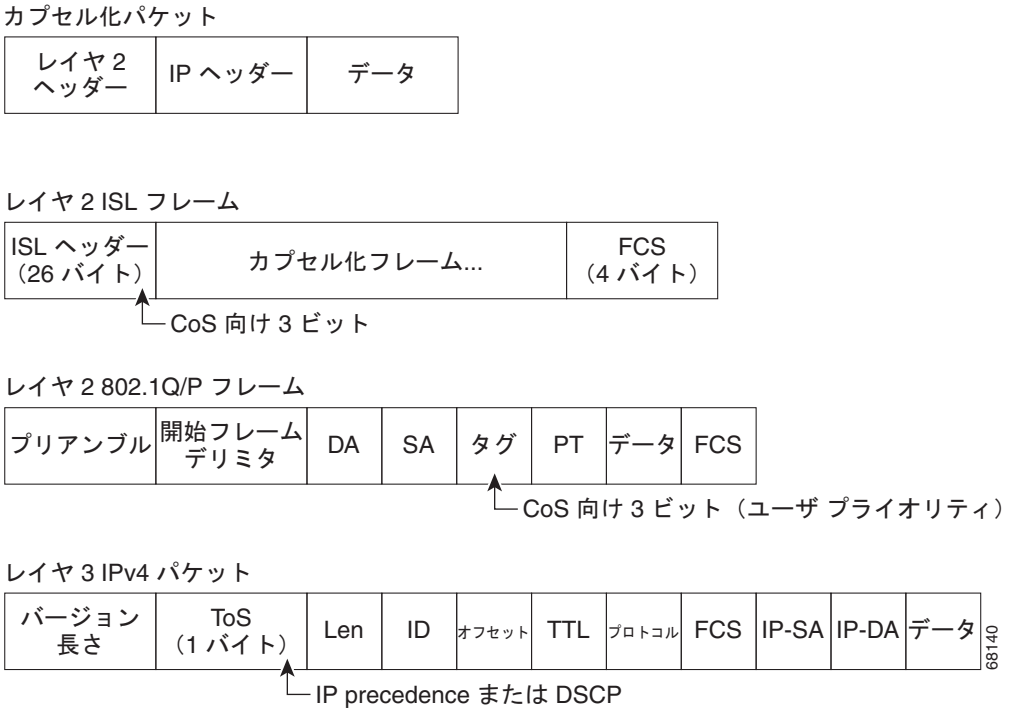
- レイヤ 3 パケット内の優先順位ビット：

  レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point（DSCP; DiffServ コード ポイント）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。

  IP precedence 値の範囲は、0 ～ 7 です。

  DSCP 値の範囲は 0 ～ 63 です。

**図 30-1　　フレームおよびパケット内の 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。設定されたポリシー、パケットの詳しい検証、またはその両方に基づき、エンド ホストあるいは途中にあるスイッチまたはルータによって、パケット内のクラス情報が割り当てられる場合があります。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。

パス上にあるスイッチおよびルータは、クラス情報を使用して、トラフィック クラスごとに割り当てられるリソースの量を制限できます。DiffServ アーキテクチャで個々の装置がトラフィックを処理するときの動作を、Per-Hop Behavior といいます。パス上のすべての装置が一貫性のある Per-Hop Behavior を提供する場合、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なります。

# QoS の用語

QoS 機能についての説明では、次の用語が使用されます。

- *パケット*：レイヤ 3 でトラフィックを伝送します。
- *フレーム*：レイヤ 2 でトラフィックを伝送します。レイヤ 2 フレームはレイヤ 3 パケットを伝送します。
- *ラベル*：レイヤ 3 パケットおよびレイヤ 2 フレームで伝送されるプライオリティ値です。
  - レイヤ 2 Class of Service（CoS; サービス クラス）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 Inter-Switch Link（ISL; スイッチ間リンク）フレーム ヘッダーには、1 バイトのユーザ フィールド（最下位ビット 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、最上位ビット 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 フィールドの最上位ビット 3 ビットを IP precedence と定義しています。IP precedence 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 Differentiated Services Code Point（DSCP; DiffServ コード ポイント）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 フィールドのうち最上位ビット 6 ビットを DSCP と定義しています。個々の DSCP 値が表す Per-Hop Behavior は、設定変更可能です。DSCP 値の範囲は 0 ～ 63 です。「DSCP マップの設定」（P.30-59）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 30-1 を参照してください。

**表 30-1　IP precedence 値および DSCP 値**

| 3 ビットの IP precedence | ToS の 6 MSB[1] | | | | | | 6 ビットの DSCP | | 3 ビットの IP precedence | ToS の 6 MSB[1] | | | | | | 6 ビットの 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 30-1　IP precedence 値および DSCP 値 （続き）

| 3 ビットの IP precedence | ToS の 6 MSB[1] | | | | | | 6 ビットの DSCP | | 3 ビットの IP precedence | ToS の 6 MSB[1] | | | | | | 6 ビットの 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.30-14）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ドロップが可能になります。

# QoS の基本モデル

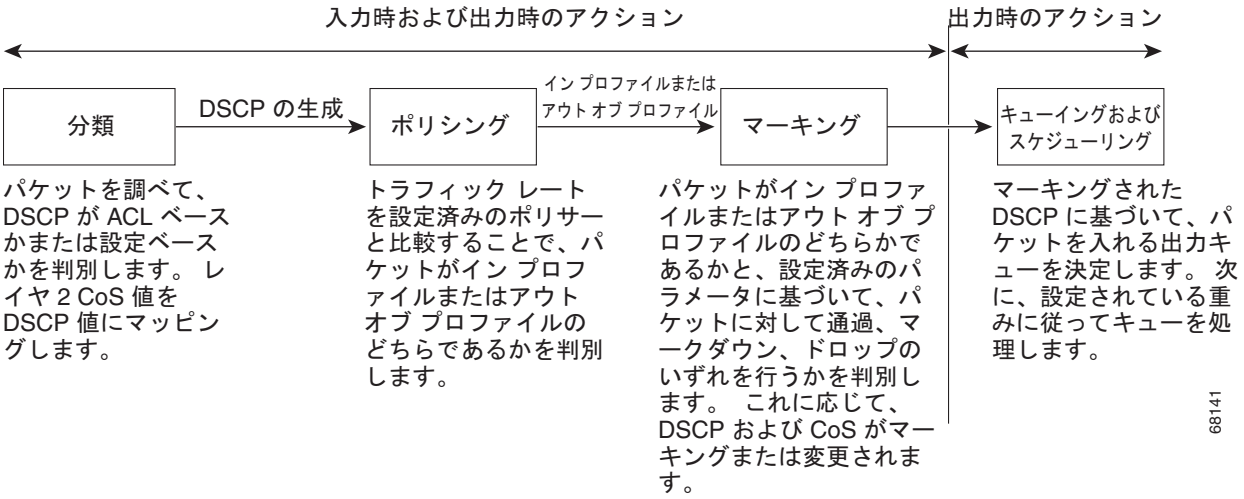
図 30-2 に QoS の基本モデルを示します。入力インターフェイスおよび出力インターフェイスで行われるアクションには、トラフィックの分類、ポリシング、およびマーキングがあります。

- 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.30-6）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.30-10）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.30-10）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.30-15）を参照してください。

**図 30-2　QoS の基本モデル**




# 分類

分類は、パケットの各フィールドを検証することで、トラフィックの種類を区別するプロセスです。スイッチ上で QoS がグローバルにイネーブルに設定されている場合にかぎり、分類がイネーブルになります。デフォルトでは、QoS はグローバルでディセーブルに設定されているため、分類は行われません。

フレームまたはパケットの、どのフィールドを使用して着信トラフィックを分類するかを、ユーザが指定します。

図 30-3 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（ポートを Trust CoS に設定する）。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 ISL フレーム ヘッダーでは、1 バイトのユーザ フィールドの LSB 3 ビットを使用して CoS 値を伝送します。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。

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。

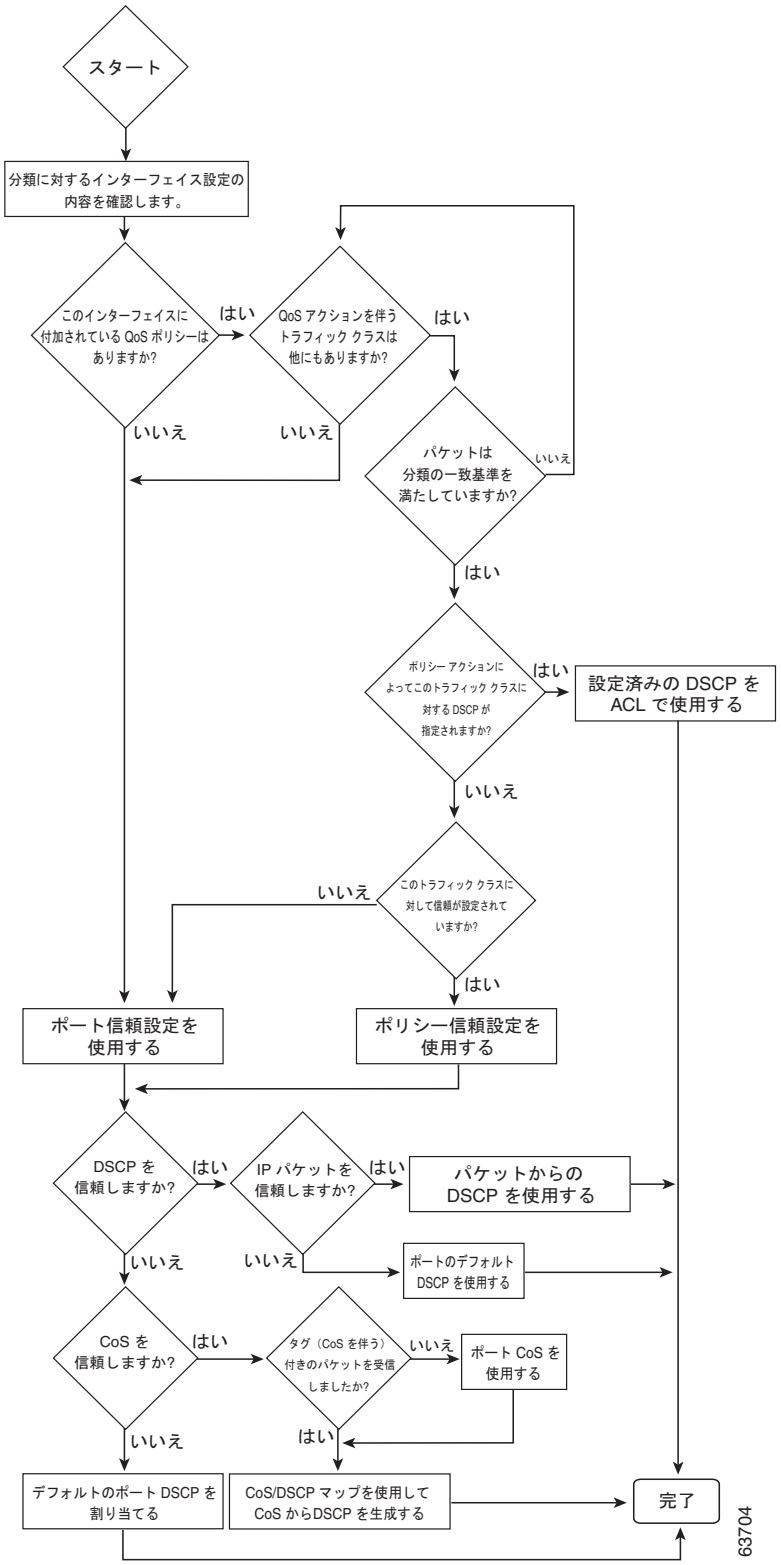
- 着信パケットの IP DSCP を信頼し（ポートを Trust DSCP に設定し）、パケットに同じ DSCP を割り当てて内部的に使用します。IETF は、1 バイトの Type of Service（ToS; タイプ オブ サービス）フィールドの最上位ビット 6 ビットを DSCP として定義しています。個々の DSCP 値が表すプライオリティは、設定変更可能です。DSCP 値の範囲は 0 ～ 63 です。
- 着信パケットの CoS 値（存在する場合）を信頼し、CoS/DSCP マップを使用して DSCP を生成します。
- 設定された IP 標準 ACL または拡張 ACL（IP 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。

ここで説明するマップについての詳細は、「マッピング テーブル」（P.30-15）を参照してください。ポートの信頼状態の設定手順については、「インターフェイスの信頼状態の設定」（P.30-54）を参照してください。

図 30-3　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.30-9）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、なおかつパケットがそれを満たしている場合、そのパケットは QoS 分類の一致基準に「一致した」ことになります。
- 「deny」を指定している ACE を検出し、なおかつパケットがそれを満たしている場合、そのパケットは QoS 分類の一致基準に「一致しない」ことになります。
- 一致する許可（permit）アクションが検出されないまま、すべての ACE の検証が終わった場合、そのパケットは QoS 分類の基準に「一致しない」ことになります。

（注）　アクセス リストを作成するとき、アクセス リストの末尾にはデフォルトで、リストの末尾に達しても一致が見つからなかった場合に使用される、暗黙の拒否（deny）文がある点に留意してください。

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。ポリシーでは、複数のクラスのそれぞれについて、アクションを指定できます。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付加して、そのポート上でポリシーを有効にします。

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。詳しい設定手順については、「QoS ポリシーの設定」（P.30-33）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（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。複数のタイプのトラフィックを分類する必要がある場合は、別のクラス マップを別の名前で作成します。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、スイッチはクラス マップ コンフィギュレーション モードになります。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 マップを作成して名前を付けるには、**policy-map** グローバル コンフィギュレーション コマンドを使用します。このコマンドを入力すると、スイッチはポリシー マップ コンフィギュレーション モードになります。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対応付けます。

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.30-10）を参照してください。

ポリシー マップには、次のような特性もあります。

- 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。

詳しい設定手順については、「QoS ポリシーの設定」（P.30-33）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 30-4 を参照）。

ポリシングを行うには、トラフィックの帯域幅制限を指定するポリサーを作成します。この制限を超過するパケットは、*アウト オブ プロファイル*つまり*不適合*パケットです。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べき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.30-15）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を QoS が累積的に適用します。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。集約ポリサーは、1 つのポリシー マップ内で複数のトラフィック クラスによって共有されます。

- 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.30-43）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。

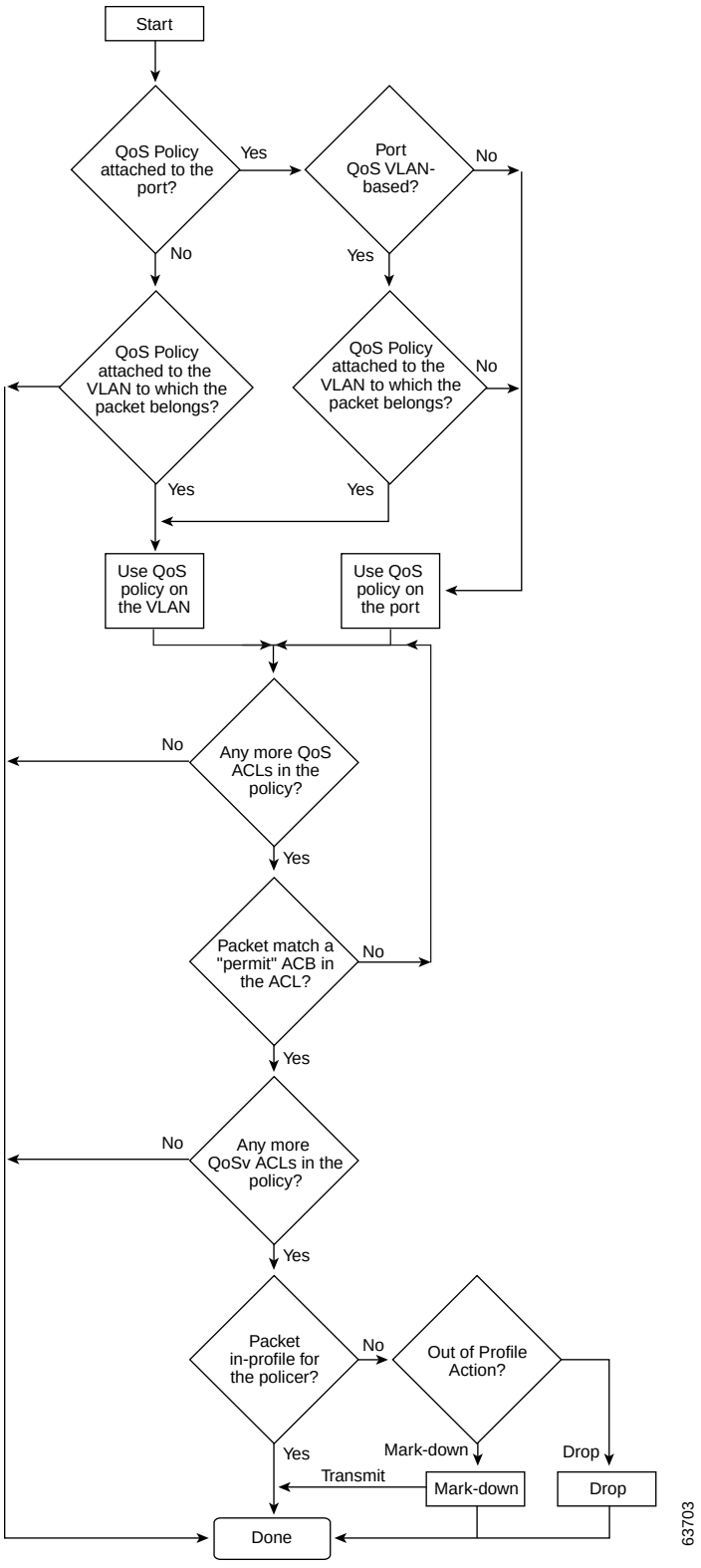
  - 100,000 より多いフローをマイクロフロー ポリシングできます。

**（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.44-7）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。詳しい設定手順については、「QoS ポリシーの設定」（P.30-33）および「名前付き集約ポリサーの作成」（P.30-31）を参照してください。

図 30-4　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」（P.30-14）
- 「出力 ToS および CoS の作成元」（P.30-14）

## 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、次の項目に基づいて内部 DSCP 値を導き出します。

- 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.30-59）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ビット 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 30-1」（P.30-4）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.30-61）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）。この設定変更可能なマップを、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。

詳しい設定手順については、「DSCP マップの設定」（P.30-59）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。

詳しい設定手順については、「送信キューの設定」（P.30-56）を参照してください。

## アクティブ キュー管理

Active Queue Management（AQM; アクティブ キュー管理）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 Explicit Congestion Notification（ECN; 明示的輻輳通知）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

パケットの分類、ポリシング、およびキューイングによって、QoS が提供されます。次のプロセスで、パケットの変更が行わ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。
- ポリシングでは、IP パケットおよび IP 以外のパケットに別の DSCP が割り当てられます（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 DSCP が指定されている場合）。この場合にも、パケットの DSCP は変更されませんが、マークダウン後の値が伝えられます。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。

## per-Port per-VLAN QoS

per-Port per-VLAN QoS（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 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.30-56）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.30-61）を参照してください。

# Auto-QoS の設定

Auto-QoS 機能を使用すると、既存の QoS 機能の使用を簡略化できます。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 （デフォルトでは、QoS はディセーブルです。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。スイッチはこの分類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。そのあと、Auto-QoS は次の機能を実行します。

- IP Phone の有無を検出します。
- QoS 分類を設定します。
- 出力キューを設定します。

ここでは、スイッチ上で Auto-QoS を設定する手順について説明します。

- 「生成される Auto-QoS 設定」（P.30-19）
- 「Auto-QoS の設定上の影響」（P.30-20）
- 「設定時の注意事項」（P.30-20）

- 「VoIP 用の Auto-QoS のイネーブル化」（P.30-20）

# 生成される Auto-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 Auto-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 30-2 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; シスコ検出プロトコル）を使用して Cisco IP Phone の有無を検出します。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、「信頼境界の設定によるポート セキュリティの確保」（P.30-27）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 30-2 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 30-2　生成される Auto-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`<br>`Switch(config)# qos map cos 3 to 26`<br>`Switch(config)# qos dbl`<br>`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`<br>`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`<br>または<br>`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`<br>`Switch(config-pmap)# class class-default`<br>`Switch(config-pmap-c)# dbl` |

表 30-2　生成される Auto-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。<br>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`<br>`Switch(config-if-tx-queue)# priority high`<br>`Switch(config-if-tx-queue)# shape percent 33`<br>`Switch(config-if-tx-queue)# bandwidth percent 33` |

# Auto-QoS の設定上の影響

Auto-QoS がイネーブルの場合、**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

Auto-QoS を設定する前に、次の点を理解する必要があります。

- 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。必要であれば、QoS 設定をきめ細かく調整できますが、Auto-QoS 設定が完了したあとに行うことを推奨します。
- 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 ポート上で Auto-QoS を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。Auto-QoS を適切に機能させるには、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 用の Auto-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。<br>キーワードの意味は次のとおりです。<br>• **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にだけ信頼されます。<br>• **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。<br>このコマンドは、最初に適用された Auto-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、インターフェイス GigabitEthernet 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、Auto-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
```

# Auto-QoS 情報の表示

初期 Auto-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。ユーザが変更した設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。**show auto qos** コマンドと **show running-config** コマンド出力を比較することで、ユーザが定義した QoS 設定を識別できます。

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。

# Auto-QoS 設定例

ここでは、ネットワーク内で Auto-QoS を実装する方法について説明します（図 30-5 を参照）。

**図 30-5　Auto-QoS を設定したネットワークの例**

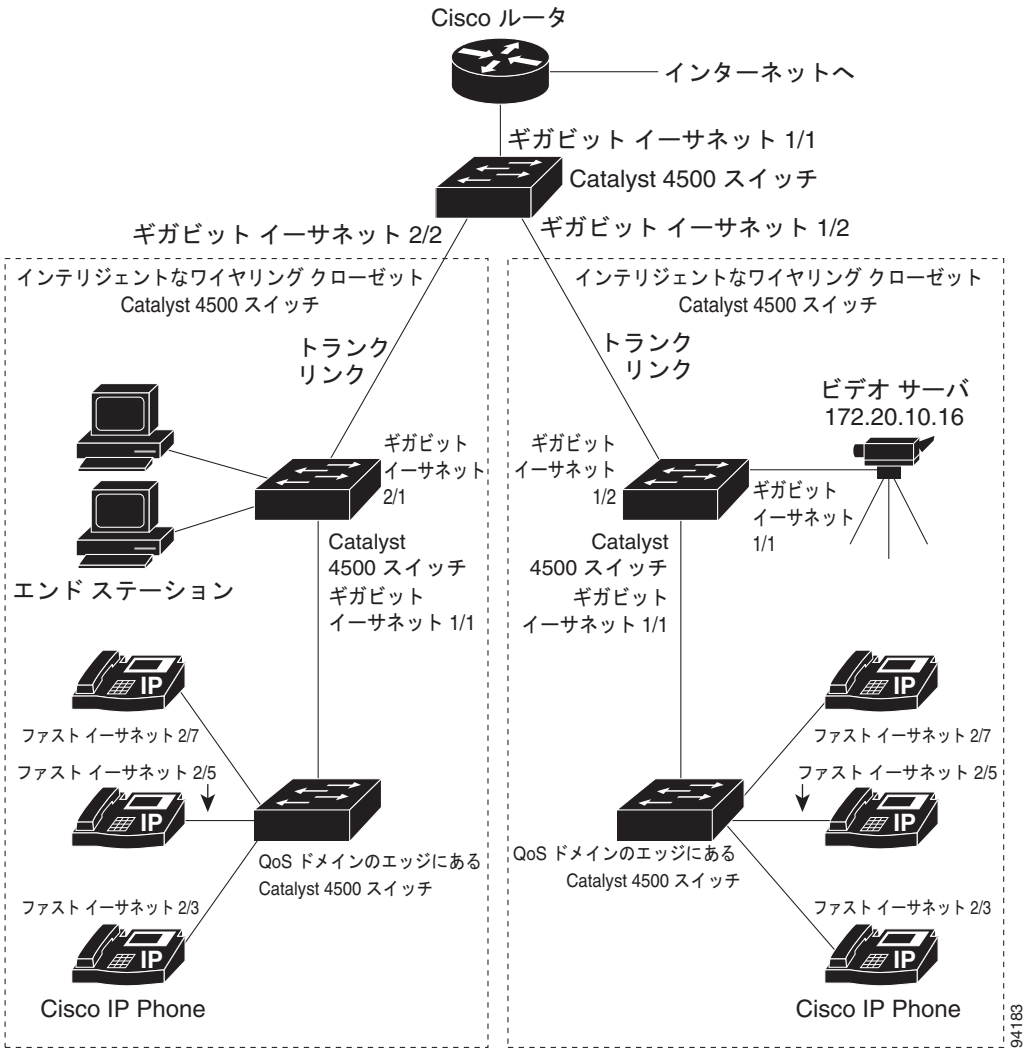


図 30-5 のインテリジェントなワイヤリング クローゼットは、Catalyst 4500 スイッチで構成されています。この例では、VoIP トラフィックを他のすべてのトラフィックよりも優先させることを目的としています。これを実行するには、ワイヤリング クローゼット内の QoS ドメインのエッジにあるスイッチ上で Auto-QoS をイネーブルにします。

（注）　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。QoS 設定をきめ細かく調整できますが、Auto-QoS 設定が完了したあとに行うことを推奨します。

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。デバッグがイネーブルに設定されると、スイッチは Auto-QoS がイネーブルにな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 はイネーブルです。 |
| 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。<br>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。<br>このコマンドは、最初に適用された Auto-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。<br>Auto-QoS の影響を受ける QoS 設定に関する情報については、「Auto-QoS 情報の表示」（P.30-21）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。<br>このコマンドは、最初に適用された Auto-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。 |

# 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上のトラフィック パターン
- トラフィックの特性およびネットワークの要件。バースト性のトラフィックかどうか。音声およびビデオ ストリーム用に帯域幅を予約する必要があるかどうか
- 帯域幅の要件およびネットワークの速度
- ネットワーク上の輻輳発生箇所

ここでは、Catalyst 4000 ファミリー 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 30-3 に、QoS のデフォルト設定を示します。

表 30-3　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<br>（CoS 値から設定された DSCP） | CoS 0 = DSCP　0<br>CoS 1 = DSCP　8<br>CoS 2 = DSCP 16<br>CoS 3 = DSCP 24<br>CoS 4 = DSCP 32<br>CoS 5 = DSCP 40<br>CoS 6 = DSCP 48<br>CoS 7 = DSCP 56 |
| DSCP/CoS マップ<br>（DSCP 値から設定された CoS） | DSCP　0 ～ 7　= CoS 0<br>DSCP　8 ～ 15 = CoS 1<br>DSCP 16 ～ 23 = CoS 2<br>DSCP 24 ～ 31 = CoS 3<br>DSCP 32 ～ 39 = CoS 4<br>DSCP 40 ～ 47 = CoS 5<br>DSCP 48 ～ 55 = CoS 6<br>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） | マークダウンされた DSCP 値は元の DSCP 値（マークダウンなし）と等しい |
| 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<br>DSCP 16 ～ 31 キュー 2<br>DSCP 32 ～ 47 キュー 3<br>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 | untrusted（信頼性がない） |

# 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 が、トラフィックの分類に使用される ACL に追加される必要があります。

```
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。<br>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#
```

# 信頼境界の設定によるポート セキュリティの確保

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 31 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 Class of Service（CoS; サービス クラス）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 リリース 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。これ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.30-56）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 が稼動していない場合、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。<br>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。 |

| | コマンド | 目的 |
|---|---|---|
| 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、ポートは trusted になっていません。 |
| 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。<br>信頼境界と Auto-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）は相互に排他的なので、同時にイネーブルにできません。 |
| 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

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、「アクティブ キュー管理」（P.30-15）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.30-28）
- 「DBL の選択的イネーブル化」（P.30-29）

## 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。<br>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。 |
| 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.30-29）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.30-30）を参照）。

次の事項が可能です。

- 「特定 IP DSCP 値での DBL のイネーブル化」（P.30-29）
- 「特定 CoS 値での DBL のイネーブル化」（P.30-30）

### 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.30-56）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 アトリビュートに基づいて 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.30-37））。

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 フローの出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.30-29）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` | ユーザが指定する名前でポリシー 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。 |

| | コマンド | 目的 |
|---|---|---|
| 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.30-42）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 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、もう 1 つのポリサー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を行います。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。

名前付き集約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.30-26）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。

（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。
  - 一致するすべてのアウト 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。

- 「QoS ポリシー設定の概要」（P.30-34）
- 「クラス マップの設定（任意）」（P.30-34）
- 「ポリシー マップの設定」（P.30-37）
- 「インターフェイスへのポリシー マップの付加」（P.30-41）

（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 リストのサポート | 拡張アクセス リストのサポート | 名前付きアクセス リストのサポート |
|---|---|---|---|
| IP | あり：<br>1 ～ 99<br>1300 ～ 1999 | あり：<br>100 ～ 199<br>2000 ～ 2699 | あり |

  - Catalyst4500 シリーズ スイッチ上の ACL については、第 37 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.30-34）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。


- 「クラス マップの作成」（P.30-35）
- 「クラス マップでのフィルタリングの設定」（P.30-35）
- 「クラス マップの設定の確認」（P.30-36）


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。<br>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。<br>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。<br>**（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.30-33）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。<br>非 IPv4 トラフィックについては、「設定時の注意事項」（P.30-20）を参照してください。 |
| `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 リリース 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 リリース 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 ファミリー 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 マップの設定

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 つにかぎられます。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.30-37）
- 「ポリシー マップ クラス アクションの設定」（P.30-37）


## 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` | ユーザが指定する名前でポリシー マップを作成します。<br>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.30-37）
- 「ポリシー マップ クラスの信頼状態の設定」（P.30-38）
- 「ポリシー マップ クラスの DBL 状態の設定」（P.30-38）
- 「ポリシー マップ クラスのポリシングの設定」（P.30-38）
- 「名前付き集約ポリサーの使用」（P.30-38）
- 「インターフェイス別ポリサーの設定」（P.30-39）


### 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。<br>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.30-14）を参照）。<br>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（「アクティブ キュー管理」（P.30-15）を参照）。<br>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.30-38）
- 「インターフェイス別ポリサーの設定」（P.30-39）

### 名前付き集約ポリサーの使用

名前付き集約ポリサーを使用するには（「名前付き集約ポリサーの作成」（P.30-31）を参照）、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。<br>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のポリサーを設定するには（「ポリシングおよびマーキング」（P.30-10）を参照）、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。<br>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際、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（32000 と入力）
  - 最大：32 Gbps（32000000000 と入力）

**（注）** 「設定時の注意事項」（P.30-26）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.30-60）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。<br>（注）　ポリシー マップに別のクラスを作成するには、**class** コマンドを追加入力します。 |
| 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 マップの付加

ポリシー マップをインターフェイスに付加するには、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] 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付加します。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。「`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

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 ネットワーク内にディファレンシエーテッド サービスを提供できます。

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.44-8）を参照）。**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。
**ip destination-address ip protocol L4 source-address L4 destination-address** キーワードを使用して **match flow** コマンドを指定すると、一意の IP 送信元、IP 宛先、IP プロトコル、およびレイヤ 4 送信元、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 protocl 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

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、送信元アドレスが 192.168.10.20 と 192.168.10.21 であるとします。次の例は、許可されるバースト値を 9000 バイトにして 1 Mbps でそれぞれのフローを維持する方法を示しています。

```
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。次の例は、許可されるバースト値を 9000 バイトにして 1 Mbps でそれぞれのフローを維持する方法を示しています。

```
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**

インターフェイス FastEthernet 6/1 上に 2 つのアクティブ フローが存在すると想定します。

```
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
```

次の設定の場合、各フローは許可されるバースト値を 9,000 にして 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

**（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
```

# per-Port per-VLAN QoS のイネーブル化

per-Port per-VLAN QoS 機能により、所定のインターフェイスの異なる VLAN 上で異なる QoS 設定を指定できます。通常、この機能はトランク ポートまたは音声 VLAN（Cisco IP Phone）ポートなど、複数の VLAN に所属するポート上で使用します。

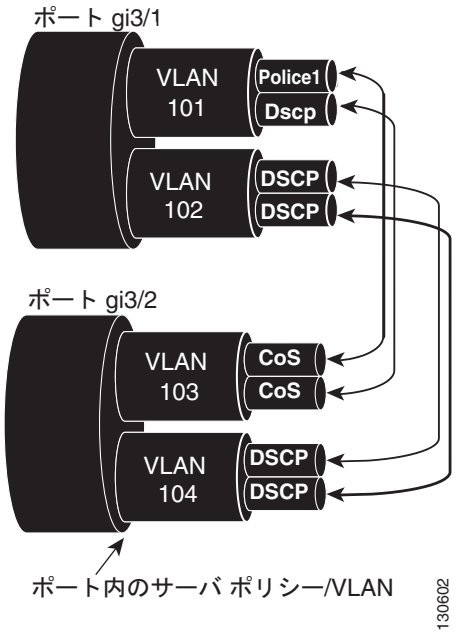
per-Port per-VLAN QoS を設定するには、次の作業を行います。

| | 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 30-6 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 30-6　per-Port per-VLAN のトポロジ




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、インターフェイス GigabitEthernet 6/1 はトランク ポートで、VLAN 20、300 ～ 301、および 400 に属していると仮定します。次に、VLAN 20 と VLAN 400 のトラフィックにポリシーマップ p1、VLAN 300 ～ 301 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、インターフェイス GigabitEthernet 6/1 上で設定された VLAN 20 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 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。<br>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 マップの付加」（P.30-41）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。<br>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 ポリシーを付加します。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が untrusted です。

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。<br>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 リリース 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影響を受けません。送信キューについては、「送信キューの設定」（P.30-56）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。<br>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。<br>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.30-57）
- 「送信キュー間での帯域幅の割り当て」（P.30-57）
- 「送信キューのトラフィック シェーピングの設定」（P.30-58）
- 「ハイ プライオリティ送信キューの設定」（P.30-58）

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。<br>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。<br>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。<br>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。 |

| | コマンド | 目的 |
|---|---|---|
| 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。<br>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。 |
| 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。ここで説明する設定情報は次のとおりです。

- 「CoS/DSCP マップの設定」（P.30-59）
- 「ポリシング済み DSCP マップの設定」（P.30-60）
- 「DSCP/CoS マップの設定」（P.30-61）

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 マップは、着信パケットの CoS 値を、DSCP 値（トラフィックのプライオリティを表すために QoS が内部的に使用する）にマッピングする目的で使用します。

表 30-4 に、デフォルトの CoS/DSCP マップを示します。

**表 30-4　デフォルトの CoS/DSCP マップ**

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

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。

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。<br>*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。<br>*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。 |
| 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。 |

次に、入力 CoS/DSCP マッピングで CoS を 0 に設定する例を示します。

```
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。

次に、CoS/DSCP マッピング テーブル全体をクリアする例を示します。

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

## ポリシング済み DSCP マップの設定

ポリシング済み DSCP マップは、ポリシングおよびマーキング アクションの結果、DSCP 値を新しい値にマークダウンする目的で使用します。

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。<br>• *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。<br>• *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。 |

| | コマンド | 目的 |
|---|---|---|
| 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、マークダウンされた 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）** 上記のポリシング済み 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。カラム d1 は、元の DSCP の上位桁を表し、行 d2 は、元の DSCP の下位桁を表します。d1 と d2 が交わった部分にある値が、マークダウン後の値です。たとえば、元の DSCP 値が 53 である場合、対応するマークダウン後の 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 30-5 に、デフォルトの DSCP/CoS マップを示します。

**表 30-5　デフォルトの DSCP/CoS マップ**

| DSCP 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。<br>• *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。<br>• *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。<br>DSCP の範囲は 0 ～ 63、CoS の範囲は 0 ～ 7 です。<br>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、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）　上記の 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。カラム d1 は、DSCP の上位桁を表し、行 d2 は、DSCP の下位桁を表します。d1 と d2 が交わった部分にある値が、CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値 08 は CoS 値 0 に対応しています。