CHAPTER 39

QoS の設定

この章では、IE 3000 スイッチで Automatic QoS（auto-QoS）コマンドを使用して、または標準 QoS コマンドを使用して Quality of Service（QoS; サービス品質）を設定する手順について説明します。QoS を使用すると、特定のタイプのトラフィックを他のトラフィックよりも優先的に処理することができます。QoS を使用しないと、パケットの内容やサイズにかかわらず、スイッチは各パケットにベストエフォートサービスを提供します。パケットは、信頼性、遅延限界、またはスループットが保証されない状態で送信されます。QoS は、物理ポートおよび Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）で設定できます。ポリシー マップを適用するだけではなく、分類、キューイング、スケジューリングなどの QoS 設定を、物理ポートと SVI で同様に設定します。物理ポートで QoS を設定する場合は、非階層ポリシー マップをポートに適用します。SVI で QoS を設定する場合は、非階層または階層ポリシー マップを適用します。Catalyst 3750 Metro スイッチのドキュメンテーションでは、非階層ポリシー マップは非階層シングルレベル ポリシー マップと呼ばれ、階層ポリシー マップは階層デュアルレベル ポリシー マップと呼ばれます。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

このスイッチは、一部の Modular QoS CLI（MQC; モジュラー QoS コマンドライン インターフェイス）コマンドをサポートしています。MQC コマンドの詳細については、次の URL の「Modular Quality of Service Command-Line Interface Overview」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd908.html

QoS の概要

ネットワークは通常、ベスト エフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、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。輻輳が発生した場合に廃棄される可能性についても、すべてのトラフィックで同等です。

QoS 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、その相対的な重要度に基づいてプライオリティを設定し、輻輳管理および輻輳回避技術を使用して優先的に処理することができます。QoS をネットワークに実装することで、ネットワーク パフォーマンスが予測しやすくなり、帯域幅をより効率的に利用できるようになります。

QoS の実装は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）の新しい標準である Differentiated Service（Diff-Serv; ディファレンシエーテッド サービス）アーキテクチャに基づいて行われます。このアーキテクチャは、各パケットがネットワークに入るときに分類されることを既定してします。

この分類は IP パケット ヘッダー内で、非推奨の IP Type of Service（ToS; サービス タイプ）フィールドの 6 ビットを使用して、分類（クラス）情報として伝送されます。分類はレイヤ 2 フレームでも伝送できます。レイヤ 2 フレームまたはレイヤ 3 パケットのこれらの特別なビットについてここで説明し、図 39-1 に示します。

- レイヤ 2 フレームのプライオリティ ビット：

  レイヤ 2 Inter-Switch Link（ISL; スイッチ間リンク）フレーム ヘッダーには、Class of Service（CoS; サービス クラス）値の IEEE 802.1p クラスを最下位 3 ビットで 伝送する、1 バイトの User 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は ISL フレームに含まれます。

  レイヤ 2 IEEE 802.1Q フレーム ヘッダーには、ユーザ プライオリティ ビットと呼ばれる最上位 3 ビットで CoS 値を伝送する 2 バイトの Tag Control Information フィールドがあります。レイヤ 2 IEEE 802.1Q トランクとして設定されたポートでは、ネイティブ VLAN のトラフィックを除き、全てのトラフィックは IEEE 802.1Q フレームに含まれます。

  その他のフレーム タイプはレイヤ 2 CoS 値を伝送できません。

  レイヤ 2 CoS 値は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）の範囲で指定できます。

- レイヤ 3 パケットのプライオリティ ビット：

  レイヤ 3 IP パケットは、IP precedence 値または Differentiated Services Code Point（DSCP）値を伝送できます。DSCP 値には IP precedence 値との下位互換性があるため、QoS はいずれの値の使用もサポートします。

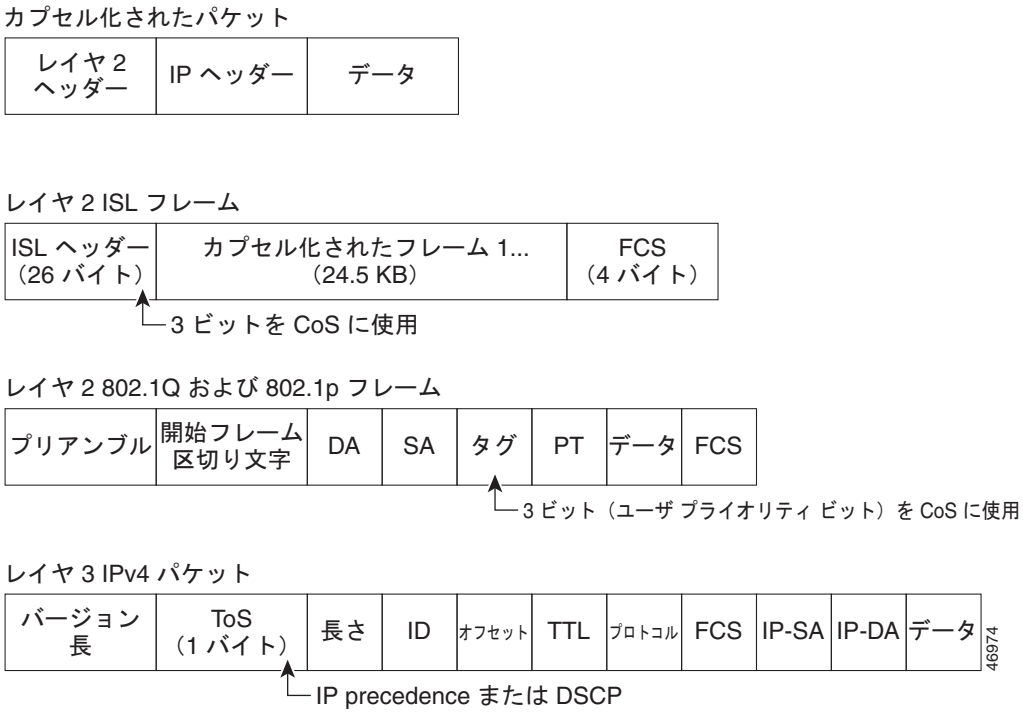
  IP precedence 値の範囲は 0 ～ 7 です。

  DSCP 値の範囲は 0 ～ 63 です。

（注） Cisco IOS Release 12.2(52)SE 以降は、デュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを使用した、IPv6 ポートベースの信頼をサポートします。IPv6 を実行しているスイッチでは、デュアル IPv4/IPv6 テンプレートを使用してスイッチをリロードしなければなりません。詳細については、第 10 章「SDM テンプレートの設定」を参照してください。

（注） IPv6 QoS はこのリリースではサポートされていません。

図 39-1　フレームおよびパケットの QoS 分類レイヤ



インターネットにアクセスするすべてのスイッチとルータは、クラス情報に基づいて、同じクラス情報を持つパケットは同じ方法で転送処理し、異なるクラス情報を持つパケットは異なる処理をします。パケットのクラス情報は、設定済みのポリシー、パケットの詳細な確認、またはその両方に基づいて、エンド ホストにより、または転送中にスイッチやルータにより、割り当てることができます。パケットの詳細な確認は、コア スイッチやルータがこの作業で過負荷にならないように、ネットワークのエッジの近くで行われます。

パス上のスイッチとルータは、クラス情報を使用して、トラフィック クラスごとに割り当てるリソースの量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの個々の装置の動作は、Per-Hop Behavior（PHB）と呼ばれます。パス上のすべての装置が一貫した PHB を提供することにより、エンドツーエンドの QoS ソリューションを構築できます。

ネットワークに QoS を実装する作業は、インターネットワーキング装置により提供される 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、また、着信および発信トラフィックに必要な制御の細かさのレベルによって、単純にも複雑にもなります。

基本的な QoS モデル

QoS を実装するには、スイッチが個々のパケットまたはフローを区別（分類）し、パケットがスイッチを通過するときに特定のサービス品質を示すためのラベルを割り当て、設定済みのリソースの使用限界にパケットが準拠するようにし（ポリシングおよびマーキング）、リソースの競合が発生するすべての状況でさまざまな処理を提供する（キューイングおよびスケジューリング）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（シェイピング）必要もあります。

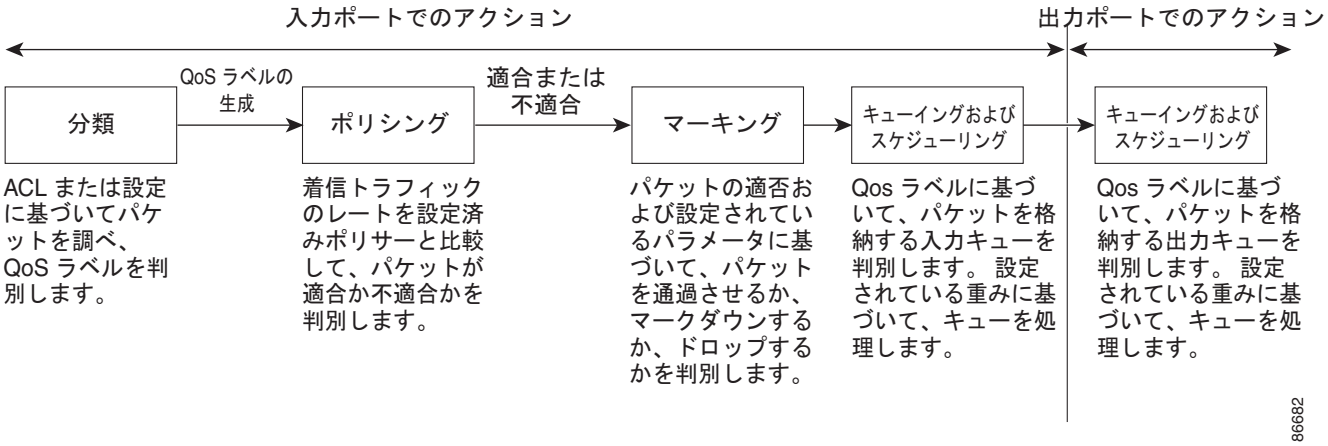
図 39-2 に、基本的な QoS モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、スケジューリングが含まれます。

- 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、トラフィックの種類を区別します。生成される QoS ラベルは、このパケットで今後実行されるすべての QoS アクションを識別します。詳細については、「分類」（P.39-5）を参照してください。
- ポリシングでは、着信トラフィックのレートを設定済みのポリサーと比較することにより、パケットがプロファイル内かプロファイル外かを判別します。ポリサーは、トラフィック フローにより消費される帯域幅を制限します。その結果はマーカに渡されます。詳細については、「ポリシングおよびマーキング」（P.39-9）を参照してください。
- マーキングでは、パケットがプロファイル外のときに実行するアクションのポリサーおよび設定情報を評価し、パケットの処理（無修正でのパケットの通過、パケット内の QoS ラベルのマークダウン、またはパケットの廃棄）を決定します。詳細については、「ポリシングおよびマーキング」（P.39-9）を参照してください。
- キューイングでは、QoS ラベルとそれに対応する DSCP または CoS 値を評価し、2 つの入力キューのどちらにパケットを格納するかを選択します。キューイングは、輻輳回避メカニズムである Weighted Tail-Drop（WTD）アルゴリズムにより拡張されています。スレッシュホールドを超えると、パケットは廃棄されます。詳細については、「キューイングとスケジューリングの概要」（P.39-14）を参照してください。
- スケジュールでは、設定された Shaped Round Robin（SRR; シェイプド ラウンド ロビン）の重みに基づいてキューを処理します。入力キューの 1 つはプライオリティ キューであり、SRR は他のキューを処理する前に、設定済みの共有に従いプライオリティ キューを処理します。詳細については、「SRR のシェーピングおよび共有」（P.39-15）を参照してください。

出力ポートでのアクションには、キューイングとスケジューリングがあります。

- キューイングでは、4 つの出力キューのどれを使用するかを選択する前に、QoS パケット ラベルとそれに対応する DSCP または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートにデータを同時に送信すると輻輳が発生するため、WTD でトラフィック クラスを区別し、QoS ラベルに基づいてパケットに異なるスレッシュホールドを適用します。スレッシュホールドを超えると、パケットは廃棄されます。詳細については、「キューイングとスケジューリングの概要」（P.39-14）を参照してください。
- スケジューリングでは、設定済みの SRR の共有された、またはシェーピングされた重みに基づいて 4 つの出力キューを処理します。キューの 1 つ（キュー 1）を緊急キューにできます。緊急キューは、他のキューを処理する前に、空になるまで処理されます。

図 39-2　基本的な QoS モデル



分類

分類は、パケットのフィールドを確認することで、トラフィックの種類を区別するプロセスです。分類は、スイッチで QoS がグローバルにイネーブルになっている場合に限りイネーブルになります。デフォルトでは、QoS はグローバルにディセーブルになるため、分類は行われません。

分類中にスイッチは検索を行い、QoS ラベルをパケットに割り当てます。QoS ラベルは、パケットに対して実行されるすべての QoS アクションと、パケットの送信元のキューを識別します。

QoS ラベルは、パケットの DSCP または CoS 値に基づいており、そのパケットに対して実行されるキューイング アクションとスケジューリング アクションを決定します。図 39-3（P.39-7）に示すように、ラベルは信頼設定とパケット タイプに応じてマッピングされます。

着信トラフィックの分類に使用するフレームまたはパケットのフィールドは、ユーザが指定します。非 IP トラフィックでは、図 39-3 に示す分類オプションがあります。

- 着信フレームの CoS 値を信頼します（CoS を信頼するようにポートを設定する）。次に、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 ISL フレーム ヘッダーは、1 バイトの User フィールドの最下位 3 ビットで CoS 値を伝送します。レイヤ 2 IEEE 802.1Q フレーム ヘッダーは、Tag Control Information フィールドの最上位 3 ビットで CoS 値を伝送します。CoS 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。
- 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 トラフィックでは意味がありません。これらのいずれかのオプションを使用してポートを設定したときに非 IP トラフィックを受信すると、スイッチは CoS 値を割り当て、CoS/DSCP マップから内部 DSCP 値を生成します。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す CoS 値を生成します。
- 設定されたレイヤ 2 MAC Access Control List（ACL; アクセス制御リスト）に基づいて分類を行います。この場合、MAC 送信元アドレス、MAC 宛先アドレス、その他のフィールドを確認できます。ACL が設定されていない場合は、DSCP および CoS 値としてパケットに 0 が割り当てられます。これはベストエフォート トラフィックを意味します。ACL が設定されている場合は、ポリシーマップ アクションが DSCP または CoS 値を指定し、着信フレームに割り当てます。

IP トラフィックでは、図 39-3 に示す分類オプションがあります。

- 着信パケットの DSCP 値を信頼（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 フィールドの最上位 6 ビットを DSCP として定義します。特定の DSCP 値によって表されるプライオリティは設定が可能です。DSCP 値の範囲は 0 ～ 63 です。

  2 つの QoS 管理ドメイン間の境界にあるポートでは、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に修正できます。

- 着信パケットの IP precedence 値を信頼（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 Version 4 の仕様では、1 バイトの ToS フィールドの最上位 3 ビットを IP precedence として定義しています。IP precedence 値の範囲は、0（ロー プライオリティ）～ 7（ハイ プライオリティ）です。

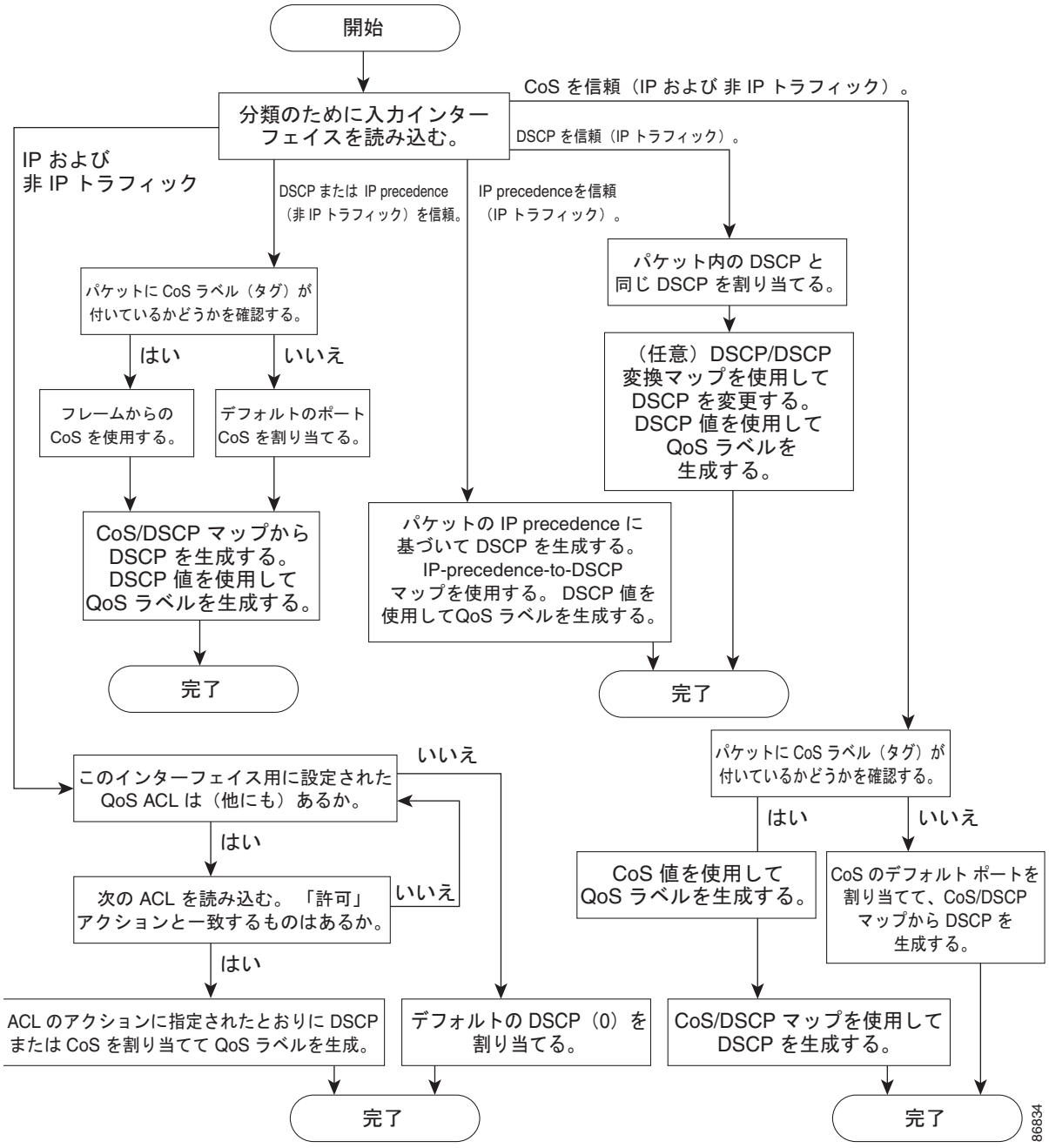
- 着信パケットの CoS 値（ある場合）を信頼し、CoS/DSCP マップを使用することで、パケットの DSCP 値を生成します。CoS 値がない場合は、デフォルトのポート CoS 値を使用します。

- 設定された IP 標準 ACL または拡張された ACL に基づいて分類を行います。この場合、IP ヘッダーのさまざまなフィールドを確認します。ACL が設定されていない場合は、DSCP および CoS 値としてパケットに 0 が割り当てられます。これはベストエフォート トラフィックを意味します。ACL が設定されている場合は、ポリシーマップ アクションが DSCP または CoS 値を指定し、着信フレームに割り当てます。

このセッションで説明したマップについては、「マッピング テーブル」（P.39-13）を参照してください。ポートの信頼状態の設定については、「ポートの信頼状態を使用した分類の設定」（P.39-38）を参照してください。

分類後、パケットはポリシング、マーキング、入力キューイングおよびスケジューリングの各段階に送信されます。

図 39-3　分類のフローチャート



QoS ACL に基づく分類

IP 標準 ACL、IP 拡張 ACL、またはレイヤ 2 MAC ACL を使用して、同じ特性を持つパケットのグループ（クラス）を定義できます。QoS のコンテキストでは、Access Control Entry（ACE; アクセス制御エントリ）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発生すると（最初の一致の原則）、指定された QoS に関連するアクションが実行されます。
- 拒否アクションとの一致が発生すると、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発生しないまま、すべての ACE の確認が終了すると、パケットでは QoS の処理は行われず、スイッチはパケットにベストエフォートサービスを提供します。
- 複数の ACL がポートで設定されている場合は、許可アクションを使用する最初の ACL にパケットが一致した後に検索が停止し、QoS 処理が開始されます。

（注）　アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。

トラフィック クラスが ACL を使用して定義された後、このクラスにポリシーを付加できます。ポリシーには、それぞれ指定されたアクションを持つ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）、またはクラスをレート制限するコマンドが含まれることがあります。次に、このポリシーを特定のポートに付加すると、その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には、**access-list** グローバル コンフィギュレーション コマンドを使用してします。レイヤ 2 MAC ACL を実装して 非 IP トラフィックを分類するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します、設定の詳細については、「QoS ポリシーの設定」（P.39-44）を参照してください。

クラス マップとポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）を指定し、これを他のすべてのトラフィックから分離するために使用するメカニズムです。クラス マップでは、さらに詳細に分類するために、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 によって定義されるアクセス グループとの照合や、DSCP または 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。分類するトラフィックのタイプが 2 つ以上ある場合は、別のクラス マップを作成して別の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 マップは、対象のトラフィック クラスを指定します。アクションには、トラフィック クラスの CoS、DSCP、または IP precedence 値の信頼、トラフィック クラスの特定への DSCP または IP precedence 値の設定、またはトラフィック帯域幅の制限と、トラフィックがプロファイル外のときに実行するアクションの指定などが含まれます。ポリシー マップを有効にするには、あらかじめこれをポートに付加する必要があります。

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 コマンドを作成します。多くのポートでマップを共有する場合は、**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、スイッチはクラスマップ コンフィギュレーション モードに入ります。このモードでは、**match** クラスマップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

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。分類されないトラフィック（トラフィック クラスで指定されている一致基準に適合しないトラフィック）は、デフォルト トラフィックとして処理されます。

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、ポリシー マップを作成し、名前を指定します。このコマンドを入力すると、スイッチはポリシーマップ コンフィギュレーション モードに入ります。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の制限、制限を超えたときに実行する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ができます。

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付加します。

非階層ポリシー マップは物理ポートまたは SVI に適用できます。ただし、階層ポリシー マップは SVI だけに適用できます。階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。2 つ目はインターフェイス レベルで、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。インターフェイスレベルのアクションは、インターフェイスレベルのポリシー マップで指定されます。

詳細については、「ポリシングおよびマーキング」（P.39-9）を参照してください。設定の詳細については、「QoS ポリシーの設定」（P.39-44）を参照してください。

ポリシングおよびマーキング

パケットを分類し、DSCP または CoS ベースの QoS ラベルを割り当てた後、図 39-4 に示すように、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含まれます。限度を超えたパケットは、*プロファイル外*または*不適合*と見なされます。各ポリサーは、パケットがプロファイル内かプロファイル外かをパケットごとに確認し、パケットに対するアクションを指定します。マーカによって実行されるこれらのアクションには、無修正でのパケットの通過、パケットの廃棄、またはパケットに割り当てられた DSCP を修正（マークダウン）した上でのパケットの通過の許可などが含まれます。設定可能なポリシングされた DSCP マップは、新しい DSCP ベースの QoS ラベルをパケットに提供します。ポリシングされた DSCP マップについては、「マッピング テーブル」（P.39-13）を参照してください。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、フローのパケットの順番が乱れないようにします。

（注） ブリッジドであるか、ルーテッドであるかにかかわらず、すべてのトラフィックにはポリサーが適用されます（ポリサーが設定されている場合）。その結果、ブリッジド パケットは、ポリシングおよびマーキングされるときに廃棄されたり、DSCP または CoS フィールドが修正されたりすることがあります。

ポリシング（individual または aggregate ポリサー）は、物理ポートまたは SVI で設定できます。物理ポートでは、信頼状態の設定、パケットの新しい DSCP または IP precedence 値の設定、individual または aggregate ポリサーの定義ができます。物理ポートでのポリシングの設定の詳細については、「物理ポートでのポリシング」（P.39-10）を参照してください。SVI でポリシー マップを設定する場合は、セカンダリ インターフェイスレベル ポリシー マップだけで、階層ポリシー マップを作成して、individual ポリサーを定義できます。詳細については、「SVI でのポリシング」（P.39-11）を参照してください。

ポリシー マップとポリシング アクションを設定した後、**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、ポリシーを入力ポートまたは SVI に付加します。設定情報については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）、「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）、および「aggregate ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング」（P.39-62）を参照してください。

物理ポートでのポリシング

物理ポートのポリシー マップでは、次のタイプのポリサーを作成できます。

- individual：QoS は、ポリサーで指定された帯域幅限度を、一致する各トラフィック クラスに個別に適用します。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 マップ内部で設定します。
- aggregate：QoS はポリサーで指定された帯域幅限度を、一致する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、ポリシー マップ内部で aggregate ポリサー名を指定することで設定します。ポリサーの帯域幅限度は、**mls qos aggregate-policer** グローバル コンフィギュレーション コマンドを使用して指定します。このように、aggregate ポリサーは、ポリシー マップ内の複数のトラフィック クラスにより共有されます。

（注） SVI には individual ポリサーだけを設定できます。

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より受信されると、トークンがバケットに追加されます。バケットには穴があり、平均トラフィック レート（ビット/秒）として指定したレートでリークが発生します。トークンがバケットに追加されるたびに、スイッチはバケットに十分な空間があることを確認します。十分な空間がない場合は、パケットに不適合のマークが付き、指定されたポリサー アクションが実行されます（廃棄またはマークダウン）。

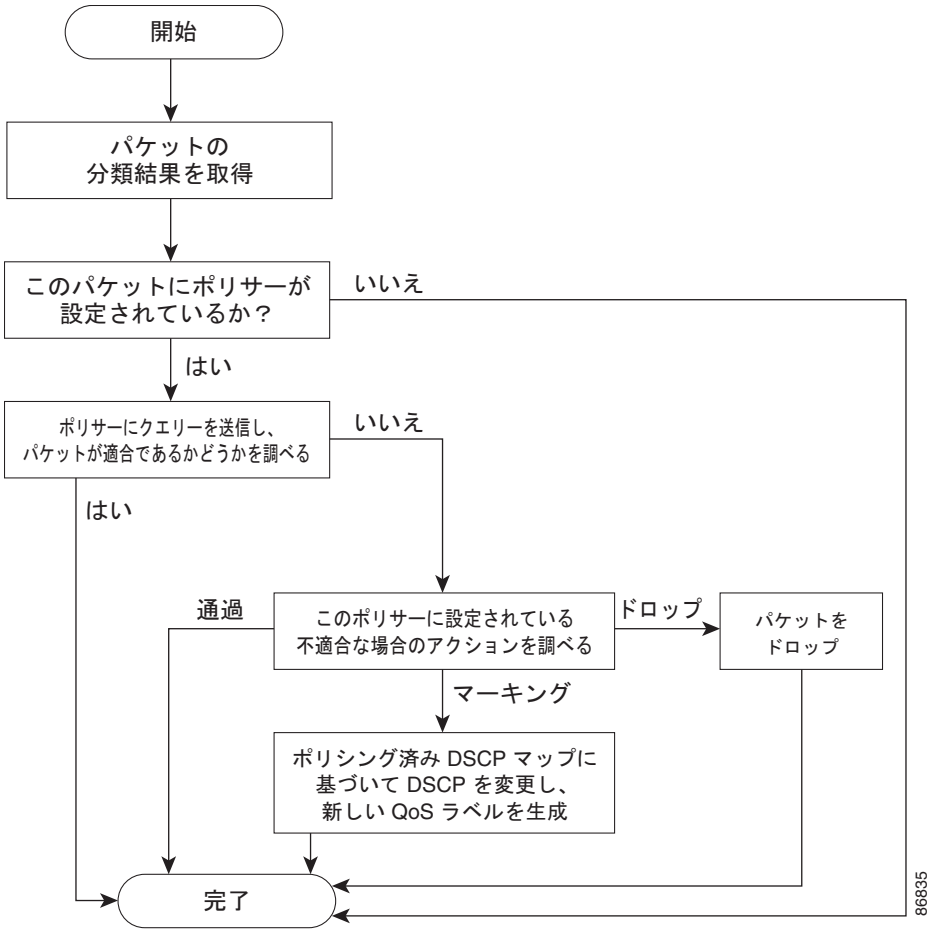
バケットが満杯になるまでの速度は、バケットの深さ（burst-byte）、トークンの削除レート（rate-b/s）、および平均レートを超えているバーストの継続時間によって決まります。バケットのサイズによりバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バーストが短い場合は、バケットがオーバーフローすることはなく、トラフィック フローに対してアクションは実行されません。しかし、バーストが長く、レートが高い場合は、バケットがオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

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 39-4 に、ポリシングおよびマーキング プロセスを示します。次のタイプのポリシー マップが設定されます。

- 物理ポートの非階層ポリシー マップ。
- SVI に付加されたインターフェイス レベルの階層ポリシー マップ。物理ポートは、このセカンダリ ポリシー マップで指定されます。

図 39-4　物理ポートでのポリシングおよびマーキングのフローチャート



SVI でのポリシング

（注）　SVI で individual ポリサーを使用して階層ポリシー マップを設定する前に、その SVI に属する物理ポートで、VLAN ベースの QoS をイネーブルにする必要があります。ポリシー マップは SVI に付加されますが、individual ポリサーは、階層ポリシー マップのセカンダリ インターフェイス レベルで指定された物理ポート上のトラフィックだけに影響を与えます。

階層ポリシー マップには 2 つのレベルがあります。1 つは VLAN レベルで、SVI のトラフィック フローに対して実行するアクションを指定します。もう 1 つはインターフェイス レベルで、インターフェイス レベルのポリシー マップに指定されていて、SVI に属する物理ポートのトラフィックに対して実行するアクションを指定します。

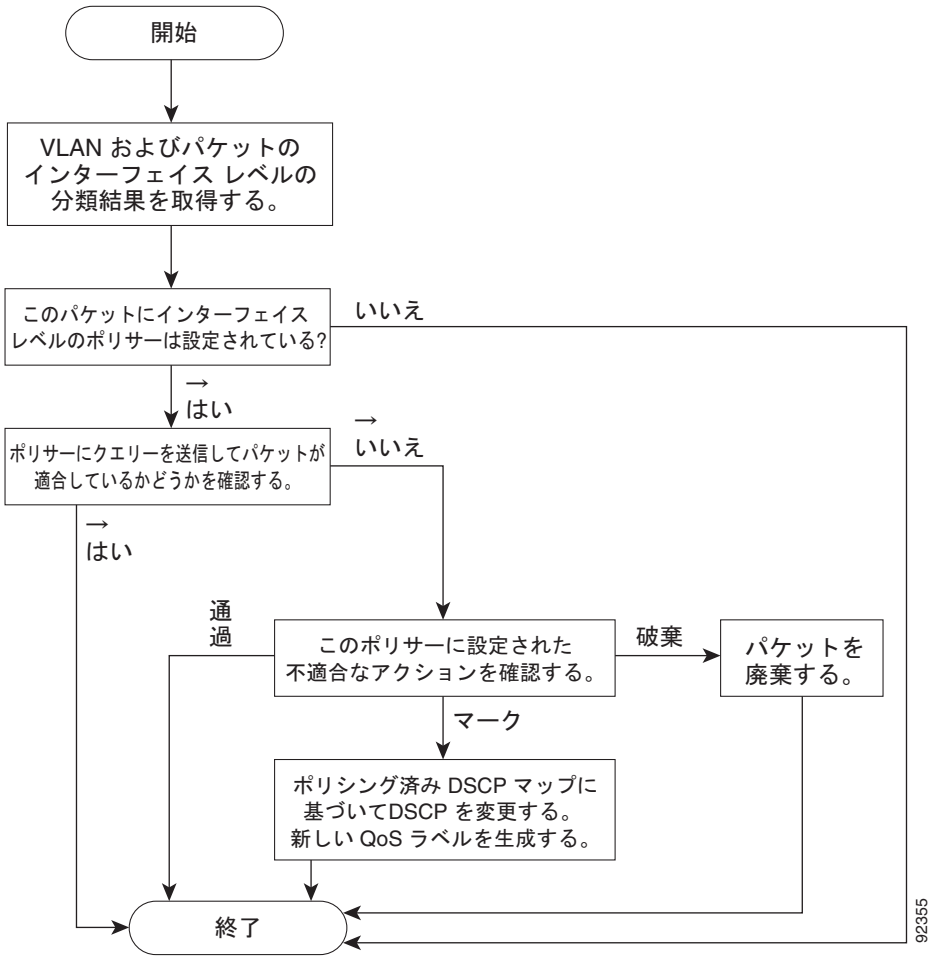
SVI にポリシングを設定する場合は、次の 2 つのレベルを持つ階層ポリシー マップを作成および設定できます。

- VLAN レベル：ポートの信頼状態を指定する、またはパケットの新しい DSCP または IP precedence 値を設定するクラス マップおよびクラスを設定することにより、このプライマリ レベルを作成します。VLAN レベルのポリシー マップは、SVI の VLAN だけに適用され、ポリサーはサポートしません。
- インターフェイス レベル：SVI に属する物理ポートの individual ポリサーを指定するクラス マップとクラスを設定することにより、このセカンダリ レベルを作成します。インターフェイスレベルのポリシー マップは individual ポリサーだけをサポートし、aggregate ポリサーはサポートしません。VLAN レベルのポリシー マップで定義されたクラスごとに、異なるインターフェイス レベル ポリシー マップを設定できます。

階層ポリシー マップの例は、「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）を参照してください。

図 39-5 に、SVI に階層ポリシーがマップされている場合のポリシングおよびマーキングのプロセスを示します。

図 39-5　SVI でのポリシングとマーキングのフローチャート



マッピング テーブル

QoS 処理の実行時に、スイッチでは、分類段階の DSCP または CoS 値に基づく QoS ラベルを使用して、全てのトラフィック（非 IP トラフィックも含む）のプライオリティが表されます。

- 分類中に、QoS は設定可能なマッピング テーブルを使用して、受信した 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 マップなどが含まれます。これらのマップは、**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 コマンドを使用して設定します。

  DSCP 信頼状態で設定された入力ポートで、DSCP 値が QoS ドメイン間で異なる場合は、設定可能な DSCP/DSCP 変換マップを、2 つの QoS ドメイン間の境界上のポートに適用できます。このマップは、**mls qos map dscp-mutation** グローバル コンフィギュレーション コマンドを使用して設定します。

- ポリシングの実行中に、QoS は別の DSCP 値を IP または非 IP パケットに割り当てることができます（パケットがプロファイル外で、ポリサーがマークダウン値を指定している場合）。この設定可能なマップは、ポリシングされた DSCP マップと呼ばれます。このマップは、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用して設定します。

- トラフィックがスケジューリング段階に入る前に、QoS は、QoS ラベルに従ってパケットを入力および出力キューに格納します。QoS ラベルは、パケットの DSCP または CoS 値に基づいており、DSCP 入力および出力キュー スレッシュホールド マップによって、または CoS 入力および出力キュー スレッシュホールド マップによってキューを選択します。入力または出力キューに加えて、QOS ラベルは WTD スレッシュホールド値も識別します。これらのマップは、**mls qos srr-queue** {**input** | **output**} **dscp-map** および **mls qos srr-queue** {**input** | **output**} **cos-map** グローバル コンフィギュレーション コマンドを使用して設定します。

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

デフォルトの DSCP/DSCP 変換マップとデフォルトのポリシングされた DSCP マップはヌル マップであり、着信 DSCP 値を同じ DSCP 値にマッピングします。DSCP/DSCP 変換マップは、特定のポートに適用す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。

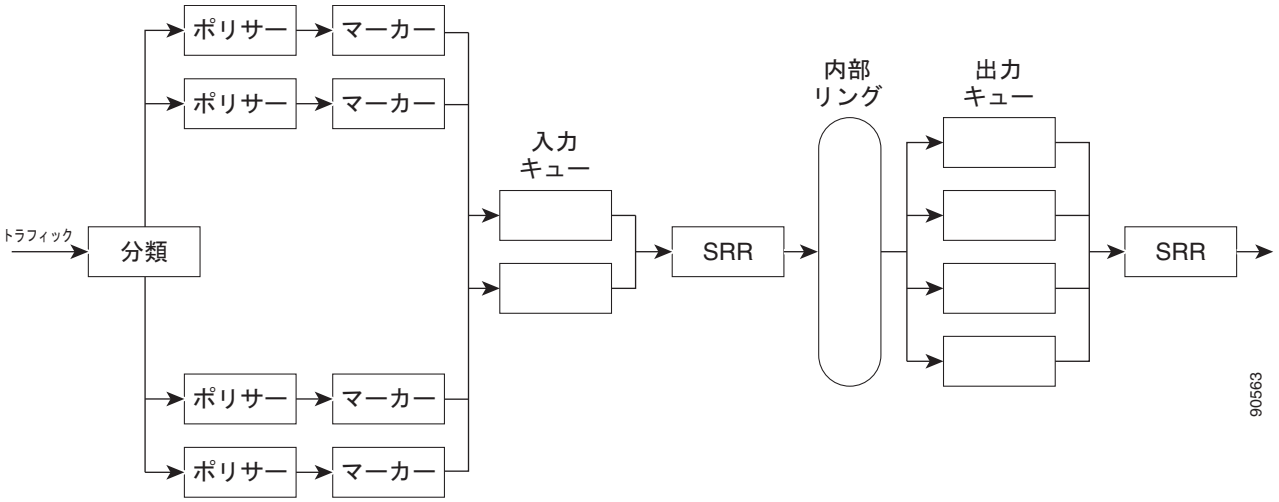
設定の詳細については、「DSCP マップの設定」（P.39-65）を参照してください。

DSCP および CoS 入力キューのスレッシュホールド マップについては、「入力キューでのキューイングおよびスケジューリング」（P.39-16）を参照してください。DSCP および CoS 出力キューのスレッシュホールド マップについては、「出力キューでのキューイングおよびスケジューリング」（P.39-18）を参照してください。

キューイングとスケジューリングの概要

図 39-6 に示すように、スイッチには、輻輳の防止に役立つキューが特定のポイントにあります。

図 39-6　入力および出力キューの場所



すべてのポートの入力帯域幅の合計が内部リングの帯域幅を超えることがあるため、入力キューは、パケットの分類、ポリシング、およびマーキングの後、かつスイッチ ファブリックへのパケットの転送前に配置されます。複数の入力ポートが出力ポートにパケットを同時に送信し、輻輳の原因になることがあるため、出力キューは内部リングの後に配置されます。

WTD

入力キューと出力キューのいずれも、weighted tail drop（WTD）と呼ばれるテール廃棄輻輳回避メカニズムの拡張バージョンを使用しています。WTD は、キューの長さを管理し、トラフィック分類別の廃棄優先度を設定する目的で、キューに実装されます。

フレームが特定のキューに入れられると、WTD は、そのフレームに割り当てられた QoS ラベルを使用して別のスレッシュホールドを適用します。その QoS ラベルのスレッシュホールドを超えると（宛先キューで使用可能な領域がフレームのサイズを下回ると）、スイッチはフレームを廃棄します。

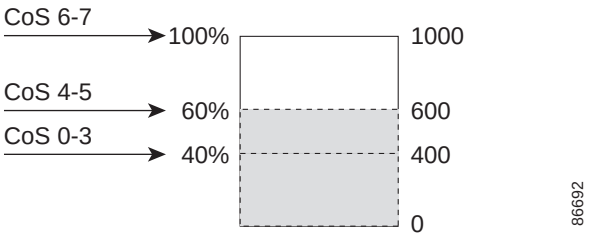
各キューには 3 つのスレッシュホールド値があります。QOS ラベルは、3 つのスレッシュホールド値からフレームに適用する値を決定します。3 つのスレッシュホールドのうち、2 つは設定可能で（明示的）、1 つは設定変更ができません（暗黙）。

図 39-7 に、サイズが 1000 フレームのキューに対して機能する WTD の例を示します。3 つの廃棄パーセンテージ、40%（400 フレーム）、60%（600 フレーム）、100%（1000 フレーム）が設定されています。これらのパーセンテージは、40% のスレッシュホールドでは最大 400 のフレームを、60% のスレッシュホールドでは最大 600 のフレームを 、100% のスレッシュホールドでは最大 1000 のフレームをキューに入れられることを意味します。

この例では、CoS 値 6 および 7 は他の CoS 値よりも重要であり、100% の廃棄スレッシュホールドに割り当てられます（キューが満杯の状態）。CoS 値 4 および 5 は 60% のスレッシュホールドに、CoS 値 0 ～ 3 は 40% のスレッシュホールドに割り当てられます。

すでに 600 のフレームでキューが満杯になっているときに、新しいフレームが到着したとします。このフレームには、CoS 値 4 および 5 が含まれ、60% のスレッシュホールドが適用されます。このフレームがキューに追加されると、スレッシュホールドを超えるため、スイッチはそのフレームを廃棄します。

図 39-7　　WTD およびキューの動作



詳細については、「DSCP または CoS 値の入力キューへのマッピングと、WTD スレッシュホールドの設定」（P.39-71）、「出力キューセットのバッファ領域の割り当てと WTD スレッシュホールドの設定」（P.39-75）、および「DSCP または CoS 値の出力キューとスレッシュホールド ID へのマッピング」（P.39-78）を参照してください。

SRR のシェーピングおよび共有

入力キューと出力キューは、いずれもパケットの送信レートを制御する SRR によって処理されます。入力キューでは、SRR はパケットを内部リングに送信します。出力キューでは、SRR はパケットを出力ポートに送信します。

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。ただし、入力キューでは、共有がデフォルトのモードであり、サポートされる唯一のモードです。

シェーピング モードでは、出力キューは帯域幅のパーセンテージが保証され、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越えて使用できません。シェーピングによって、トラフィック フローの時間的変動がより均一になり、バースト性の高いトラフィックによるピークや谷が軽減されます。シェーピングでは、各重みの絶対値を使用して、そのキューで使用可能な帯域幅を計算します。

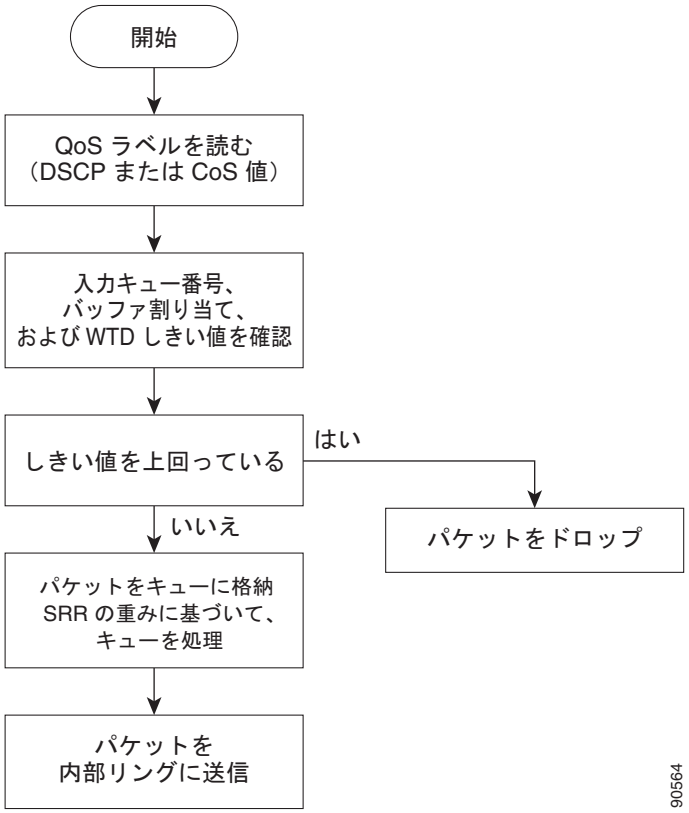
共有モードでは、設定された重みによりキュー間で帯域幅が共有されます。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、キューが空でそれ以上リンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。共有では、デキューイングの頻度は重みの比によって制御され、絶対値には意味はありません。シェーピングと共有は、インターフェイスごとに設定されます。各インターフェイスには固有の設定が可能です。

詳細については、「入力キュー間での帯域幅の割り当て」（P.39-73）、「出力キューでの SRR のシェーピングされた重みの設定」（P.39-79）、および「出力キューでの SRR の共有された重みの設定」（P.39-80）を参照してください。

入力キューでのキューイングおよびスケジューリング

図 39-8 に、入力ポートのキューイングとスケジューリングのフローチャートを示します。

図 39-8　　入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



（注）　SRR は、他のキューを処理する前に、その設定済みの共有に従いプライオリティ キューを処理します。

スイッチは 2 つの設定可能な入力キューをサポートしています。これらのキューは、共有モードの SRR だけで処理されます。表 39-1 でキューについて説明します。

表 39-1　　入力キューのタイプ

キューのタイプ[1]	機能
標準	標準のプライオリティと見なされるユーザ トラフィック。フローを区別するために 3 つの異なるスレッシュホールドを設定できます。**mls qos srr-queue input threshold**、**mls qos srr-queue input dscp-map**、および **mls qos srr-queue input cos-map** グローバル コンフィギュレーション コマンドを使用できます。
緊急	Differentiated Service（DF; ディファレンシエーテッド サービス）緊急転送または音声トラフィックなどのプライオリティの高いユーザ トラフィック。このトラフィックに必要な帯域幅を、**mls qos srr-queue input priority-queue** 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、総トラフィックのパーセンテージとして設定できます。緊急キューには保証された帯域幅があります。

1. スイッチは、適切なネットワーク動作に不可欠なトラフィック用に、設定変更ができない 2 つのキューを使用します。

スイッチを通過する各パケットを、キューとスレッショルドに割り当てます。具体的には、DSCP または CoS 値を入力キューに割り当て、DSCP または CoS 値をスレッショルド ID に割り当てます。**mls qos srr-queue input dscp-map** queue *queue-id* {*dscp1...dscp8* | **threshold** *threshold-id dscp1...dscp8*} または **mls qos srr-queue input 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 入力キュー スレッショルド マップおよび CoS 入力キュー スレッショルド マップは、**show mls qos maps** 特権 EXEC コマンドを使用して表示できます。

WTD スレッショルド

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廃棄パーセンテージをサポートします。各キューには 3 つの廃棄スレッショルドがあります。そのうちの 2 つは設定可能な（*明示的な*）WTD スレッショルドで、1 つは、キューが満杯の状態に事前設定されていて設定変更ができない（*暗黙の*）スレッショルドです。スレッショルド ID 1 および ID 2 用に、2 つの明示的な WTD スレッショルド パーセンテージを入力キューに割り当てるには、**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2* 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。各スレッショルドは、キューに割り当てられたバッファの総数に対する割合です。スレッショルド ID 3 の廃棄スレッショルドは、キューが満杯の状態に事前設定されており、修正はできません。WTD の動作の詳細については、「WTD」（P.39-14）を参照してください。

バッファと帯域幅の割り当て

2 つのキューの間で入力バッファを分割する（領域の大きさを割り当てる）比率を定義するには、**mls qos srr-queue input buffers** *percentage1 percentage2* 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。バッファ割り当てと帯域幅割り当てを組み合わせることにより、パケットの廃棄前にバッファリングし、送信できるデータの大きさを制御します。帯域幅をパーセンテージとして割り当てるには、**mls qos srr-queue input bandwidth** *weight1 weight2* 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。重みの比率は、SRR スケジューラがパケットを各キューから送信する頻度の比率です。

プライオリティ キューイング

mls qos srr-queue input priority-queue *queue-id* **bandwidth** *weight* 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、1 つの入力キューをプライオリティ キューとして設定できます。プライオリティ キューは、内部リングの負荷にかかわらず帯域幅が保証されたキューの一部であるため、確実な配信を必要とするトラフィック（音声など）に使用します。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に SRR は、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定された重みに従い、両方の入力キューで残りの帯域幅を共有し、キューを処理します。

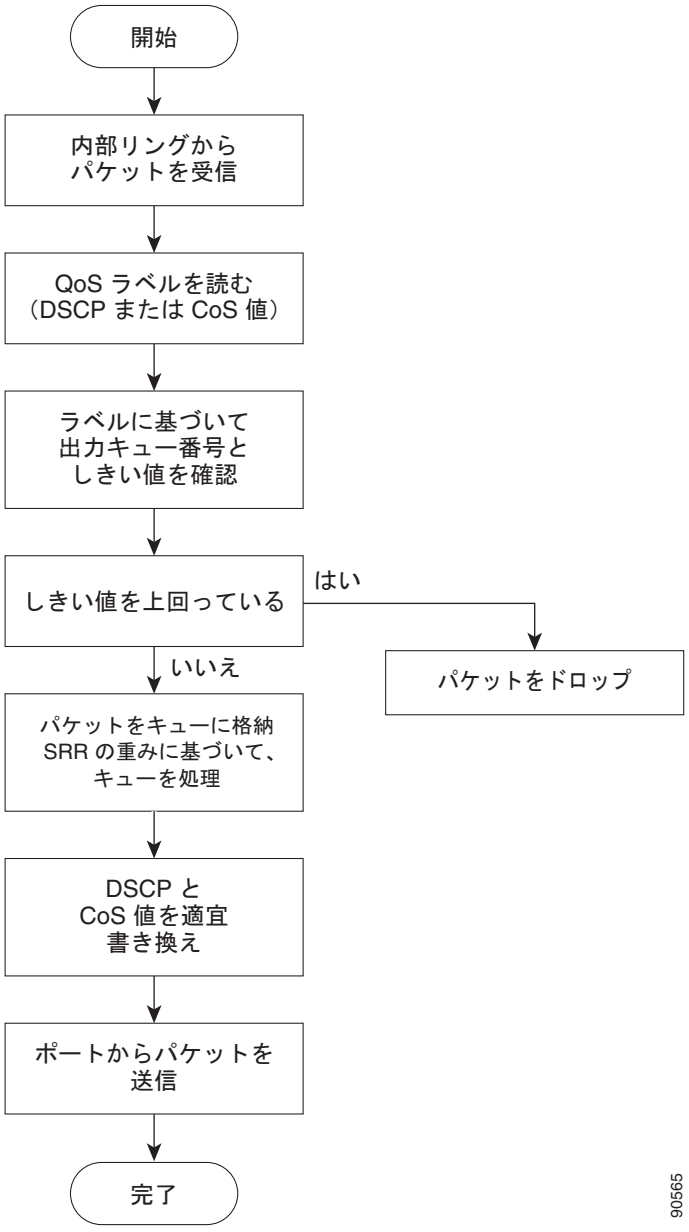
この項で説明するコマンドを組み合わせて、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティの低いパケットが廃棄されるようにキューのスレッショルドを調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「入力キューの特性の設定」（P.39-70）を参照してください。

出力キューでのキューイングおよびスケジューリング

図 39-9 に、出力ポートのキューイングとスケジューリングのフローチャートを示します。

（注）　緊急キューがイネーブルになっている場合、SRR は、他の 3 つのキューを処理する前に、そのキューが空になるまで処理します。

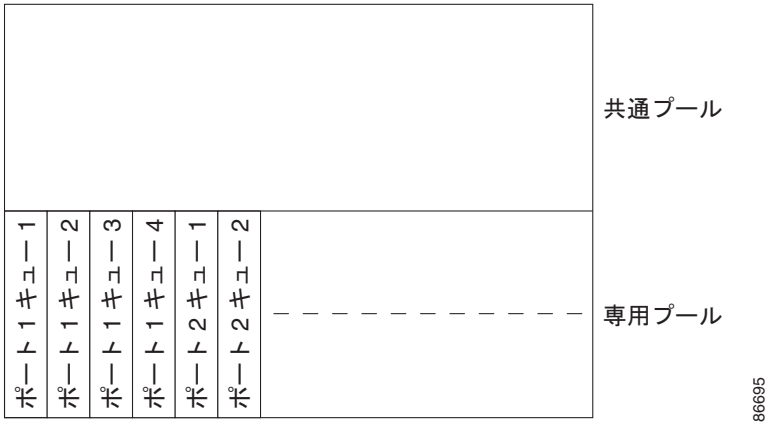
図 39-9　出力ポートのキューイングおよびスケジューリングのフローチャート



各ポートは 4 つの出力キューをサポートしており、そのうちの 1 つ（キュー 1）を出力緊急キューにできます。これらのキューはキューセットにより設定されます。出力ポートからのすべてのトラフィックは、これらの 4 つのキューの 1 つを通過し、パケットに割り当てられた QoS ラベルに基づいてスレッシュホールドが適用されます。

図 39-10 に出力キュー バッファを示します。バッファ領域は、共通のプールと予約済みプールとにわかれます。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量を予約し、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がバッファを使用できなくなるのを防ぎ、バッファ スペースを要求元のキューに許可するかどうかを制御します。スイッチは、ターゲット キューが予約量を超えるバッファを消費していないかどうか（アンダーリミット）、その最大バッファをすべて消費したかどうか（オーバーリミット）、共通のプールが空（空きバッファがない）か、または空でない（空きバッファ）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廃棄します。

図 39-10　出力キュー バッファの割り当て



バッファおよびメモリの割り当て

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 コマンドを使用して、バッファのアベイラビリティを保証し、廃棄スレッシュホールドを設定し、キューセットの最大メモリ割り当てを設定します。各スレッシュホールド値は、キューに割り当てられたメモリのパーセンテージであり、**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 コマンドを使用して指定します。割り当てられたすべてのバッファの合計が予約済みプールになり、残りのバッファは共通のプールの一部になります。

バッファ割り当てによって、ハイ プライオリティ トラフィックを確実にバッファリングできます。たとえば、バッファ領域が 400 の場合は、その 70% をキュー 1 に割り当て、10% をキュー 2 ～ 4 に割り当てることができます。この結果、キュー 1 には 280 のバッファが割り当てられ、キュー 2 ～ 4 には、それぞれ 40 のバッファが割り当てられます。

割り当てられたバッファがキューセットの特定のキュー用に予約されていることを保証できます。たとえば、キューに 100 のバッファがある場合は、50%（50 のバッファ）を予約できます。スイッチは、残りの 50 のバッファを共通のプールに返します。また、最大スレッシュホールドを設定することにより、フル状態のキューが予約済みのバッファを超える大きさのバッファを取得できるようにすることもできます。スイッチは、共通のプールが空でない場合に、必要なバッファを共通のプールから割り当てることができます。

WTD スレッショルド

スイッチを通過する各パケットを、キューとスレッショルドに割り当てできます。具体的には、DSCP または CoS 値を出力キューに割り当て、DSCP または CoS 値をスレッショルド ID に割り当てます。**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 スレッショルド マップおよび CoS 出力キュー スレッショルド マップは、**show mls qos maps** 特権 EXEC コマンドを使用して表示できます。

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廃棄パーセンテージをサポートします。各キューには 3 つの廃棄スレッショルドがあります。そのうちの 2 つは設定可能な（*明示的な*）WTD スレッショルドで、1 つは、キューが満杯の状態に事前設定されていて設定変更ができない（*暗黙の*）スレッショルドです。スレッショルド ID 1 および ID 2 用の 2 つの WTD スレッショルド パーセンテージを割り当てます。スレッショルド ID 3 の廃棄スレッショルドは、キューが満杯の状態に事前設定されており、修正はできません。**queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用して、ポートをキューセットにマッピングします。WTD スレッショルドのパーセンテージを変更するには、キューセットの設定を修正します。WTD の動作の詳細については、「WTD」（P.39-14）を参照してください。

シェーピング モードまたは共有モード

SRR は、共有モードまたはシェーピング モードでキューセットを処理します。**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 コマンドを使用して、共有重みまたはシェーピングされた重みをポートに割り当てます。シェーピングと共有の違いについては、「SRR のシェーピングおよび共有」（P.39-15）を参照してください。

バッファ割り当てと SRR の重み比率を組み合わせることにより、パケットの廃棄前にバッファリングし、送信できるデータの大きさを制御します。重みの比率は、SRR スケジューラがパケットを各キューから送り出す頻度の比率です。

緊急キューがイネーブルでない限り、4 つのキューすべてが SRR に関与します。この場合、1 番めの帯域幅の重みは無視されて、比率の計算には使用されません。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 コマンドを使用してイネーブルにします。

この項で説明するコマンドを組み合わせて、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、プライオリティの低いパケットが廃棄されるようにキューのスレッショルドを調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「出力キューの特性の設定」（P.39-75）を参照してください。

（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だけ、設定を変更してください。

パケットの変更

QoS を提供するために、パケットは、分類され、ポリシングされ、キューイングされます。このプロセス中に、次のようにパケットが変更されることがあります。

- IP および非 IP パケットの分類では、受信したパケットの DSCP または CoS に基づいて、QoS ラベルがパケットに割り当てられます。ただし、パケットはこの段階では変更されず、割り当てられた DSCP または CoS 値の指定だけが伝送されます。これは、QoS の分類と転送の検索が並行して行われるためです。パケットを元の DSCP のまま CPU に転送し、そこでソフトウェアによって再度処理することもできます。
- ポリシングの実行中に、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（パケットがプロファイル外で、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の DSCP は変更されず、マークダウンされた値の指定が伝送されます。IP パケットでは、パケットの変更は後の段階で行われます。非 IP パケットでは、DSCP が CoS に変換され、キューイングや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 ラベルと選択した変換に応じて、フレームの DSCP 値と CoS 値が書き換えられます。変換マップを設定していないときに、着信フレームの DSCP を信頼するようにポートを設定すると、フレームの DSCP 値は変更されませんが、CoS は DSCP/CoS マップに従っ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を設定し、これが IP パケットの場合は、フレームの CoS 値は変更されませんが、DSCP は CoS/DSCP マップに従って変更されることがあります。

  入力変換により、DSCP は、選択した DSCP の新しい値に応じて書き換えられます。ポリシーマップの設定されたアクションによっても、DSCP の書き換えが発生します。

auto-QoS の設定

auto-QoS 機能を使用して、QoS 機能の導入を簡易化できます。auto-QoS はネットワーク設計を判断し、スイッチで異なるトラフィック フローの優先順位付けができるように、QoS 設定をイネーブルにします。デフォルトの（ディセーブルにされた）QoS 動作を使用する代わりに、入力キューと出力キューを使用します。スイッチは、パケットの内容やサイズにかかわらずベストエフォート サービスを各パケットに提供し、単一のキューからパケットを送信します。

auto-QoS をイネーブルにすると、トラフィックのタイプと入力パケットのラベルに従ってトラフィックが自動的に分類されます。スイッチは分類結果を使用して、適切な出力キューを選択します。

auto-QoS コマンドを使用して、次のシスコ デバイスに接続されているポートを識別します。

- Cisco IP Phones
- Cisco SoftPhone アプリケーションが動作しているデバイス

また、アップリンクを介して信頼されたトラフィックを受信するポートを識別するためにも、これらのコマンドを使用します。auto-QoS は次の機能を実行します。

- 条件付きの信頼できるインターフェイスによる auto-QoS 装置の有無の検出
- QoS の分類の設定
- 出力キューの設定

ここでは、次の設定情報について説明します。

- 「生成される auto-QoS の設定」（P.39-22）
- 「設定に与える auto-QoS の影響」（P.39-29）
- 「auto-QoS 設定時の注意事項」（P.39-30）
- 「Auto-QoS のイネーブル化」（P.39-30）

生成される auto-QoS の設定

デフォルトでは、auto-QoS はすべてのポートでディセーブルになっています。パケットは変更されません。つまり、パケットの CoS、DSCP、および IP precedence の値は変更されません。

インターフェイスの最初のポートで auto-QoS 機能をイネーブルにすると、次のようになります。

- 入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力キューと出力キューの設定が行われます。
- QoS はグローバルにイネーブル化され（**mls qos** グローバル コンフィギュレーション コマンド）、その他のグローバル コンフィギュレーション コマンドが自動的に生成されます（表 39-6 を参照）。
- スイッチが信頼境界機能をイネーブルにし、サポート対象の装置があるかどうかを Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を使用して検出します。
- ポリシングを使用してパケットがプロファイル内にあるのかプロファイル外にあるのかを確認し、そのパケットに対するアクションを指定します。

VOIP 装置固有

- Cisco IP Phone に接続されたネットワーク エッジにあるポートで **auto qos voip cisco-phone** コマンドを入力すると、スイッチは信頼境界機能をイネーブルにします。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。Cisco IP Phone がない場合、入力ポートでの分類は、パケットの QoS ラベルを信頼しないように設定されます。ポリシングは、スイッチが信頼境界機能をイネーブルにする前に、ポリシーマップの分類に一致するトラフィックに適用されます。
- Cisco SoftPhone が動作する装置に接続されたネットワーク エッジにあるポートで **auto qos voip cisco-softphone** 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、スイッチはポリシングを使用してパケットがプロファイル内にあるのかプロファイル外にあるのかを確認し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。
- ネットワーク内部に接続されたポートで **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチは、入力パケット内の非ルーテッド ポートの CoS 値、またはルーテッド ポートの DSCP 値を信頼します（トラフィックが他のエッジ装置ですでに分類されていることが前提条件になります）。

スイッチは、ポートの入力キューと出力キューを、表 39-2 および表 39-3 の設定値に従って設定します。

表 39-2　トラフィック タイプ、パケット ラベル、およびキュー

	VoIP[1] データ トラフィック	VoIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP BPDU トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP	46	24、26	48	56	34	–	
CoS	5	3	6	7	3	–	
CoS から入力キューへのマッピング	4、5（キュー 2）					0、1、2、3、6、7（キュー 1）	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

1. VoIP = Voice over IP

表 39-3　入力キューに対する auto-QoS の設定

入力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	キュー（バッファ）サイズ
SRR 共有	1	0、1、2、3、6、7	70%	90%
プライオリティ	2	4、5	30%	10%

表 39-4　出力キューに対する auto-QoS の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キューの重み（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

信頼境界機能の詳細については、「ポート セキュリティを保証するための信頼境界の設定」（P.39-41）を参照してください。

auto qos voip cisco-phone、**auto qos voip cisco-softphone** 、または **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを使用して auto-QoS をイネーブルにする場合、スイッチは、トラフィックのタイプと入力パケットのラベルに基づいて QoS の設定を自動的に生成し、表 39-6 に示すコマンドをポートに適用します。

グローバル auto-QoS の設定

表 39-5　生成される auto-QoS の設定

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは、標準の QoS を自動的にイネーブルにし、CoS/DSCP マップを設定します（着信パケットの CoS 値を DSCP 値にマッピングする）。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 24 32 46 48 56**
スイッチは、入力キューとスレッシュホールド ID に CoS 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 3** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 4**

表 39-5　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは、出力キューとスレッシュホールド ID に CoS 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 4 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 2 3** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 0** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 1**
スイッチは、入力キューとスレッシュホールド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 24** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 42 43 44 45** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 46 47**

表 39-5　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは、出力キューとスレッシュホールド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 2 24** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14**

表 39-5　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}	自動生成される拡張コマンド {Video|Trust|Classify}
スイッチは入力キューを自動的に設定します。キュー 2 がプライオリティ キューで、キュー 1 が共有モードです。スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 90 10** Switch(config)# **mls qos srr-queue input threshold 1 8 16** Switch(config)# **mls qos srr-queue input threshold 2 34 66** Switch(config)# **mls qos srr-queue input buffers 67 33**	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 70 30** Switch(config)# **mls qos srr-queue input threshold 1 80 90** Switch(config)# **mls qos srr-queue input priority-queue 2 bandwidth 30**
スイッチは、出力キューのバッファ サイズを自動的に設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	Switch(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-queue out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**	Switch(config)# **mls qos queue-set output 1 threshold 2 100 100 50 200** Switch(config)# **mls qos queue-set output 1 threshold 2 125 125 100 400** Switch(config)# **mls qos queue-set output 1 threshold 3 100 100 100 400** Switch(config)# **mls qos queue-set output 1 threshold 4 60 150 50 200** Switch(config)# **mls qos queue-set output 1 buffers 15 25 40 20**

VoIP 装置に対して生成される auto-QoS の設定

表 39-6　生成される auto-QoS の設定

説明	自動生成されるコマンド {voip}
スイッチは、標準の QoS を自動的にイネーブルにし、CoS/DSCP マップを設定します（着信パケットの CoS 値を DSCP 値にマッピングする）。	Switch(config)# **mls qos** Switch(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**
スイッチは入力キューを自動的に設定します。キュー 2 がプライオリティ キューで、キュー 1 が共有モードです。スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input cos-map** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** Switch(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** Switch(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**
スイッチは、出力キューとスレッショルド ID に CoS 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output cos-map** Switch(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** Switch(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** Switch(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** Switch(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**
スイッチは、入力キューとスレッショルド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue input dscp-map** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** Switch(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**

表 39-6　生成される auto-QoS の設定 （続き）

説明	自動生成されるコマンド {voip}
スイッチは、出力キューとスレッシュホールド ID に DSCP 値を自動的にマッピングします。	Switch(config)# **no mls qos srr-queue output dscp-map** Switch(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** Switch(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** Switch(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** Switch(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**
スイッチは入力キューを自動的に設定します。キュー 2 がプライオリティ キューで、キュー 1 が共有モードです。スイッチは、入力キューの帯域幅とバッファ サイズも設定します。	Switch(config)# **no mls qos srr-queue input priority-queue 1** Switch(config)# **no mls qos srr-queue input priority-queue 2** Switch(config)# **mls qos srr-queue input bandwidth 90 10** Switch(config)# **mls qos srr-queue input threshold 1 8 16** Switch(config)# **mls qos srr-queue input threshold 2 34 66** Switch(config)# **mls qos srr-queue input buffers 67 33**
スイッチは、出力キューのバッファ サイズを自動的に設定します。ポートにマッピングされた出力キューの帯域幅と SRR モード（シェーピングまたは共有）を設定します。	Switch(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** Switch(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** Switch(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** Switch(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** Switch(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** Switch(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** Switch(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** Switch(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** Switch(config)# **mls qos queue-set output 1 buffers 10 10 26 54** Switch(config)# **mls qos queue-set output 2 buffers 16 6 17 61** Switch(config-if)# **priority-que out** Switch(config-if)# **srr-queue bandwidth share 10 10 60 20**

auto qos voip cisco-phone コマンドを入力すると、スイッチは、CDP を使用して Cisco IP Phone の存在を検出する信頼境界機能を自動的にイネーブルにします。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチはクラス マップとポリシー マップを自動的に作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-SoftPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成した後、スイッチは、*AutoQoS-Police-SoftPhone* と呼ばれるポリシー マップを、Cisco SoftPhone 機能を持つ auto-QoS がイネーブルにされている入力インターフェイスに自動的に適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

auto qos voip cisco-phone コマンドを入力すると、スイッチはクラス マップとポリシー マップを自動的に作成します。

```
Switch(config-if)# mls qos trust device cisco-phone
```

auto qos voip cisco-softphone コマンドを入力すると、スイッチはクラス マップとポリシー マップを自動的に作成します。

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-CiscoPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

クラス マップとポリシー マップを作成した後、スイッチは、*AutoQoS-Police-SoftPhone* と呼ばれるポリシー マップを、Cisco SoftPhone 機能を持つ auto-QoS がイネーブルにされている入力インターフェイスに自動的に適用します。

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

設定に与える auto-QoS の影響

auto-QoS がイネーブルになっていると、**auto qos** インターフェイス コンフィギュレーション コマンドと生成されたグローバル設定が、実行コンフィギュレーションに追加されます。

スイッチは、CLI からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドが適用されない場合は、以前の実行コンフィギュレーションが復元されます。

auto-QoS 設定時の注意事項

auto-QoS を設定する前に、次の点に注意してください。

- auto-QoS では、非ルーテッド ポートとルーテッドポート上に Cisco IP Phone がある VoIP 用にスイッチが設定されます。auto-QoS はまた、Cisco SoftPhone アプリケーションを実行している装置を使用する VoIP 用にスイッチを設定します。
- Cisco SoftPhone が動作する装置が、非ルーテッド ポートまたはルーテッド ポートに接続されている場合、スイッチはポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。
- auto-Qos VoIP では、**priority-queue** インターフェイス コンフィギュレーション コマンドを出力インターフェイスに使用します。Cisco IP phone の同一インターフェイス上でポリシーマップと信頼する装置を設定することもできます。
- auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。必要に応じて QoS 設定を微調整できますが、これは、auto-QoS の設定が完了した後に限り実行することを推奨します。詳細については、「設定に与える auto-QoS の影響」（P.39-29）を参照してください。
- auto-QoS をイネーブルにしたあと、名前に *AutoQoS* を含むポリシー マップや aggregate ポリサーを変更しないでください。ポリシー マップや aggregate ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成したポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップをインターフェイスに適用します。
- スタティック ポート、ダイナミック アクセス ポート、音声 VLAN アクセス ポート、およびトランク ポートで auto-QoS をイネーブルにできます。
- デフォルトでは、auto-CDP はすべてのポートでイネーブルになっています。auto-QoS が正しく動作するように、CDP はディセーブルにしないでください。
- ルーテッド ポートにある Cisco IP Phone で auto-QoS をイネーブルにする場合は、スタティック IP アドレスを IP Phone に割り当てる必要があります。
- このリリースでは、Cisco IP SoftPhone バージョン 1.3(3) 以降だけがサポートされます。
- 接続される装置は Cisco CallManager バージョン 4 以降を使用する必要があります。

Auto-QoS のイネーブル化

QoS パフォーマンスを最適にするには、ネットワーク内部のすべての装置で自動 QoS をイネーブルにします。

特権 EXEC モードで開始し、次の手順に従って、QoS ドメイン内部で auto-QoS 装置をイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	ビデオ装置に接続されているポート、またはネットワーク内部の別の信頼できるスイッチまたはルータに接続されているアップリンク 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 モードに入ります。

	コマンド	目的
ステップ 3	**auto qos voip** {**cisco-phone** | **cisco-softphone** | **trust**} または	auto-QoS をイネーブルにします。 キーワードの意味は次のとおりです。 • **cisco-phone**：ポートが Cisco IP Phone に接続されている場合は、電話が検出されたときに限り、着信パケットの QoS ラベルが信頼されます。 • **cisco-softphone**：ポートは、Cisco SoftPhone 機能を実行している装置に接続されています。 • **trust**：アップリンク ポートは信頼できるスイッチまたはルータに接続されており、VoIP トラフィックの分類が
ステップ 4	**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 5	**interface** *interface-id*	信頼できるスイッチまたはルータに接続されていると識別されるスイッチ 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 モードに入ります。
ステップ 6	**auto qos trust**	ポートで auto-QoS をイネーブルにし、そのポートを信頼できるルータまたはスイッチに接続することを指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show auto qos interface** *interface-id*	設定を確認します。 このコマンドは、auto-QoS がイネーブルにされていたインターフェイスの auto-QoS コマンドを表示します。auto-QoS 設定とユーザによる変更を表示するには、**show running-config** 特権 EXEC コマンドを使用できます。

auto-QoS コマンドのトラブルシューティング

auto-QoS をイネーブルまたはディセーブルにしたときに自動的に生成される QoS コマンドを表示するには、auto-QoS をイネーブルにする*前に* **debug auto qos** 特権 EXEC コマンドを入力します。詳細については、このリリースのコマンド リファレンスの **debug autoqos** コマンドを参照してください。

ポート上で auto-QoS をディセーブルにするには、auto qos コマンド インターフェイス コンフィギュレーション コマンドの **no** 形式（**no auto qos voip** など）を使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

no mls qos グローバル コンフィギュレーション コマンドを使用して、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドをディセーブルにできます。QoS がディセーブルの場合、パケットが修正されなくなるため（パケットの CoS、DSCP、IP precedence の値は変更されない）、ポートの信頼性に関する概念はなくなります。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）。

auto-QoS 情報の表示

auto-QoS の初期設定を表示するには、**show auto qos** [**interface** [*interface-id*]] 特権 EXEC コマンドを使用します。その設定に対するユーザの変更を表示するには、**show running-config** 特権 EXEC コマンドを使用します。**show auto qos** コマンドと **show running-config** コマンドの出力を比較して、ユーザ定義の QoS 設定を識別できます。

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

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface** [*interface-id*] [**buffers** | **queueing**]
- **show mls qos maps** [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-output-q**]
- **show mls qos input-queue**
- **show running-config**

標準の QoS の設定

次の項目について十分に理解したうえで、標準の QoS を設定してください。

- 使用するアプリケーションのタイプと、ネットワーク上のトラフィック パターン。
- トラフィックの特性と、ネットワークのニーズ。トラフィックのバースト性が高いかどうか。音声およびビデオ ストリーム用に帯域幅を予約する必要があるかどうか。
- ネットワークの帯域幅要件と速度。
- ネットワーク内の輻輳ポイントの位置。

ここでは、次の設定情報について説明します。

- 「標準の QoS のデフォルト設定」（P.39-33）
- 「標準の QoS 設定の注意事項」（P.39-35）
- 「QoS をグローバルにイネーブルにする方法」（P.39-37）（必須）
- 「物理ポートでの VLAN ベースの QoS のイネーブル化」（P.39-38）（任意）
- 「ポートの信頼状態を使用した分類の設定」（P.39-38）（必須）
- 「QoS ポリシーの設定」（P.39-44）（必須）
- 「DSCP マップの設定」（P.39-65）（任意、DSCP/DSCP 変換マップまたはポリシングされた DSCP マップを使用する必要がある場合を除く）
- 「入力キューの特性の設定」（P.39-70）（任意）
- 「出力キューの特性の設定」（P.39-75）（任意）

標準の QoS のデフォルト設定

QoS はディセーブルです。パケットが変更されない（パケット内の CoS、DSCP、および IP precedence 値は変更されない）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存在しません。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 コマンドによって QoS がイネーブルにされ、その他のすべての QoS 設定値がデフォルト値に設定されている場合、トラフィックはポリシングされず、ベスト エフォート（DSCP 値と CoS 値は 0 に設定される）として分類されます。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。入力および出力キューのデフォルト設定については、「入力キューのデフォルト設定」（P.39-33）および「出力キューのデフォルト設定」（P.39-34）で説明します。

入力キューのデフォルト設定

表 39-7 に、QoS がイネーブルになっているときの入力キューのデフォルト設定を示します。

表 39-7　入力キューのデフォルト設定

機能	キュー 1	キュー 2
バッファ割り当て	90%	10%
帯域幅割り当て [1]	4	4
プライオリティ キューの帯域幅 [2]	0	10
WTD 廃棄スレッシュホールド 1	100%	100%
WTD 廃棄スレッシュホールド 2	100%	100%

1. 帯域幅はキューの間で均等に分配されます。SRR は、共有モードだけでパケットを送信します。
2. キュー 2 はプライオリティ キューです。SRR は、他のキューを処理する前に、その設定済みの共有に従いプライオリティ キューを処理します。

表 39-8 に、QoS をイネーブルにしたときのデフォルトの CoS 入力キュー スレッシュホールド マップを示します。

表 39-8　デフォルトの CoS 入力キュー スレッシュホールド マップ

CoS 値	キュー ID - スレッシュホールド ID
0 ～ 4	1–1
5	2–1
6、7	1–1

表 39-9 に、QoS をイネーブルにしたときのデフォルトの DSCP 入力キュー スレッシュホールド マップを示します。

表 39-9　デフォルトの DSCP 入力キュー スレッシュホールド マップ

DSCP 値	キュー ID - スレッシュホールド ID
0 ～ 39	1–1

表 39-9　デフォルトの DSCP 入力キュー スレッシュホールド マップ （続き）

DSCP 値	キュー ID - スレッシュホールド ID
40 ～ 47	2–1
48 ～ 63	1–1

出力キューのデフォルト設定

表 39-10 に、QoS をイネーブルにしたときの各キュー セットの出力キューのデフォルト設定を示します。すべてのポートがキューセット 1 にマッピングされます。ポートの帯域幅限度は 100% に、レートは無制限に設定されます。

表 39-10　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 廃棄スレッシュホールド 1	100%	200%	100%	100%
WTD 廃棄スレッシュホールド 2	100%	200%	100%	100%
予約済みスレッシュホールド	50%	50%	50%	50%
最大スレッシュホールド	400%	400%	400%	400%
SRR のシェーピングされた重み（絶対値）[1]	25	0	0	0
SRR の共有された重み [2]	25	25	25	25

1. シェーピングされた重み 0 は、このキューが共有モードで動作していることを示します。
2. 帯域幅の 4 分の 1 が各キューに割り当てられます。

表 39-11 に、QoS をイネーブルにしたときのデフォルトの CoS 出力キュー スレッシュホールド マップを示します。

表 39-11　デフォルトの CoS 出力キュー スレッシュホールド マップ

CoS 値	キュー ID - スレッシュホールド ID
0、1	2–1
2、3	3–1
4	4–1
5	1–1
6、7	4–1

表 39-12 に、QoS をイネーブルにしたときのデフォルトの DSCP 出力キュー スレッシュホールド マップを示します。

表 39-12　デフォルトの DSCP 出力キュー スレッシュホールド マップ

DSCP 値	キュー ID - スレッシュホールド ID
0 ～ 15	2–1
16 ～ 31	3–1

表 39-12　デフォルトの DSCP 出力キュー スレッシュホールド マップ （続き）

DSCP 値	キュー ID - スレッシュホールド ID
32 ～ 39	4–1
40 ～ 47	1–1
48 ～ 63	4–1

デフォルトのマッピング テーブルの設定

デフォルトの CoS/DSCP マップを表 39-13（P.39-65）に示します。

デフォルトの IP precedence/DSCP マップを表 39-14（P.39-66）に示します。

デフォルトの DSCP/CoS マップを表 39-15（P.39-68）に示します。

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。

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（マークダウンなし）。

標準の QoS 設定の注意事項

QoS 設定を開始する前に、次の項の情報に注意してください。

- 「QoS ACL の注意事項」（P.39-35）
- 「インターフェイスへの QoS の適用」（P.39-35）
- 「ポリシングの注意事項」（P.39-36）
- 「QoS の一般的な注意事項」（P.39-37）

QoS ACL の注意事項

- IP フラグメントと設定済みの IP 拡張 ACL を照合することによって、QoS は適用できません。IP フラグメントはベストエフォート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表されます。
- クラス マップごとに 1 つの ACL と、1 つの **match** クラスマップ コンフィギュレーション コマンドだけがサポートされます。ACL は、フィールドをパケットの内容と照合する ACE を複数持つことができます。
- ポリシー マップの信頼文には、ACL 行ごとに複数の TCAM エントリが必要です。入力サービス ポリシー マップで ACL に信頼文が含まれる場合は、アクセスリストが大きすぎるために使用可能な QoS TCAM に収まらず、ポリシー マップをポートに適用したときにエラーが発生することがあります。可能な限り、QoS ACL の行数を最小限に抑えてください。

インターフェイスへの QoS の適用

次のガイドラインが、物理ポートおよび SVI（レイヤ 3 インターフェイス）での QoS の設定に適用されます。

- QoS は、物理ポートと SVI に設定できます。QoS を物理ポートで設定する場合は、非階層ポリシー マップを作成し、適用します。QoS を SVI に設定する場合は、非階層ポリシー マップおよび階層ポリシー マップを適用できます。
- 着信トラフィックは、トラフィックがブリッジングされるか、ルーティングされるか、CPU に送信されるかにかかわらず、分類され、ポリシングされ、マークダウンされます（設定されている場合）。ブリジッド フレームが廃棄されたり、その DSCP および CoS 値が修正されたりすることもあります。
- 物理ポートまたは SVI にポリシー マップを設定する場合は、次の注意事項に従ってください。
  - 物理ポートと SVI に同じポリシー マップを適用できません。
  - VLAN ベースの QoS を物理ポートで設定すると、スイッチは、そのポート上のポートベースのポリシー マップをすべて削除します。それによって、この物理ポート上のトラフィックは、物理ポートが属する SVI に付加されたポリシー マップの適用を受けるようになります。
  - SVI に付加された階層ポリシー マップでは、ポート上のトラフィックの帯域幅限度を指定するために、物理ポート上のインターフェイス レベルで individual ポリサーを設定することだけができます。入力ポートは、トランクとして、またはスタティック アクセス ポートとして設定する必要があります。階層ポリシー マップの VLAN レベルではポリサーを設定できません。
  - スイッチは、仮想ポリシー マップで aggregate ポリサーをサポートしません。
  - 階層ポリシー マップを SVI に適用した後は、インターフェイス レベルのポリシー マップを変更したり、階層ポリシー マップから削除したりできません。階層ポリシー マップに、新しいインターフェイス レベル ポリシー マップを追加することもできません。このような変更を行いたい場合は、まず階層ポリシー マップを SVI から削除する必要があります。また、階層ポリシー マップで指定されたクラス マップは、追加することも削除することもできません。

ポリシングの注意事項

- 2 つ以上の物理ポートを制御するポート ASIC 装置は、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。たとえば、32 個のポリサーをギガビット イーサネット ポート上で、8 個のポリサーをファスト イーサネット ポート上で設定できます。または、64 個のポリサーをギガビット イーサネット ポート上で、5 個のポリサーをファスト イーサネット ポート上で設定できます。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。ポートごとのポリサーの予約はできません（特定のポートがいずれかのポリサーに割り当てられるという保証はありません）。
- 入力ポートでは、1 つのパケットに 1 つのポリサーだけが適用されます。設定できるパラメータは、平均レートと認定バーストだけです。
- 同じ非階層ポリシー マップ内部の複数のトラフィック クラスによって共有される aggregate ポリサーを作成できます。ただし、aggregate ポリサーを異なるポリシー マップにわたって使用することはできません。
- QoS 用に設定されたポートでは、そのポートを通じて受信されるすべてのトラフィックが、ポートに付加されたポリシー マップに従って分類され、ポリシングされ、マーキングされます。QoS 用に設定されたトランク ポートでは、そのポートを通じて受信されるすべての VLAN のトラフィックが、ポートに付加されたポリシー マップに従って分類され、ポリシングされ、マーキングされます。
- スイッチで EtherChannel ポートを設定している場合は、QoS の分類、ポリシング、マッピング、およびキューイングを、EtherChannel を構成している個々の物理ポートで設定する必要があります。EtherChannel のすべてのポートで QoS 設定が一致していなければならない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、まずポリシー マップをすべてのインターフェイスから削除し、それからポリシー 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。最初にポリシー マップをすべてのインターフェイスから削除しなかった場合、CPU 使用率が高くなり、その結果、コンソールが長時間停止することがあります。

QoS の一般的な注意事項

QoS の一般的な注意事項を次に示します。

- スイッチによって受信される制御トラフィック（スパニング ツリー Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）やルーティング アップデート パケットなど）は、すべて入力 QoS 処理の対象となります。
- キューの設定を変更するとデータが失われることがあるため、トラフィックが最小のときに変更を行うようにしてください。

IP サービス イメージを実行しているスイッチは、Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップでの QoS DSCP および IP precedence の照合をサポートしていて、次の制限があります。

- QoS DSCP 変換マップと PBR ルート マップを同じインターフェイスに適用することはできません。
- DSCP の透過性と PBR DSCP ルート マップを同じスイッチに設定することはできません。

QoS をグローバルにイネーブルにする方法

デフォルトでは、QoS はスイッチ上でディセーブルになっています。

特権 EXEC モードで開始し、次の手順に従って QoS をイネーブルにします。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	QoS をグローバルにイネーブルにします。 QoS は、「標準の QoS のデフォルト設定」（P.39-33）、「入力キューでのキューイングおよびスケジューリング」（P.39-16）、および「出力キューでのキューイングおよびスケジューリング」（P.39-18）で説明したデフォルトの設定で実行されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

QoS 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。

物理ポートでの VLAN ベースの QoS のイネーブル化

デフォルトでは、VLAN ベースの QoS はすべての物理スイッチ ポートでディセーブルになっています。スイッチは、クラス マップとポリシー マップを含む QoS を、物理ポート ベースだけに適用できます。VLAN ベースの QoS は、スイッチ ポートでイネーブルにできます。

特権 EXEC モードで開始し、次の手順に従って VLAN ベースの QoS をイネーブルにします。この手順は、SVI 上の階層ポリシー マップのインターフェイス レベルで指定された物理ポートで必要となります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	物理ポートを指定し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 3	**mls qos vlan-based**	ポートで VLAN ベースの QoS をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id*	物理ポートで VLAN ベースの QoS がイネーブルになっているかどうかを確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

物理ポートで VLAN ベースの QoS をディセーブルにするには、**no mls qos vlan-based** 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。

ポートの信頼状態を使用した分類の設定

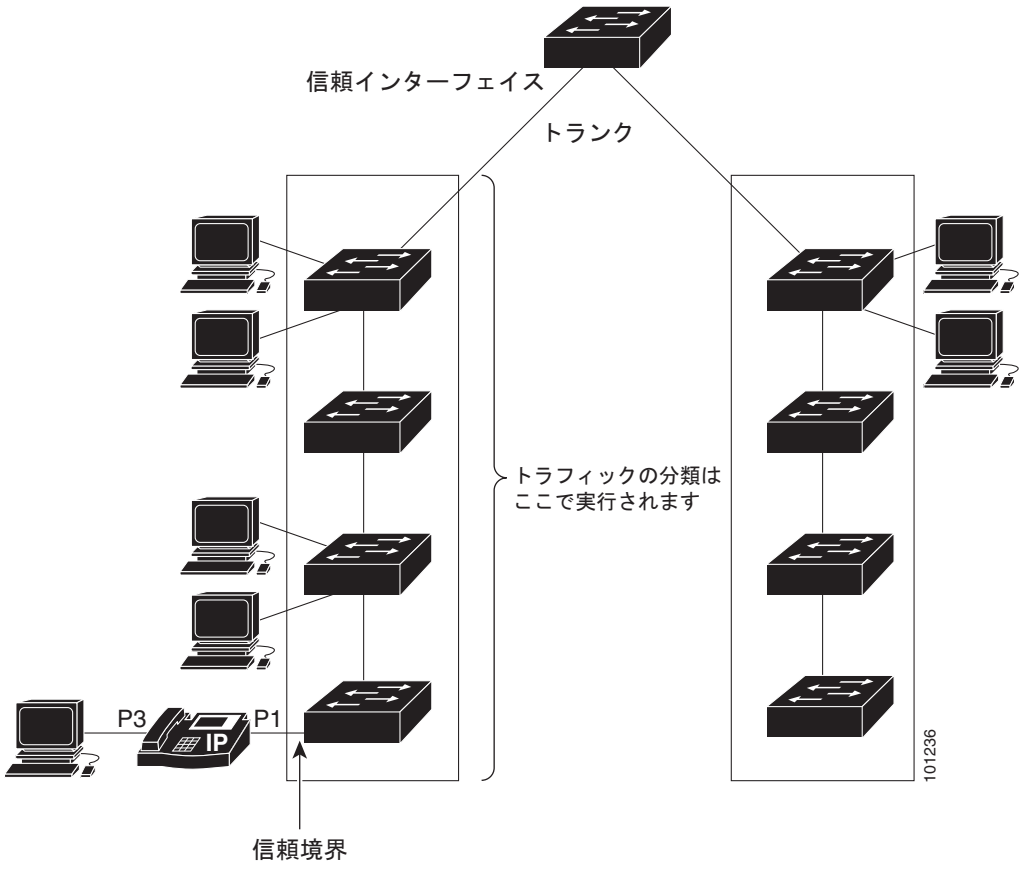
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワークの設定に応じて、次の 1 つ以上の作業、または「QoS ポリシーの設定」（P.39-44）の 1 つ以上の作業を実行する必要があります。

- 「QoS ドメイン内部のポートでの信頼状態の設定」（P.39-38）
- 「インターフェイスの CoS 値の設定」（P.39-40）
- 「ポート セキュリティを保証するための信頼境界の設定」（P.39-41）
- 「DSCP 透過性モードのイネーブル化」（P.39-42）
- 「別の QoS ドメインと境界を接しているポート上での DSCP 信頼状態の設定」（P.39-43）

QoS ドメイン内部のポートでの信頼状態の設定

QoS ドメインに着信するパケットは、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場合は、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ため、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 39-11 に、ネットワーク トポロジの例を示します。

図 39-11　QoS ドメイン内部でのポートの信頼状態



特権 EXEC モードで開始し、次の手順に従って、受信するトラフィックの分類を信頼するようにポートを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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 モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 3	**mls qos trust** [**cos** | **dscp** | **ip-precedence**]	ポートの信頼状態を設定します。 デフォルトでは、ポートは信頼されません。キーワードを指定しないと、デフォルトの **dscp** が使用されます。 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。タグのない非 IP パケットの場合、デフォルト ポートの 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はパケット CoS 値が使用されます。タグがないパケットでは、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はパケット CoS 値が使用されます。タグがないパケットでは、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。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートを信頼されない状態に戻すには、**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 CoS 値の変更方法については、「インターフェイスの CoS 値の設定」（P.39-40）を参照してください。CoS/DSCP マップの設定方法については、「CoS/DSCP マップの設定」（P.39-65）を参照してください。

インターフェイスの CoS 値の設定

QoS は、**mls qos cos** インターフェイス コンフィギュレーション コマンドを使用して指定された CoS 値を、信頼できるポートと信頼できないポートで受信したタグなしフレームに割り当てます。

特権 EXEC モードで開始し、次の手順に従って、ポートのデフォルトの CoS 値を定義するか、デフォルトの CoS 値をそのポートのすべての着信パケットに割り当てます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 3	**mls qos cos** {*default-cos* | **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は、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。デフォルト値は 0 です。 • 着信パケットにあらかじめ設定されている信頼状態を上書きし、すべての着信パケットのポートにデフォルトのポート CoS 値を適用するには、**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なっています。 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ても、このコマンドはそれまでに設定済みの信頼状態を上書きし、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、パケットの CoS 値は、入力ポートで、ポートのデフォルト CoS を使用して変更されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**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。

ポート セキュリティを保証するための信頼境界の設定

一般的なネットワークでは、図 39-11（P.39-39）に示すように、Cisco IP Phone をスイッチ ポートに接続し、データ パケットを生成する装置を電話機の背面からカスケード接続します。Cisco IP Phone は、音声パケットの CoS レベルをハイ プライオリティ（CoS = 5）にし、データ パケットをロー プライオリティ（CoS = 0）にすることで、共有データ リンクの音声品質を保証します。電話機からスイッチに送信されるトラフィックには、通常は、IEEE 802.1Q ヘッダーを使用するタグのマークが付きます。このヘッダーには VLAN 情報と、パケットのプライオリティを示す CoS の 3 ビット フィールドが含まれます。

ほとんどの Cisco IP Phone の設定では、音声トラフィックのプライオリティが、ネットワークの他のタイプのトラフィックよりも高く設定されるように、電話機からスイッチに送信されるトラフィックが信頼されています。**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、電話機を接続するスイッチ ポートが、そのポートで受信するすべてのトラフィックの CoS ラベルを信頼するように設定します。**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、電話機を接続するルーテッド ポートが、そのポートで受信するすべてのトラフィックの DSCP ラベルを信頼するように設定します。

信頼設定では、信頼境界機能を使用して、ユーザが電話機をバイパスし、PC をスイッチに直接接続したときに、ハイ プライオリティ キューが誤って使用されるのを防ぐこともできます。信頼境界を使用しないと、PC によって生成された CoS ラベルがスイッチにより信頼されてしまいます（CoS 設定が信頼されるため）。これに対し、信頼境界機能は CDP を使用して、スイッチ ポート上の Cisco IP Phone（Cisco IP Phone 7910、7935、7940、7960 など）の存在を検出します。電話が検出されなかった場合、信頼境界機能はスイッチ ポートの信頼設定をディセーブルにし、ハイ プライオリティ キューが誤って使用されないようにします。スイッチに接続されたハブに PC と Cisco IP Phone が接続されている場合は、信頼境界機能が機能しないことに注意してください。

Cisco IP Phone に接続された PC がハイ プライオリティ データ キューを使用するのを防ぐことができる場合もあります。スイッチ CLI から **switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信したトラフィックのプライオリティを上書するように電話機を設定することができます。

特権 EXEC モードで開始し、次の手順に従ってポートの信頼境界をイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**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 はイネーブルになっています。
ステップ 3	**interface** *interface-id*	Cisco IP Phone に接続されたポートを指定し、インターフェイス コンフィギュレーション モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**cdp enable**	ポートで CDP をイネーブルにします。デフォルトでは、CDP はイネーブルになっています。
ステップ 5	**mls qos trust cos** または **mls qos trust dscp**	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、ポートは信頼されません。
ステップ 6	**mls qos trust device cisco-phone**	Cisco IP Phone が信頼できる装置であることを指定します。 信頼境界と auto-QoS（**auto qos voip** インターフェイス コンフィギュレーション コマンド）は同時にイネーブルにできません。これらは互いに排他的です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show mls qos interface**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

DSCP 透過性モードのイネーブル化

スイッチは、DSCP 透過性機能をサポートしています。この機能は、出力におけるパケットの DSCP フィールドだけに影響を与えます。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 QoS（Quality of Service）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。

（注）　DSCP 透過性をイネーブルにしても、IEEE 802.1Q トンネリング ポート上のポート信頼性の設定には影響しません。

DSCP 透過性の設定にかかわらず、スイッチは、トラフィックのプライオリティを表すサービス クラス（CoS）値の生成に使用するパケットの内部 DSCP 値を変更します。また、スイッチは内部 DSCP 値を使用して、出力キューおよびスレッシュホールドを選択します。

特権 EXEC モードで開始し、次の手順に従ってスイッチの DSCP 透過性をイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**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**	DSCP 透過性をイネーブルにします。スイッチは、IP パケットの DSCP フィールドを修正しないように設定されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

信頼設定に基づいて、または（DSCP 透過性をディセーブルにすることにより）ACL に基づいて DSCP 値を修正するようにスイッチを設定するには、**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。

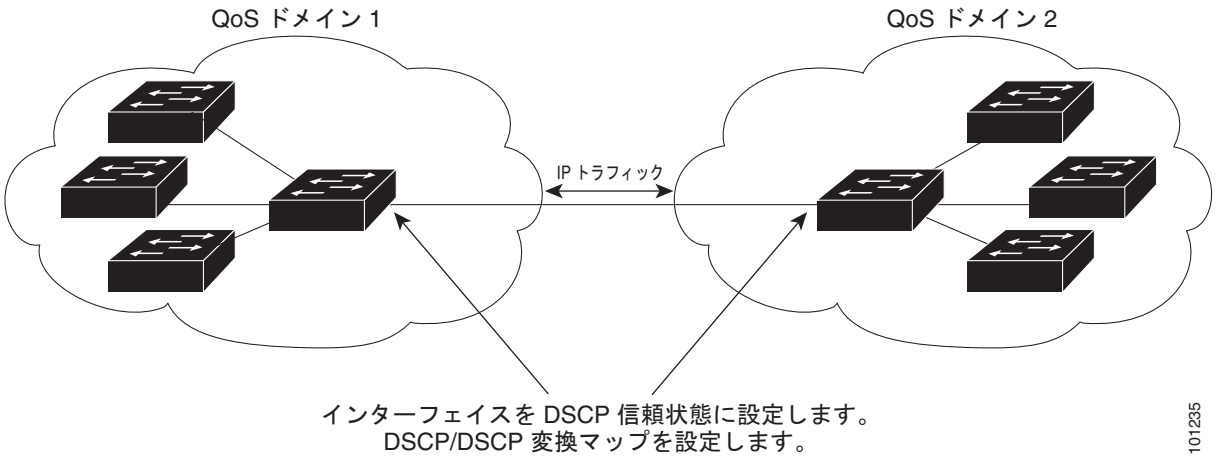
no mls qos グローバル コンフィギュレーション コマンドを使用して QoS をディセーブルにした場合は、CoS および DSCP 値は変更されません（デフォルトの QoS 設定）。

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 透過性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 コマンドを入力しても、DSCP 透過性はイネーブルのままです。

別の QoS ドメインと境界を接しているポート上での DSCP 信頼状態の設定

管理している 2 つの個別の QoS ドメイン間に、IP トラフィックの QoS 機能を実装する場合は、図 39-12 に示すように、それらのドメインの境界に位置するスイッチ ポートを DSCP 信頼状態に設定できます。これで、受信ポートが DSCP 信頼値を受け入れ、QoS の分類段階を省略できるようになります。2 つのドメインが異なる DSCP 値を使用している場合は、DSCP/DSCP 変換マップを設定して、DSCP 値のセットをもう一方のドメインの定義に一致するように変換できます。

図 39-12　別の QoS ドメインと境界を接するポート上での DSCP 信頼状態



特権 EXEC モードで開始し、次の手順に従ってポートで DSCP 信頼状態を設定し、DSCP/DSCP 変換マップを修正します。両方の QoS ドメインでマッピングの方法に一貫性を持たせるには、両方のドメインのポートで次の手順を実行する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを修正します。 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-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、最大で 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。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	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 モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**mls qos trust dscp**	入力ポートを DSCP の信頼できるポートとして設定します。デフォルトでは、ポートは信頼されません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された入力 DSCP の信頼できる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。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos maps dscp-mutation**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ポートを信頼されない状態に戻すには、**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。

次に、ポートを DSCP 信頼状態に設定し、10 ～ 13 の着信 DSCP 値を DSCP 30 にマッピングするように DSCP/DSCP 変換マップ（*gi0/2-mutation*）を修正する例を示します。

```
Switch(config)# mls qos map dscp-mutation gi1/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi1/2-mutation
Switch(config-if)# end
```

QoS ポリシーの設定

QoS ポリシーを設定するには、通常は、トラフィックのクラスへの分類、これらのトラフィック 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が必要です。

基本的な情報については、「分類」（P.39-5）および「ポリシングおよびマーキング」（P.39-9）を参照してください。設定の注意事項については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。

ここでは、トラフィックを分類し、ポリシングし、マーキングする方法について説明します。ネットワークの設定に応じて、次の 1 つまたは複数の作業を実行する必要があります。

- 「ACL を使用したトラフィックの分類」（P.39-45）
- 「クラス マップを使用したトラフィックの分類」（P.39-48）
- 「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）
- 「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）
- 「aggregate ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング」（P.39-62）

ACL を使用したトラフィックの分類

IP トラフィックは、IP 標準 ACL または IP 拡張 ACL を使用して分類できます。非 IP トラフィックは、レイヤ 2 MAC ACL を使用して分類できます。

特権 EXEC モードで開始し、次の手順に従って、IP トラフィックの IP 標準 ACL を作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* にはアクセス リスト番号を入力します。指定できる範囲は 1 ～ 99 および 1300 ～ 1999 です。 • 条件が一致したときに特定のタイプのトラフィックを許可するには、**permit** キーワードを使用します。条件が一致したときに特定のタイプのトラフィックを拒否するには、**deny** キーワードを使用します。 • *source* には、パケットの送信元のネットワークまたはホストを入力します。**any** キーワードは、0.0.0.0 255.255.255.255 の略として使用できます。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード 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 を指定します。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

次に、指定された 3 つのネットワーク上のホストだけにアクセスを許可する例を示します。ワイルドカード ビットが、ネットワーク アドレスのホスト部分に適用されます。アクセス リスト ステートメントに一致しない発信元アドレスを持つホストは拒否されます。

```
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)
```

特権 EXEC モードで開始し、次の手順に従って、IP トラフィックの IP 拡張 ACL を作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**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。指定できる範囲は 100 ～ 199 および 2000 ～ 2699 です。 • 条件が一致したときに特定のタイプのトラフィックを許可するには、**permit** キーワードを使用します。条件が一致したときに特定のタイプのトラフィックを拒否するには、**deny** キーワードを使用します。 • *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、使用可能なプロトコルのキーワードのリストが表示されます。 • *source* には、パケットの送信元のネットワークまたはホストを入力します。これを指定するには、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 の略として **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 を入れて、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 進を使用したり、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の略として **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、パケットの送信先のネットワークまたはホストを入力します。*destination* と *destination-wildcard* の指定には、*source* と *source-wildcard* で説明したものと同じオプションを使用できます。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

次に、任意の送信元から、DSCP 値が 32 に設定された着信先への 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、precedence 値が 5 に設定された 10.1.1.2 の着信先ホストまでの 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 host 10.1.1.1 host 10.1.1.2 precedence 5
```

次に、任意のソースから、DSCP が 32 に設定された着信先グループ アドレス 224.0.0.2 への PIM 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 102 permit pim any 224.0.0.2 dscp 32
```

特権 EXEC モードで開始し、次の手順に従って、非 IP トラフィックのレイヤ 2 MAC ACL を作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mac access-list extended** *name*	リストの名前を指定して、レイヤ 2 MAC ACL を作成します。 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 モードに変わります。
ステップ 3	{**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	条件が一致したときに許可または拒否するトラフィックのタイプを指定し、必要な回数だけコマンドを入力します。 • *src-MAC-addr* には、パケットの送信元ホストの MAC アドレスを入力します。これを指定するには、16 進フォーマット（H.H.H）を使用したり、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の略として **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 を入れて、ワイルドカード ビットを指定します。 • *dst-MAC-addr* には、パケットの送信先ホストの MAC アドレスを入力します。これを指定するには、16 進フォーマット（H.H.H）を使用したり、*source* 0.0.0、*source-wildcard* ffff.ffff.ffff の略として **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、パケットのプロトコルを識別します。*type* の指定できる範囲は 0 ～ 65535 です。通常は 16 進数で指定します。*mask* には、一致をテストする前に Ethertype に適用する *don't care* ビットを入力します。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*access-list-number* | *access-list-name*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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 コマンドを使用します。

次に、2 つの許可ステートメントを持つレイヤ 2 MAC ACL を作成する例を示します。最初のステートメントにより、MAC アドレスが 0001.0000.0001 のホストから MAC アドレスが 0002.0000.0001 のホストへのトラフィックが許可されます。次のステートメントでは、MAC アドレスが 0001.0000.0002 のホストから MAC アドレスが 0002.0000.0002 のホストへの、Ethertype が XNS-IDP のトラフィックだけが許可されます。

```
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)
```

クラス マップを使用したトラフィックの分類

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、特定のトラフィック フロー（またはクラス）の名前を指定し、他のすべてのトラフィックから分離します。クラス マップは、さらに詳細に分類するために、特定のトラフィック フローと照合する基準を定義します。一致ステートメントには、ACL、IP precedence 値、DSCP 値などの基準を入れることができます。一致基準は、クラスマップ コンフィギュレーション モードで 1 つの一致ステートメントを入力することにより定義されます。

（注） **class** ポリシーマップ コンフィギュレーション コマンドを使用して、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。詳細については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）および「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）を参照してください。

特権 EXEC モードで開始し、次の手順に従ってクラス マップを作成し、トラフィックを分類するための一致基準を定義します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] または **access-list** *access-list-number* {**deny** | **permit**} *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] または **mac access-list extended** *name* {**permit** | **deny**} {**host** *src-MAC-addr mask* | **any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask*]	IP トラフィック用の IP 標準 ACL または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「ACL を使用したトラフィックの分類」（P.39-45）を参照してください。 **（注）** アクセス リストを作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。

	コマンド	目的
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **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）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
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基準を定義します。 デフォルトでは、一致基準は定義されません。 クラス マップごとに 1 つの一致基準だけがサポートされます。また、クラス マップごとに 1 つの ACL だけがサポートされます。 • **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。 • **ip dscp** *dscp-list* には、着信パケットと照合する最大で 8 つの IP DSCP 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する最大で 8 つの IP-precedence 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show class-map**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス 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。一致基準を削除するには、**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。

次に、*class1* という名前のクラス マップを設定する例を示します。*class1* には 1 つの一致基準（アクセス リスト 103）があります。この基準は、任意のホストから、DSCP 値 10 に一致する着信先へのトラフィックを許可します。

```
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 10、11、および 12 を持つ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 5、6、および 7 を持つ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#
```

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

アクションの対象とするトラフィック クラスを指定する非階層ポリシー マップを物理ポートで設定できます。アクションには、トラフィック クラスの CoS、DSCP、または IP precedence 値の信頼、トラフィック クラスへの特定の DSCP または IP precedence 値の設定、また一致する各トラフィック クラスのトラフィック帯域幅の制限（ポリサー）と、トラフィックがプロファイル外のときに実行するアクションの指定（マーキング）が含まれます。

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、それぞれが異なる一致基準とポリサーを持つ複数のクラス ステートメントを含めることができます。
- ポリシー マップには、あらかじめ定義されたデフォルト トラフィック クラスを含めることができます。これはマップの末尾に明示的に配置されます。
- 1 つのポートを通じて受信されるトラフィックのタイプごとに、個別のポリシーマップ クラスを持つことができます。
- ポリシーマップの信頼状態とポートの信頼状態は互いに排他的で、後で設定した方が優先されます。

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

- 入力ポートごとに 1 つのポリシー マップだけを付加できます。
- **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 マップを設定すると、この設定は、IP precedence 値を信頼するように設定された入力インターフェイス上のパケットだけに影響を与えます。ポリシー マップで、**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と、出力 DSCP 値は IP precedence/DSCP マップの影響を受けません。出力 DSCP 値を入力値とは異なる値にする場合は、**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** コマンドを入力するか、またはすでに使用していると、このコマンドはスイッチの設定で **set dscp** に変更されます。
- **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 コマンドを使用して、パケットの 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。
- ポートについて定義されたクラスごとに、第 2 レベルのポリシー マップを個別に設定できます。第 2 レベルのポリシー マップは、各トラフィック クラスで実行するポリシング アクションを指定します。階層ポリシー マップの設定については、「階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング」（P.39-56）を参照してください。

- ポリシーマップとポートの信頼状態の両方を、1 つの物理インターフェイス上で実行できます。ポリシーマップは、ポートの信頼状態の前に適用します。
- **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 トラフィック クラスを設定すると、分類されないトラフィック（トラフィック クラスで指定されている一致基準に適合しないトラフィック）は、デフォルト トラフィック クラス（**class-default**）として処理されます。

特権 EXEC モードで開始し、次の手順に従って非階層ポリシー マップを作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	クラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **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）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードに入ります。 デフォルトでは、ポリシー マップは定義されません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合に DSCP が 0 に、パケットがタグ付きの場合に CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 4	**class** [*class-map-name* | **class-default**]	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 モードに入ります。 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ません。 **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 クラスがすでに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 クラスはあらかじめ定義されていて、任意のポリシーに追加できます。これは常に、ポリシー マップの末尾に配置されます。**class-default** クラスには **match any** が暗黙的に含まれているため、他のトラフィック クラスに一致しなかったパケットはすべて、**class-default** に一致します。

	コマンド	目的
ステップ 5	**trust** [**cos** | **dscp** | **ip-precedence**]	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 が使用する信頼状態を設定します。 **（注）** このコマンドは、同じポリシー マップ内では **set** コマンドと互いに排他的です。**trust** コマンドを入力する場合は、ステップ 6 に進みます。 デフォルトでは、ポートは信頼されません。キーワードが指定されず、コマンドが入力されている場合、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 値またはデフォルトのポート CoS 値と、CoS/DSCP マップを使用して DSCP 値を導出します。 • **dscp**：QoS は、入力パケットの DSCP 値を使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは､QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 • **ip-precedence**：QoS は、入力パケットの IP precedence 値と IP precedence/DSCP マップを使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは、QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 詳細については、「CoS/DSCP マップの設定」（P.39-65）を参照してください。
ステップ 6	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットで新しい値を設定することにより IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類し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、分類し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。

	コマンド	目的
ステップ 7	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類したトラフィックの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ません。サポートされているポリサーの数については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。 • *rate-bps* には、平均トラフィック レートをビット/秒（b/s）単位で指定します。指定できる範囲は 8000 ～ 10000000000 です。 *burst-byte* には、通常のバースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超えたときに実行するアクションを指定します。パケットを廃棄するには、**exceed-action drop** キーワードを使用します。（ポリシング設定 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。詳細については、「ポリシング設定 DSCP マップの設定」（P.39-67）を参照してください。
ステップ 8	**exit**	ポリシー マップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *interface-id*	ポリシー マップを付加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 モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 11	**service-policy input** *policy-map-name*	ポリシー マップ名を指定し、これを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 12	**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*]]	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス 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。信頼されない状態に戻すには、**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。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。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。ポリシー マップとポートの関連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。

次に、ポリシー マップを作成し、入力ポートに適用する例を示します。この設定では、IP 標準 ACL は、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。この分類に一致するトラフィックでは、着信パケットの DSCP 値は信頼されます。一致するトラフィックが、平均トラフィック レートの 48000 b/s と通常のバースト サイズの 8000 バイトを超える場合は、（ポリシング設定 DSCP マップに基づいて）その DSCP がマークダウンされ、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 gigabitethernet1/1
Switch(config-if)# service-policy input flow1t
```

次に、2 つの許可ステートメントを使用してレイヤ 2 MAC ACL を作成し、入力ポートに付加する例を示します。最初の許可ステートメントにより、MAC アドレスが 0001.0000.0001 のホストから MAC アドレスが 0002.0000.0001 のホストまでのトラフィックが許可されます。次の許可ステートメントでは、MAC アドレスが 0001.0000.0002 のホストから MAC アドレスが 0002.0000.0002 のホストまでの Ethertype XNS-IDP トラフィックだけが許可されます。

```
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 gigabitethernet1/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

次の例では、IPv4 トラフィックと IPv6 トラフィックの両方に適用されるとともに、分類されないトラフィックに適用されるデフォルト クラスを含むクラス マップの作成方法を示します。

```
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
```

階層ポリシー マップを使用した、SVI でのトラフィックの分類、ポリシング、およびマーキング

階層ポリシー マップは SVI では設定できますが、他のタイプのインターフェイスでは設定できません。階層ポリシングでは、VLAN レベルとインターフェイスレベルのポリシー マップを組み合わせて 1 つのポリシー マップを作成します。

SVI では、VLAN レベルのポリシー マップは、アクションの対象となるトラフィック クラスを指定します。アクションには、CoS、DSCP、または IP precedence 値の信頼設定や、トラフィック クラスの特定の DSCP または IP precedence 値の設定などが含まれます。individual ポリサーの影響を受ける物理ポートを指定するには、インターフェイスレベルのポリシー マップを使用します。

階層ポリシー マップを設定する場合は、次の注意事項に従ってください。

- 階層ポリシー マップを設定する前に、ポリシー マップのインターフェイス レベルで指定する物理ポートで VLAN ベースの QoS をイネーブルにする必要があります。
- 入力ポートまたは SVI ごとに 1 つのポリシー マップだけを付加できます。
- ポリシー マップには、それぞれ異なる一致基準とアクションを持つ複数のクラス ステートメントを含めることができます。
- SVI で受信されるトラフィックのタイプごとに、個別のポリシーマップ クラスを持つことができます。
- ポリシーマップとポートの信頼状態の両方を、1 つの物理インターフェイス上で実行できます。ポリシーマップは、ポートの信頼状態の前に適用します。
- **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 マップを設定すると、この設定は、IP precedence 値を信頼するように設定された入力インターフェイス上のパケットだけに影響を与えます。ポリシー マップで、**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と、出力 DSCP 値は IP precedence/DSCP マップの影響を受けません。出力 DSCP 値を入力値とは異なる値にする場合は、**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** コマンドを入力するか、またはすでに使用していると、このコマンドはスイッチの設定で **set dscp** に変更されます。**set ip dscp** コマンドを入力すると、スイッチ コンフィギュレーションではこの設定は **set dscp** として表示されます。
- **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 コマンドを使用して、パケットの 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。
- VLAN ベースの QoS をイネーブルにすると、階層ポリシー マップは、それまでに設定されているポートベースのポリシー マップよりも優先されます。
- 階層ポリシー マップは SVI に付加され、VLAN に属するすべてのトラフィックに影響を与えます。VLAN レベルのポリシー マップで指定されたアクションは、SVI に属するトラフィックに影響を与えます。ポートレベルのポリシー マップでのポリシング アクションは、関連する物理インターフェイス上の入力トラフィックに影響を与えます。
- トランク ポートで階層ポリシー マップを設定する場合は、VLAN の範囲が重なってはなりません。範囲が重なると、ポリシー マップで指定されたアクションが、重なった VLAN の入力トラフィックと出力トラフィックに影響を与えます。
- 階層ポリシー マップでは aggregate ポリサーはサポートされていません。
- VLAN ベースの QoS を有効にすると、スイッチは、VLAN マップなどの VLAN ベースの機能をサポートします。
- 階層ポリシー マップは、プライベート VLAN のプライマリ VLAN だけで設定できます。

- **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 トラフィック クラスを設定すると、分類されないトラフィック（トラフィック クラスで指定されている一致基準に適合しないトラフィック）は、デフォルト トラフィック クラス（**class-default**）として処理されます。

特権 EXEC モードで開始し、次の手順に従って階層ポリシー マップを作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map** [**match-all** | **match-any**] *class-map-name*	VLAN レベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。クラス マップの作成については、「クラス マップを使用したトラフィックの分類」（P.39-48）を参照してください。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **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）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
ステップ 3	**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基準を定義します。 デフォルトでは、一致基準は定義されません。 クラス マップごとに 1 つの一致基準だけがサポートされます。また、クラス マップごとに 1 つの ACL だけがサポートされます。 • **access-group** *acl-index-or-name* には、ACL の番号または名前を指定します。 • **ip dscp** *dscp-list* には、着信パケットと照合する最大で 8 つの IP DSCP 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。 • **ip precedence** *ip-precedence-list* には、着信パケットと照合する最大で 8 つの IP-precedence 値のリストを入力します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
ステップ 4	**exit**	クラスマップ コンフィギュレーション モードに戻ります。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	**class-map** [**match-all** | **match-any**] *class-map-name*	インターフェイスレベルのクラス マップを作成し、クラスマップ コンフィギュレーション モードに入ります。 デフォルトでは、クラス マップは定義されません。 • （任意）このクラス マップのすべての一致ステートメントで論理 AND を実行するには、**match-all** キーワードを使用します。クラス マップ内のすべての一致基準が一致する必要があります。 • （任意）このクラス マップのすべての一致ステートメントで論理 OR を実行するには、**match-any** キーワードを使用します。1 つまたは複数の一致基準が一致する必要があります。 • *class-map-name* には、クラス マップの名前を指定します。 **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）** クラス マップごとに 1 つの **match** コマンドだけがサポートされるため、**match-all** キーワードと **match-any** キーワードの機能は同じです。
ステップ 7	**match input-interface** *interface-id-list*	インターフェイスレベルのクラス マップの対象となる物理ポートを指定します。最大で 6 つのポートを次のように指定できます。 • 単一のポート（1 つのエントリとしてカウントされる） • スペースで区切られたポートのリスト（各ポートが 1 つのエントリとしてカウントされる） • ハイフンで区切られたポートの範囲（2 つのエントリとしてカウントされる） このコマンドは、子レベルのポリシー マップでだけ使用でき、子レベルのポリシー マップ内での唯一の一致条件である必要があります。
ステップ 8	**exit**	クラスマップ コンフィギュレーション モードに戻ります。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**policy-map** *policy-map-name*	ポリシーマップ名を入力してインターフェイスレベルのポリシー 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 モードに入ります。 デフォルトでは、ポリシー マップは定義されず、ポリシングは実行されません。
ステップ 11	**class-map** *class-map-name*	インターフェイスレベルのトラフィックの分類を定義し、ポリシーマップ コンフィギュレーション モードに入ります。 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ません。 **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 クラスがすでに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。

	コマンド	目的
ステップ 12	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **policed-dscp-transmit**}]	分類されたトラフィックに individual 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ません。サポートされているポリサーの数については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。 *rate-bps* には、平均トラフィック レートをビット/秒（b/s）単位で指定します。指定できる範囲は 8000 ～ 10000000000 です。 • *burst-byte* には、通常のバースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • （任意）レートを超えたときに実行するアクションを指定します。パケットを廃棄するには、**exceed-action drop** キーワードを使用します。（ポリシング設定 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。詳細については、「ポリシング設定 DSCP マップの設定」（P.39-67）を参照してください。
ステップ 13	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 14	**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 15	**policy-map** *policy-map-name*	ポリシーマップ名を入力して VLAN レベルのポリシー 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 モードに入ります。 デフォルトでは、ポリシー マップは定義されません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合に DSCP が 0 に、パケットがタグ付きの場合に CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 16	**class** [*class-map-name* | **class-default**]	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 モードに入ります。 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ません。 **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 クラスがすでに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 クラスはあらかじめ定義されていて、任意のポリシーに追加できます。これは常に、ポリシー マップの末尾に配置されます。**class-default** クラスには **match any** が暗黙的に含まれているため、他のトラフィック クラスに一致しなかったパケットはすべて、**class-default** に一致します。

	コマンド	目的
ステップ 17	**trust** [**cos** | **dscp** | **ip-precedence**]	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 が使用する信頼状態を設定します。 （注）　このコマンドは、同じポリシー マップ内では **set** コマンドと互いに排他的です。**trust** コマンドを入力する場合は、ステップ 18 を飛ばします。 デフォルトでは、ポートは信頼されません。キーワードが指定されず、コマンドが入力されている場合、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 値またはデフォルトのポート CoS 値と、CoS/DSCP マップを使用して DSCP 値を導出します。 • **dscp**：QoS は、入力パケットの DSCP 値を使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは､QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 • **ip-precedence**：QoS は、入力パケットの IP precedence 値と IP precedence/DSCP マップを使用して DSCP 値を導出します。タグ付きの非 IP パケットでは、QoS は受信した CoS 値を使用して DSCP 値を導出します。タグなしの非 IP パケットでは、QoS はデフォルトのポート CoS 値を使用して DSCP 値を導出します。いずれの場合でも、DSCP 値は CoS/DSCP マップから導出されます。 詳細については、「CoS/DSCP マップの設定」（P.39-65）を参照してください。
ステップ 18	**set** {**dscp** *new-dscp* | **ip precedence** *new-precedence*}	パケットで新しい値を設定することにより IP トラフィックを分類します。 • **dscp** *new-dscp* には、分類し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、分類し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。
ステップ 19	**service-policy** *policy-map-name*	インターフェイスレベルのポリシーマップ名を指定し（ステップ 10 より）、これを VLAN レベルのポリシー マップと関連付けます。 VLAN レベルのポリシー マップが複数のクラスを指定する場合は、Cisco IOS Release 12.2(25)SED 以降、各クラスに異なる **service-policy** *policy-map-name* コマンドを使用できます。
ステップ 20	**exit**	ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 21	**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 22	**interface** *interface-id*	階層ポリシー マップを付加する SVI を指定し、インターフェイス コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 23	**service-policy input** *policy-map-name*	VLAN レベルのポリシーマップ名を指定し、SVI に適用します。前のステップとこのコマンドを繰り返し、ポリシー マップを他の SVI に適用します。 階層 VLAN レベルのポリシー マップに複数のインターフェイスレベルのポリシー マップがある場合は、すべてのクラス マップを、**service-policy** *policy-map-name* コマンドで指定された同じ VLAN レベルのポリシー マップに設定しなければなりません。
ステップ 24	**end**	特権 EXEC モードに戻ります。
ステップ 25	**show policy-map** [*policy-map-name* [**class** *class-map-name*]] または **show mls qos vlan-based**	設定を確認します。
ステップ 26	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

既存のポリシー マップを削除するには、**no policy-map** *policy-map-name* グローバル コンフィギュレーション コマンドを使用します。既存のクラス 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。

ポリシー マップで信頼されない状態に戻すには、**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。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。

（注）　インターフェイスレベルのポリシー マップで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。階層ポリシー マップとポートの関連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。

次に、階層ポリシー マップを作成する例を示します。

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
```

次に、新しいマップを SVI に付加する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input g3/0/1 - g3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
```

```
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

次の例では、ポリシー マップにデフォルト トラフィック クラスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c) set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust cos
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

次の例では、class-default が先に設定されていても、ポリシー マップ pm3 の末尾にデフォルト トラフィック クラスが自動的に配置される様子を示します。

```
Switch# show policy-map pm3
  Policy Map pm3
    Class cm-3
      set dscp 4
    Class cm-4
      trust cos
    Class class-default
      police 8000 80000 exceed-action drop
Switch#
```

aggregate ポリサーを使用したトラフィックの分類、ポリシング、およびマーキング

aggregate ポリサーを使用することで、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、aggregate ポリサーは、異なるポリシー マップ間やポート間では使用できません。

aggregate ポリサーは、物理ポートの非階層ポリシー マップだけで設定できます。

特権 EXEC モードで開始し、次の手順に従って aggregate ポリサーを作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**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、aggregate ポリサーは定義されません。サポートされているポリサーの数については、「標準の QoS 設定の注意事項」（P.39-35）を参照してください。 • *aggregate-policer-name* には、aggregate 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（b/s）単位で指定します。指定できる範囲は 8000 ～ 10000000000 です。 • *burst-byte* には、通常のバースト サイズをバイト単位で指定します。指定できる範囲は 8000 ～ 1000000 です。 • レートを超えたときに実行するアクションを指定します。パケットを廃棄するには、**exceed-action drop** キーワードを使用します。（ポリシング設定 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。詳細については、「ポリシング設定 DSCP マップの設定」（P.39-67）を参照してください。
ステップ 3	**class-map** [**match-all** | **match-any**] *class-map-name*	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。詳細については、「クラス マップを使用したトラフィックの分類」（P.39-48）を参照してください。
ステップ 4	**policy-map** *policy-map-name*	ポリシー マップ名を入力してポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードに入ります。 詳細については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）を参照してください。
ステップ 5	**class** [*class-map-name* | **class-default**]	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 モードに入ります。 詳細については、「ポリシー マップを使用した、物理ポートでのトラフィックの分類、ポリシング、およびマーキング」（P.39-50）を参照してください。
ステップ 6	**police aggregate** *aggregate-policer-name*	同じポリシー マップ内の複数のクラスに aggregate 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。
ステップ 7	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *interface-id*	ポリシー マップを付加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 モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。

	コマンド	目的
ステップ 9	**service-policy input** *policy-map-name*	ポリシー マップ名を指定し、これを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**	特権 EXEC モードに戻ります。
ステップ 11	**show mls qos aggregate-policer** [*aggregate-policer-name*]	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定された aggregate 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 モードを使用します。aggregate ポリサーとそのパラメータを削除するには、**no mls qos 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。

次に、aggregate ポリサーを作成し、これをポリシー マップ内の複数のクラスに付加する例を示します。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では、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では、パケットの DSCP が 56 に変更されます。ネットワーク 10.1.0.0 とホスト 11.3.1.1 からのトラフィック レートがポリシングされます。トラフィックの平均レートが 48000 b/s を超え、通常のバースト サイズが 8000 バイトを超える場合は、（ポリシング設定 DSCP マップに基づいて）その DSCP がマークダウンされ、送信されます。ポリシー マップは入力ポートに付加されます。

```
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 gigabitethernet1/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

DSCP マップの設定

ここでは、次の設定情報について説明します。

- 「CoS/DSCP マップの設定」（P.39-65）（任意）
- 「IP precedence/DSCP マップの設定」（P.39-66）（任意）
- 「ポリシング設定 DSCP マップの設定」（P.39-67）（任意、マップのヌル設定が適切でない場合を除く）
- 「DSCP/CoS マップの設定」（P.39-68）（任意）
- 「DSCP/DSCP 変換マップの設定」（P.39-69）（任意、マップのヌル設定が適切でない場合を除く）

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

CoS/DSCP マップの設定

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

表 39-13 に、デフォルトの CoS/DSCP マップを示します。

表 39-13　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

これらの値がネットワークに適していない場合は、値を修正する必要があります。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map cos-dscp** *dscp1...dscp8*	CoS/DSCP マップを修正します。 *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。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps cos-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

次に、CoS/DSCP マップを修正し、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
```

IP precedence/DSCP マップの設定

IP precedence/DSCP マップを使用して、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で使用する DSCP 値にマッピングします。

表 39-14 に、デフォルトの IP precedence/DSCP マップを示します。

表 39-14　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
5	40
6	48
7	56

これらの値がネットワークに適していない場合は、値を修正する必要があります。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map ip-prec-dscp** *dscp1...dscp8*	IP precedence/DSCP マップを修正します。 *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。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps ip-prec-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

次の例に、IP precedence/DSCP マップを修正し、表示する方法を示します。

```
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
```

ポリシング設定 DSCP マップの設定

ポリシング設定 DSCP マップを使用し、ポリシングおよびマーキング アクションの結果として、DSCP 値を新しい値にマークダウンします。

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。

特権 EXEC モードで開始し、次の手順に従ってポリシング設定 DSCP マップを修正します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map policed-dscp** *dscp-list* **to** *mark-down-dscp*	ポリシング設定 DSCP マップを修正します。 • *dscp-list* には、最大で 8 つの DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 • *mark-down-dscp* には、対応するポリシング設定（マークダウンされた）DSCP 値を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps policed-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

次に、DSCP 50 を 57 にマッピングし、DSCP 値 0 をマークダウンする例を示します。

```
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）　このポリシング設定 DSCP マップでは、マークダウンされた DSCP 値はマトリクスの本体に表示されます。d1 列は元の DSCP の最上位桁を指定し、d2 行は元の DSCP の最下位桁を指定します。d1 値と d2 値の交点がマークダウン値を示します。たとえば、元の DSCP 値 53 は、マークダウンされた DSCP 値 0 に対応します。

DSCP/CoS マップの設定

DSCP/CoS マップを使用して、4 つの出力キューの 1 つを選択するために使用する CoS 値を生成します。

表 39-15 に、デフォルトの DSCP/CoS マップを示します。

表 39-15　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

これらの値がネットワークに適していない場合は、値を修正する必要があります。

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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-cos** *dscp-list* **to** *cos*	DSCP/CoS マップを修正します。 • *dscp-list* には、最大で 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 値が対応する 1 つの CoS 値を入力します。 指定できる DSCP の範囲は 0 ～ 63 で、CoS の範囲は 0 ～ 7 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps dscp-to-cos**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

次に、DSCP 値 0、8、16、24、32、40、48、50 を CoS 値 0 にマッピングし、この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） この DSCP/CoS マップでは、CoS 値がマトリクスの本体に表示されています。d1 列は DSCP の最上位桁を指定し、d2 行は DSCP の最下位桁を指定します。d1 値と d2 値の交点が CoS 値を示します。たとえば、この DSCP/CoS マップでは、DSCP 値 08 は CoS 値 0 に対応します。

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインが異なる DSCP 定義を持つ場合は、DSCP/DSCP 変換マップを使用して、一方の DSCP 値のセットをもう一方のドメインの定義に適合するように変換します。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）。

入力変換では、新しい DSCP 値がパケット内の値を上書きし、QoS はこの新しい値を使用してパケットを処理します。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。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-mutation** *dscp-mutation-name in-dscp* **to** *out-dscp*	DSCP/DSCP 変換マップを修正します。 • *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、最大で 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。 指定できる DSCP の範囲は 0 ～ 63 です。
ステップ 3	**interface** *interface-id*	マップを付加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 モードに入ります。 指定できるインターフェイスとして、物理ポートも含まれます。
ステップ 4	**mls qos trust dscp**	入力ポートを DSCP の信頼できるポートとして設定します。デフォルトでは、ポートは信頼されません。
ステップ 5	**mls qos dscp-mutation** *dscp-mutation-name*	指定された入力 DSCP の信頼できる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**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show mls qos maps dscp-mutation**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

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エントリはすべて変更されません（ヌル マップ内の指定のままです）。

```
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 gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
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） この DSCP/DSCP 変換マップでは、変換される値がマトリクスの本体に表示されています。d1 列は元の DSCP の最上位桁を指定し、d2 行は元の DSCP の最下位桁を指定します。d1 値と d2 値の交点が変換される値を示します。たとえば、DSCP 値 12 が変換される値 10 に対応します。

入力キューの特性の設定

ネットワークと QoS ソリューションの複雑さによっては、次の項の作業をすべて実行しなければならないことがあります。次の特性を決定する必要があります。

- （DSCP または CoS 値によって）各キューに割り当てるパケット
- 各キューに適用する廃棄スレッシュホールド（%）と、各スレッシュホールドにマッピングする CoS または DSCP 値
- 各キューに割り当てる使用可能なバッファ領域の大きさ
- 各キューに割り当てる使用可能な帯域幅の大きさ
- 高いプライオリティを割り当てる必要があるトラフィック（音声など）があるかどうか

ここでは、次の設定情報について説明します。

- 「DSCP または CoS 値の入力キューへのマッピングと、WTD スレッシュホールドの設定」（P.39-71）（任意）
- 「入力キュー間でのバッファ領域の割り当て」（P.39-72）（任意）
- 「入力キュー間での帯域幅の割り当て」（P.39-73）（任意）
- 「入力プライオリティ キューの設定」（P.39-74）（任意）

DSCP または CoS 値の入力キューへのマッピングと、WTD スレッシュホールドの設定

特定の DSCP または CoS を持つパケットを特定のキューに置き、低いプライオリティを持つパケットが廃棄されるように、キューのスレッシュホールドを調整することで、トラフィックのプライオリティを設定できます。

特権 EXEC モードで開始し、次の手順に従って、DSCP または CoS 値を入力キューにマッピングし、WTD スレッシュホールドを設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue input cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を、入力キューとスレッシュホールド ID にマッピングします。 デフォルトでは、DSCP 値 0 ～ 39 および 48 ～ 63 は、キュー 1 およびスレッシュホールド 1 にマッピングされます。DSCP 値 40 ～ 47 は、キュー 2 およびスレッシュホールド 1 にマッピングされます。 デフォルトでは、CoS 値 0 ～ 4、6、7 は、キュー 1 およびスレッシュホールド 1 にマッピングされます。CoS 値 5 は、キュー 2 およびスレッシュホールド 1 にマッピングされます。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。スレッシュホールド 3 の廃棄スレッシュホールド（%）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。
ステップ 3	**mls qos srr-queue input threshold** *queue-id threshold-percentage1 threshold-percentage2*	スレッシュホールド 1 および 2 の 2 つの WTD スレッシュホールド（%）を入力キューに割り当てます。デフォルトでは、両方のスレッシュホールドが 100% に設定されます。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • *threshold-percentage1 threshold-percentage2* では、指定できる範囲は 1 ～ 100 です。各値はスペースで区切ります。 各スレッシュホールドは、キューに割り当てられたキュー記述子の総数に対する割合です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show mls qos maps**	設定を確認します。 DSCP 入力キュー スレッシュホールド マップがマトリクスとして表示されます。d1 列は DSCP 番号の最上位桁を指定し、d2 行は DSCP 番号の最下位桁を指定します。d1 値と d2 値の交点がキュー ID とスレッシュホールド ID です。たとえば、キュー 2 とスレッシュホールド 1（02-01）のようになります。 CoS 入力キュー スレッシュホールド マップは、一番上の行に CoS 値を、2 番めの行に対応するキュー ID とスレッシュホールド ID を示します。たとえば、キュー 2 とスレッシュホールド 2（2-2）のようになります。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの CoS 入力キュー スレッシュホールド マップまたはデフォルトの DSCP 入力キュー スレッシュホールド マップに戻すには、**no mls qos srr-queue input cos-map** または **no mls qos srr-queue input dscp-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。デフォルトの WTD スレッシュホールド（%）に戻すには、**no mls qos srr-queue input 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。

次の例では、DSCP 値 0 ～ 6 を、入力キュー 1 と廃棄スレッシュホールド 50% のスレッシュホールド 1 にマッピングする方法を示します。DSCP 値 20 と 26 は、入力キュー 1 とスレッシュホールド 70% のスレッシュホールド 2 にマッピングします。

```
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26
Switch(config)# mls qos srr-queue input threshold 1 50 70
```

次の例では、DSCP 値（0 ～ 6）が WTD スレッシュホールド 50% に割り当てられ、WTD スレッシュホールド 70% に割り当てられた DSCP 値（20 ～ 26）よりも早く廃棄されます。

入力キュー間でのバッファ領域の割り当て

2 つのキューの間で入力バッファを分割する（領域の大きさを割り当てる）比率を定義します。バッファおよび帯域幅割り当ては、パケットを廃棄する前にバッファリングできるデータの量を制御します。

特権 EXEC モードで開始し、次の手順に従って入力キューの間でバッファを割り当てます。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input buffers** *percentage1 percentage2*	入力キュー間にバッファを割り当てます。 デフォルトでは、90% のバッファをキュー 1 に割り当て、10% のバッファをキュー 2 に割り当てます。 *percentage1 percentage2* では、指定できる範囲は 0 ～ 100 です。各値はスペースで区切ります。 キューがバースト性のある着信トラフィックを処理できるようにバッファを割り当てる必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show mls qos interface buffer** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには。**no mls qos srr-queue input 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。

次の例では、入力キュー 1 にバッファ スペースの 60% を、入力キュー 2 にバッファ スペースの 40% を割り当てる方法を示します。

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

入力キュー間での帯域幅の割り当て

入力キューの間に割り当てる使用可能な帯域幅の大きさを指定する必要があります。重みの比率は、SRR スケジューラがパケットを各キューから送信する頻度の比率です。帯域幅割り当てとバッファ割り当ては、パケットを廃棄する前にバッファリングできるデータの大きさを制御します。入力キューでは、SRR は共有モードだけで動作します。

特権 EXEC モードで開始し、次の手順に従って入力キュー間で帯域幅を割り当てます。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input bandwidth** *weight1 weight2*	共有ラウンド ロビンの重みを入力キューに割り当てます。 *weight1* と *weight2* のデフォルト設定は 4 です（帯域幅の 1/2 が 2 つのキューの間で均等に共有されます）。 *weight1* および *weight2* では、指定可能な範囲は 1 ～ 100 です。各値はスペースで区切ります。 SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に SRR は、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定された重みに従い、両方の入力キューで残りの帯域幅を共有し、キューを処理します。詳細については、「入力プライオリティ キューの設定」（P.39-74）を参照してください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos interface queueing** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no mls qos srr-queue input bandwidth** グローバル コンフィギュレーション コマンドを使用します。

次に、キューに入力帯域幅を割り当てる例を示します。プライオリティ キューイングはディセーブルです。割り当てられる共有帯域幅の比率は、キュー 1 が 25/（25+75）、キュー 2 が 75/（25+75）です。

```
Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75
```

入力プライオリティ キューの設定

プライオリティ キューは、優先して進める必要があるトラフィックにだけ使用してください（遅延とジッタを最小限にとどめる必要のある音声トラフィックなど）。

プライオリティ キューは帯域幅の一部が保証されており、オーバーサブスクライブ型のリング上でネットワーク トラフィックが多い場合（バックプレーンが送達できる量よりもトラフィックが多い場合、およびキューが満杯でフレームを廃棄している場合）に、遅延とジッタを軽減します。

SRR は、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight* グローバル コンフィギュレーション コマンドの **bandwidth** キーワードで指定されたとおり、設定済みの重みに従いプライオリティ キューにサービスを提供します。次に SRR は、**mls qos srr-queue input bandwidth** *weight1 weight2* グローバル コンフィギュレーション コマンドで設定された重みに従い、両方の入力キューで残りの帯域幅を共有し、キューを処理します。

特権 EXEC モードで開始し、次の手順に従ってプライオリティ キューを設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue input priority-queue** *queue-id* **bandwidth** *weight*	キューをプライオリティ キューとして割り当て、リングが輻輳している場合に内部リングの帯域幅を保証します。 デフォルトのプライオリティ キューはキュー 2 で、帯域幅の 10% が割り当てられています。 • *queue-id* で指定できる範囲は 1 ～ 2 です。 • **bandwidth** *weight* には、内部リングの帯域幅のパーセンテージを割り当てます。指定できる範囲は 0 ～ 40 です。大きい値はリング全体に影響を与え、パフォーマンスを低下させることがあるため、保証可能な帯域幅の大きさには制限があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos interface queueing** または **show mls qos input-queue**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no mls qos srr-queue input priority-queue** *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。プライオリティ キューイングをディセーブルにするには、帯域幅の重みを 0 に設定します。たとえば、**mls qos srr-queue input priority-queue** *queue-id* **bandwidth 0** と入力します。

次に、キューに入力帯域幅を割り当てる例を示します。キュー 1 は割り当てられた帯域幅の 10% を持つプライオリティ キューです。キュー 1 とキュー 2 に割り当てられた帯域幅の比率は、4/（4+4）です。SRR は最初、設定された 10% の帯域幅をキュー 1（プライオリティ キュー）にサービスします。そのあと、SRR は残りの 90% の帯域幅をキュー 1 とキュー 2 にそれぞれ 45% ずつ均等に分配します。

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

出力キューの特性の設定

ネットワークと QoS ソリューションの複雑さによっては、次の項の作業をすべて実行しなければならないことがあります。次の特性を決定する必要があります。

- DSCP または CoS 値によって各キューおよびスレッショホールド ID にマッピングされるパケット
- キューセットに適用する廃棄スレッショホールド（%）（ポート 1 つあたり 4 つの出力キュー）と、そのトラフィック タイプに予約するメモリと最大メモリの大きさ
- キューセットに割り当てる固定バッファ領域の大きさ
- ポートの帯域幅をレート制限する必要があるかどうか
- 出力キューを処理する頻度と、使用する方法（シェーピング、共有、またはその両方）

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」（P.39-75）
- 「出力キューセットのバッファ領域の割り当てと WTD スレッショホールドの設定」（P.39-75）（任意）
- 「DSCP または CoS 値の出力キューとスレッショホールド ID へのマッピング」（P.39-78）（任意）
- 「出力キューでの SRR のシェーピングされた重みの設定」（P.39-79）（任意）
- 「出力キューでの SRR の共有された重みの設定」（P.39-80）（任意）
- 「出力緊急キューの設定」（P.39-81）（任意）
- 「出力インターフェイスでの帯域幅の制限」（P.39-82）（任意）

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にされており、SRR のシェーピングされた重みが設定されていない場合は、SRR は共有モードでこのキューを処理します。

出力キューセットのバッファ領域の割り当てと WTD スレッショホールドの設定

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 コマンドを使用して、バッファの可用性を保証し、WTD スレッショホールドを設定し、キューセットの最大割り当てを設定できます。

各スレッシュホールドは、キューに割り当てられたメモリのパーセンテージであり、**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 コマンドを使用して指定します。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廃棄パーセンテージをサポートします。

（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だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って、キューセットのメモリ割り当てと廃棄スレッシュホールドを設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4*	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、キューセットのキューごとに 1 つずつ、4 つのパーセンテージを指定します。*allocation1*、*allocation3*、および *allocation4* に指定できる範囲は 0 ～ 99 です。*allocation2* の場合、指定できる範囲は 1 ～ 100 です（CPU バッファを含む）。 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、ベストエフォート トラフィックを含むキューには大きな割合のバッファを与えます。

	コマンド	目的
ステップ 3	**mls qos queue-set output** *qset-id* **threshold** *queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold*	WTD スレッシュホールドを設定し、バッファの可用性を保証し、キューセットの最大メモリ割り当てを設定します（ポート 1 つあたり 4 つの出力キュー）。 デフォルトでは、キュー 1、3、4 の WTD スレッシュホールドは 100% に設定されます。キュー 2 のスレッシュホールドは 200% に設定されます。キュー 1、2、3、4 の予約済みスレッシュホールドは 50% に設定されます。すべてのキューの最大スレッシュホールドは 400% に設定されます。 • *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、コマンドを実行するキューセット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、キューに割り当てられたメモリのパーセンテージとして表される 2 つの WTD スレッシュホールドを指定します。指定できる範囲は 1 ～ 3200% です。 • *reserved-threshold* には、キューに保証（予約）するメモリの大きさを、割り当てられるメモリのパーセンテージとして入力します。指定できる範囲は 1 ～ 100% です。 • *maximum-threshold* では、フル状態のキューが予約量を超えるバッファを取得できるようにします。これは、共通のプールが空ではない場合に、キューがパケットを廃棄せずに保持できる最大メモリです。指定できる範囲は 1 ～ 3200% です。
ステップ 4	**interface** *interface-id*	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 モードに入ります。
ステップ 5	**queue-set** *qset-id*	ポートをキューセットにマッピングします。 *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**	特権 EXEC モードに戻ります。
ステップ 7	**show mls qos interface** [*interface-id*] **buffers**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**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 スレッシュホールド（%）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。

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 にバッファ スペースの 40 % を、出力キュー 2、3、4 にそれぞれ 20 % を割り当てます。キュー 2 の廃棄スレッシュホールドを、割り当てられたメモリの 40% と 60% に設定し、割り当てられたメモリの 100% を保証（予約）して、このキューがパケットを廃棄せずに保持可能な最大メモリを 200% に設定します。

```
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 gigabitethernet1/1
Switch(config-if)# queue-set 2
```

DSCP または CoS 値の出力キューとスレッショルド ID へのマッピング

特定の DSCP または CoS を持つパケットを特定のキューに置き、低いプライオリティを持つパケットが廃棄されるようにキューのスレッショルドを調整することで、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だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って DSCP または CoS 値を出力キューにマッピングし、スレッショルド ID を設定します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos srr-queue output dscp-map queue** *queue-id* **threshold** *threshold-id dscp1...dscp8* または **mls qos srr-queue output cos-map queue** *queue-id* **threshold** *threshold-id cos1...cos8*	DSCP または CoS 値を、出力キューとスレッショルド 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 およびスレッショルド 1 にマッピングされます。DSCP 値 16 ～ 31 は、キュー 3 およびスレッショルド 1 にマッピングされます。DSCP 値 32 ～ 39 および 48 ～ 63 は、キュー 4 およびスレッショルド 1 にマッピングされます。DSCP 値 40 ～ 47 は、キュー 1 およびスレッショルド 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 およびスレッショルド 1 にマッピングされます。CoS 値 2 および 3 は、キュー 3 およびスレッショルド 1 にマッピングされます。CoS 値 4、6、7 は、キュー 4 およびスレッショルド 1 にマッピングされます。CoS 値 5 は、キュー 1 およびスレッショルド 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。 • *threshold-id* で指定できる範囲は 1 ～ 3 です。スレッショルド 3 の廃棄スレッショルド（%）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。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show mls qos maps**	設定を確認します。 DSCP 出力キュースレッシュホールド マップがマトリクスとして表示されます。d1 列は DSCP 番号の最上位桁を指定し、d2 行は DSCP 番号の最下位桁を指定します。d1 値と d2 値の交点がキュー ID とスレッシュホールド ID です。たとえば、キュー 2 とスレッシュホールド 1（02-01）のようになります。 CoS 出力キュースレッシュホールド マップは、一番上の行に CoS 値を、2 番めの行に対応するキュー ID とスレッシュホールド ID を示します。たとえば、キュー 2 とスレッシュホールド 2（2-2）のようになります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの DSCP 出力キュースレッシュホールド マップまたはデフォルトの CoS 出力キュー スレッシュホールド 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。

次に、DSCP 値 10 および 11 を出力キュー 1 およびスレッシュホールド 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
```

出力キューでの SRR のシェーピングされた重みの設定

各キューに割り当てる使用可能な帯域幅を指定できます。重みの比率は、SRR スケジューラがパケットを各キューから送出する頻度の比率です。

出力キューでは、シェーピングされた重みか共有された重み、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。シェーピングされた重みについては、「SRR のシェーピングおよび共有」（P.39-15）を参照してください。共有された重みについては、「出力キューでの SRR の共有された重みの設定」（P.39-80）を参照してください。

特権 EXEC モードで開始し、次の手順に従ってシェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キューで帯域幅のシェーピングをイネーブルにします。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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 モードに入ります。

	コマンド	目的
ステップ 3	**srr-queue bandwidth shape** *weight1 weight2 weight3 weight4*	SRR の重みを出力キューに割り当てます。 デフォルトでは、weight1 は 25 に設定され、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、シェーピングするポートのパーセンテージ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（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。 重み 0 を設定すると、対応するキューは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。同じキューセットのキューにシェーピングと共有を混在させて設定する場合、最小番号のキューにシェーピングを設定します。 シェーピング モードは、共有モードを無効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**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。

次に、キュー 1 で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、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 gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

出力キューでの SRR の共有された重みの設定

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、1 つのキューが空になってリンク共有を必要としない場合、残りのキューは未使用の帯域幅まで拡大し、キュー間でこの帯域幅を共有できます。共有では、デキューイングの頻度は重みの比によって制御され、絶対値には意味はありません。

（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だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って共有された重みを割り当て、ポートにマッピングされた 4 つの出力キューでの帯域幅の共有をイネーブルにします。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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 モードに入ります。

	コマンド	目的
ステップ 3	**srr-queue bandwidth share** *weight1 weight2 weight3 weight4*	SRR の重みを出力キューに割り当てます。 デフォルトでは、4 つの重みはすべて 25 です（帯域幅の 1/4 が各キューに割り当てられます）。 *weight1 weight2 weight3 weight4* には、SRR スケジューラがパケットを送出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。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** *interface-id* **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**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。

次の例では、出力ポートで稼動する SRR スケジューラの重みの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 1、2、3、4 の各キューに割り当てられる帯域幅はそれぞれ 1/（1+2+3+4）、2/（1+2+3+4）、3/（1+2+3+4）、および 4/（1+2+3+4）です（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 gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

出力緊急キューの設定

特定のパケットを出力緊急キューに入れることで、そのパケットのプライオリティを他のパケットよりも高く設定できます。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。

特権 EXEC モードで開始し、次の手順に従って出力緊急キューをイネーブルにします。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos**	スイッチで QoS をイネーブルにします。
ステップ 3	**interface** *interface-id*	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 モードに入ります。
ステップ 4	**priority-queue out**	出力緊急キューをイネーブルにします。このキューは、デフォルトではディセーブルです。 このコマンドを設定すると、SRR に参加するキューの数が 1 つ少なくなるため、SRR の重みとキュー サイズの比に影響を与えます。これは、**srr-queue bandwidth shape** または **srr-queue bandwidth share** コマンドの *weight1* が無視されることを意味します（比率の計算に使用されません）。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

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 gigabitethernet1/1
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
```

出力インターフェイスでの帯域幅の制限

出力ポートでは帯域幅を制限できます。たとえば、ある顧客が、高速リンクの一部しか費用を負担しない場合は、帯域幅をそのパーセンテージまで制限できます。

（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だけ、設定を変更してください。

特権 EXEC モードで開始し、次の手順に従って出力ポートで帯域幅を制限します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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 モードに入ります。
ステップ 3	**srr-queue bandwidth limit** *weight1*	制限するポート速度のパーセンテージを指定します。指定できる範囲は 10 ～ 90 です。 デフォルトでは、ポートはレート制限されず、100% に設定されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mls qos interface** [*interface-id*] **queueing**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**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。

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 gigabitethernet1/1
Switch(config-if)# srr-queue bandwidth limit 80
```

このコマンドを 80% に設定した場合、ポートは 20% の時間はアイドル状態になります。ラインレートは接続速度の 80% まで下がります（800 Mb/s）。ただし、ハードウェアはラインレートが 6 つずつ増加するよう調整しているので、この値は厳密ではありません。

標準の QoS 情報の表示

標準の QoS 情報を表示するには、表 39-16 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 39-16　標準の QoS 情報を表示するためのコマンド

コマンド	目的
show class-map [*class-map-name*]	トラフィックを分類するための一致基準を定義する QoS クラスマップを表示します。
show mls qos	グローバルな QoS 設定情報を表示します。
show mls qos aggregate-policer [*aggregate-policer-name*]	aggregate ポリサーの設定を表示します。
show mls qos input-queue	入力キューの QoS 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、ポリサーを設定したポート、キューイング方法、入力および出力の統計情報など、ポート レベルの QoS 情報を表示します。
show mls qos maps [**cos-dscp** | **cos-input-q** | **cos-output-q** | **dscp-cos** | **dscp-input-q** | **dscp-mutation** *dscp-mutation-name* | **dscp-output-q** | **ip-prec-dscp** | **policed-dscp**]	QoS 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。
show mls qos vlan *vlan-id*	指定された SVI に付加されたポリシー マップを表示します。
show policy-map [*policy-map-name* [**class** *class-map-name*]]	着信トラフィックの分類基準を定義する QoS ポリシー マップを表示します。 **（注）** 着信トラフィックの分類情報を表示する目的で **show policy-map interface** 特権 EXEC コマンドは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。