QoS の設定

この章では、自動 Quality of Service（QoS）コマンドを使用して、またはスイッチで標準の QoS コマンドを使用して QoS を設定する方法について説明します。

- 機能情報の確認，1 ページ
- QoS の前提条件，2 ページ
- QoS の制約事項，4 ページ
- QoS の概要，4 ページ
- QoS の設定方法，28 ページ
- 標準 QoS のモニタリング，84 ページ
- QoS の設定例，85 ページ
- 次の作業，93 ページ
- その他の関連資料，94 ページ
- QoS の機能履歴と情報，95 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

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

QoS の前提条件

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 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。 たとえば、ネットワークのトラフィックがバーストであるかどうか 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

QoS ACL の注意事項

アクセス コントロール リスト（ACL）を使用してQoS設定する場合は、次のガイドラインに従ってください。

- IP フラグメントと設定されている IP 拡張 ACL を照合することによって、QoS を実施することはできません。 IP フラグメントはベストエフォート型として送信されます。 IP フラグメントは IP ヘッダーのフィールドで示されます。
- 1 つのクラス マップごとに使用できる ACL は 1 つだけ、使用できる **match** クラスマップ コンフィギュレーション コマンドは 1 つだけです。 ACL には、フィールドとパケットの内容を照合する ACE を複数指定できます。
- ポリシー マップの信頼ステートメントには、1 つの ACL 行につき複数のハードウェア エントリが必要になります。 入力サービス ポリシー マップの ACL に信頼ステートメントが含まれている場合、アクセス リストが大きくなりすぎて使用可能な QoS ハードウェア メモリに収容できない可能性があり、ポリシー マップをポートに適用したときにエラーになることがあります。 QoS ACL の行数はできる限り少なくする必要があります。

関連トピック

IPv4 トラフィック用の IP 標準 ACL の作成, （41 ページ）
IPv4 トラフィック用の IP 拡張 ACL の作成, （43 ページ）
IPv6 トラフィック用の IPv6 ACL の作成, （45 ページ）
非 IP トラフィック用のレイヤ 2 MAC ACL の作成, （47 ページ）
例：ACL によるトラフィックの分類, （85 ページ）

ポリシングの注意事項

（注） ポリシングを使用するには、スイッチが LAN Base イメージを実行している必要があります。

- 複数の物理ポートを制御するポート ASIC デバイスは、256 個のポリサー（255 個のユーザ設定可能なポリサーと 1 個のシステムの内部使用向けに予約されたポリサー）をサポートします。 ポートごとにサポートされるユーザ設定可能なポリサーの最大数は 63 です。 ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよびASICの限界によって制約されます。

  ポートごとにポリサーを確保することはできません。ポートがいずれかのポリサーに割り当てられる保証はありません。

- 入力ポートでは 1 つのパケットに適用できるポリサーは 1 つだけです。 設定できるのは、平均レート パラメータおよび認定バースト パラメータだけです。

- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに結合されたポリシーマップに基づいて分類、ポリシング、およびマーキングが行われます。 QoS 対応として設定されているトランク ポートの場合、ポートを介して受信したすべての VLAN のトラフィックは、そのポートに結合されたポリシー マップに基づいて分類、ポリシング、およびマーキングが行われます。

- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理ポートにQoSの分類、ポリシング、マッピング、およびキューイングを設定する必要があります。 また、QoS の設定を EtherChannel のすべてのポートで照合するかどうかを決定する必要があります。

- 既存の QoS ポリシーのポリシー マップを変更する必要がある場合は、最初にすべてのインターフェイスからポリシー マップを削除し、その後ポリシー マップを変更またはコピーします。 変更が終了したら、変更したポリシー マップをインターフェイスに適用します。 最初にすべてのインターフェイスからポリシーマップを削除しなかった場合、CPU使用率が高くなり、コンソールが長期間停止する可能性があります。

一般的な QoS の注意事項

一般的な QoS の注意事項を次に示します。

- QoS を設定できるのは物理ポートだけです。VLAN のレベルでは QoS はサポートされていません。

- スイッチで受信された制御トラフィック（スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）やルーティング アップデート パケットなど）には、入力 QoS 処理がすべて行われます。

- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。
- スイッチは同種スタックおよび混合スタック構成をサポートします。混合スタック構成は、Catalyst 2960-S スイッチだけでサポートされます。 同種スタックは 8 つまで、混合スタックは 4 つまでのスタック メンバーを含めることができます。 スイッチ スタック内のすべてのスイッチが LAN Base イメージを実行している必要があります。

QoS の制約事項

以下は、QoS の制約事項を示しています。

- 次の機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。スタック構成、DSCP、自動 QoS、信頼境界、ポリシング、マーキング、マッピング テーブル、および重み付けテール ドロップ。
- 入力キューイングはサポートされません。
- QoS を設定できるのは物理ポートのみです。 VLAN-based QoS はサポートされません。 分類、キューイングおよびスケジューリングのようなQoSが設定できます。また、ポートにポリシー マップも適用できます。 物理ポートに QoS を設定した場合は、非階層型のポリシー マップをポートに適用します。
- スイッチが LAN Lite イメージを実行中の場合、ACL を設定できますが、その ACL を物理インターフェイスに接続できません。 ACL を VLAN インターフェイスに接続して CPU へのトラフィックをフィルタリングします。
- 次の QoS 機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。
  - ポリシー マップ
  - ポリシングおよびマーキング
  - マッピング テーブル
  - WTD

QoS の概要

QoS の実装

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。

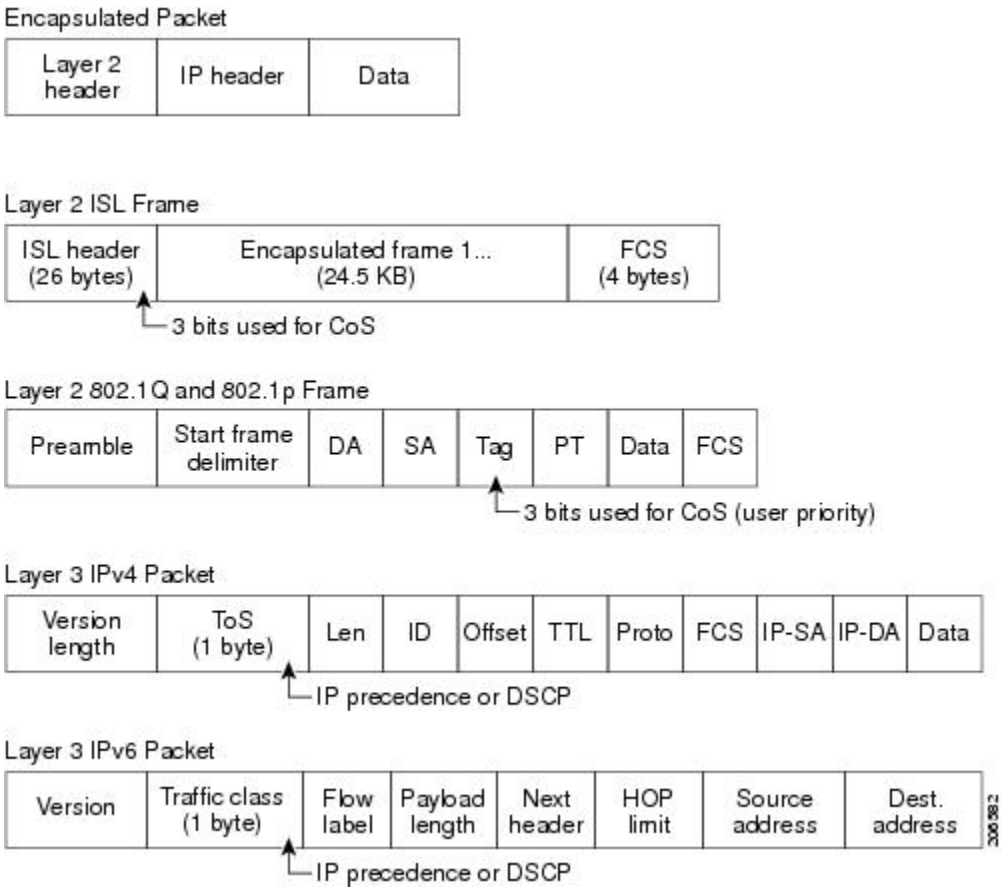
QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、相対的な重要性に応じてそのトラフィックに優先度を指定し、輻輳管理および輻輳回避技術を使用して、優先処理を実行できます。 ネットワークに QoS を実装すると、ネットワーク パフォーマンスがさらに予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS は、インターネット技術特別調査委員会（IETF）の規格である Differentiated Services（Diff-Serv）アーキテクチャに基づいて実装されます。 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パケットヘッダーに格納され、推奨されない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）情報として伝達されます。 分類情報をレイヤ 2 フレームでも伝達できます。

次の図にレイヤ 2 フレームまたはレイヤ 3 パケットの特殊ビットを示します。

図 *1*：フレームおよびパケットにおける *QoS* 分類レイヤ



レイヤ 2 フレームのプライオリティ ビット

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ポートでは、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 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ポートでは、ネイティブ Virtual LAN（VLAN）のトラフィックを除く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。

分類を使用したエンドツーエンドの QoS ソリューション

インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。 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。 パケットの詳細な検証は、コア スイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

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。 Diff-Serv 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。

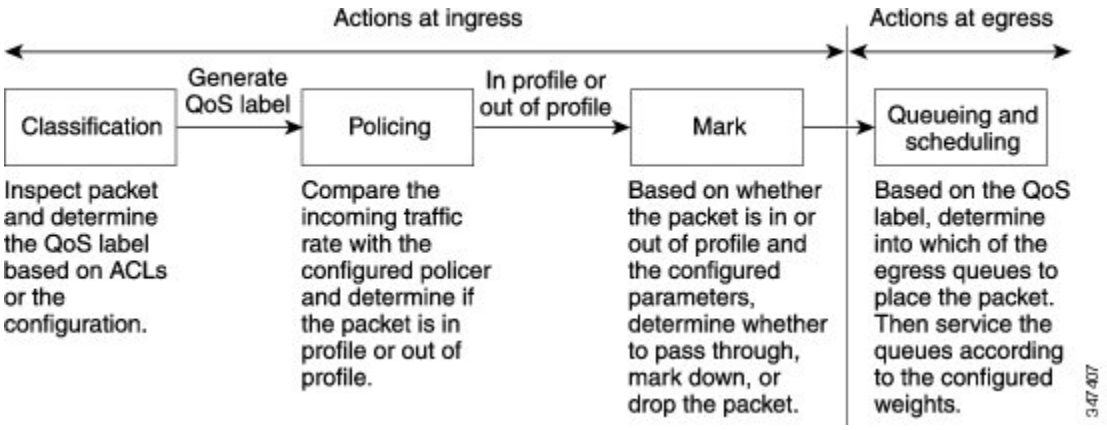
ネットワーク上で QoS を実装する作業は、インターネットワーキング デバイスが提供する QoS 機能、ネットワークのトラフィック タイプおよびパターン、さらには着信および発信トラフィックに求める制御のきめ細かさによって、簡単にも複雑にもなります。

QoS 基本モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別し（分類）、パケットがスイッチを通過するときに所定の QoS を表すラベルを割り当て、設定されたリソース使用率制限にパケットを適合させ（ポリシングおよびマーキング）、リソース競合が発生する状況に応じて異なる処理（キューイングおよびスケジューリング）を行う必要があります。 また、スイッチか

ら送信されたトラフィックが特定のトラフィック プロファイルを満たすようにする必要もあります（シェーピング）。

図 *2* : *QoS* 基本モデル



入力ポートでのアクション

入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、、およびスケジューリングがあります。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。 スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。 生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。
- ポリシングでは、着信トラフィックのレートを設定済みポリサーと比較して、パケットが適合か不適合かを判別します。 ポリサーは、トラフィック フローで消費される帯域幅を制限します。 その判別結果がマーカーに渡されます。
- マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。

（注） キューイングおよびスケジューリングは、スイッチの出力でのみサポートされ、入力ではサポートされません。

出力ポートでのアクション

出力ポートでのアクションには、キューイングおよびスケジューリングがあります。

- 4 つの出力キューのどれを使用するかを選択する前に、キューイングでは、QoS パケット ラベルおよび対応する DSCP または CoS 値を評価します。 複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。 しきい値を超過している場合、パケットはドロップされます。
- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。 キューの 1 つ（キュー 1）は、他のキューの処理前に空になるまで処理される緊急キューにできます。

分類の概要

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。

分類中に、スイッチは検索処理を実行し、パケットに QoS ラベルを割り当てます。 QoS ラベルは、パケットに対して実行するすべての QoS アクション、およびパケットの送信元キューを識別します。

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングおよびスケジューリング アクションを決定します。 QoS ラベルは信頼設定およびパケット タイプに従ってマッピングされます（分類フローチャート，（11 ページ）を参照）。

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。

Non-IP のトラフィック分類

次の表は、QoS 設定の非 IP トラフィックの分類オプションを示しています。

表 *1*：非 *IP* トラフィックの分類

Non-IP のトラフィック分類	説明
CoS 値の信頼	着信フレーム内の CoS 値を信頼し（CoS を信頼するようにポートを設定）、設定可能な CoS/DSCP マップを使用してパケットの DSCP 値を生成します。 レイヤ 2 の ISL フレーム ヘッダーは、1 バイトのユーザ フィールドの下位 3 ビットで CoS 値を伝達します。 レイヤ 2 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。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。

Non-IP のトラフィック分類	説明
DSCP を信頼するか、または IP precedence 値を信頼します。	着信フレームの DSCP または IP precedence 値を信頼します。 これらの設定は、非 IP トラフィックの場合は無意味です。 これらのいずれかの方法で設定されているポートに非IP トラフィックが着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。 スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成します。
設定されたレイヤ 2 の MAC ACL に基づいた分類	設定されたレイヤ 2 の MAC アクセス コントロール リスト（ACL）に基づいて分類を実行します。レイヤ 2 の MAC ACL は、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。 ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。 ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

分類されたパケットは、ポリシングおよびマーキングの各段階に送られます。

IP のトラフィック分類

次の表は、QoS 設定の IP トラフィック分類オプションを示します。

表 *2*：*IP* のトラフィック分類

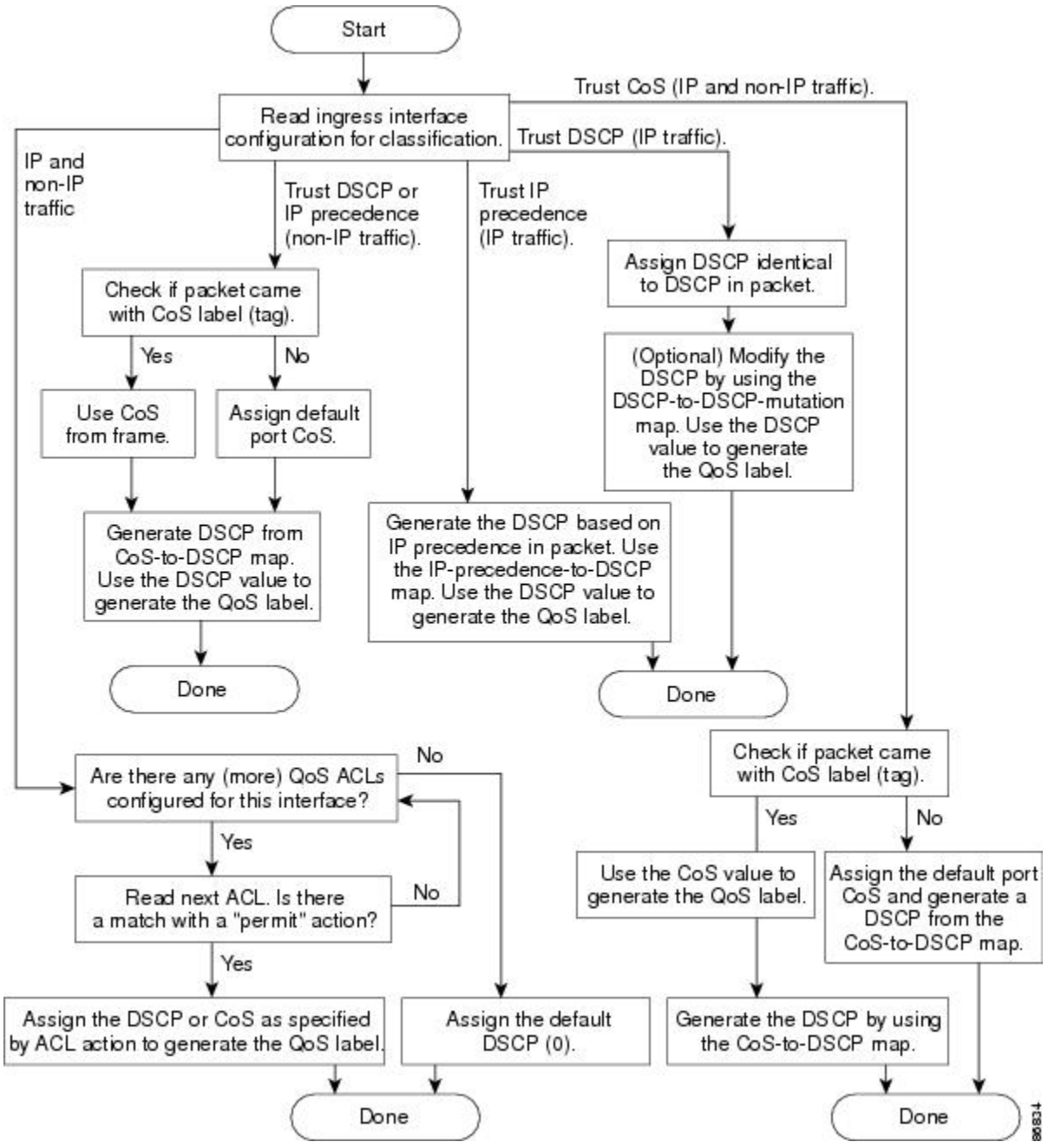
IP のトラフィック分類	説明
DSCP 値の信頼	着信パケットの DSCP 値を信頼し（DSCP を信頼するようにポートを設定し）、同じ DSCP 値をパケットに割り当てます。 IETF は、1 バイトの ToS フィールドの上位 6 ビットを DSCP として定義しています。 特定の DSCP 値が表すプライオリティは、設定可能です。 DSCP 値の範囲は 0 ～ 63 です。 また IPv6 DSCP に基づいて IP トラフィックを分類することもできます。 2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に変更できます。

IP のトラフィック分類	説明
IP precedence 値の信頼	着信パケットの IP precedence 値を信頼し（IP precedence を信頼するようにポートを設定し）、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。 IP バージョン 4 仕様では、1 バイトの ToS フィールドの上位 3 ビットが IP precedence として定義されています。 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。 また IPv6 precedence に基づいて IP トラフィックを分類することもできます。
CoS 値の信頼	着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。
IP 標準または拡張 ACL	設定された IP 標準 ACL または IP 拡張 ACL（IP ヘッダーの各フィールドを調べる）に基づいて、分類を実行します。 ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。 ACL が設定されている場合は、ポリシーマップ アクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。
設定された CoS の上書き	着信パケットに設定された CoS を上書きし、デフォルトのポート CoS 値を適用します。 IPv6 パケットの場合、DSCP 値は CoS/DSCP マップとポートのデフォルトの CoS を使用して書き換えられます。 これは、IPv4 と IPv6 の両方のトラフィックに対して実行できます。

分類されたパケットは、ポリシングおよびマーキングの各段階に送られます。

分類フローチャート

図 *3* : 分類フローチャート



アクセス コントロール リスト

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用すると、同じ特性を備えたパケット グループ（クラス）を定義できます。 また IPv6 ACL に基づいて IP トラフィックを分類することもできます。

QoS のコンテキストでは、アクセス コントロール エントリ（ACE）の許可および拒否アクションの意味が、セキュリティ ACL の場合とは異なります。

- 許可アクションとの一致が検出されると（最初の一致の原則）、指定の QoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、スイッチによってベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかると、それ以降の検索処理は中止され、QoS 処理が開始されます。

（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。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。 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、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。 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 ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。 レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

クラス マップおよびポリシー マップに基づく分類

ポリシーマップを使用するには、スイッチが LAN Base イメージを実行している必要があります。

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）に名前を付けて、他のすべてのトラフィックと区別するためのメカニズムです。 クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。 この条件には、ACL で定義されたアクセス グループとの照合、または DSCP 値や IP precedence 値の特定のリストとの照合を含めることができます。 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。 パケットをクラス マップ条件と照合した後で、ポリシー マップを使用してさらに分類します。

ポリシー マップでは、作用対象のトラフィック クラスを指定します。 トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクションや、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限やトラフィックが不適合な場合の対処法を指定するアクションなどを指定できます。 ポリシーマップを効率的に機能させるには、ポートにポリシー マップを結合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 コマンドまたは **class** 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。 多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。 **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、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。 分類されていないトラフィック（ポリシー マップで設定された他のトラフィック クラスで指定されているトラフィック）は、デフォルト トラフィックとして処理されます。

ポリシーマップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。 このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。 このモードでは、**class**、**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るアクションを指定します。

ポリシー マップには、ポリサー、トラフィックの帯域幅限度、および限度を超えた場合のアクションを定義する **police** および **police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを含めることもできます。

ポリシーマップをイネーブルにするには、**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ートにマップを結合します。

関連トピック

クラス マップによるトラフィックの分類, （49 ページ）

例：クラス マップによるトラフィックの分類, （87 ページ）

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング, （55 ページ）

例：ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング, （88 ページ）

ポリシングおよびマーキングの概要

パケットを分類し、DSCP または CoS に基づいて QoS ラベルを割り当てたあとで、ポリシングおよびマーキング プロセスを開始できます。

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。 各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。 こ

れらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられたDSCP値を変更（マークダウン）してパケットの通過を許可するアクションなどがあります。 設定可能なポリシング済みDSCPマップを使用すると、パケットに新しいDSCPベースQoSラベルが設定されます。 マークダウンされたパケットは、元のQoSラベルと同じキューを使用して、フロー内のパケットの順番が崩れないようにします。

（注） すべてのトラフィックは、ブリッジングされるかルーティングされるかに関係なく、ポリサーの影響を受けます（ポリサーが設定されている場合）。その結果、ブリッジングされたパケットは、ポリシングまたはマーキングが行われたときにドロップされたり、DSCP または CoS フィールドが変更されたりすることがあります。

ポリシングは物理ポートに対して設定できます。 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後で、**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、ポリシーを統合します。

物理ポートのポリシング

物理ポートのポリシー マップでは、次のポリサー タイプを作成できます。

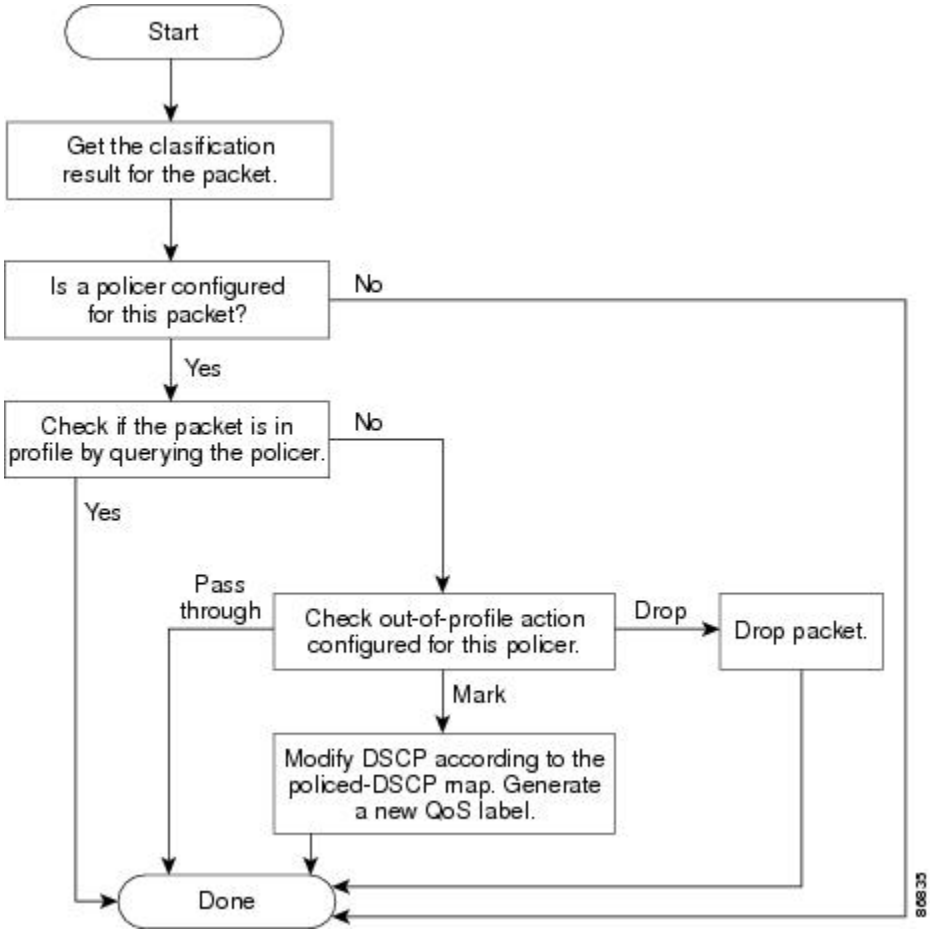
- Individual：QoSはポリサーに指定された帯域幅限度を、一致したトラフィック クラスごとに別々に適用します。 このタイプのポリサーは、**police** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップの中で設定します。
- Aggregate：QoS はポリサーで指定された帯域幅限度を、一致したすべてのトラフィック フローに累積的に適用します。 このタイプのポリサーは、**police aggregate** ポリシー マップ クラス コンフィギュレーション コマンドを使用して、ポリシー マップ内で集約ポリサー名を指定することにより設定します。 ポリサーの帯域幅限度を指定するには、**mls 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。

ポリシングは、トークン バケット アルゴリズムを使用します。 各フレームがスイッチに着信すると、バケットにトークンが追加されます。バケットにはホールがあり、平均トラフィック レートとして指定されたレート（ビット/秒）で送信されます。バケットにトークンが追加されるたびに、スイッチは、バケット内に十分なスペースがあるかを確認します。 十分なスペースがなければ、パケットは不適合とマーキングされ、指定されたポリサー アクション（ドロップまたはマークダウン）が実行されます。

バケットが満たされる速度は、バケット深度（burst-byte）、トークンが削除されるレート（rate-bps）、および平均レートを上回るバースト期間によって決まります。 バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。 ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

バケットの深さ（バケットがオーバーフローするまでの許容最大バースト）を設定するには、**police** ポリシー マップ クラス コンフィギュレーション コマンドの burst-byte オプションまたは **mls 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。 トークンがバケットから削除される速度（平均速度）を設定するには、*police* ポリシー マップ クラス コンフィギュレーション コマンドの **rate-bps** オプションまたは **mls 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。

図 *4*：物理ポートのポリシングおよびマーキング フローチャート



関連トピック

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング，（60 ページ）
例：集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング，（89 ページ）

マッピング テーブルの概要

QoS を処理している間、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティは、分類段階で取得された DSCP または CoS 値に基づいて、QoS ラベルで表されます。

次の表は、QoS 処理とマッピング テーブルについて説明しています。

表 *3*：*QoS* 処理およびマッピング テーブル

QoS 処理段階	マッピング テーブルの使用
分類	分類段階で、QoS は設定可能なマッピング テーブルを使用して、受信された CoS、DSCP、または IP precedence 値から、対応する DSCP または CoS 値を取得します。 これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。 これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-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。 DSCP 信頼状態で設定された入力ポートの DSCP 値が QoS ドメイン間で異なる場合は、2 つの QoS ドメイン間の境界にあるポートに、設定可能な DSCP/DSCP 変換マップを適用できます。 このマップを設定するには、**mls qos map dscp-mutation** 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。
ポリシング	ポリシング段階で、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって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。 このマップを設定するには、**mls qos map policed-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。
プレスケジュール	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 QoS ラベルに従って、出力キューにパケットを格納します。 QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 出力キューしきい値マップまたは CoS 出力キューしきい値マップを使用してキューを選択します。 出力のキューに加えて、QOS ラベルは WTD しきい値も識別します。 これらのマップを設定するには、**mls qos srr-queue** { **output**} **dscp-map** および **mls qos srr-queue** { **output**} **cos-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。

CoS/DSCP、DSCP/CoS、および IP precedence/DSCP マップのデフォルト値は、使用しているネットワークに適する場合と適さない場合があります。

デフォルトの DSCP/DSCP 変換マップおよびデフォルトのポリシング済み DSCP マップは、空のマップです。これらのマップでは、着信した DSCP 値が同じ DSCP 値にマッピングされます。DSCP/DSCP 変換マップは、特定のポートに適用できる唯一のマップです。 その他のすべてのマップはスイッチ全体に適用されます。

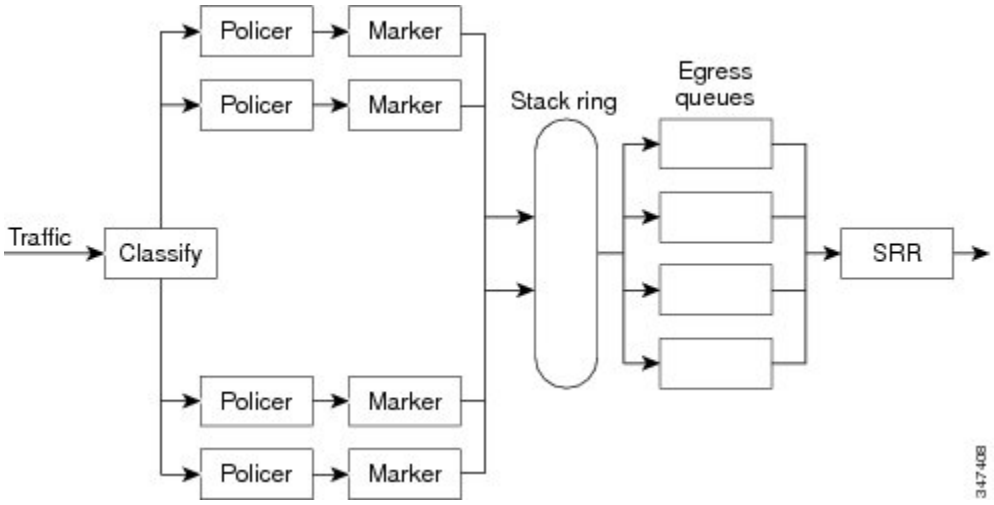
関連トピック

- CoS/DSCP マップの設定，（63 ページ）
- IP precedence/DSCP マップの設定，（64 ページ）
- ポリシング済み DSCP マップの設定，（66 ページ）
- DSCP/CoS マップの設定，（67 ページ）
- DSCP/DSCP 変換マップの設定，（68 ページ）
- 例：DSCP マップの設定，（90 ページ）
- 例：DSCP 信頼状態へのポートの設定および DSCP/DSCP 変換マップの変更，（85 ページ）

キューイングおよびスケジューリングの概要

スイッチは、輻輳を防ぐために特定の場所にキューがあります。

図 5：スイッチの出力キューの位置



WTD

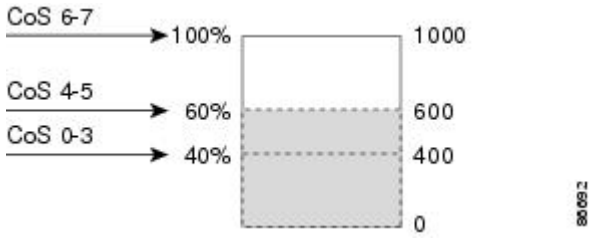
出力キューは、重み付けテール ドロップ（WTD）と呼ばれるテール ドロップ輻輳回避メカニズムの拡張バージョンを使用します。 WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。

フレームが特定のキューにキューイングされると、WTD はフレームに割り当てられた QoS ラベルを使用して、それぞれ異なるしきい値を適用します。 この QoS ラベルのしきい値を超えると（宛先キューの空きスペースがフレーム サイズより小さくなると）、フレームはドロップされます。

各キューには 3 つのしきい値があります。 QoS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。 3 つのしきい値のうち、2 つは設定可能（明示的）で、1 つは設定不可能（暗示的）です。

次の図は、サイズが 1000 フレームであるキューでの WTD の動作の例を示しています。 ドロップ割合は次のように設定されています。40%（400 フレーム）、60%（600 フレーム）、および 100%（1000 フレーム）です。 これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

図 *6*：*WTD* およびキューの動作



この例では、CoS 値 6 および 7 は他の CoS 値よりも重要度が高く、100% ドロップしきい値に割り当てられます（キューフル ステート）。 CoS 値 4 および 5 は 60% しきい値に、CoS 値 0 ～ 3 は 40% しきい値に割り当てられます。

600 個のフレームが格納されているキューに、新しいフレームが着信したとします。 このフレームの CoS 値は 4 および 5 で、60% のしきい値が適用されます。 このフレームがキューに追加されると、しきい値を超過するため、フレームは廃棄されます。

関連トピック

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定, （71 ページ）

例：出力キューの特性の設定, （92 ページ）

SRR のシェーピングおよび共有

出力キューはシェーピング ラウンド ロビン（SRR）で処理され、SRR によってパケットの送信レートが制御されます。 出力キューでは、SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。

シェーピング モードでは、出力キューの帯域幅割合が保証され、この値にレートが制限されます。 リンクがアイドルの場合でも、シェーピングされたトラフィックは割り当てられた帯域幅を超えて使用できません。 シェーピングを使用すると、時間あたりのトラフィック フローがより均一になり、バースト トラフィックの最高時と最低時を削減します。 シェーピングの場合は、各重みの絶対値を使用して、キューに使用可能な帯域幅が計算されます。

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。 このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。 たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。 共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。 重みの絶対値は関係ありません。 シェーピングおよび共有は、インターフェイスごとに設定されます。 各インターフェイスは、一意に設定できます。

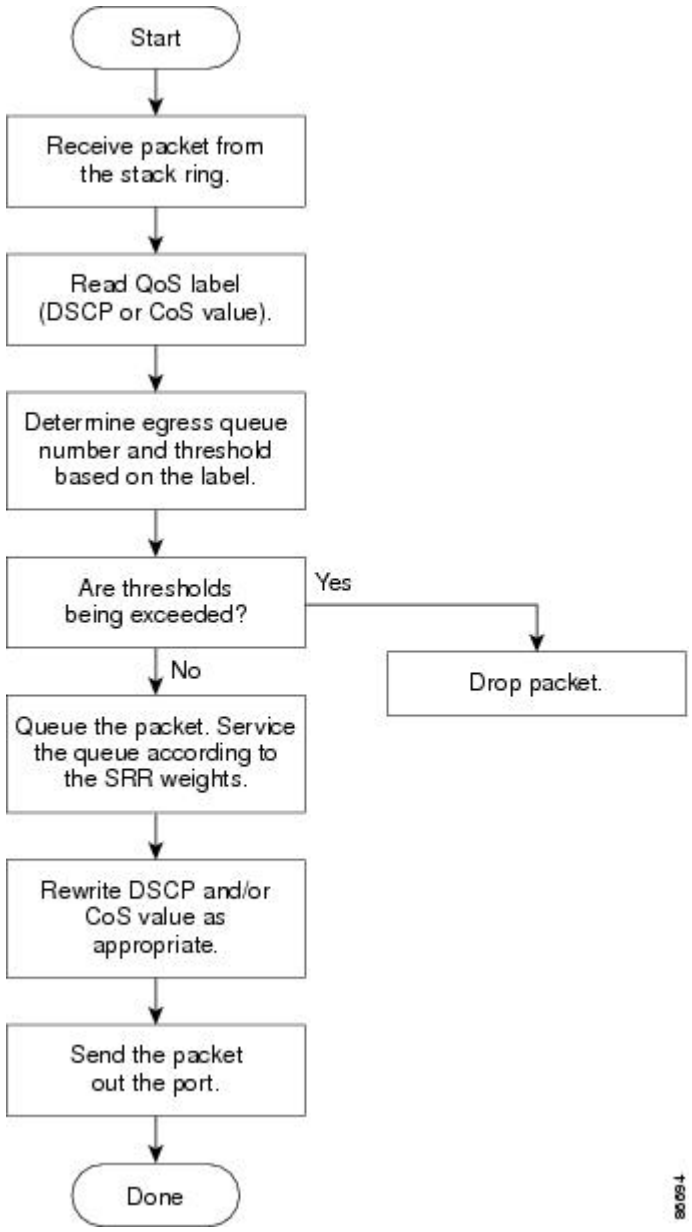
関連トピック

出力キューでの SRR シェーピング重みの設定，（77 ページ）
出力キューでの SRR 共有重みの設定，（78 ページ）
例：出力キューの特性の設定，（92 ページ）

出力キューでのキューイングおよびスケジューリング

次の図は、スイッチの出力ポートのキューイングおよびスケジューリングのフロー チャートを示しています。

図 7: スイッチの出力ポートのキューイングおよびスケジューリング フロー チャート



（注） 緊急キューがイネーブルの場合、SRRによって空になるまで処理されてから、他の3つのキューが処理されます。

出力緊急キュー

各ポートは、そのうち1つ（キュー1）を出力緊急キューにできる、4つの出力キューをサポートしています。これらのキューはキューセットに割り当てられます。スイッチに存在するすべてのトラフィックは、パケットに割り当てられたQoSラベルに基づいて、これらの4つのキューのいずれかを通過し、しきい値の影響を受けます。

（注） 緊急キューがイネーブルの場合、SRRによって空になるまで処理されてから、他の3つのキューが処理されます。

関連トピック

出力緊急キューの設定，（80 ページ）
例：出力キューの特性の設定，（92 ページ）

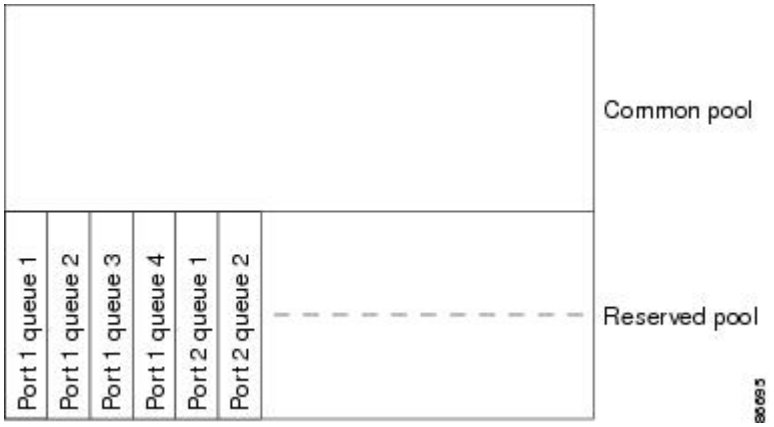
出力キューのバッファ割り当て

次の図は、出力キューのバッファを示しています。

バッファスペースは共通プールと専用プールで構成されます。スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファサイズを確保します。これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューのバッファが不足することがなくなり、要求元のキューにバッファスペースを割り当てるかどうかが制御されます。スイッチは、目的のキューが確保された量（限度内）を超えるバッファを消費していないかどうか、最大バッファ（限度超）をすべて消費しているかどうか、および共通プールが空である（空きバッファなし）か、または空でない（空きバッファあり）かを検出します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファスペー

スを割り当てることができます。 共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

図 *8* : 出力キューのバッファ割り当て



バッファおよびメモリの割り当て

バッファのアベイラビリティの保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* 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。 各しきい値はキューに割り当てられたメモリの割合です。このパーセント値を指定するには、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* 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。割り当てられたすべてのバッファの合計が専用プールになります。残りのバッファは共通プールの一部になります。

バッファ割り当てを行うと、ハイプライオリティ トラフィックを確実にバッファに格納できます。 たとえば、バッファ スペースが 400 の場合、バッファ スペースの 70% をキュー 1 に割り当てて、10% をキュー 2 ～ 4 に割り当てることができます。 キュー 1 には 280 バッファが割り当てられ、キュー 2 ～ 4 にはそれぞれ 40 バッファが割り当てられます。

割り当てられたバッファをキューセット内の特定のキュー用に確保するよう保証できます。 たとえば、キュー用として 100 バッファがある場合、50%（50 バッファ）を確保できます。 残りの 50 バッファは共通プールに戻されます。 また、最大しきい値を設定することにより、いっぱいになったキューが確保量を超えるバッファを取得できるようにすることもできます。 共通プールが空でない場合、必要なバッファを共通プールから割り当てることができます。

キューおよび WTD しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。

特に、出力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。 **mls qos srr-queue output dscp-map queue** *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*} または **mls qos srr-queue output cos-map queue** *queue-id* {*cos1...cos8* | **threshold** *threshold-id cos1...cos8*} 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。 DSCP 出力

キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（明示的）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（暗示的）なしきい値です。 しきい値 ID 1 および ID 2 用の 2 つの WTD しきい値割合を割り当てます。 しきい値 ID 3 のドロップしきい値は、キューフルステートに設定済みで、変更できません。キューセットにポートをマッピングするには、**queue-set qset-id** 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。 WTD しきい値の割合を変更するには、キューセット設定を変更します。

関連トピック

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定，（71 ページ）

例：出力キューの特性の設定，（92 ページ）

出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング，（74 ページ）

例：出力キューの特性の設定，（92 ページ）

シェーピング モードまたは共有モード

SRR は、シェーピング モードまたは共有モードでキューセットを処理します。 キューセットにポートをマッピングするには、**queue-set** *qset-id* 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。 ポートに共有重みまたはシェーピング重みを割り当てるには、**srr-queue bandwidth share** *weight1 weight2 weight3 weight4* または **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* 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。

バッファ割り当てと SRR 重み比率を組み合わせることにより、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。 重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

緊急キューがイネーブルでない限り、4 つのキューはすべて SRR に参加し、この場合、1 番めの帯域幅重みは無視されて比率計算に使用されません。 緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。 緊急キューをイネーブルにするには、**priority-queue out** 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。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

関連トピック

出力キューでの SRR シェーピング重みの設定，（77 ページ）

出力キューでの SRR 共有重みの設定，（78 ページ）

例：出力キューの特性の設定，（92 ページ）

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。 QoS を提供するプロセス中に次のパケットの変更が発生することがあります。

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。 ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定のみがパケットとともに伝達されます。 これは、QoS の分類および転送検索が並行して発生するためです。パケットを元の DSCP のまま CPU に転送し、CPU でソフトウェアによる再処理を行うことができます。
- 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 パケットの場合は、この後の段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。 テーブルマップを設定しない場合、および着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されませんが、CoS は、DSCP/CoS マップに基づいて書き換えられます。 着信フレームの CoS を信頼するようにポートが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されないで、CoS/DSCP マップに従って DSCP が変更されることがあります。

  入力変換が行われると、選択された新しい DSCP 値に応じて DSCP が書き換えられます。 ポリシー マップの設定アクションによっても、DSCP が書き換えられます。

標準 QoS のデフォルト設定

標準 QoS はデフォルトでディセーブルになっています。

パケットが変更されないため、信頼できるポートまたは信頼できないポートといった概念はありません。 パケット内の CoS、DSCP、および IP precedence 値は変更されません。

トラフィックは Pass-Through モードでスイッチングされます。 パケットは書き換えられることなくスイッチングされ、ポリシングなしのベスト エフォートに分類されます。

mls qos 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 QoS をイネーブルにし、その他のすべての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエ

フォート型として分類されます（DSCP および CoS 値は 0 に設定されます）。 ポリシー マップは設定されません。 すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。

関連トピック

QoS のグローバルなイネーブル化, （28 ページ）

出力キューのデフォルト設定

次の表は、QoS がイネーブルの場合の各キュー セットに対するデフォルトの出力キューを示しています。 すべてのポートはキューセット 1 にマッピングされます。 ポートの帯域幅限度は 100% に設定され、レートは制限されません。 SRR シェーピング重み（絶対）機能では、ゼロのシェーピング重みはキューが共有モードで動作していることを示しています。 SRR 共有重み機能では、帯域幅の 4 分の 1 が各キューに割り当てられます。

表 *4*：出力キューのデフォルト設定

機能	キュー 1	キュー 2	キュー 3	キュー 4
バッファ割り当て	25%	25%	25%	25%
WTD ドロップしきい値 1	100%	200%	100%	100%
WTD ドロップしきい値 2	100%	200%	100%	100%
予約済みしきい値	50%	100%	50%	50%
最大しきい値	400%	400%	400%	400%
SRR シェーピング重み（絶対）	25	0	0	0
SRR 共有重み	25	25	25	25

（注） WTD ドロップしきい値 1、WTD ドロップしきい値 2、予約しきい値、および最大しきい値のユーザ設定可能な最大値はそれぞれ 3200 パーセントです。

次の表は、QoS がイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示しています。

表 *5*：デフォルトの *CoS* 出力キューしきい値マップ

CoS 値	キュー ID - しきい値 ID
0、1	2 - 1
2、3	3 - 1
4	4 - 1
5	1 - 1
6、7	4 - 1

次の表は、QoS がイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示しています。

表 *6*：デフォルトの *DSCP* 出力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ～ 15	2 - 1
16 ～ 31	3 - 1
32 ～ 39	4 - 1
40 ～ 47	1 - 1
48 ～ 63	4 - 1

マッピング テーブルのデフォルト設定

デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌルマップです。

デフォルトのポリシング済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする（マークダウンしない）空のマップです。

DSCP マップ

DSCP/DSCP 変換マップを除くすべての DSCP マップはグローバルに定義され、すべてのポートに適用されます。

デフォルトの CoS/DSCP マップ

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。 次の表に、デフォルトの CoS/DSCP マップを示します。 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。

表 *7*：デフォルトの *CoS/DSCP* マップ

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

デフォルトの IP Precedence/DSCP マップ

着信パケットの IP precedence 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 値にマッピングするには、IP precedence/DSCP マップを使用します。 次の表は、デフォルトの IP Precedence/DSCP マップを示しています。 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。

表 *8*：デフォルトの *IP Precedence/DSCP* マップ

IP precedence 値	DSCP 値
0	0
1	8
2	16
3	24
4	32

IP precedence 値	DSCP 値
5	40
6	48
7	56

デフォルトの DSCP/CoS マップ

4 つの出力キューのうち 1 つを選択するために使用される CoS 値を生成するには、DSCP/CoS マップを使用します。 次の表に、デフォルトの DSCP/CoS マップを示します。 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。

表 *9*：デフォルトの *DSCP/CoS* マップ

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

QoS の設定方法

QoS のグローバルなイネーブル化

デフォルトでは、QoS はスイッチ上でディセーブルに設定されています。

QoS をイネーブルにするために次の手順が必要です。

手順の概要

1. **configure terminal**
2. **mls qos**
3. **end**
4. **show mls qos**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos** 例： `Switch(config)# mls qos`	QoS をグローバルにイネーブルにします。 QoS は、次の関連トピックのセクションで説明されているデフォルト設定で動作します。 （注） QoS をディセーブルにするには、**no mls qos** 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	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos** 例： `Switch# show mls qos`	QoS の設定を確認します。
ステップ 5	**copy running-config startup-config** 例： `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。

関連トピック

標準 QoS のデフォルト設定, （24 ページ）

ポートの信頼状態による分類の設定

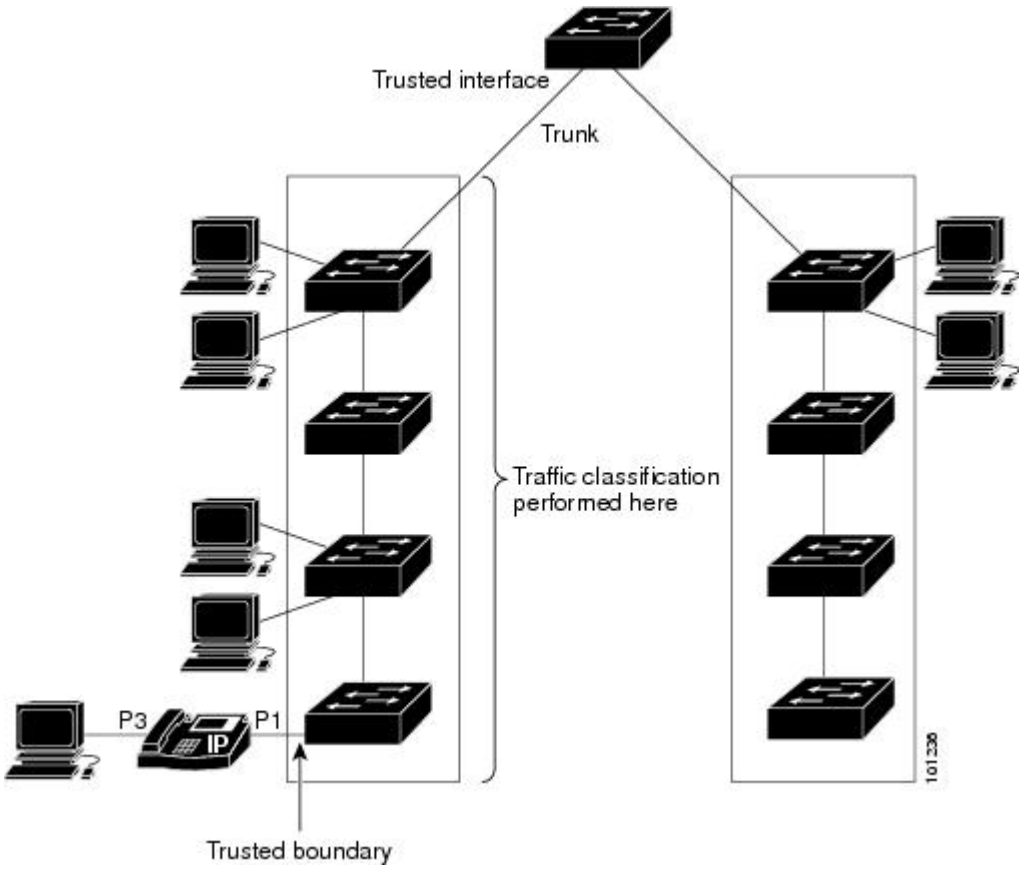
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。

（注） ネットワークの設定によって、このモジュールのこれらのタスクの 1 つ以上または 37 ～ 47 ページのQoS ポリシーの設定の項のタスクの 1 つ以上を実行する必要があります。

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。 パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートをいずれか 1 つの信頼状態に設定できます。

図 *9* : *QoS* ドメイン内のポートの信頼状態



手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **mls qos trust** [**cos** | **dscp** | **ip-precedence**]
4. **end**
5. **show mls qos interface**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/2`	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。
ステップ 3	**mls qos trust** [**cos**	**dscp**	**ip-precedence**] 例： `Switch(config-if)# mls qos trust cos`	ポートの信頼状態を設定します。 デフォルトでは、ポートは trusted ではありません。 キーワードを指定しない場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：パケットの CoS 値を使用して入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。 デフォルトのポート CoS 値は 0 です。 • **dscp**：パケットの DSCP 値を使用して入力パケットを分類します。 非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。 スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • **ip-precedence**：パケットの IP precedence 値を使用して入力パケットを分類します。 非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。 スイッチは、

	コマンドまたはアクション	目的
		内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 untrusted ステートにポートを戻す場合は、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** 例： `Switch# show mls qos interface`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `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。

インターフェイスの CoS 値の設定

QoS は、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、**mls qos cos** インターフェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

ポートのデフォルト CoS 値を定義する場合、またはポート上のすべての着信パケットにデフォルト CoS 値を割り当てる場合には、特権 EXEC モードから次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **mls qos cos** {*default-cos* | **override**}
4. **end**
5. **show mls qos interface**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/1/1`	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 3	**mls qos cos** {*default-cos* | **override**} 例： `Switch(config-if)# mls qos override`	ポートのデフォルトの CoS 値を設定します。 • *default-cos* には、ポートに割り当てるデフォルトの CoS 値を指定します。 パケットがタグなしの場合、デフォルトの CoS 値がパケットの CoS 値になります。 指定できる CoS 範囲は 0 ～ 7 です。デフォルトは 0 です。 • 着信パケットにすでに設定されている信頼状態を変更し、すべての着信パケットにデフォルトのポート CoS 値を適用する場合は、**override** キーワードを使用します。 デフォルトでは、CoS の上書きはディセーブルに設定されています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、**override** キーワードを使用します。 ポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されている場合でも、設定済みの信頼状態がこのコマンドによって上書き変更され、すべての着信 CoS 値にこのコマンドで設定されたデフォルトの CoS 値が割り当てられます。 着信パケットがタグ付きの場合、入力ポートで、ポートのデフォルト CoS を使用してパケットの CoS 値が変更されます。 （注） デフォルトの設定に戻す場合は、**no mls qos cos** {*default-cos* | **override**} 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。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show mls qos interface** 例： `Switch# show mls qos interface`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `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。

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

一般的なネットワークでは、スイッチ ポートに Cisco IP Phone を接続し、電話の背後からデータ パケットを生成するデバイスをカスケードします。 Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ（CoS = 5）にマーキングし、データ パケットをロー プライオリティ（CoS = 0）にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からスイッチに送信されたトラフィックは通常 802.1Q ヘッダーを使用するタグでマーキングされています。 ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビット フィールドが含まれています。

ほとんどの Cisco IP Phone 設定では、電話からスイッチに送信されるトラフィックは、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に対して適切にプライオリティ付けがされていることを保証するように信頼されています。 **mls qos trust cos** インターフェイス コンフィギュレーション コマンドを使用して、ポートで受信されるすべてのトラフィックの CoS ラベルを信頼するように、電話が接続されているスイッチ ポートを設定します。 **mls qos trust dscp** 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、ポートで受信されるすべてのトラフィックの DSCP ラベルを信頼するように、電話が接続されているルーテッド ポートを設定します。

信頼設定により、ユーザが電話をバイパスして PC を直接スイッチに接続する場合に、ハイプライオリティ キューの誤使用を避けるのにも信頼境界機能を使用できます。信頼境界機能を使用しないと、（信頼性のある CoS 設定により）PC が生成した CoS ラベルがスイッチで信頼されてしまいます。 それに対して、信頼境界機能は CDP を使用してスイッチ ポートにある Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出します。 電話が検出されない場合、信頼境界機能がハイプライオリティ キューの誤使用を避けるためにスイッチ ポートの信頼設定を無効にします。 信頼境界機能は、PC および Cisco IP Phone がスイッチに接続されているハブに接続されている場合は機能しないことに注意してください。

Cisco IP Phone に接続した PC でハイ プライオリティのデータ キューを利用しないようにすることもできる場合があります。 **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 から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

手順の概要

1. **configure terminal**
2. **cdp run**
3. **interface** *interface-id*
4. **cdp enable**
5. 次のいずれかを使用します。
   - **mls qos trust cos**
   - **mls qos trust dscp**
6. **mls qos trust device cisco-phone**
7. **end**
8. **show mls qos interface**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**cdp run** 例： `Switch(config)# cdp run`	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 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 2/1/1`	Cisco IP Phone に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。

	コマンドまたはアクション	目的
ステップ 4	**cdp enable** 例： `Switch(config-if)# cdp enable`	ポート上で CDP を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 5	次のいずれかを使用します。 • **mls qos trust cos** • **mls qos trust dscp** 例： `Switch(config-if)# mls qos trust cos`	Cisco IP Phone から受信したトラフィックの CoS 値を信頼するようにスイッチ ポートを設定します。 または Cisco IP Phone から受信したトラフィックの DSCP 値を信頼するようにルーテッド ポートを設定します。 デフォルトでは、ポートは trusted ではありません。
ステップ 6	**mls qos trust device cisco-phone** 例： `Switch(config-if)# mls 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。 （注） 信頼境界機能をディセーブルにするには、**no mls qos trust device** 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。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show mls qos interface** 例： `Switch# show mls qos interface`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `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。

DSCP トランスペアレント モードのイネーブル化

スイッチは透過的な DSCP 機能をサポートします。 この機能は発信パケットの DSCP フィールドのみに作用します。 デフォルトでは、DSCP 透過性はディセーブルです。 スイッチでは着信パケットの DSCP フィールドが変更され、発信パケットの DSCP フィールドは、ポートの信頼設定、ポリシングとマーキング、DSCP/DSCP 変換マップを含めて Quality of Service（QoS）に基づきます。

no mls qos rewrite ip dscp コマンドを使用して DSCP 透過がイネーブルになっている場合、スイッチは着信パケットの DSCP フィールドは変更せず、送信パケットの DSCP フィールドも着信パケットのものと同じになります。

透過的な DSCP 設定にかかわらず、スイッチはパケット内部の DSCP 値を変更し、トラフィックのプライオリティを提示する CoS 値を生成します。 また、スイッチは内部 DSCP 値を使用して、出力キューおよびしきい値を選択します。

手順の概要

1. **configure terminal**
2. **mls qos**
3. **no mls qos rewrite ip dscp**
4. **end**
5. **show mls qos interface** [*interface-id*]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos** 例： `Switch(config)# mls qos`	QoS をグローバルにイネーブルにします。
ステップ 3	**no mls qos rewrite ip dscp** 例： `Switch(config)# no mls qos rewrite ip dscp`	DSCP 透過性をイネーブルにします。 スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*] 例： `Switch# show mls qos interface gigabitethernet 2/1/1`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `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。

DSCP 透過モード

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変更させる設定にするには、**mls qos rewrite ip 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。

no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS および DSCP 値は変更されません（デフォルトの QoS 設定）。

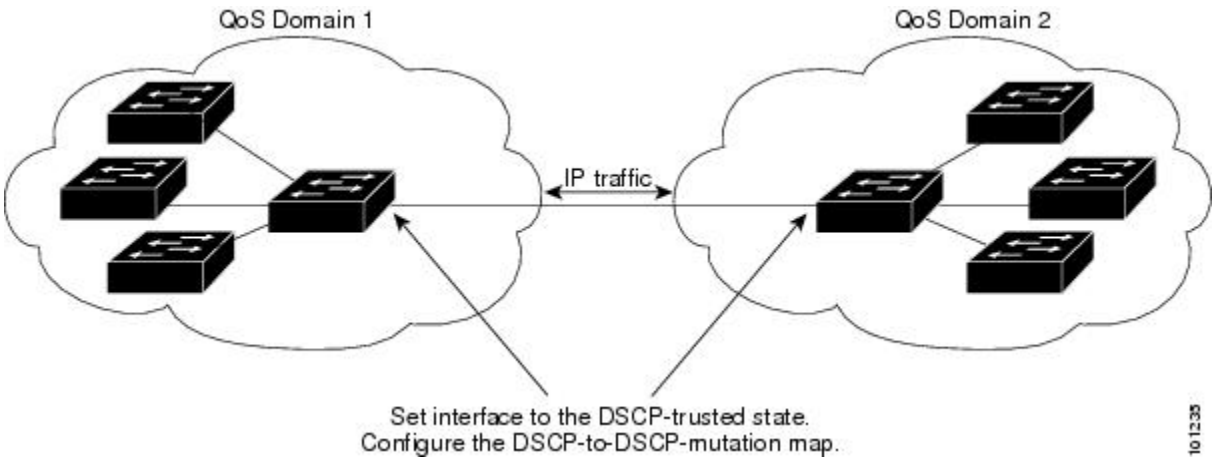
no mls qos rewrite ip dscp グローバル コンフィギュレーション コマンドを入力して DSCP 透過をイネーブルにしてから、**mls qos trust** [**cos** | **dscp**] インターフェイス コンフィギュレーション コマンドを入力した場合、DSCP 透過はイネーブルのままとなります。

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定できます。 受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分類手順が省略されま

す。 2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内での定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 *10*：別の *QoS* ドメインとの境界ポートの *DSCP* 信頼状態



ポート上に DSCP trusted ステートを設定して、DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。 両方の QoS ドメインに一貫した方法でマッピングするには、両方のドメイン内のポート上で次の手順を実行する必要があります。

手順の概要

1. **configure terminal**
2. **mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*
3. **interface** *interface-id*
4. **mls qos trust dscp**
5. **mls qos dscp-mutation** *dscp-mutation-name*
6. **end**
7. **show mls qos maps dscp-mutation**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを変更します。

	コマンドまたはアクション	目的
	例： `Switch(config)# mls qos map dscp-mutation gigabitethernet1/0/2-mutation 10 11 12 13 to 30`	デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。 • *dscp-mutation-name* には、変換マップ名を入力します。 新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* 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。 • *out-dscp* には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/2`	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**mls qos trust dscp** 例： `Switch(config-if)# mls qos trust dscp`	DSCP trusted ポートとして入力ポートを設定します。 デフォルトでは、ポートは trusted ではありません。 （注） ポートを trusted 以外のステートに戻すには、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name* 例： `Switch(config-if)# mls qos dscp-mutation gigabitethernet1/0/2-mutation`	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で作成した変換マップ名を指定します。 1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。 （注） デフォルトの DSCP/DSCP 変換マップ値に戻すには、**no mls qos map dscp-mutation** *dscp-mutation-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。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation** 例： `Switch# show mls qos maps`	入力を確認します。

	コマンドまたはアクション	目的
	dscp-mutation	
ステップ 8	**copy running-config startup-config** 例： `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。 （注） ポートを trusted 以外のステートに戻すには、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、**no mls qos map dscp-mutation** *dscp-mutation-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。

QoS ポリシーの設定

QoS ポリシーを設定するには、次のタスクが必要です。

- トラフィックのクラスへの分類
- 各トラフィック クラスに適用するポリシーの設定
- ポートへのポリシーの付加

ここでは、トラフィックを分類、ポリシング、マーキングする方法について説明します。 ネットワーク設定に応じて、この項のモジュールの 1 つ以上を実行します。

ACL によるトラフィックの分類

IPv4 標準 ACLS、IPv4 拡張 ACL または IPv6 ACL を使用して IP トラフィックを分類できます。

非 IP トラフィックの分類はレイヤ 2 MAC ACL でできます。

IPv4 トラフィック用の IP 標準 ACL の作成

はじめる前に

この作業を実行する前に、QoS 設定のために使用するアクセス リストを決定します。

手順の概要

1. **configure terminal**
2. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
3. **end**
4. **show access-lists**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Switch(config)# access-list 1 permit 192.2.255.0 1.1.1.255`	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。 有効範囲は 1 ～ 99 および 1300 ～ 1999 です。 • **permit** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。 **deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *source* には、パケットの送信元となるネットワークまたはホストを指定します。 **any** キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。 無視するビット位置には 1 を設定します。 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。 （注） アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** 例： `Switch# show access-lists`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `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。

関連トピック

QoS ACL の注意事項, （2 ページ）
例：ACL によるトラフィックの分類, （85 ページ）

IPv4 トラフィック用の IP 拡張 ACL の作成

はじめる前に

この作業を実行する前に、QoS 設定のために使用するアクセス リストを決定します。

手順の概要

1. **configure terminal**
2. **access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*
3. **end**
4. **show access-lists**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*	IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、アクセス リスト番号を入力します。 有効範囲は 100 ～ 199 および 2000 ～ 2699 です。

	コマンドまたはアクション	目的
	例： `Switch(config)# access-list 100 permit ip any any dscp 32`	• **permit** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。 **deny** キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 • *protocol* には、IP プロトコルの名前または番号を入力します。 疑問符（?）を使用すると、使用できるプロトコル キーワードのリストが表示されます。 • *source* には、パケットの送信元となるネットワークまたはホストを指定します。 ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用したり、**source** 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として *any* キーワードを使用したり、**source** 0.0.0.0 を表す *host* キーワードを使用します。 • *source-wildcard* では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。 ワイルドカードを指定するには、ドット付き 10 進表記を使用したり、**source** 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として *any* キーワードを使用したり、**source** 0.0.0.0 を表す *host* キーワードを使用します。 • *destination* には、パケットの宛先となるネットワークまたはホストを指定します。 *destination* および *destination-wildcard* には、*source* および *source-wildcard* での説明と同じオプションを使用できます。 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。 （注） アクセス リストを削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** 例： `Switch# show access-lists`	入力を確認します。
ステップ 5	**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。

	コマンドまたはアクション	目的
	例： `Switch# copy-running-config startup-config`	

関連トピック

QoS ACL の注意事項，（2 ページ）
例：ACL によるトラフィックの分類，（85 ページ）

IPv6 トラフィック用の IPv6 ACL の作成

はじめる前に

この作業を実行する前に、QoS 設定のために使用するアクセス リストを決定します。

手順の概要

1. **configure terminal**
2. **ipv6 access-list** *access-list-name*
3. {**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]
4. **end**
5. **show ipv6 access-list**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**ipv6 access-list** *access-list-name* 例： `Switch(config)# ipv6`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 アクセス リスト名にはスペースまたは引用符を含めることはできません。また、数字で開始することもできません。

	コマンドまたはアクション	目的
	access-list ipv6_Name_ACL	（注） アクセス リストを削除するには、**no ipv6 access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	{**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] 例： `Switch(config-ipv6-acl)# permit ip host 10::1 host 11::2 host`	条件が一致した場合に、パケットを拒否するには **deny**、許可する場合には **permit** を入力します。 次に、条件について説明します。 *protocol* には、インターネット プロトコルの名前または番号を入力します。**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp**、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、**any** を入力します。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）*operator* には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。 オペランドには、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、**range**（包含範囲）があります。 *source-ipv6-prefix/prefix-length* 引数のあとの operator は、送信元ポートに一致する必要があります。 *destination-ipv6- prefix/prefix-length* 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）*port-number* は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。 TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。 UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）**dscp** *value* を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。 • （任意）**fragments** を入力して、先頭ではないフラグメントを確認します。 このキーワードが表示されるのは、プロトコルが IPv6 の場合だけです。 • （任意）**log** を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。 **log-input** を指定する

	コマンドまたはアクション	目的
		と、ログ エントリに入力インターフェイスが追加されます。 ロギングはルータ ACL でだけサポートされます。 • （任意）**routing** を入力して、IPv6 パケットのルーティングを指定します。 • （任意）**sequence** *value* を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4294967295 です。 • （任意）**time-range** *name* を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 4	**end** 例： `Switch(config-ipv6-acl)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 access-list** 例： `Switch# show ipv6 access-list`	アクセス リストの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `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。

関連トピック

QoS ACL の注意事項, （2 ページ）
例：ACL によるトラフィックの分類, （85 ページ）

非 IP トラフィック用のレイヤ 2 MAC ACL の作成

はじめる前に

この作業を実行する前に、レイヤ 2 の MAC アクセス リストが QoS 設定に必要であることを決定します。

手順の概要

1. **configure terminal**
2. **mac access-list extended** *name*
3. {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]
4. **end**
5. **show access-lists** [*access-list-number* | *access-list-name*]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mac access-list extended** *name* 例： `Switch(config)# mac access-list extended maclist1`	リストの名前を指定することによって、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに切り替わります。 （注） アクセス リストを削除するには、**no mac access-list extended** *access-list-name* グローバル コンフィギュレーション コマンドを入力します。

ステップ 3	{**permit**	**deny**} {**host** *src-MAC-addr mask*	**any**	**host** *dst-MAC-addr*	*dst-MAC-addr mask*} [*type mask*]
					
					例：
					`Switch(config-ext-mac1) # permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0`
					
					`Switch(config-ext-mac1) # permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp`
						条件が一致した場合に許可または拒否するトラフィック タイプを指定します。必要な回数だけコマンドを入力します。
						• *src-MAC-addr* には、パケットの送信元となるホストの MAC アドレスを指定します。 MAC アドレスを指定するには、16 進表記（H.H.H）を使用したり、**source** 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として *any* キーワードを使用したり、**source** 0.0.0 を表す *host* キーワードを使用します。
						• *mask* では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。
						• *dst-MAC-addr* には、パケットの宛先となるホストの MAC アドレスを指定します。 MAC アドレスを指定するには、16 進表記（H.H.H）を使用したり、**source** 0.0.0、*source-wildcard* ffff.ffff.ffff の短縮形として *any* キーワードを使用したり、**source** 0.0.0 を表す *host* キーワードを使用します。
						• （任意）*type mask* には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロ

	コマンドまたはアクション	目的
		トコルを識別します。 *type* の範囲は 0 ～ 65535 です。通常は 16 進数で指定します。 *mask* では、一致をテストする前に Ethertype に適用される *don't care* ビットを入力します。 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。
ステップ 4	**end** 例： `Switch(config-ext-mac1)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*access-list-number* | *access-list-name*] 例： `Switch# show access-lists`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `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。

関連トピック

QoS ACL の注意事項, （2 ページ）
例：ACL によるトラフィックの分類, （85 ページ）

クラス マップによるトラフィックの分類

個々のトラフィック フロー（またはクラス）を他のすべてのトラフィックから分離して名前を付けるには、**class-map** グローバル コンフィギュレーション コマンドを使用します。 クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合する条件を定義します。 match ステートメントには、ACL、IP precedence 値、DSCP 値などの条件を指定できます。 一致条件は、クラス マップ コンフィギュレーション モードの中で match ステートメントを 1 つ入力することによって定義します。

（注） **class** ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの作成時にクラス マップを作成することもできます。

手順の概要

1. **configure terminal**
2. 次のいずれかを使用します。
   - **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
   - **access-list** *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*]
   - **ipv6 access-list** *access-list-name* {**deny** | **permit**} *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]
   - **mac access-list extended** *name* {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}
5. **end**
6. **show class-map**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	次のいずれかを使用します。 • **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] • **access-list** *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] • **ipv6 access-list** *access-list-name* {**deny** | **permit**} *protocol*	必要な回数だけコマンドを繰り返し、IP 標準または IP 拡張 ACL、IP トラフィック用の IPv6 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成します。 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。

	コマンドまたはアクション	目的
	{*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] • **mac access-list extended** *name* {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*] 例： `Switch(config)# access-list 103 permit ip any any dscp 10`	
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Switch(config)# class-map class1`	クラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 AND を実行するには、**match-all** キーワードを使用します。 この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。 この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 （注） 既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**match** {**access-group** *acl-index-or-name* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。

	コマンドまたはアクション	目的
	例： `Switch(config-cmap)# match ip dscp 10 11 12`	クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 • **access-group** *acl-index-or-name* には、ステップ 2 で作成した ACL の番号または名前を指定します。 • IPv6 トラフィックを **match access-group** コマンドでフィルタリングするには、ステップ 2 の手順で IPv6 ACL を作成します。 • **ip dscp** *dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する IP precedence 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 7 です。 （注） 一致条件を削除するには、**no match** {**access-group** *acl-index-or-name* | **ip dscp** | **ip precedence**} クラス マップ コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config-cmap)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show class-map** 例： `Switch# show class-map`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `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。

関連トピック

クラス マップおよびポリシー マップに基づく分類, （12 ページ）
例：クラス マップによるトラフィックの分類, （87 ページ）

クラスマップの使用と IPv6 トラフィックのフィルタリングによるトラフィックの分類

プライマリ一致基準を IPv4 トラフィックに対してのみ適用するには、**match protocol** コマンドで **ip** キーワードを使用します。 プライマリ一致基準を IPv6 トラフィックに対してのみ適用するには、**match protocol** コマンドで **ipv6** キーワードを使用します。

手順の概要

1. **configure terminal**
2. **class-map** {**match-all**} *class-map-name*
3. **match protocol** [*ip* | *ipv6*]
4. **match** {**ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*}
5. **end**
6. **show class-map**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**class-map** {**match-all**} *class-map-name* 例： `Switch(config)# class-map cm-1`	クラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 **match protocol** コマンドを使用する場合、**match-all** キーワードのみがサポートされます。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。 （注） 既存のクラス マップを削除するには、**no class-map** [**match-all** | **match-any**] *class-map-name* グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 3	**match protocol** [*ip* | *ipv6*] 例： `Switch(config-cmap)# match protocol ip`	（任意）クラス マップを適用する IP プロトコルを指定します。 • IPv4 トラフィックを指定するには引数 *ip*、IPv6 トラフィックを指定するには *ipv6* をそれぞれ指定します。 • **match protocol** コマンドを使用する場合、**class-map** コマンドでは **match-all** キーワードのみがサポートされます。
ステップ 4	**match** {**ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list*} 例： `Switch(config-cmap)# match ip dscp 10`	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件は定義されていません。 • **ip dscp** *dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する IP precedence 値を 8 つまで入力します。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 7 です。 （注） 一致条件を削除するには、no match {**access-group** *acl-index-or-name* | **ip dscp** | **ip precedence**} クラス マップ コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Switch(config-cmap)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show class-map** 例： `Switch# show class-map`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `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。

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング

作用対象となるトラフィック クラスを指定するポリシー マップを、物理ポート上に設定できます。 トラフィック クラスの CoS 値、DSCP 値、または IP precedence 値を信頼するアクション、トラフィック クラスに特定の DSCP 値または IP precedence 値を設定するアクション、および一致する各トラフィック クラスにトラフィック帯域幅限度を指定するアクション（ポリサー）や、トラフィックが不適合な場合の対処法を指定するアクション（マーキング）などを指定できます。

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、それぞれ異なる一致条件とポリサーを指定した複数のクラス ステートメントを指定できます。
- ポリシー マップには、事前に定義されたデフォルトのトラフィック クラスを含めることができます。デフォルトのトラフィック クラスはマップの末尾に明示的に配置されます。
- 1 つのポートから受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。

物理ポートでポリシー マップを設定する場合には、次の注意事項に従ってください。

- 入力ポートごとに付加できるポリシー マップは、1 つだけです。
- **mls qos map ip-prec-dscp** *dscp1...dscp8* 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 IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。 ポリシー マップでは、**set ip precedence** *new-precedence* 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パケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。 出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、パケット IP Precedence 値を変更できます。 スイッチ コンフィギュレーションではこの設定は set ip precedence として表示されます。
- ポリシーマップとポート信頼状態は、両方とも物理インターフェイス上で有効にすることができます。 ポリシー マップは、ポート信頼状態の前に適用されます。
- **class class-default** ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィック クラスを設定すると、未分類トラフィック（トラフィック クラスで指定された一致基準に一致しないトラフィック）はデフォルトのトラフィック クラス（class-default）として処理されます。

手順の概要

1. **configure terminal**
2. **class-map** [**match-all** | **match-any**] *class-map-name*
3. **policy-map** *policy-map-name*
4. **class** [*class-map-name* | **class-default**]
5. **trust** [**cos** | **dscp** | **ip-precedence**]
6. **set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}
7. **police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]
8. **exit**
9. **exit**
10. **interface** *interface-id*
11. **service-policy input** *policy-map-name*
12. **end**
13. **show policy-map** [*policy-map-name* [**class** *class-map-name*]]
14. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Switch(config)# class-map ipclass1`	クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 AND を実行するには、**match-all** キーワードを使用します。 この場合は、クラスマップ内のすべての一致条件と一致する必要があります。 • （任意）このクラスマップ配下のすべての一致ステートメントの論理 OR を実行するには、**match-any** キーワードを使用します。 この場合は、1 つまたは複数の一致条件と一致する必要があります。 • *class-map-name* には、クラス マップ名を指定します。 **match-all** または **match-any** のどちらのキーワードも指定されていない場合、デフォルトは **match-all** です。

	コマンドまたはアクション	目的
ステップ 3	**policy-map** *policy-map-name* 例： `Switch(config-cmap)# policy-map flowit`	ポリシーマップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシーマップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。 ポリシングは実行されません。 （注） 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。
ステップ 4	**class** [*class-map-name* | **class-default**] 例： `Switch(config-pmap)# class ipclass1`	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップ クラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **class-default** トラフィック クラスは定義済みで、どのポリシーにも追加できます。 このトラフィック クラスは、常にポリシー マップの最後に配置されます。 暗黙の **match any** が **class-default** クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは **class-default** と一致します。 （注） 既存のクラス マップを削除するには、**no class** *class-map-name* ポリシー マップ コンフィギュレーション コマンドを使用します。
ステップ 5	**trust** [**cos** | **dscp** | **ip-precedence**] 例： `Switch(config-pmap-c)# trust dscp`	CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。 このコマンドと **set** コマンドは、同じポリシー マップ内で相互に排他的になります。 **trust** コマンドを入力する場合は、ステップ 6 へ進んでください。 デフォルトでは、ポートは trusted ではありません。 キーワードを指定せずにコマンドを入力した場合、デフォルトは **dscp** です。 キーワードの意味は次のとおりです。 • **cos**：QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • **dscp**：QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。 タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。 いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。

	コマンドまたはアクション	目的
		• **ip-precedence**：QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。 タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非IPパケットの場合、QoSはデフォルトのポートCoS値を使用してDSCP値を抽出します。 いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 （注） untrusted ステートに戻すには、**no trust** 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。
ステップ 6	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*} 例： `Switch(config-pmap-c)# set dscp 45`	パケットに新しい値を設定することによって、IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類されたトラフィックに割り当てる新しいDSCP値を入力します。 指定できる範囲は 0 ～ 63 です。 • **ip precedence** *new-precedence* には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。 指定できる範囲は 0 ～ 7 です。 （注） 割り当てられた DSCP または IP precedence 値を削除するには、**no set** {**dscp** *new-dscp* | **ip** precedence *new-precedence*} 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。
ステップ 7	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] 例： `Switch(config-pmap-c)# police 100000 80000 drop`	分類したトラフィックにポリサーを定義します。 デフォルトでは、ポリサーは定義されていません。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。 指定できる範囲は 8000 ～ 10000000000 です • *burst-byte* には、標準バースト サイズをバイト数で指定します。 指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。 （ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。 （注） 既存のポリサーを削除するには、**no police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}] 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。
ステップ 8	**exit** 例： `Switch(config-pmap-c)# 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。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `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 10	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 2/0/1`	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 11	**service-policy input** *policy-map-name* 例： `Switch(config-if)# service-policy input flowit`	ポリシー マップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。 （注） ポリシー マップとポートの対応付けを削除するには、**no service-policy** *input policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 12	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] 例： `Switch# show policy-map`	入力を確認します。
ステップ 14	**copy running-config startup-config** 例： `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。

関連トピック

クラス マップおよびポリシー マップに基づく分類，（12 ページ）
例：ポリシー マップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング，（88 ページ）

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

集約ポリサーを使用すると、同じポリシーマップ内の複数のトラフィック クラスで共有されるポリサーを作成できます。ただし、集約ポリサーを複数の異なるポリシーマップまたはポートにわたって使用することはできません。

集約ポリサーは、物理ポートの非階層型ポリシー マップにだけ設定できます。

手順の概要

1. **configure terminal**
2. **mls qos aggregate-policer** *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop** | **policed-dscp-transmit**}
3. **class-map** [**match-all** | **match-any**] *class-map-name*
4. **policy-map** *policy-map-name*
5. **class** [*class-map-name* | **class-default**]
6. **police aggregate** *aggregate-policer-name*
7. **exit**
8. **interface** *interface-id*
9. **service-policy input** *policy-map-name*
10. **end**
11. **show mls qos aggregate-policer** [*aggregate-policer-name*]
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos aggregate-policer** *aggregate-policer-name rate-bps burst-byte* **exceed-action** {**drop**	**policed-dscp-transmit**}	同じポリシーマップ内の複数のトラフィック クラスに適用できるポリサー パラメータを定義します。 デフォルトでは、集約ポリサーは定義されていません。

	コマンドまたはアクション	目的
	例： `Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action policed-dscp-transmit`	• *aggregate-policer-name* には、集約ポリサーの名前を指定します。 • *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。 指定できる範囲は 8000 ～ 10000000000 です • *burst-byte* には、標準バースト サイズをバイト数で指定します。 指定できる範囲は 8000 ～ 1000000 です。 • レートを超過した場合に実行するアクションを指定します。 パケットをドロップする場合は、**exceed-action drop** キーワードを使用します。（ポリシング済み DSCP マップを使用して）DSCP 値をマークダウンし、パケットを送信するには、**exceed-action policed-dscp-transmit** キーワードを使用します。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name* 例： `Switch(config)# class-map ipclass1`	必要に応じて、トラフィックを分類するクラス マップを作成します。
ステップ 4	**policy-map** *policy-map-name* 例： `Switch(config-cmap)# policy-map aggflow1`	ポリシーマップ名を入力することによってポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 5	**class** [*class-map-name* | **class-default**] 例： `Switch(config-cmap-p)# class ipclass1`	トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 6	**police aggregate** *aggregate-policer-name* 例： `Switch(configure-cmap-p)# police aggregate transmit1`	同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。 *aggregate-policer-name* には、ステップ 2 で指定した名前を入力します。 指定された集約ポリサーをポリシー マップから削除するには、**no police aggregate** *aggregate-policer-name* ポリシー マップ コンフィギュレーション コマンドを使用します。 集約ポリサーおよびそのパラメータを削除するには、**no mls qos**

	コマンドまたはアクション	目的
		aggregate-policer *aggregate-policer-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。
ステップ 7	**exit** 例： `Switch(configure-cmap-p)# 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	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 2/0/1`	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 9	**service-policy input** *policy-map-name* 例： `Switch(config-if)# service-policy input aggflow1`	ポリシー マップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 10	**end** 例： `Switch(configure-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show mls qos aggregate-policer** [*aggregate-policer-name*] 例： `Switch# show mls qos aggregate-policer transmit1`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `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。

関連トピック

物理ポートのポリシング，（14 ページ）

例：集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング，（89 ページ）

DSCP マップの設定

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。

CoS/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos map cos-dscp** *dscp1...dscp8*
3. **end**
4. **show mls qos maps cos-dscp**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos map cos-dscp** *dscp1...dscp8* 例： `Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45`	CoS/DSCP マップを変更します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。 各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。 （注） デフォルトのマップに戻すには、**no mls qos cos-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。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show mls qos maps cos-dscp** 例： `Switch# show mls qos maps cos-dscp`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `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。

関連トピック

マッピング テーブルの概要, （15 ページ）
例：DSCP マップの設定, （90 ページ）

IP precedence/DSCP マップの設定

着信パケットの IP precedence 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 値にマッピングするには、IP precedence/DSCP マップを使用します。

IP precedence/DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos map ip-prec-dscp** *dscp1...dscp8*
3. **end**
4. **show mls qos maps ip-prec-dscp**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos map ip-prec-dscp** *dscp1...dscp8* 例： `Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45`	IP precedence/DSCP マップを変更します。 *dscp1...dscp8* には、IP precedence 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。 各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ～ 63 です。 （注） デフォルトのマップに戻すには、**no mls qos ip-prec-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。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps ip-prec-dscp** 例： `Switch# show mls qos maps ip-prec-dscp`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `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。

関連トピック

マッピング テーブルの概要，（15 ページ）
例：DSCP マップの設定，（90 ページ）

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。

ポリシング済み DSCP マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp*
3. **end**
4. **show mls qos maps policed-dscp**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp* 例： `Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0`	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。 （注） デフォルトのマップに戻すには、**no mls qos policed-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。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**show mls qos maps policed-dscp** 例： `Switch(config)# show mls qos maps policed-dscp`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `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。

関連トピック

マッピング テーブルの概要，（15 ページ）
例：DSCP マップの設定，（90 ページ）

DSCP/CoS マップの設定

特権 EXEC モードで開始し、次の手順に従って DSCP/CoS マップを修正します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos map dscp-cos** *dscp-list* **to** *cos*
3. **end**
4. **show mls qos maps dscp-to-cos**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 2	**mls qos map dscp-cos** *dscp-list* **to** *cos* 例： `Switch# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0`	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、DSCP 値と対応する CoS 値を入力します。 DSCP の範囲は 0 ～ 63、CoS の範囲は 0 ～ 7 です。 （注） デフォルトのマップに戻すには、**no mls qos dscp-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	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps dscp-to-cos** 例： `Switch# show mls qos maps dscp-to-cos`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `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。

関連トピック

マッピング テーブルの概要，（15 ページ）
例：DSCP マップの設定，（90 ページ）

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します（入力変換）。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値をパケットに適用します。 スイッチは、新しい DSCP 値とともにそのパケットをポートへ送出します。

1 つの入力ポートに複数の DSCP/DSCP 変換マップを設定できます。 デフォルトの DSCP/DSCP 変換マップは、着信 DSCP 値を同じ DSCP 値にマッピングするヌル マップです。

DSCP/DSCP 変換マップを変更するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*
3. **interface** *interface-id*
4. **mls qos trust dscp**
5. **mls qos dscp-mutation** *dscp-mutation-name*
6. **end**
7. **show mls qos maps dscp-mutation**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp* 例： `Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0`	DSCP/DSCP 変換マップを変更します。 • *dscp-mutation-name* には、変換マップ名を入力します。新しい名前を指定することにより、複数のマップを作成できます。 • *in-dscp* 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。 • *out-dscp* には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ～ 63 です。 （注） デフォルトのマップに戻すには、**no mls qos dscp-mutation** *dscp-mutation-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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	**mls qos trust dscp** 例： `Switch(config-if)# mls qos trust dscp`	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name* 例： `Switch(config-if)# mls qos dscp-mutation mutation1`	指定された DSCP trusted 入力ポートにマップを適用します。 *dscp-mutation-name* には、ステップ 2 で指定した変換マップ名を入力します。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation** 例： `Switch# show mls qos maps dscp-mutation`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `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。

関連トピック

マッピング テーブルの概要，（15 ページ）
例：DSCP マップの設定，（90 ページ）

出力キューの特性の設定

ネットワークおよびQoS ソリューションの複雑さに応じて、次のモジュールで示す作業をすべて実行しなければならない場合があります。 次の特性を決定する必要があります。

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット（ポートごとの 4 つの出力キュー）に適用されるドロップしきい値の割合、およびトラフィック タイプに必要なメモリの確保量および最大メモリ
- キュー セットに割り当てる固定バッファ スペースの量
- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

設定時の注意事項

緊急キューがイネーブルにされているとき、またはSRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルで、SRR シェーピング重みが設定されていない場合、SRR はこのキューを共有モードで処理します。

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定

バッファのアベイラビリティの保証、WTD しきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* 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。

各しきい値はキューに割り当てられたバッファの割合です。このパーセント値を指定するには、**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* 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。 キューはWTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

キューセットのメモリ割り当てとドロップしきい値を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4*
3. **mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*
4. **interface** *interface-id*
5. **queue-set** *qset-id*
6. **end**
7. **show mls qos interface** [*interface-id*] **buffers**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* 例： `Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20`	バッファをキューセットに割り当てます。 デフォルトでは、すべての割り当て値は 4 つのキューに均等にマッピングされます（25、25、25、25）。 各キューがバッファ スペースの 1/4 を持ちます。 • *qset-id* には、キューセットの ID を入力します。 指定できる範囲は 1 ～ 2 です。 各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。 • *allocation1 ... allocation4* には、キューセット内のキューごとに 1 つずつ、合計 4 つのパーセンテージを指定します。 *allocation1*、*allocation3*、*allocation4* の場合、使用可能な範囲は 0 ～ 99 です。 *allocation2* の場合、範囲は 1 ～ 100 です（CPU バッファを含める）。

	コマンドまたはアクション	目的
		トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。 （注） デフォルトの設定に戻すには、**no mls qos queue-set output** *qset-id* **buffers** 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	**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold* 例： `Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200`	WTD しきい値を設定し、バッファのアベイラビリティを保証し、キューセット（ポートごとに 4 つの出力キュー）の最大メモリ割り当てを設定します。 デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定されています。 キュー 2 の WTD は 200% に設定されています。 キュー 1、2、3、および 4 の専用は 50% に設定されています。 すべてのキューの最大しきい値はデフォルトで 400% に設定されています。 • *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。 指定できる範囲は 1 ～ 2 です。 • *queue-id* には、コマンドの実行対象となるキューセット内の特定のキューを入力します。 指定できる範囲は 1 ～ 4 です。 • *drop-threshold1 drop-threshold2* には、キューの割り当てメモリの割合として表される 2 つの WTD しきい値を指定します。 指定できる範囲は 1 ～ 3200% です。 • *reserved-threshold* には、割り当てメモリの割合として表されるキューに保証（確保）されるメモリ サイズを入力します。 指定できる範囲は 1 ～ 100% です。 • *maximum-threshold* を指定すると、いっぱいになったキューが確保量を超えるバッファを取得できるようになります。 この値は、共通プールが空でない場合に、パケットがドロップされるまでキューが使用できるメモリの最大値です。 指定できる範囲は 1 ～ 3200% です。 （注） デフォルトの WTD の割合に戻すには、**no mls qos queue-set output** *qset-id* **threshold** [*queue-id*] 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 4	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	発信トラフィックのポートを指定し、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。

	コマンドまたはアクション	目的
ステップ 5	**queue-set** *qset-id* 例： `Switch(config-id)# queue-set 2`	キューセットにポートをマッピングします。 *qset-id* には、ステップ 2 で指定したキューセットの ID を入力します。指定できる範囲は 1 ～ 2 です。 デフォルトは 1 です。
ステップ 6	**end** 例： `Switch(config-id)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos interface** [*interface-id*] **buffers** 例： `Switch# show mls qos interface buffers`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `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。 デフォルトの設定に戻すには、**no mls qos queue-set output** *qset-id* **buffers** 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。 デフォルトの WTD しきい値の割合に戻すには、**no mls qos queue-set output** *qset-id* **threshold** [*queue-id*] 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。

関連トピック

WTD, （17 ページ）
キューおよび WTD しきい値, （22 ページ）
例：出力キューの特性の設定, （92 ページ）

出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング

トラフィックにプライオリティを設定するには、特定の DSCP または CoS を持つパケットを特定のキューに格納し、より低いプライオリティを持つパケットがドロップされるようにキューのしきい値を調整します。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 デフォルト設定の変更が必要となるのは、出力キューについて完全に理解している場合、およびデフォルトの設定がご使用の QoS ソリューションを満たしていない場合だけです。

DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. 次のいずれかを使用します。
   - **mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8*
   - **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*
3. **end**
4. **show mls qos maps**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	次のいずれかを使用します。 • **mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* • **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8* 例： `Switch(config)# mls qos`	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 15 はキュー 2 およびしきい値 1 に、DSCP 値 16 ～ 31 はキュー 3 およびしきい値 1 に、 DSCP 値 32 ～ 39 および 48 ～ 63 はキュー 4 およびしきい値 1 に、 DSCP 値 40 ～ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、 CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、 CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 に、 CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 4 です。

	コマンドまたはアクション	目的
	`srr-queue output dscp-map queue 1 threshold 2 10 11`	• *threshold-id* で指定できる範囲は 1 ～ 3 です。 しきい値 3 のドロップしきい値（%）は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • *dscp1...dscp8* には、各値をスペースで区切って、最大 8 の値を入力します。 指定できる範囲は 0 ～ 63 です。 • *cos1...cos8* には、最大 8 個の値をスペースで区切って入力します。指定できる範囲は 0 ～ 7 です。 （注） デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、**no mls qos srr-queue output dscp-map** または no mls qos srr-queue output cos-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。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps** 例： `Switch# show mls qos maps`	入力を確認します。 DSCP 出力キューしきい値マップは、表形式で表示されます。 d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。 d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1（02-01）のようになります。 CoS 出力キューしきい値マップでは、先頭行に CoS 値、2 番めの行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2（2-2）のようになります。
ステップ 5	**copy running-config startup-config** 例： `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 DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、**no mls qos srr-queue output dscp-map** または **no mls qos srr-queue output cos-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。

関連トピック

キューおよび WTD しきい値, （22 ページ）
例：出力キューの特性の設定, （92 ページ）

出力キューでの SRR シェーピング重みの設定

各キューに割り当てられる使用可能な帯域幅の量を指定できます。 重みの比率は、SRR スケジューラが各キューからパケットを送信する頻度の比率です。

出力キューにシェーピング重み、共有重み、またはその両方を設定できます。 バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。

ポートにマッピングされた 4 つの出力キューにシェーピング重みを割り当てて、帯域幅のシェーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **srr-queue bandwidth shape** *weight1 weight2 weight3 weight4*
4. **end**
5. **show mls qos interface** *interface-id* **queueing**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	発信トラフィックのポートを指定し、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 3	**srr-queue bandwidth shape** *weight1 weight2 weight3 weight4* 例： `Switch(config-if)# srr-queue bandwidth shape 8 0 0 0`	出力キューに SRR 重みを割り当てます。 デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 *weight1 weight2 weight3 weight4* には、シェーピングされるポートの割合を制御する重みを入力します。 このキューのシェーピング帯域幅は、インバース比率（1/weight）によって制御されます。 各値はスペースで区切ります。 指定できる範囲は 0 ～ 65535 です。

	コマンドまたはアクション	目的
		重み 0 を設定した場合は、対応するキューが共有モードで動作します。 **srr-queue bandwidth shape** コマンドで指定された重みは無視され、**srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。シェーピングおよび共有の両方に対して同じキューセットのキューを設定した場合は、必ず番号が最も小さいキューにシェーピングを設定してください。 シェーピング モードは、共有モードを無効にします。 デフォルトの設定に戻すには、**no srr-queue bandwidth shape** 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。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing** 例： `Switch# show mls qos interface interface-id queuing`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `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。 デフォルトの設定に戻すには、**no srr-queue bandwidth shape** 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。

関連トピック

シェーピング モードまたは共有モード，（23 ページ）
SRR のシェーピングおよび共有，（18 ページ）
例：出力キューの特性の設定，（92 ページ）

出力キューでの SRR 共有重みの設定

共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。 このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。 たとえば、特定のキューが空であ

り、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有ができます。 共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

ポートにマッピングされた 4 つの出力キューに共有重みを割り当てて、帯域幅の共有をイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **srr-queue bandwidth share** *weight1 weight2 weight3 weight4*
4. **end**
5. **show mls qos interface** *interface-id* **queueing**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	発信トラフィックのポートを指定し、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 3	**srr-queue bandwidth share** *weight1 weight2 weight3 weight4* 例： `Switch(config-id)# srr-queue bandwidth share 1 2 3 4`	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です（各キューに帯域幅の 1/4 が割り当てられています）。 *weight1 weight2 weight3 weight4* には、SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。 指定できる範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
		デフォルトの設定に戻すには、**no srr-queue bandwidth share** 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。
ステップ 4	**end** 例： `Switch(config-id)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing** 例： `Switch# show mls qos interface interface_id queuing`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `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。 デフォルトの設定に戻すには、**no srr-queue bandwidth share** 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。

関連トピック

シェーピング モードまたは共有モード，（23 ページ）
SRR のシェーピングおよび共有，（18 ページ）
例：出力キューの特性の設定，（92 ページ）

出力緊急キューの設定

出力緊急キューにパケットを入れることにより、特定のパケットのプライオリティを他のすべてのパケットより高く設定できます。 SRR は、このキューが空になるまで処理してから他のキューを処理します。

出力緊急キューをイネーブルにするには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **mls qos**
3. **interface** *interface-id*
4. **priority-queue out**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**mls qos** 例： `Switch(config)# mls qos`	スイッチの QoS をイネーブルにします。
ステップ 3	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	出力ポートを指定し、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 4	**priority-queue out** 例： `Switch(config-if)# priority-queue out`	デフォルトでディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。つまり、**srr-queue bandwidth shape** または **srr-queue bandwidth share** コマンドの *weight1* が無視されます（比率計算に使用されません）。 （注） 出力緊急キューをディセーブルにするには、**no priority-queue out** 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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `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。 出力緊急キューをディセーブルにするには、**no priority-queue out** 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。

関連トピック

出力緊急キュー，（21 ページ）
例：出力キューの特性の設定，（92 ページ）

出力インターフェイスの帯域幅の制限

出力ポートの帯域幅は制限できます。 たとえば、カスタマーが高速リンクの一部しか費用を負担しない場合は、帯域幅をその量に制限できます。

（注） 出力キューのデフォルト設定は、ほとんどの状況に適しています。 出力キューについて十分理解したうえで、この設定がユーザの QoS ソリューションを満たさないと判断した場合に限り、設定を変更してください。

出力ポートの帯域幅を制限するには、特権 EXEC モードで次の手順を実行します。 この手順は任意です。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **srr-queue bandwidth limit** *weight1*
4. **end**
5. **show mls qos interface** [*interface-id*] **queueing**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet2/0/1`	レートを制限するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**srr-queue bandwidth limit** *weight1* 例： `Switch(config-if)# srr-queue bandwidth limit 80`	ポートの上限となるポート速度の割合を指定します。 指定できる範囲は 10 ～ 90 です。 デフォルトでは、ポートのレートは制限されず、100% に設定されています。 （注） デフォルトの設定に戻すには、**no srr-queue bandwidth limit** 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。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*] **queueing** 例： `Switch# show mls qos interface interface_id queueing`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `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。 デフォルトの設定に戻すには、**no srr-queue bandwidth limit** 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。

関連トピック

例：出力キューの特性の設定，（92 ページ）

標準 QoS のモニタリング

表 *10*：スイッチ上で標準 *QoS* をモニタリングするためのコマンド

コマンド	説明
show class-map [*class-map-name*]	トラフィックを分類するための一致基準を定義した QoS クラス マップを表示します。
show mls qos	グローバル QoS コンフィギュレーション情報を表示します。
show mls qos aggregate-policer [*aggregate-policer-name*]	集約ポリサーの設定を表示します。
show mls qos interface [*interface-id*] [**buffers** | **policers** | **queueing** | **statistics**]	バッファ割り当て、ポリサーが設定されているポート、キューイング方式、入出力統計情報など、ポート レベルの QoS 情報が表示されます。
show mls qos maps [**cos-dscp** | |**cos-output-q** | **dscp-cos** | |**dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	QoS のマッピング情報を表示します。
show mls qos queue-set [*qset-id*]	出力キューの QoS 設定を表示します。

コマンド	説明
show policy-map [*policy-map-name* [**class** *class-map-name*]]	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。 着信トラフィックの分類情報を表示する場合は、**show policy-map interface** 特権 EXEC コマンドを使用しないでください。 **control-plane** および **interface** キーワードはサポートされていません。表示される統計情報は無視してください。
show running-config | include rewrite	DSCP 透過性設定を表示します。

QoS の設定例

例：DSCP 信頼状態へのポートの設定および DSCP/DSCP 変換マップの変更

次に、ポートが DSCP を信頼する状態に設定し、着信した DSCP 値 10 ～ 13 が DSCP 値 30 にマッピングされるように DSCP/DSCP 変換マップ（*gi1/0/2-mutation*）を変更する例を示します。

```
Switch(config)# mls qos map dscp-mutation gigabitethernet1/0/2-mutation
10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gigabitethernet1/0/2-mutation
Switch(config-if)# end
```

関連トピック

マッピング テーブルの概要, （15 ページ）

例：ACL によるトラフィックの分類

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。 ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。 アクセス リストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

```
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)
```

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

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

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

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

次に、任意の送信元からアドレス 224.0.0.2 の宛先グループへの PIM トラフィック（DSCP 値は 32）を許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
```

次に、任意の送信元から、DSCP 値が 32 に設定されている任意の宛先への IPv6 トラフィックを許可する ACL を作成する例を示します。

```
Switch(config)# ipv6 access-list 100 permit ip any any dscp 32
```

次に、10.1.1.1 の送信元ホストから 10.1.1.2 の宛先ホストへの IPv6 トラフィック（precedence 値は 5）を許可する ACL を作成する例を示します。

```
Switch(config)# ipv6 access-list ipv6_Name_ACL permit ip host 10::1 host 10.1.1.2
precedence 5
```

次に、2 つの許可（permit）ステートメントを指定したレイヤ 2 の MAC ACL を作成する例を示します。 最初のステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。 2 番めのステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

関連トピック

IPv4 トラフィック用の IP 標準 ACL の作成, （41 ページ）
IPv4 トラフィック用の IP 拡張 ACL の作成, （43 ページ）
IPv6 トラフィック用の IPv6 ACL の作成, （45 ページ）
非 IP トラフィック用のレイヤ 2 MAC ACL の作成, （47 ページ）
QoS ACL の注意事項, （2 ページ）

例：クラス マップによるトラフィックの分類

次に、*class1* というクラス マップの設定例を示します。 *class1* にはアクセス リスト 103 という一致条件が 1 つ設定されています。 このクラス マップによって、任意のホストから任意の宛先へのトラフィック（DSCP 値は 10）が許可されます。

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

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

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

次に、IP precedence 値が 5、6、および 7 である着信トラフィックと照合する、*class3* という名前のクラス マップを作成する例を示します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```

次に、IP DSCP および IPv6 と照合するクラス マップを設定する例を示します。

```
Switch(config)# Class-map cm-1
Switch(config-cmap)# match ip dscp 10
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# Class-map cm-2
Switch(config-cmap)# match ip dscp 20
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# Policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G1/0/1
Switch(config-if)# service-policy input pm1
```

次に、IPv4 トラフィックと IPv6 トラフィックの両方に適用するクラス マップを設定する例を示します。

```
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# Class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
```

```
Switch(config-cmap)# exit
Switch(config)# Policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

関連トピック

クラス マップによるトラフィックの分類, （49 ページ）
クラス マップおよびポリシー マップに基づく分類, （12 ページ）

例：ポリシーマップを使用した物理ポートのトラフィックの分類、ポリシング、およびマーキング

次に、ポリシー マップを作成し、入力ポートに結合する例を示します。 この設定では、IP 標準 ACL でネットワーク 10.1.0.0 からのトラフィックを許可します。 この分類にトラフィックが一致した場合、着信パケットの DSCP 値が信頼されます。 一致したトラフィックが平均トラフィック レート（48000 bps）、および標準バースト サイズ（8000 バイト）を超過している場合は、（ポリシング済み DSCP マップに基づいて）DSCP はマークダウンされて、送信されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input flow1t
```

次に、2 つの許可ステートメントを指定してレイヤ 2 MAC ACL を作成し、入力ポートに結合する例を示します。 最初の許可ステートメントでは、MAC アドレスが 0001.0000.0001 であるホストから、MAC アドレスが 0002.0000.0001 であるホストへのトラフィックが許可されます。 2 番めの許可ステートメントでは、MAC アドレスが 0001.0000.0002 であるホストから、MAC アドレスが 0002.0000.0002 であるホストへの、Ethertype が XNS-IDP のトラフィックのみが許可されます。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
```

```
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

次に、分類されていないトラフィックに適用されるデフォルト クラスを使用して、IPv4 と IPv6 の両方のトラフィックに適用されるクラス マップを作成する例を示します。

```
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

関連トピック

ポリシーマップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング，（55 ページ）

クラス マップおよびポリシー マップに基づく分類，（12 ページ）

例：集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

次に、集約ポリサーを作成して、ポリシーマップ内の複数のクラスに結合する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。 ネットワーク 10.1.0.0 から着信するトラフィックの場合は、着信パケットの DSCP が信頼されます。 ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。 ネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。 トラフィックが平均レート（48000 bps）、および標準バースト サイズ（8000

バイト）を超過している場合は、（ポリシング済み DSCP マップに基づいて）DSCP がマークダウンされて、送信されます。 ポリシー マップは入力ポートに結合されます。

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action
policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

関連トピック

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング，（60 ページ）
物理ポートのポリシング，（14 ページ）

例：DSCP マップの設定

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

次に、IP precedence/DSCP マップを変更して表示する例を示します。

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   10 15 20 25 30 35 40 45
```

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(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
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） このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。 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。

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(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls 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 値が表形式で示されています。 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。

次の例では、DSCP/DSCP 変換マップを定義する方法を示します。 明示的に設定されていないすべてのエントリは変更されません（空のマップで指定された値のままです）。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
   mutation1:
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
```

```
----------------------------------------
 0 :    00 00 00 00 00 00 00 00 10 10
 1 :    10 10 10 10 14 15 16 17 18 19
 2 :    20 20 20 23 24 25 26 27 28 29
 3 :    30 30 30 30 30 35 36 37 38 39
 4 :    40 41 42 43 44 45 46 47 48 49
 5 :    50 51 52 53 54 55 56 57 58 59
 6 :    60 61 62 63
```

（注） 上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。 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 の交点の値が、変換される値です。 たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

関連トピック

CoS/DSCP マップの設定，（63 ページ）
IP precedence/DSCP マップの設定，（64 ページ）
ポリシング済み DSCP マップの設定，（66 ページ）
DSCP/CoS マップの設定，（67 ページ）
DSCP/DSCP 変換マップの設定，（68 ページ）
マッピング テーブルの概要，（15 ページ）

例：出力キューの特性の設定

次の例では、ポートをキューセット 2 にマッピングする方法を示します。 出力キュー 1 にはバッファ スペースの 40%、出力キュー 2、3、および 4 には 20% が割り当てられます。 キュー 2 のドロップしきい値は割り当てメモリの 40 および 60% に設定され、割り当てメモリの 100% が保証（確保）され、パケットがドロップされるまでこのキューが使用できる最大メモリが 200% に設定されます。

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# queue-set 2
```

次に、DSCP 値 10 および 11 を出力キュー 1 およびしきい値 2 にマッピングする例を示します。

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

次に、キュー 1 に帯域幅のシェーピングを設定する例を示します。 キュー 2、3、4 の重み比が 0 に設定されているので、これらのキューは共有モードで動作します。 キュー 1 の帯域幅の重みは 1/8（12.5%）です。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

次の例では、出力ポートで稼働する SRR スケジューラの重み比を設定する方法を示します。 4 つのキューが使用され、共有モードで各キューに割り当てられる帯域幅の比率は、キュー1、2、3、

および 4 に対して 1/(1 + 2 + 3 + 4)、2/(1 + 2 + 3 + 4)、3/(1 + 2 + 3 + 4)、および 4/(1 + 2 + 3 + 4) になります（それぞれ、10、20、30、および 40%）。 キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。 出力緊急キューは、設定された SRR ウェイトを上書きします。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

次に、ポートの帯域幅を 80% に制限する例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定すると、ポートは該当期間の 20% はアイドルになります。 回線レートは接続速度の 80%（800 Mbps）に低下します。 ただし、ハードウェアはライン レートを 6%単位で調整しているため、この値は厳密ではありません。

関連トピック

出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定, （71 ページ）
WTD, （17 ページ）
キューおよび WTD しきい値, （22 ページ）
出力キューでの SRR シェーピング重みの設定, （77 ページ）
出力キューでの SRR 共有重みの設定, （78 ページ）
シェーピング モードまたは共有モード, （23 ページ）
SRR のシェーピングおよび共有, （18 ページ）
出力緊急キューの設定, （80 ページ）
出力緊急キュー, （21 ページ）
出力インターフェイスの帯域幅の制限, （82 ページ）
出力キューおよびしきい値 ID への DSCP または CoS 値のマッピング, （74 ページ）
キューおよび WTD しきい値, （22 ページ）

次の作業

QoS 設定でこれらの自動機能を使用できるかどうかについては、自動 QoS のマニュアルを参照してください。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
このマニュアルで使用するコマンドの構文および使用方法の詳細。	*Catalyst 2960-X Switch Quality of Service Command Reference*

標準および RFC

標準/RFC	タイトル
—	—

MIB

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

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

QoS の機能履歴と情報

リリース	変更内容
Cisco IOS 15.0(2)EX	この機能が導入されました。