



CHAPTER 37

QoS の設定

この章では、自動 Quality of Service (QoS) コマンドを使用して、またはスイッチで標準の QoS コマンドを使用して QoS を設定する方法について説明します。QoS を使用すると、特定のトラフィックを他のトラフィック タイプよりも優先的に処理できます。QoS を使用しなかった場合、スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。特に明記しない限り、スイッチという用語は、スタンドアロンスイッチおよびスイッチ スタックを指します。

Cisco IOS Release 12.2(52)SE 以降のリリースでは、デュアル IPv4/IPv6 SDM テンプレートが設定されている場合、IPv4 および IPv6 の両方のトラフィックの QoS をサポートします。

QoS は物理ポートおよびスイッチ仮想インターフェイス (SVI) に設定できます。ポリシー マップを適用する他に、分類、キューイング、およびスケジューリングなどの QoS を同じ方法で物理ポートおよび SVI に設定します。物理ポートに QoS を設定すると、非階層型のポリシー マップが適用されません。SVI に QoS を設定すると、非階層型、または階層型のポリシー マップが適用されます。



(注)

この章で使用す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。

- 「QoS の概要」 (P.37-2)
- 「auto-QoS の設定」 (P.37-21)
- 「自動 QoS 情報の表示」 (P.37-35)
- 「標準 QoS の設定」 (P.37-35)
- 「標準 QoS 情報の表示」 (P.37-95)

スイッチは、Modular QoS Command Line Interface (MQC; モジュラ QoS コマンドライン インターフェイス) コマンドの一部をサポートします。MQC コマンドの詳細については、『Cisco IOS Modular Quality of Service Command-Line Interface Overview』のマニュアルを参照してください。

QoS の概要

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

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

QoS は、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の新しい規格である Differentiated Services (DiffServ) アーキテクチャに基づいて実装されます。このアーキテクチャでは、ネットワークに入るときに各パケットを分類することが規定されています。

この分類は IP パケット ヘッダーに格納され、推奨されない IP タイプ オブ サービス (ToS) フィールドの 6 ビットを使用して、分類 (クラス) 情報として伝達されます。分類情報をレイヤ 2 フレームでも伝達できます。レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて説明します (図 37-1 を参照)。

- レイヤ 2 フレームのプライオリティ ビット

レイヤ 2 802.1Q フレーム ヘッダーには、2 バイトのタグ制御情報フィールドがあり、上位 3 ビット (ユーザ プライオリティ ビット) で CoS 値が伝達されます。レイヤ 2 802.1Q トランクとして設定されたポートでは、ネイティブ Virtual LAN (VLAN) のトラフィックを除くすべてのトラフィックが 802.1Q フレームに収められます。

他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

レイヤ 2 CoS 値の範囲は、0 (ロー プライオリティ) ~ 7 (ハイ プライオリティ) です。

- レイヤ 3 パケットのプライオリティ ビット

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

IP precedence 値の範囲は 0 ~ 7 です。

DSCP 値の範囲は 0 ~ 63 です。



(注)

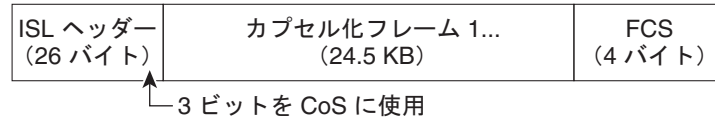
Cisco IOS Release 12.2(52)SE 以降から、デュアル IPv4/IPv6 SDM テンプレートを使用して、スイッチまたはスイッチ スタックでグローバルに IPv6 QoS をイネーブルにできるようになりました。デュアル IPv4/IPv6 テンプレートの設定後にスイッチをリロードする必要があります。詳細については、第 8 章「SDM テンプレートの設定」を参照してください。

図 37-1 フレームおよびパケットにおける QoS 分類レイヤ

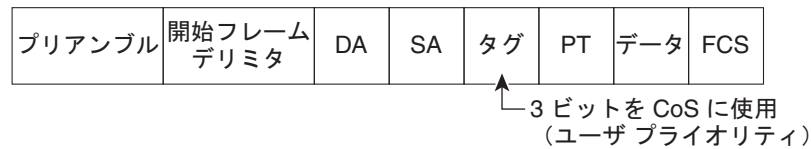
カプセル化されたパケット



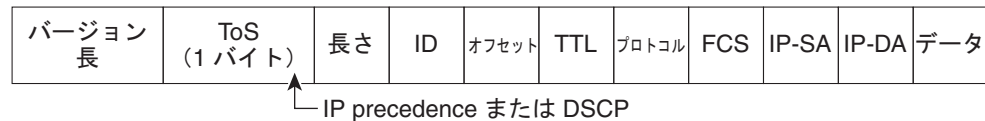
レイヤ 2 ISL フレーム



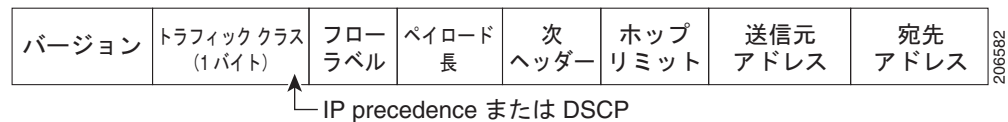
レイヤ 2 802.1Q および 802.1p フレーム



レイヤ 3 IPv4 パケット



レイヤ 3 IPv6 パケット



インターネットにアクセスするすべてのスイッチおよびルータはクラス情報に基づいて、同じクラス情報が与えられているパケットは同じ扱いで転送を処理し、異なるクラス情報のパケットはそれぞれ異なる扱いをします。パケットのクラス情報は、設定されているポリシー、パケットの詳細な検証、またはその両方に基づいて、エンドホストが割り当てるか、または伝送中にスイッチまたはルータで割り当てることができます。パケットの詳細な検証は、コアスイッチおよびルータの負荷が重くならないように、ネットワークのエッジ付近で行います。

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

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

QoS の基本モデル

QoS を実装するには、スイッチ上でパケットまたはフローを相互に区別し（分類）、パケットがスイッチを通過するときに所定の QoS を指定するラベルを割り当て、設定されたリソース使用率制限にパケットを適合させ（ポリシングおよびマーキング）、リソース競合が発生する状況に応じて異なる処理（キューイングおよびスケジューリング）を行う必要があります。また、スイッチから送信されたトラフィックが特定のトラフィック プロファイルを満たすようにする必要もあります（シェーピング）。

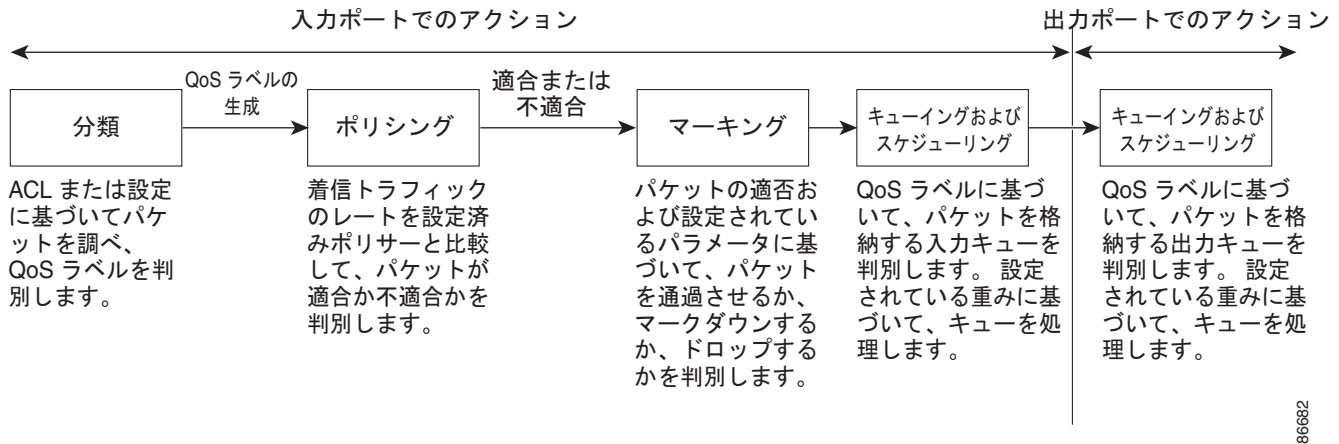
図 37-2 に、QoS の基本モデルを示します。入力ポートでのアクションには、トラフィックの分類、ポリシング、マーキング、キューイング、およびスケジューリングがあります。

- パケットと QoS ラベルを関連付けて、パケットごとに異なるパスを分類します。スイッチはパケット内の CoS または DSCP を QoS ラベルにマッピングして、トラフィックの種類を区別します。生成された QoS ラベルは、このパケットでこれ以降に実行されるすべての QoS アクションを識別します。詳細については、「[分類](#)」(P.37-5) 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ポリサーと比較して、パケットが適合か不適合かを判別します。ポリサーは、トラフィック フローで消費される帯域幅を制限します。その判別結果がマーカーに渡されます。詳細については、「[ポリシングおよびマーキング](#)」(P.37-9) を参照してください。
- マーキングでは、パケットが不適合の場合の対処法に関して、ポリサーおよび設定情報を検討し、パケットの扱い（パケットを変更しないで通過させるか、パケットの QoS ラベルをマークダウンするか、またはパケットをドロップするか）を決定します。詳細については、「[ポリシングおよびマーキング](#)」(P.37-9) を参照してください。
- キューイングでは、QoS ラベルおよび対応する DSCP または CoS 値を評価して、パケットを 2 つの入力キューのどちらに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) アルゴリズムによって拡張されます。しきい値を超過している場合、パケットはドロップされます。詳細については、「[キューイングおよびスケジューリングの概要](#)」(P.37-14) を参照してください。
- スケジューリングでは、設定されている 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 つがプライオリティ キューです。共有が設定されている場合、SRR はプライオリティ キューを処理してから他の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.37-15) を参照してください。

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

- 4 つの出力キューのどれを使用するかを選択する前に、キューイングでは、QoS パケット ラベルおよび対応する DSCP または CoS 値を評価します。複数の入力ポートが 1 つの出力ポートに同時にデータを送信すると輻輳が発生することがあるため、WTD を使用してトラフィック クラスを区別し、QoS ラベルに基づいてパケットに別々のしきい値を適用します。しきい値を超過している場合、パケットはドロップされます。詳細については、「[キューイングおよびスケジューリングの概要](#)」(P.37-14) を参照してください。
- スケジューリングでは、設定されている SRR の共有重みまたはシェーピング重みに基づいて、4 つの出力キューを処理します。キューの 1 つ（キュー 1）は、他のキューの処理前に空になるまで処理される緊急キューにできます。

図 37-2 QoS の基本モデル



分類

分類とは、パケットのフィールドを検証して、トラフィックの種類を区別するプロセスです。QoS がスイッチ上でグローバルにイネーブルになっている場合のみ、分類はイネーブルです。デフォルトでは、QoS はグローバルにディセーブルになっているため、分類は実行されません。

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

QoS ラベルは、パケット内の DSCP または CoS 値に基づいて、パケットに実行されるキューイングおよびスケジューリングアクションを決定します。QoS ラベルは信頼設定およびパケットタイプに従ってマッピングされます (図 37-3 (P.37-7) を参照)。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。非 IP トラフィックには、次の分類オプションを使用できます (図 37-3 を参照)。

- 着信フレームの CoS 値を信頼します (ポートが CoS を信頼するように設定します)。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 2 802.1Q フレームのヘッダーは、タグ制御情報フィールドの上位 3 ビットで CoS 値を伝達します。CoS 値の範囲は、0 (ロープライオリティ) ~ 7 (ハイプライオリティ) です。
- 着信フレームの DSCP または IP precedence 値を信頼します。これらの設定は、非 IP トラフィックの場合は無意味です。これらのいずれかの方法で設定されているポートに非 IP トラフィックが着信した場合は、CoS 値が割り当てられ、CoS/DSCP マップから内部 DSCP 値が生成されます。スイッチは内部 DSCP 値を使用して、トラフィックのプライオリティを表示する CoS 値を生成します。
- 設定されたレイヤ 2 の MAC アクセスコントロールリスト (ACL) に基づいて分類を実行します。レイヤ 2 の MAC ACL は、MAC 送信元アドレス、MAC 宛先アドレス、およびその他のフィールドを調べることができます。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップアクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

IP トラフィックには、次の分類オプションを使用できます (図 37-3 を参照)。

- 着信パケットの DSCP 値を信頼し (DSCP を信頼するようにポートを設定し)、同じ DSCP 値をパケットに割り当てます。IETF は、1 バイトの ToS フィールドの上位 6 ビットを DSCP として定義しています。特定の DSCP 値が表すプライオリティは、設定可能です。DSCP 値の範囲は 0 ~ 63 です。

2 つの QoS 管理ドメインの境界上にあるポートの場合は、設定可能な DSCP/DSCP 変換マップを使用して、DSCP を別の値に変更できます。

Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 DSCP に基づいて IP トラフィックを分類するオプションがあります。

- 着信パケットの IP precedence 値を信頼し (IP precedence を信頼するようにポートを設定し)、設定可能な IP precedence/DSCP マップを使用してパケットの DSCP 値を生成します。IP バージョン 4 仕様では、1 バイトの ToS フィールドの上位 3 ビットが IP precedence として定義されています。IP precedence 値の範囲は 0 (ロープライオリティ) ~ 7 (ハイプライオリティ) です。

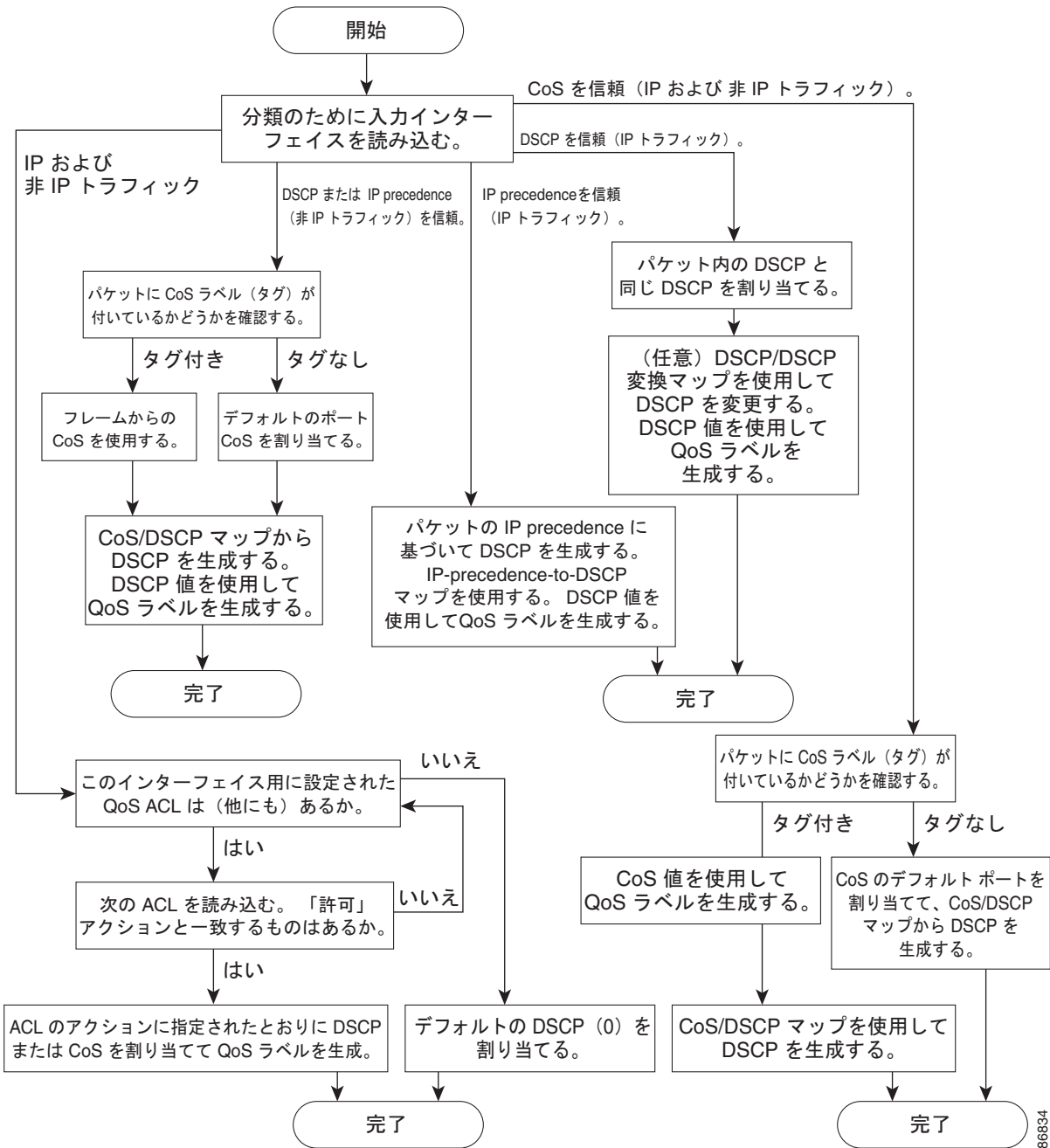
Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 IP precedence に基づいて IP トラフィックを分類するオプションがあります。

- 着信パケットに CoS 値がある場合には、その CoS 値を信頼し、CoS/DSCP マップを使用してパケットの DSCP 値を生成します。CoS 値が存在しない場合は、デフォルトのポート CoS 値を使用します。
- 着信パケットに設定された CoS を上書きし、デフォルトのポート CoS 値を適用します。IPv6 パケットの場合、DSCP 値は CoS/DSCP マップとポートのデフォルトの CoS を使用して書き換えられます。Cisco IOS Release 12.2(52)SE 以降のリリースでは、これを IPv4 および IPv6 の両方トラフィックで実行できます。
- 設定された IP 標準 ACL または IP 拡張 ACL (IP ヘッダーの各フィールドを調べる) に基づいて、分類を実行します。ACL が設定されていない場合、パケットには DSCP および CoS 値として 0 が割り当てられ、トラフィックがベストエフォート型であることを意味します。ACL が設定されている場合は、ポリシーマップアクションによって、着信フレームに割り当てられる DSCP または CoS 値が指定されます。

ここで説明されているマップの詳細については、「マッピング テーブル」(P.37-13) を参照してください。ポートの信頼状態の設定情報については、「ポートの信頼状態による分類の設定」(P.37-42) を参照してください。

分類されたパケットは、ポリシング、マーキング、および入力キューイングとスケジューリングの各段階に送られます。

図 37-3 分類フローチャート



86834

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 を使用すると、同じ特性を備えたパケットグループ（クラス）を定義できます。Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 ACL に基づいて IP トラフィックを分類できます。QoS のコンテキストでは、Access Control Entry (ACE; アクセスコントロール 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検出されると（最初の一一致の原則）、指定の QoS 関連アクションが実行されます。
- 拒否アクションと一致した場合は、処理中の ACL がスキップされ、次の ACL が処理されます。
- 許可アクションとの一致が検出されないまま、すべての ACE の検証が終了した場合、そのパケットでは QoS 処理は実行されず、ベストエフォート型サービスが実行されます。
- ポートに複数の ACL が設定されている場合に、許可アクションを含む最初の ACL とパケットの一致が見つかり、それ以降の検索処理は中止され、QoS 処理が開始されます。



(注)

アクセスリストを作成するときは、アクセスリストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一一致が見つからなかったすべてのパケットに適用されることに注意してください。

ACL でトラフィック クラスを定義した後で、そのトラフィック クラスにポリシーを結合できます。ポリシーにはそれぞれにアクションを指定した複数のクラスを含めることができます。ポリシーには、特定の集約としてクラスを分類する（DSCP を割り当てるなど）コマンドまたはクラスのレート制限を実施するコマンドを含めることができます。このポリシーを特定のポートに結合すると、そのポートでポリシーが有効になります。

IP ACL を実装して IP トラフィックを分類する場合は、**access-list** グローバル コンフィギュレーション コマンドを使用します。レイヤ 2 MAC ACL を実装して非 IP トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。設定の詳細については、「[QoS ポリシーの設定](#)」(P.37-49) を参照してください。

クラス マップおよびポリシー マップに基づく分類

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

ポリシー マップでは、作用対象のトラフィック クラスを指定します。トラフィック クラスの CoS、DSCP、または IP precedence 値を信頼するアクションや、トラフィック クラスに特定の DSCP または IP precedence 値を設定するアクション、またはトラフィック帯域幅の制限やトラフィックが不適合な場合の対処法を指定するアクションなどを指定できます。ポリシー マップを効率的に機能させるには、ポートにポリシー マップを結合する必要があります。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **class** ポリシー マップ コンフィギュレーション コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用する必要があります。**class-map** コマンドを入力すると、クラス マップ コンフィギュレーション モードが開始されます。このモードで、**match** クラス マップ コンフィギュレーション コマンドを使用して、トラフィックの一致条件を定義します。

class class-default ポリシー マップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。分類されていないトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルト トラフィックとして処理されます。

ポリシー マップは、**policy-map** グローバル コンフィギュレーション コマンドを使用して作成し、名前を付けます。このコマンドを入力すると、ポリシー マップ コンフィギュレーション モードが開始されます。このモードでは、**class**、**trust**、または **set** ポリシー マップ コンフィギュレーション コマンドおよびポリシー マップ クラス コンフィギュレーション コマンドを使用して、特定のトラフィック クラスに対して実行するアクションを指定します。

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

ポリシー マップをイネーブルにするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用してポートにマップを結合します。

非階層型のポリシー マップは、物理ポートまたは SVI に対して適用できます。ただし、階層型のポリシー マップに関しては、SVI に対してだけしか適用できません。階層型のポリシー マップには 2 つのレベルがあります。1 番めは 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 番めはインターフェイス レベルで、SVI の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.37-9) 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.37-49) を参照してください。

ポリシングおよびマーキング

パケットを分類して、DSCP ベースまたは CoS ベースの QoS ラベルを割り当てた後で、ポリシングおよびマーキング プロセスを開始できます (図 37-4 を参照)。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「アウト オブ プロファイル」または「不適合」になります。各ポリサーはパケットごとに、パケットが適合か不適合かを判別し、パケットに対するアクションを指定します。これらのアクションはマーカーによって実行されます。パケットを変更しないで通過させるアクション、パケットをドロップするアクション、またはパケットに割り当てられた DSCP 値を変更 (マークダウン) してパケットの通過を許可するアクションなどがあります。設定可能なポリシング済み DSCP マップを使用すると、パケットに新しい DSCP ベース QoS ラベルが設定されます。ポリシング済み DSCP マップの詳細については、「[マッピング テーブル](#)」(P.37-13) 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、フロー内のパケットの順番が崩れないようにします。



(注)

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

物理ポートまたは SVI 上でポリシング (個別または集約ポリサー) を設定できます。物理ポートのポリシング設定の詳細については、「[物理ポートのポリシング](#)」(P.37-10) を参照してください。SVI にポリシー マップを設定する場合、階層型のポリシー マップを作成して、ポリシー マップの 2 番めのインターフェイス レベルにだけ個別にポリサーを定義します。詳細については、「[SVI のポリシング](#)」(P.37-11) を参照してください。

ポリシー マップおよびポリシング アクションを設定したあとで、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、入力ポートまたは SVI にポリシーを統合します。設定情報については、「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-60)、「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-66)、および「[集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-74) を参照してください。

物理ポートのポリシング

物理ポートのポリシー マップでは、次のポリサー タイプを作成できます。

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



(注) SVI には個別のポリサーだけを設定します。

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

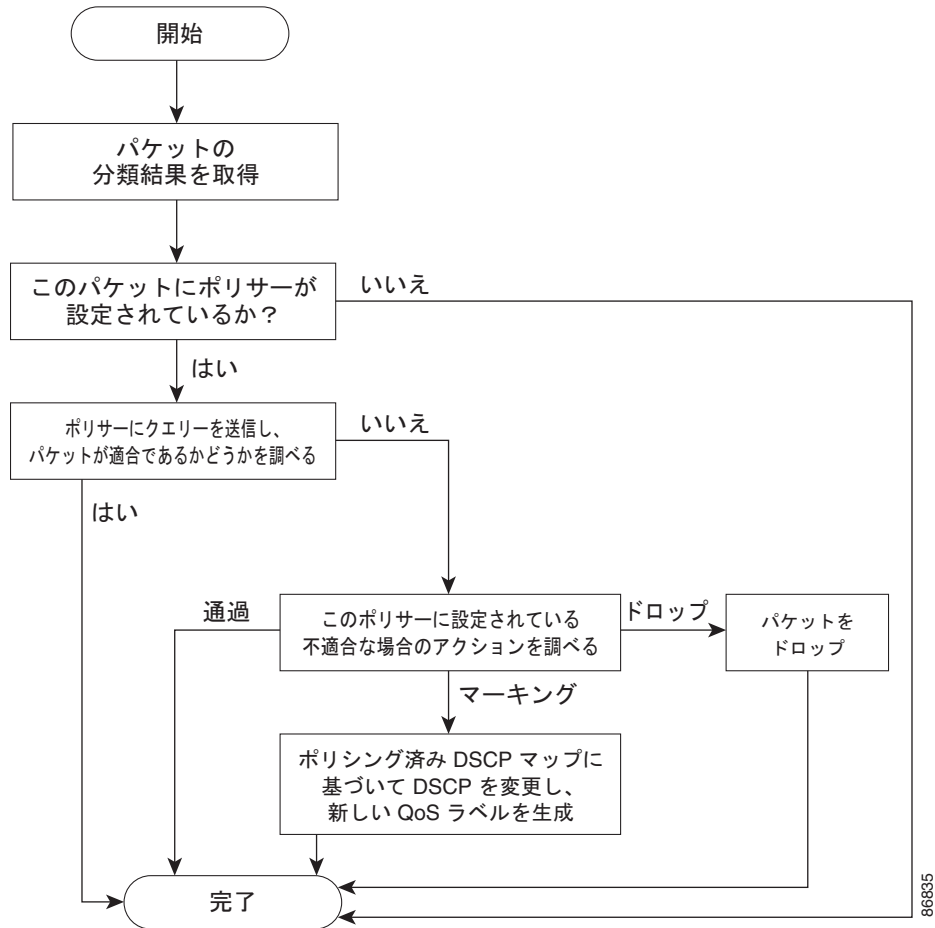
バケットが満たされる速度は、バケット深度 (**burst-byte**)、トークンが削除されるレート (**rate-bps**)、および平均レートを上回るバースト期間によって決まります。バケットのサイズによってバースト長に上限が設定され、バックツーバックで送信できるフレーム数が制限されます。バースト期間が短い場合、バケットはオーバーフローせず、トラフィック フローに何のアクションも実行されません。ただし、バースト期間が長く、レートが高い場合、バケットはオーバーフローし、そのバーストのフレームに対してポリシング アクションが実行されます。

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

次のタイプのポリシー マップが設定されると、[図 37-4](#) のようなポリシングおよびマーキングのプロセスが実行されます。

- 物理ポートの非階層型ポリシー マップ
- SVI に適用されたインターフェイス レベルの階層型ポリシー マップ。物理ポートは、このセカンダリ ポリシー マップに指定します。

図 37-4 物理ポートのポリシングおよびマーキング フローチャート



86835

SVI のポリシング



(注)

SVI に個別のポリサーで階層型のポリシー マップを設定する前に、SVI の物理ポートに対して 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 マップが SVI に適用されますが、個々のポリサーは、階層型のポリシー マップの 2 番目のインターフェイス レベルで指定した物理ポートのトラフィックに対してだけ影響します。

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。

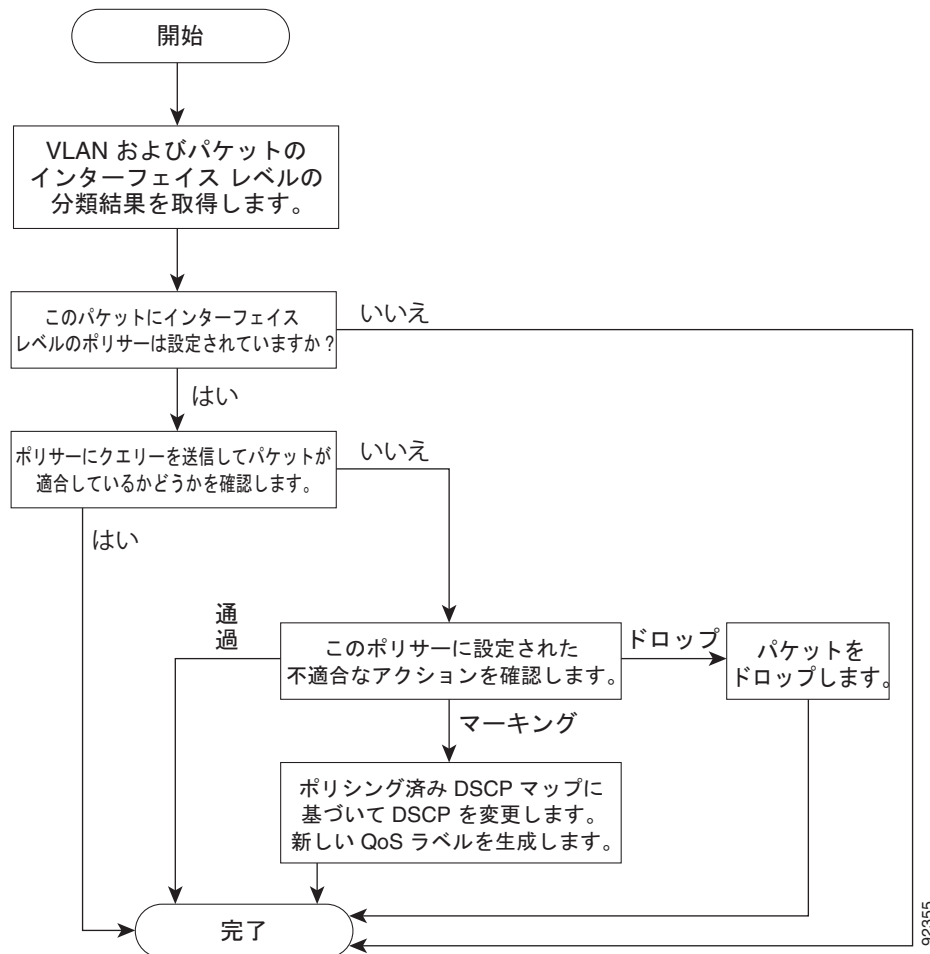
SVI にポリシーを設定する場合、次の 2 つのレベルの階層型ポリシー マップを作成および設定できます。

- VLAN レベル：クラス マップおよびポートの信頼状態を指定するクラスを設定することで、またはパケットに新規に DSCP や IP precedence 値を設定することでプライマリ 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 に対してだけ適用可能で、ポリサーはサポートしません。
- インターフェイス レベル：クラス マップおよび SVI の物理ポートに個別にポリサーを指定するクラスを設定することで、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 マップは個別のポリサーだけサポートし、集約ポリサーをサポートしません。VLAN レベルのポリシー マップで定義された各クラスに対して、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。

階層型のポリシー マップの例は、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシー マップ、およびマーキング」(P.37-66) を参照してください。

図 37-5 に、SVI に階層型のポリシー マップが設定されている場合のポリシー マップおよびマーキングのプロセスを示します。

図 37-5 SVI のポリシー マップおよびマーキング フローチャート



マッピング テーブル

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

- 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、受信された CoS、DSCP、または IP precedence 値から対応する DSCP または CoS 値を取得します。これらのマップには、CoS/DSCP マップや IP precedence/DSCP マップなどがあります。これらのマップを設定するには、**mls qos map cos-dscp** および **mls qos map ip-prec-dscp** グローバル コンフィギュレーション コマンドを使用します。

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

- ポリシング中に、QoS は IP パケットまたは非 IP パケットに別の DSCP 値を割り当てることができます（パケットが不適合で、マークダウン値がポリサーによって指定されている場合）。この設定可能なマップは、ポリシング済み DSCP マップといます。このマップを設定するには、**mls qos map policed-dscp** グローバル コンフィギュレーション コマンドを使用します。
- トラフィックがスケジューリング段階に達する前に、QoS は QoS ラベルに従って、入力および出力キューにパケットを格納します。QoS ラベルはパケット内の DSCP または CoS 値に基づいており、DSCP 入力/出力キューしきい値マップまたは CoS 入力/出力キューしきい値マップを使用してキューを選択します。入力または出力のキューに加えて、QoS ラベルは WTD しきい値も識別します。これらのマップを設定するには、**mls qos srr-queue {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 コマンドを使用します。

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

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

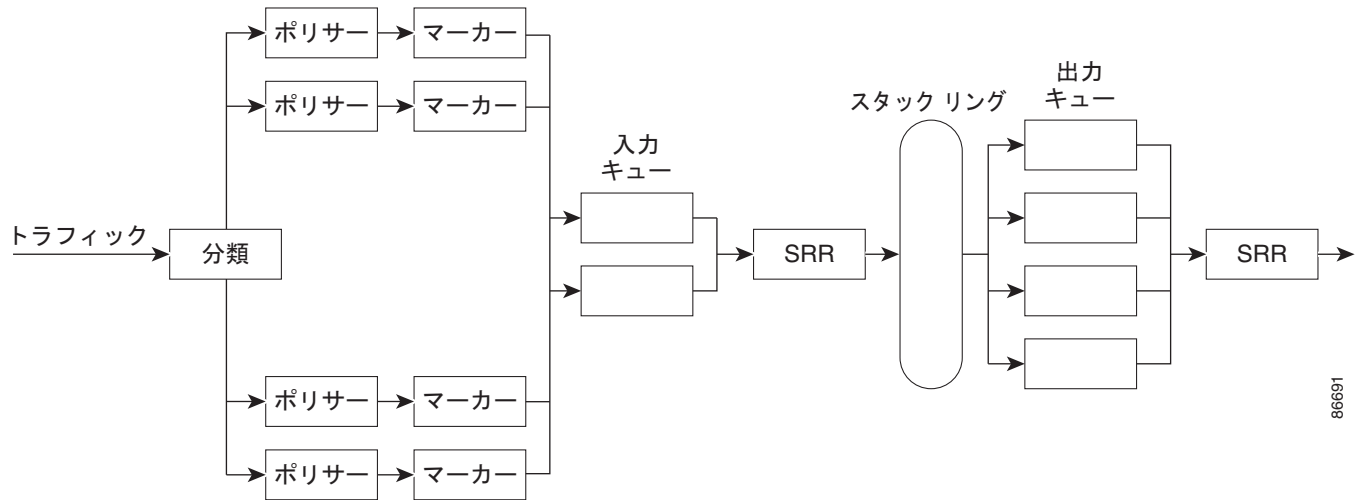
設定の詳細については、「[DSCP マップの設定](#)」(P.37-77) を参照してください。

DSCP および CoS 入力キューしきい値マップの詳細については、「[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.37-16) を参照してください。DSCP および CoS 出力キューしきい値マップの詳細については、「[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.37-18) を参照してください。

キューイングおよびスケジューリングの概要

スイッチは特定のポイントにキューを配置し、輻輳防止に役立てます (図 37-6 を参照)。

図 37-6 入力および出力キューの位置



すべてのポートの入力帯域幅の合計がスタックまたは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あと、パケットがスイッチ ファブリックに転送される前の位置に配置されています。複数の入力ポートから 1 つの出力ポートに同時にパケットが送信されて、輻輳が発生することがあるため、出力キューはスタックまたは内部リングの後に配置されています。

WTD

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

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

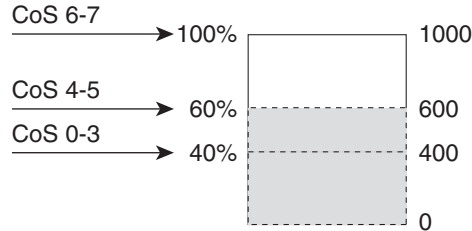
各キューには 3 つのしきい値があります。QoS ラベルは、3 つのしきい値のうちのどれがフレームの影響を受けるかを決定します。3 つのしきい値のうち、2 つは設定可能 (明示的) で、1 つは設定不可能 (暗示的) です。

図 37-7 に、サイズが 1000 フレームであるキューでの WTD の動作例を示します。ドロップ割合は次のように設定されています。40% (400 フレーム)、60% (600 フレーム)、および 100% (1000 フレーム) です。これらのパーセンテージは、40% しきい値の場合は最大 400 フレーム、60% しきい値の場合は最大 600 フレーム、100% しきい値の場合は最大 1000 フレームをキューイングできるという意味です。

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

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

図 37-7 WTD およびキューの動作



詳細については、「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」(P.37-84)、「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」(P.37-88)、および「出力キューおよび ID への DSCP または CoS 値のマッピング」(P.37-90) を参照してください。

SRR のシェーピングおよび共有

入力および出力の両方のキューは SRR で処理され、SRR によってパケットの送信レートが制御されます。入力キューでは、SRR によってパケットがスタックまたは内部リングに送信されます。出力キューでは、SRR によってパケットが出力ポートに送信されます。

出力キューでは、SRR を共有またはシェーピング用に設定できます。ただし、入力キューでは共有がデフォルト モードであり、これ以外のモードはサポートされていません。

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

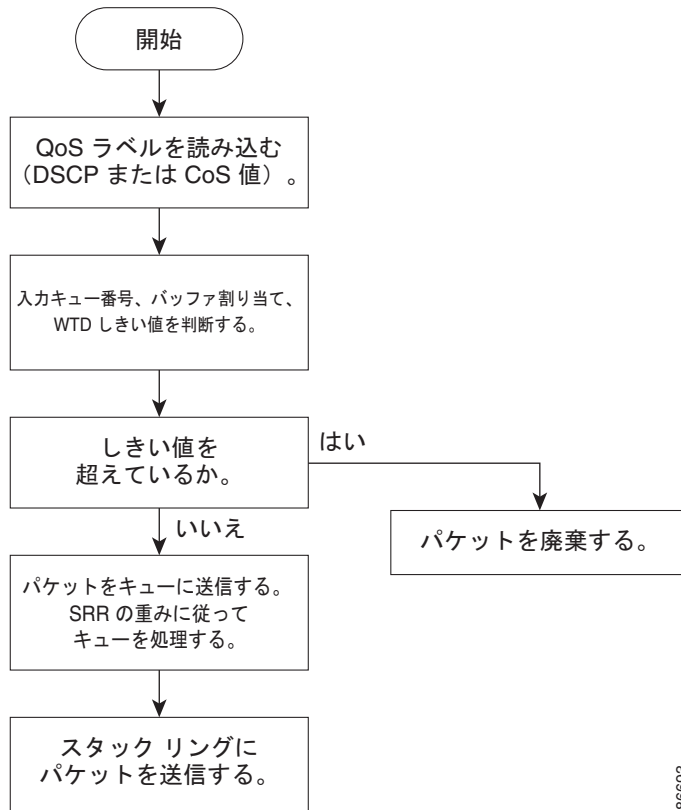
共有モードでは、各キューは設定された重みに従って帯域幅を共有します。このレベルでは帯域幅は保証されていますが、このレベルに限定されていません。たとえば、特定のキューが空であり、リンクを共有する必要がない場合、残りのキューは未使用の帯域幅を使用して、共有できます。共有の場合、キューからパケットを取り出す頻度は重みの比率によって制御されます。重みの絶対値は関係ありません。シェーピングおよび共有は、インターフェイスごとに設定されます。各インターフェイスは、一意に設定できます。

詳細については、「入力キュー間の帯域幅の割り当て」(P.37-86)、「出力キューでの SRR シェーピング重みの設定」(P.37-92)、および「出力キューでの SRR 共有重みの設定」(P.37-93) 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 37-8 に、入力ポートのキューイングおよびスケジューリング フローチャートを示します。

図 37-8 入力ポートのキューイングおよびスケジューリング フローチャート



(注)

共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

スイッチは、共有モードの SRR によってのみ処理される、設定可能な入力キューを 2 つサポートしています。表 37-1 にこれらのキューの説明を示します。

表 37-1 入力キュー タイプ

キュー タイプ ¹	機能
標準	標準プライオリティと見なされるユーザ トラフィック。各フローを区別するために、3 つの異なるしきい値を設定できます。 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 Services (DF) 緊急転送または音声トラフィックなどのハイプライオリティ ユーザ トラフィック。このトラフィックに必要な帯域幅は、 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、合計トラフィックまたは合計スタック トラフィックの割合として設定できます。緊急キューには帯域幅が保証されています。

1. スイッチでは、設定不可能なトラフィック用キューが 2 つ使用されます。これらのキューは、ネットワークおよびスタックを適切に動作させるために重要です。

キューおよびしきい値にスイッチを通過する各パケットを割り当てます。特に、入力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。 **mls qos srr-queue 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 入力キューしきい値マップおよび CoS 入力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

WTD しきい値

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（明示的）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（暗示的）なしきい値です。入力キューに 2 つの明示的 WTD しきい値の割合（しきい値 ID 1 および ID 2 用）を割り当てるには、**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。各しきい値は、キューに割り当てられたバッファの合計値に対する割合です。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。WTD の仕組みの詳細については、「[WTD](#)」(P.37-14) を参照してください。

バッファおよび帯域幅の割り当て

2 つのキュー間の入力バッファを分割する比率を定義する（スペース量を割り当てる）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、パケットがドロップされる前にバッファに格納して送信できるデータ量が制御されます。帯域幅を割合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 スケジューラが各キューからパケットを送信する頻度の比率です。

プライオリティ キューイング

特定の入力キューをプライオリティ キューとして設定するには、**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 コマンドを使用します。プライオリティ キューはスタックまたは内部リングの負荷にかかわらず帯域幅の一部が保証されているため、確実な配信を必要とするトラフィック（音声など）に使用する必要があります。

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 コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「[入力キューの特性の設定](#)」(P.37-83) 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

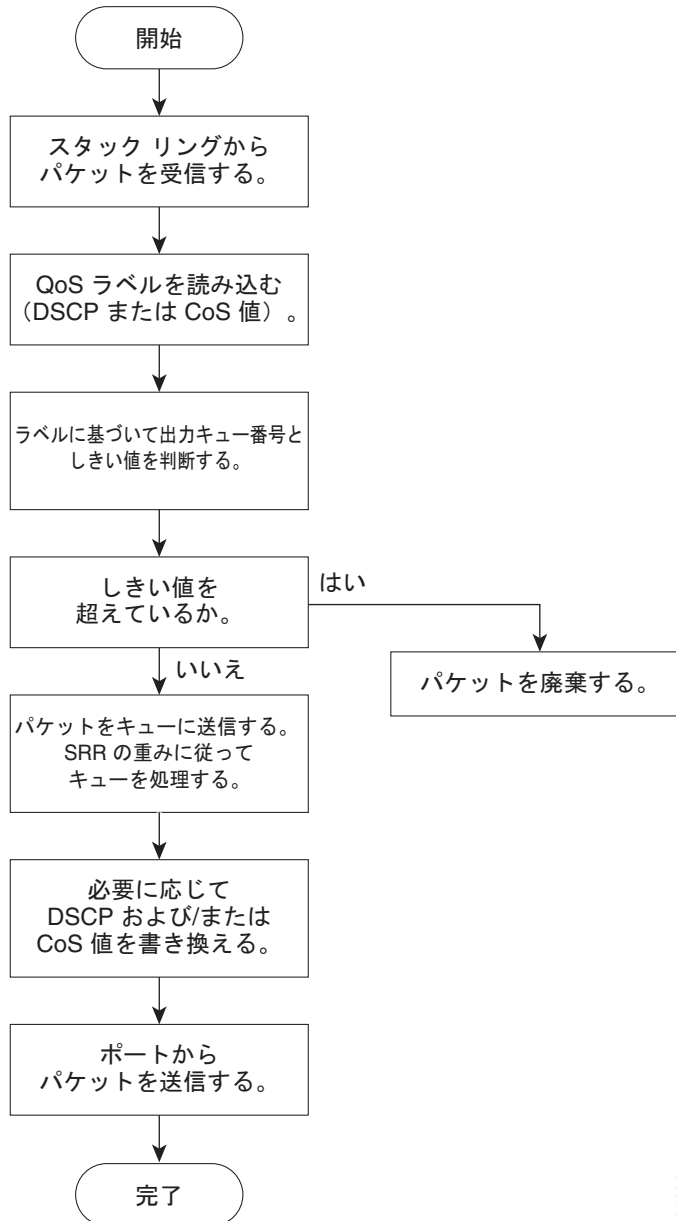
図 37-9 に、出力ポートのキューイングおよびスケジューリング フローチャートを示します。



(注)

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

図 37-9 出力ポートのキューイングおよびスケジューリング フローチャート

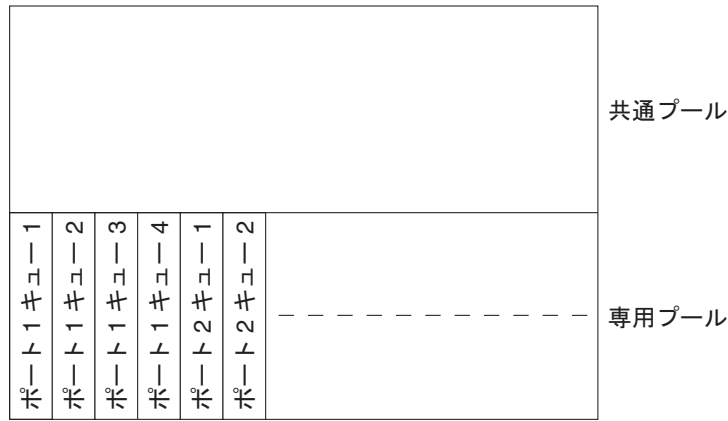


86694

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

図 37-10 に出力キュー バッファを示します。バッファ スペースは共通プールと専用プールで構成されます。スイッチはバッファ割り当て方式を使用して、出力キューごとに最小バッファ サイズを確保します。これにより、いずれかのキューまたはポートがすべてのバッファを消費して、その他のキューのバッファが不足することがなくなり、要求元のキューにバッファ スペースを割り当てるかどうかを制御されます。スイッチは、目的のキューが確保された量（限度内）を超えるバッファを消費していないかどうか、最大バッファ（限度超）をすべて消費しているかどうか、および共通プールが空である（空きバッファなし）か、または空でない（空きバッファあり）かを検出します。キューがオーバーリミットでない場合は、スイッチは予約済みプールまたは共通のプール（空でない場合）からバッファ スペースを割り当てることができます。共通のプールに空きバッファがない場合や、キューがオーバーリミットの場合、スイッチはフレームをドロップします。

図 37-10 出力キューのバッファ割り当て



バッファおよびメモリの割り当て

バッファの可用性の保証、ドロップしきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、`mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` グローバル コンフィギュレーション コマンドを使用します。各しきい値はキューに割り当てられたメモリの割合です。このパーセント値を指定するには、`mls qos queue-set output qset-id buffers allocation1 ... allocation4` グローバル コンフィギュレーション コマンドを使用します。割り当てられたすべてのバッファの合計が専用プールになります。残りのバッファは共通プールの一部になります。

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

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

WTD しきい値

スイッチを通過する各パケットをキューおよびしきい値に割り当てることができます。特に、出力キューには DSCP または CoS 値、しきい値 ID には DSCP または CoS 値をそれぞれマッピングします。**mls qos srr-queue output dscp-map queue queue-id {dscp1...dscp8 | threshold threshold-id dscp1...dscp8}**、または **mls qos srr-queue output cos-map queue queue-id {cos1...cos8 | threshold threshold-id cos1...cos8}** グローバル コンフィギュレーション コマンドを使用します。DSCP 出力キューしきい値マップおよび CoS 出力キューしきい値マップを表示するには、**show mls qos maps** 特権 EXEC コマンドを使用します。

キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。各キューには 3 つのドロップしきい値があります。そのうちの 2 つは設定可能（明示的）な WTD しきい値で、もう 1 つはキューフル ステートに設定済みの設定不可能（暗黙的）なしきい値です。しきい値 ID 1 および ID 2 用の 2 つの WTD しきい値割合を割り当てます。しきい値 ID 3 のドロップしきい値は、キューフル ステートに設定済みで、変更できません。ポートをキューセットにマッピングするには、**queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用します。WTD しきい値の割合を変更するには、キューセット設定を変更します。WTD の仕組みの詳細については、「[WTD](#)」(P.37-14) 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、シェーピング モードまたは共有モードでキューセットを処理します。キューセットにポートをマッピングするには、**queue-set qset-id** インターフェイス コンフィギュレーション コマンドを使用します。ポートに共有重みまたはシェーピング重みを割り当てるには、**srr-queue bandwidth share weight1 weight2 weight3 weight4** または **srr-queue bandwidth shape weight1 weight2 weight3 weight4** インターフェイス コンフィギュレーション コマンドを使用します。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.37-15) を参照してください。

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

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

ここに記載されたコマンドを組み合わせると、特定の DSCP または CoS を持つパケットを特定のキューに格納したり、大きなキュー サイズを割り当てたり、キューをより頻繁に処理したり、プライオリティが低いパケットがドロップされるようにキューのしきい値を調整したりして、トラフィックのプライオリティを設定できます。設定の詳細については、「[出力キューの特性の設定](#)」(P.37-87) 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に限り、設定を変更してください。

パケットの変更

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

- IP パケットおよび非 IP パケットの分類では、受信パケットの DSCP または CoS に基づいて、パケットに QoS ラベルが割り当てられます。ただし、この段階ではパケットは変更されません。割り当てられた DSCP または CoS 値の指定のみがパケットとともに伝達されます。これは、QoS の分類および転送検索が並行して発生するためです。パケットを元の DSCP のまま CPU に転送し、CPU でソフトウェアによる再処理を行うことができます。
- ポリシング中は、IP および非 IP パケットに別の DSCP を割り当てることができます（これらのパケットが不適合で、ポリサーがマークダウン DSCP を指定している場合）。この場合も、パケット内の DSCP は変更されず、マークダウン値の指定がパケットとともに伝達されます。IP パケットの場合は、この後の段階でパケットが変更されます。非 IP パケットの場合は、DSCP が CoS に変換され、キューイングおよびスケジューリングの決定に使用されます。
- フレームに割り当てられた QoS ラベル、および選択された変換マップに応じて、フレームの DSCP および CoS 値が書き換えられます。変換マップが設定されておらず、着信フレームの DSCP を信頼するようにポートが設定されている場合、フレーム内の DSCP 値は変更されずに、DSCP/CoS マップに従って CoS が書き換えられます。着信フレームの CoS を信頼するようにポートが設定されていて、着信フレームが IP パケットの場合、フレーム内の CoS 値は変更されずに、CoS/DSCP マップに従って DSCP が変更されることがあります。

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

auto-QoS の設定

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。自動 QoS は、ネットワーク設計を確認し、スイッチがさまざまなトラフィック フローに優先度を指定できるように QoS 設定をイネーブルにします。自動 QoS は、デフォルト（ディセーブル）の QoS 動作を使用せずに、入力および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関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送信します。

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

Cisco IOS Release 12.2(52)SE 以降のリリースでは、**sdm prefer dual ipv4-and-ipv6** グローバル コンフィギュレーション コマンドによってデュアル IPv4/IPv6 SDM テンプレートが設定されている場合、自動 QoS は IPv4 および IPv6 のトラフィックがサポートされます。

自動 QoS コマンドを使用して、次のシスコ デバイスに接続しているポートを識別することができます。

- Cisco IP Phone
- Cisco SoftPhone アプリケーションを実行しているデバイス
- Cisco TelePresence
- Cisco IP Camera

また、アップリンクを介して信頼のおけるトラフィックを受信するポートを指定します。自動 QoS は次の機能を実行します。

- 条件付きで信頼できるインターフェイスによる自動 QoS デバイスの有無の検出
- QoS 分類の設定

- 出力キューの設定

ここでは、次の設定について説明します。

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

ここでは、次の設定について説明します。

- 「生成される自動 QoS 設定」 (P.37-22)
- 「コンフィギュレーションにおける自動 QoS の影響」 (P.37-32)
- 「自動 QoS 設定時の注意事項」 (P.37-32)
- 「Auto-QoS のイネーブル化」 (P.37-33)
- 「自動 QoS コマンドのトラブルシューティング」 (P.37-34)

生成される自動 QoS 設定

デフォルトでは、自動 QoS はすべてのポートでディセーブルです。パケットは変更されません。つまり、パケットの CoS 値、DSCP 値、および IP precedence 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自動 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 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、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 (`mls qos` グローバル コンフィギュレーション コマンド) になり、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 37-5 を参照)。
- スイッチで信頼境界の機能がイネーブルになり、サポートされているデバイスを検出するために Cisco Discovery Protocol (CDP) が使用されます。
- パケットがプロファイル内にあるかプロファイル外にあるかを判断するためにポリシングが使用され、パケット上のアクションが指定されます。

VOIP デバイスの詳細

- **auto qos voip cisco-phone** コマンドを Cisco IP Phone に接続されたネットワーク エッジにあるポートに入力すると、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 が存在しない場合、入力分類はパケットの QoS ラベルを信用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。
- **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、Cisco SoftPhone を稼働するデバイスに接続されたネットワークのエッジのポートに入力すると、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かプロファイル外にあるかを判断し、パケット上の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上で、**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、入力パケットでルーティングされないポートの 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デバイス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、表 37-3 および表 37-4 の設定に従ってポート上の入力および出力キューを設定します。

表 37-2 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 Control 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/入力キュー マップ	4、5 (キュー 2)					0、1、2、3、6、7 (キュー 1)
CoS/出力キュー マップ	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 37-3 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 ウェイト (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 37-4 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 ウェイト (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 セキュリティを確保するための信頼境界機能の設定 \(P.37-45\)](#)」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自動 QoS をイネーブルにする場合、スイッチはトラフィック タイプおよび入力パケット ラベルに応じて自動的に QoS 設定を生成し、表 37-5 にリストされているコマンドをポートに適用します。

ビデオ、信頼、および分類用の拡張自動 QoS

Cisco IOS Release 12.2(55)SE では、自動 QoS が拡張され、ビデオがサポートされています。ここでは、Cisco TelePresence System と Cisco IP Camera からのトラフィックを分類して信頼する自動設定が生成されます。

スイッチ ポートで **auto qos {video | classify | trust}** 拡張コマンドを設定すると、次の動作が発生します。

- Cisco IOS Release 12.2(55)SE よりも前のリリースでインターフェイスに設定した **Auto qos voip** 生成コマンドが、拡張コマンドに移行します。
- グローバル値が拡張コマンドの移行とともに変更されます。実行コンフィギュレーションに適用される生成コマンドの一覧については、表 37-5 を参照してください。

自動 QoS 設定の移行

レガシー自動 QoS から拡張自動 QoS への自動 QoS 設定の移行は、次の場合に発生します。

- スイッチが 12.2(55)SE イメージで起動されます。QoS はディセーブルです。
インターフェイス上のいずれかのビデオまたは音声の信頼設定によって、拡張自動 QoS コマンドが自動的に生成されます。
- スイッチが QoS でイネーブルになっている場合（次のガイドラインが適用されます）。
 - 音声デバイスで条件付き信頼用にインターフェイスを設定すると、レガシー自動 QoS VoIP 設定だけが生成されます。
 - ビデオ デバイスで条件付き信頼用にインターフェイスを設定すると、拡張自動 QoS VoIP 設定が生成されます。
 - 新しいインターフェイスの自動 QoS コマンドに基づいて分類または条件付き信頼でインターフェイスを設定すると、拡張自動 QoS 設定が生成されます。
- **auto qos srnd4** グローバル コンフィギュレーション コマンドがイネーブルのときに、新しいデバイスを接続すると自動 QoS の移行が発生する場合。



(注)

レガシー自動 QoS で以前に設定したインターフェイスが拡張自動 QoS に移行すると、新しいグローバル QoS コマンドに合わせて音声コマンドと設定が更新されます。

拡張自動 QoS からレガシー自動 QoS への自動 QoS 設定の移行が行われるのは、インターフェイスから既存の自動 QoS 設定をすべてディセーブルにした場合だけです。

グローバルな自動 QoS 設定

表 37-5 生成される自動 QoS 設定

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video Trust Classify}
スイッチが自動的に標準 QoS をイネーブルにして Cos/DSCP マップ (着信パケットの CoS 値の DSCP 値へのマッピング) を設定します。	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
スイッチが、自動的に CoS 値を入力キューおよびしきい値 ID 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
スイッチが、自動的に CoS 値を出力キューおよびしきい値 ID にマッピングします。	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

表 37-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video Trust Classify}
スイッチが、自動的に DSCP 値を入力キューおよびしきい値 ID にマッピングします。	<pre>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</pre>	<pre>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</pre>

表 37-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video Trust Classify}
<p>スイッチが、自動的に DSCP 値を出力キューおよびしきい値 ID にマッピングします。</p>	<pre>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</pre>	<pre>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</pre>

表 37-5 生成される自動 QoS 設定 (続き)

説明	自動的に生成されるコマンド {voip}	自動的に生成される拡張コマンド {Video Trust Classify}
スイッチが自動的に入力キューを設定します。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。また、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。	<pre>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</pre>	<pre>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</pre>
スイッチが自動的に出力キューのバッファ サイズを設定します。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。	<pre>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</pre>	<pre>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</pre>

VoIP デバイス用に生成される自動 QoS 設定

auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的に信頼境界機能をイネーブルにし、CDP を使用して Cisco IP Phone の有無を検出します。

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

auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
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)# d 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 マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。

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

auto qos voip cisco-phone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

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

auto qos voip cisco-softphone コマンドを入力すると、スイッチが自動的にクラス マップおよびポリシー マップを作成します。

```
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 マップを作成すると、スイッチは自動的にポリシー マップ（別名 *AutoQoS-Police-SoftPhone*）を、Cisco SoftPhone 機能を備えた自動 QoS がイネーブルである入力インターフェイスに適用します。

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

拡張されたビデオ、信頼、および分類デバイス用に自動 QoS で生成される設定

次の拡張自動 QoS コマンドを入力すると、スイッチが CoS/DSCP マップ（着信パケットの CoS 値の DSCP 値へのマッピング）を自動的に設定します。

- auto qos video cts
- auto qos video ip-camera
- auto qos trust
- auto qos trust cos
- auto qos trust dscp

```
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
```



(注) クラス マップとポリシー マップは設定されません。

auto qos classify コマンドを入力すると、スイッチは自動的にクラス マップとポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp 0 10 18 24 26 46 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENTHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENTHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENTHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
```

auto qos classify police コマンドを入力すると、スイッチは自動的にクラス マップとポリシー マップを作成します。

```
Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIENTHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENTHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENTHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
```

```
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap-c)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
```

これは、**auto qos voip cisco-phone** コマンドの拡張コンフィギュレーションです。

```
Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

これは、**auto qos voip cisco-softphone** コマンドの拡張コンフィギュレーションです。

```
Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_MULTIHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER

Switch(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_MULTIHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
```

```

Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# police 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY

```

コンフィギュレーションにおける自動 QoS の影響

自動 QoS がイネーブルになると、**auto qos** インターフェイス コンフィギュレーション コマンドおよび生成されたグローバル コンフィギュレーション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、自動 QoS が生成したコマンドを、CLI から入力したように適用します。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。生成コマンドが適用されなかった場合、以前の実行コンフィギュレーションが復元されます。

自動 QoS 設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシー マップや集約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 マップではなくこの新しいポリシー 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、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。
- 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、自動 QoS が完了した後にのみ調整することを推奨します。詳細については、「[コンフィギュレーションにおける自動 QoS の影響](#)」(P.37-32) を参照してください。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。
- デフォルトでは、CDP 機能はすべてのポート上でイネーブルです。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。

自動 QoS VoIP に関する考慮事項

- 自動 QoS は、非ルーテッドポートおよびルーテッドポートで Cisco IP Phone に VoIP のスイッチを設定します。また、自動 QoS は Cisco SoftPhone アプリケーションを稼働するデバイスの VoIP 用にスイッチを設定します。



(注) Cisco SoftPhone を稼働するデバイス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、スイッチはポート単位で Cisco SoftPhone アプリケーション 1 つのみをサポートします。

- ルーテッドポートで Cisco IP Phone の自動 QoS をイネーブルにすると、スタティック IP アドレスを IP Phone に割り当てます。
- このリリースは、Cisco IP SoftPhone Version 1.3(3) 以降のみをサポートします。
- 接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

拡張された自動 QoS に関する考慮事項

- auto qos srnd4** グローバル コンフィギュレーション コマンドは、拡張自動 QoS 設定の結果として生成されます。
- レガシーの **auto qos voip** コマンドがスイッチで実行されて、**mls qos** コマンドがディセーブルになると、拡張自動 QoS 設定が生成されます。それ以外の場合は、レガシー自動 QoS コマンドが実行されます。

Auto-QoS のイネーブル化

QoS パフォーマンスを最適化するには、ネットワーク内のすべてのデバイスで自動 QoS をイネーブルにします。

QoS ドメイン内で自動 QoS デバイスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	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	ネットワーク内部の別の信頼性のある他のスイッチやルータに接続されたアップリンク ポートのビデオ デバイスに接続されるポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	auto qos voip {cisco-phone cisco-softphone trust} または	自動 QoS をイネーブルにします。 <ul style="list-style-type: none"> cisco-phone : ポートが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは電話が検出された場合のみ信頼されます。 cisco-softphone : ポートが Cisco SoftPhone 機能を実行するデバイスに接続されています。 trust : アップリンク ポートが信頼性のあるスイッチまたはルータに接続されていて、入力パケットの VoIP トラフィック分類が信頼されています。

コマンド	目的
auto qos video {cts ip-camera} または	ビデオ デバイス用の自動 QoS をイネーブルにします。 <ul style="list-style-type: none"> • cts : Cisco TelePresence システムに接続されているポート • ip-camera : IP Camera に接続しているポート。 着信パケットの QoS ラベルが信頼されるのは、システムが検知される場合に限りです。
auto qos classify [police] または	分類用の自動 QoS をイネーブルにします。 <ul style="list-style-type: none"> • police : QoS ポリシー マップを定義し、それらをポートに適用してポリシングを設定します (ポートベースの QoS)。
auto qos trust {cos dscp}	信頼できるインターフェイス用の自動 QoS をイネーブルにします。 <ul style="list-style-type: none"> • cos : サービス クラス。 • dscp : Differentiated Services Code Point。
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	信頼性のあるスイッチまたはルータに接続していると認識されるスイッチ 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 モードを開始します。
ステップ 6 auto qos trust	ポート上で自動 QoS をイネーブルにし、そのポートが信頼性のあるルータまたはスイッチに接続されるように指定します。
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、自動 QoS がイネーブルであるインターフェイス上の自動 QoS コマンドを表示します。自動 QoS 設定および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。

自動 QoS コマンドのトラブルシューティング

自動 QoS のイネーブルまたはディセーブル時に自動的に生成された QoS コマンドを表示するには、自動 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、このリリースに対応するコマンド リファレンスにある **debug autoqos** コマンドを参照してください。

ポートで自動 QoS をディセーブルにするには、**auto qos** コマンドのインターフェイス 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せん。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ありません。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)。

自動 QoS 情報の表示

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

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

- **show mls qos**
- **show mls qos maps cos-dscp**
- **show mls qos interface [interface-id] [buffers | queuing]**
- **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**

このコマンドの詳細については、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。

標準 QoS の設定

標準 QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン。
- トラフィックの特性およびネットワークのニーズ。バースト性の高いトラフィックかどうかの判別。音声およびビデオ ストリーム用の帯域幅確保の必要性。
- ネットワークの帯域幅要件および速度。
- ネットワーク上の輻輳発生箇所。

ここでは、次の設定について説明します。

- 「標準 QoS のデフォルト設定」 (P.37-36)
- 「標準 QoS 設定時の注意事項」 (P.37-38)
- 「QoS のグローバルなイネーブル化」 (P.37-41) (必須)
- 「物理ポートで VLAN ベースの QoS をイネーブル化」 (P.37-41) (任意)
- 「ポートの信頼状態による分類の設定」 (P.37-42) (必須)
- 「QoS ポリシーの設定」 (P.37-49) (必須)
- 「DSCP マップの設定」 (P.37-77) (任意、DSCP/DSCP 変換マップまたはポリシング済み DSCP マップを使用する必要がない場合)
- 「入力キューの特性の設定」 (P.37-83) (任意)
- 「出力キューの特性の設定」 (P.37-87) (任意)

標準 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 コマンドを使用して QoS をイネーブルにし、その他のすべての QoS 設定がデフォルトである場合、トラフィックはポリシングを伴わないベストエフォート型として分類されます（DSCP および CoS 値は 0 に設定されます）。ポリシー マップは設定されません。すべてのポート上のデフォルト ポートの信頼性は、信頼性なし（untrusted）の状態です。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.37-36) および「[出力キューのデフォルト設定](#)」(P.37-37) を参照してください。

入力キューのデフォルト設定

表 37-6 に、QoS がイネーブルの場合の入力キューのデフォルト設定を示します。

表 37-6 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 ドロップしきい値 1	100%	100%
WTD ドロップしきい値 2	100%	100%

1. 帯域幅は各キューで平等に共有されます。SRR は共有モードでのみ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。共有が設定されている場合、SRR はプライオリティ キューを処理してから、他のキューを処理します。

表 37-7 に、QoS がイネーブルの場合のデフォルトの CoS 入力キューしきい値マップを示します。

表 37-7 デフォルトの CoS 入力キューしきい値

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

表 37-8 に、QoS がイネーブルの場合のデフォルトの DSCP 入力キューしきい値マップを示します。

表 37-8 デフォルトの DSCP 入力キューしきい値マップ

DSCP 値	キュー ID - しきい値 ID
0 ~ 39	1-1
40 ~ 47	2-1
48 ~ 63	1-1

出力キューのデフォルト設定

表 37-9 に、QoS がイネーブルの場合、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。すべてのポートはキューセット 1 にマッピングされます。ポートの帯域幅限度は 100% に設定され、レートは制限されません。

表 37-9 出力キューのデフォルト設定

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

1. シェーピング重みが 0 の場合、このキューはシェーピングモードで動作します。
2. 帯域幅の 4 分の 1 が各キューに割り当てられます。

表 37-10 に、QoS がイネーブルの場合のデフォルトの CoS 出力キューしきい値マップを示します。

表 37-10 デフォルトの CoS 出力キューしきい値マップ

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

表 37-11 に、QoS がイネーブルの場合のデフォルトの DSCP 出力キューしきい値マップを示します。

表 37-11 デフォルトの DSCP 出力キューしきい値マップ

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

マッピング テーブルのデフォルト設定

デフォルトの CoS/DSCP マップは、表 37-12 (P.37-77) のとおりです。

デフォルトの IP precedence/DSCP マップは、表 37-13 (P.37-78) のとおりです。

デフォルトの DSCP/CoS マップは、表 37-14 (P.37-80) のとおりです。

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済み DSCP マップは、着信 DSCP 値を同じ DSCP 値にマッピングする（マークダウンしない）空のマップです。

標準 QoS 設定時の注意事項

QoS の設定を始める前に、次の事項を確認してください。

- 「QoS ACL の注意事項」 (P.37-38)
- 「IPv6 QoS ACL の注意事項」 (P.37-38)
- 「インターフェイスへの QoS の適用」 (P.37-38)
- 「スイッチ スタックでの IPv6 QoS の設定」 (P.37-39)
- 「ポリシングの注意事項」 (P.37-40)
- 「一般的な QoS の注意事項」 (P.37-40)

QoS ACL の注意事項

アクセス コントロール リスト (ACL) で QoS を設定する際の注意事項は次のとおりです。

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

IPv6 QoS ACL の注意事項

第 36 章「IPv6 ACL の設定」を参照してください。

インターフェイスへの QoS の適用

ここでは、QoS 物理ポートの設定時の注意事項について説明します。また、この説明は SVI (レイヤ 3 インターフェイス) にも適用されます。

- QoS は物理ポートおよび SVI に設定できます。物理ポートに QoS を設定する場合は、非階層型のポリシー マップを作成し、適用してください。SVI に QoS を設定する場合は、非階層型および階層型のポリシー マップを作成し、適用できます。
- ブリッジング、ルーティング、または CPU への送信のどれを行うかに関係なく、着信トラフィックは分類、ポリシング、およびマークダウン（設定されている場合）されます。ブリッジングされたフレームをドロップしたり、DSCP および CoS 値を変更したりできます。

- 物理ポートまたは SVI でポリシー マップを設定する場合には、次の注意事項に従ってください。
 - 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。
 - 物理ポートで VLAN ベースの QoS を設定した場合、スイッチはそのポートにあるすべてのポートベースのポリシー マップを削除します。そうすることで、物理ポートのトラフィックは、自身のポートの SVI に適用されているポリシー マップの適用を受け入れられます。
 - SVI に適用された階層型のポリシー マップでは、物理ポートのインターフェイス レベルで個別にだけポリサーを作成でき、ポートのトラフィックの帯域幅制限を指定できます。入力ポートは、トランクまたはスタティック アクセス ポイントとして設定する必要があります。階層型のポリシー 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、階層型のポリシー マップで集約ポリサーをサポートしません。
 - SVI に階層型のポリシー マップが適用されたあとは、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、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、階層型ポリシー マップで指定されたクラス マップを追加または削除できません。

スイッチ スタックでの IPv6 QoS の設定

Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 QoS をスイッチまたはスイッチ スタックでイネーブルにできます。スタックに Cisco 3560E および Cisco 3750E スイッチだけが含まれている場合、QoS 設定はすべてのトラフィックに適用されます。1 つ以上の Cisco Catalyst 3750 スイッチを含むスタックの IPv6 QoS に関する注意事項は、次のとおりです。

- どのスイッチでもスタック マスターにできます。
- IPv6 ACL を含むポリシーは、Cisco 3560E および 3750E スイッチ インターフェイスだけに適用できます。
- 付加されたポリシーを変更して、IPv6 ACL を Cisco 3560E および Cisco 3750E スイッチ インターフェイスだけに含めることができます。
- *match protocol IPv6* 分類を含むポリシーは、Cisco 3560E および Cisco 3750E スイッチ インターフェイスだけに適用されます。
- IPv4 および IPv6 の両方の分類を含む QoS ポリシーは、混合スイッチ スタックの SVI に付加できます。ただし、このポリシーは、Cisco 3750 スイッチ インターフェイスに入る IPv4 トラフィックだけ、および Cisco 3750E スイッチ インターフェイスの IPv4 および IPv6 トラフィックの両方に適用されます。
- IPv6 トラストは、Cisco 3750 および Cisco 3750E の両方のスイッチでサポートされます。
- IPv6 固有の分類 (IPv6 ACL または **match protocol ipv6** コマンドなど) を含む QoS ポリシーは、Cisco 3750E インターフェイス、および任意の SVI (Cisco 3750E スイッチがスタックの一部である場合) でサポートされます。
- 共通の IPv4 および IPv6 分類を含む QoS ポリシーは、スタックのすべての Cisco 3750E インターフェイスでサポートされます。スタック内の他のスイッチでは、IPv4 分類のみがサポートされません。

ポリシングの注意事項

ポリシングの注意事項を次に示します。

- 複数の物理ポートを制御するポート ASIC デバイスは、256 のポリサー（ユーザが設定可能な 255 のポリサーと、システムの内部用途に予約済みの 1 つのポリサー）をサポートしています。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、ギガビットイーサネットポートに 32 個のポリサー、10 ギガビットイーサネットポートに 7 個のポリサーを設定したり、ギガビットイーサネットポートに 64 個のポリサー、10 ギガビットイーサネットポートに 4 個のポリサーを設定できます。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。ポートごとにポリサーを確保することはできません。ポートがいずれかのポリサーに割り当てられる保証はありません。
- 入力ポートでは 1 つのパケットに適用できるポリサーは 1 つだけです。設定できるのは、平均レートパラメータおよび認定バーストパラメータだけです。
- 同じ非階層型のポリシーマップ内にある複数のトラフィッククラスで共有される集約ポリサーを作成できます。ただし、集約ポリサーを異なるポリシーマップにわたって使用できません。
- QoS 対応として設定されているポートを介して受信したすべてのトラフィックは、そのポートに結合されたポリシーマップに基づいて分類、ポリシング、およびマーキングが行われます。QoS 対応として設定されているトランクポートの場合、ポートを介して受信したすべての VLAN のトラフィックは、そのポートに結合されたポリシーマップに基づいて分類、ポリシング、およびマーキングが行われます。
- スイッチ上で EtherChannel ポートが設定されている場合、EtherChannel を形成する個々の物理ポートに QoS の分類、ポリシング、マッピング、およびキューイングを設定する必要があります。また、QoS の設定を EtherChannel のすべてのポートで照合するかどうかを決定する必要があります。
- 既存の QoS ポリシーのポリシーマップを変更する必要がある場合は、最初にすべてのインターフェイスからポリシーマップを削除し、その後ポリシーマップを変更またはコピーします。変更が終了したら、変更したポリシーマップをインターフェイスに適用します。最初にすべてのインターフェイスからポリシーマップを削除しなかった場合、CPU 使用率が高くなり、コンソールが長期間停止する可能性があります。

一般的な QoS の注意事項

一般的な QoS の注意事項を次に示します。

- スイッチで受信された制御トラフィック（スパニングツリーブリッジプロトコルデータユニット（BPDU）やルーティングアップデートパケットなど）には、入力 QoS 処理がすべて行われます。
- キュー設定を変更すると、データが失われることがあります。したがって、トラフィックが最小のときに設定を変更するようにしてください。
- IP サービス フィーチャセットが実行されているスイッチは、ポリシーベースルーティング（PBR）ルートマップの QoS DSCP および IP precedence マッチングをサポートしますが、次の制約があります。
 - 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できません。
 - DSCP 透過性と PBR DSCP ルートマップを同じスイッチ上に設定できません。

QoS のグローバルなイネーブル化

デフォルトでは、QoS はスイッチ上でディセーブルに設定されています。Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 QoS がサポートされます。IPv6 QoS をスイッチでイネーブルにするには、デュアル IP SDM テンプレートを設定して、スイッチをリロードする必要があります。このテンプレートにより、IPv4 と IPv6 の両方の QoS 設定がイネーブルになります。

QoS をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	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。 デフォルト設定における QoS の動作については、「標準 QoS のデフォルト設定」(P.37-36)、「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.37-16)、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.37-18)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	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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 VLAN ベースの QoS をイネーブル化

デフォルトでは、VLAN ベースの QoS はスイッチにあるすべての物理ポートでディセーブルです。スイッチは、物理ポート ベースでだけ、クラス マップおよびポリシー マップ QoS を含む QoS を適用できます。Cisco IOS Release 12.2(25)SE 以降のリリースでは、スイッチ ポートで VLAN ベースの QoS をイネーブルにできます。

特権 EXEC モードを開始して、VLAN ベースの QoS をイネーブルにするには、次の手順を実行します。この手順には、SVI にインターフェイス レベルの階層型ポリシー マップが指定されている物理ポートが必要です。

	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	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 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	VLAN ベースの QoS が物理ポートでイネーブルかどうかを確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

物理ポートで VLAN ベースの QoS をディセーブルにする場合は、`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。

ポートの信頼状態による分類の設定

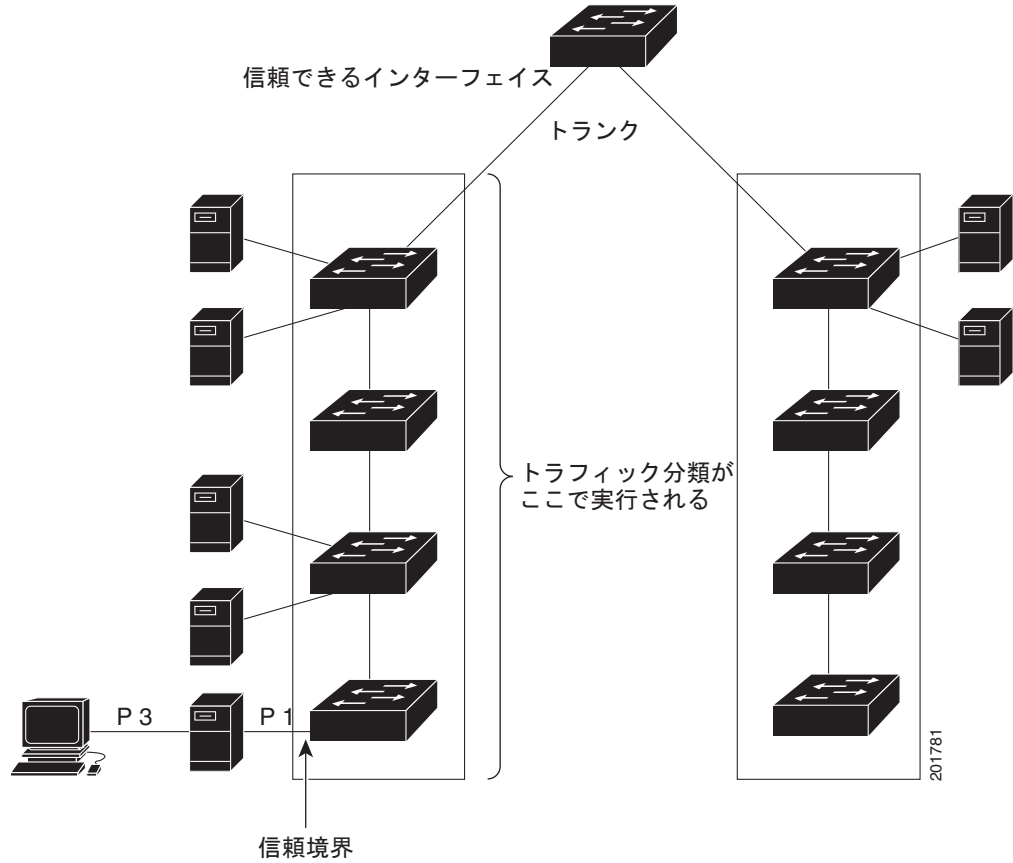
ここでは、ポートの信頼状態を使用して着信トラフィックを分類する方法について説明します。ネットワーク設定に応じて、次に示す作業または「[QoS ポリシーの設定](#)」(P.37-49)に記載されている作業を 1 つまたは複数実行する必要があります。

- 「[QoS ドメイン内のポートの信頼状態の設定](#)」(P.37-42)
- 「[インターフェイスの CoS 値の設定](#)」(P.37-45)
- 「[ポートセキュリティを確保するための信頼境界機能の設定](#)」(P.37-45)
- 「[DSCP トランスペアレントモードのイネーブル化](#)」(P.37-47)
- 「[別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定](#)」(P.37-47)

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチポートをいずれか 1 つの信頼状態に設定できます。[図 37-11](#) に、ネットワーク トポロジの例を示します。

図 37-11 QoS ドメイン内のポートの信頼状態



ポートが受信したトラフィックの分類を信頼するようにポートを設定するには、特権 EXEC モードで次の手順を実行します。

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 モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。

コマンド	目的
ステップ3 mls qos trust [cos dscp ip-precedence]	<p>ポートの信頼状態を設定します。</p> <p>デフォルトでは、ポートは trusted ではありません。キーワードを指定しない場合、デフォルトは dscp です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • cos : パケットの CoS 値を使用して入力パケットを分類します。タグのない IP パケットの場合、ポートのデフォルトの CoS 値が使用されます。デフォルトのポート CoS 値は 0 です。 • dscp : パケットの DSCP 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、内部で CoS/DSCP マップを使用して CoS 値を DSCP 値にマッピングします。 • ip-precedence : パケットの IP precedence 値を使用して入力パケットを分類します。非 IP パケットでは、パケットがタグ付きの場合、パケットの CoS 値が使用されます。パケットがタグなしの場合は、デフォルトのポート CoS が使用されます。スイッチは、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) コンフィギュレーションファイルに設定を保存します。

untrusted ステートにポートを戻す場合は、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。

デフォルトの CoS 値を変更する方法については、「[インターフェイスの CoS 値の設定](#)」(P.37-45) を参照してください。CoS/DSCP マップを設定する方法については、「[CoS/DSCP マップの設定](#)」(P.37-77) 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、trusted ポートおよび untrusted ポートで受信したタグなしフレームに、**mls qos cos** インターフェイス コンフィギュレーション コマンドで指定された CoS 値を割り当てます。

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

	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	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 3	mls qos cos {default-cos override}	デフォルトのポート CoS 値を設定します。 <ul style="list-style-type: none"> <i>default-cos</i> には、ポートに割り当てるデフォルトの CoS 値を指定します。パケットがタグなしの場合、デフォルトの CoS 値がパケットの CoS 値になります。指定できる CoS 範囲は 0 ~ 7 です。デフォルトは 0 です。 着信パケットにすでに設定されている信頼状態を変更し、すべての着信パケットにデフォルトのポート CoS 値を適用する場合は、override キーワードを使用します。デフォルトでは、CoS の上書きはディセーブルに設定されています。 特定のポートに届くすべての着信パケットに、他のポートからのパケットより高い、または低いプライオリティを与える場合には、 override キーワードを使用します。ポートがすでに DSCP、CoS、または IP precedence を信頼するように設定されている場合でも、設定済みの信頼状態がこのコマンドによって上書き変更され、すべての着信 CoS 値にこのコマンドで設定されたデフォルトの CoS 値が割り当てられます。着信パケットがタグ付きの場合、入力ポートで、ポートのデフォルト CoS を使用してパケットの CoS 値が変更されます。
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) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻す場合は、**no mls qos cos {default-cos | override}** インターフェイス コンフィギュレーション コマンドを使用します。

ポート セキュリティを確保するための信頼境界機能の設定

一般的なネットワークでは、Cisco IP Phone をスイッチ ポートに接続して (図 37-11 (P.37-43) を参照)、電話の背後からデータ パケットを生成するデバイスをカスケードします。Cisco IP Phone では、音声パケット CoS レベルをハイ プライオリティ (CoS = 5) にマーキングし、データ パケットをロープライオリティ (CoS = 0) にマーキングすることで、共有データ リンクを通して音声品質を保証しています。電話からスイッチに送信されたトラフィックは通常 802.1Q ヘッダーを使用するタグでマーキングされています。ヘッダーには VLAN 情報およびパケットのプライオリティになる CoS の 3 ビットフィールドが含まれています。

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

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

Cisco IP Phone に接続した PC でハイ プライオリティのデータ キューを利用しないようにすることもできる場合があります。 **switchport priority extend cos** インターフェイス コンフィギュレーション コマンドを使用して、PC から受信するトラフィックのプライオリティを上書きするようにスイッチ CLI を介して電話を設定できます。

信頼境界機能をポート上でイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	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 がイネーブルに設定されています。
ステップ 3	interface interface-id	Cisco IP Phone に接続するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	cdp enable	ポート上で CDP をイネーブルに設定します。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 5	mls qos trust cos 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 trusted ではありません。
ステップ 6	mls qos trust device cisco-phone	Cisco IP Phone が信頼性のあるデバイスであることを指定します。 信頼境界機能と自動 QoS (auto qos voip インターフェイス コンフィギュレーション コマンド) を同時にイネーブルにはできません。両者は相互に排他的です。
ステップ 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) コンフィギュレーション ファイルに設定を保存します。

信頼境界機能をディセーブルにするには、**no 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 トランスペアレント モードのイネーブル化

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

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



(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。

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

特権 EXEC モードを開始して、透過的な DSCP 機能をスイッチでイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	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	透過的な DSCP 機能をイネーブルにします。スイッチが IP パケットの DSCP フィールドを変更しないよう設定されます。
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) コンフィギュレーション ファイルに設定を保存します。

透過的な DSCP 機能をディセーブルにして、信頼設定または ACL に基づいてスイッチに DSCP 値を変更させる設定にするには、**mls qos rewrite ip dscp** グローバル コンフィギュレーション コマンドを使用します。

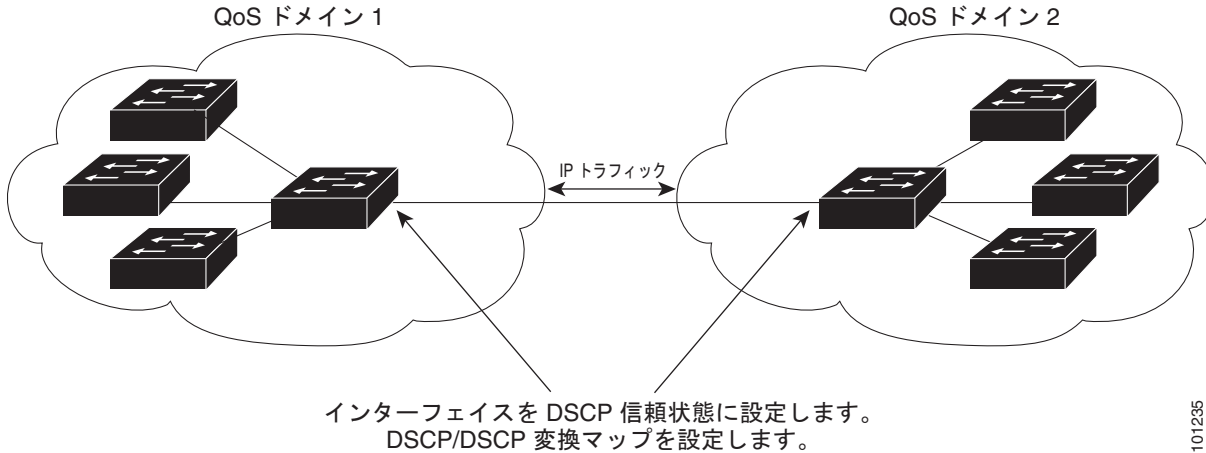
no mls qos グローバル コンフィギュレーション コマンドで、QoS をディセーブルにした場合、CoS および DSCP 値は変更されません (デフォルトの QoS 設定)。

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

別の QoS ドメインとの境界ポートでの DSCP 信頼状態の設定

2 つの異なる QoS ドメインを管理しているときに、その QoS ドメイン間の IP トラフィックに QoS 機能を実装する場合は、ドメインの境界に位置するスイッチ ポートを DSCP trusted ステートに設定できます (図 37-12 を参照)。それにより、受信ポートでは DSCP trusted 値をそのまま使用し、QoS の分類手順が省略されます。2 つのドメインで異なる DSCP 値が使用されている場合は、他のドメイン内での定義に一致するように一連の DSCP 値を変換する DSCP/DSCP 変換マップを設定できます。

図 37-12 別の QoS ドメインとの境界ポートの DSCP 信頼状態



101235

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

	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 <i>dscp-mutation-name in-dscp to out-dscp</i>	DSCP/DSCP 変換マップを変更します。 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。 <ul style="list-style-type: none"> <i>dscp-mutation-name</i> 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。 <i>in-dscp</i> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、to キーワードを入力します。 <i>out-dscp</i> には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	interface interface-id	信頼するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	mls qos trust dscp	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	mls qos dscp-mutation <i>dscp-mutation-name</i>	指定された DSCP trusted 入力ポートにマップを適用します。 <i>dscp-mutation-name</i> 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) コンフィギュレーション ファイルに設定を保存します。

ポートを **trusted** 以外のステートに戻すには、**no mls qos trust** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトの DSCP/DSCP 変換マップ値に戻すには、**no mls qos map dscp-mutation dscp-mutation-name** グローバル コンフィギュレーション コマンドを使用します。

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

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

QoS ポリシーの設定

QoS ポリシーを設定するには、通常、トラフィックをクラス別に分類し、各トラフィック クラスに適用するポリシーを設定し、ポリシーをポートに結合する必要があります。

基本的な情報については、「[分類](#)」(P.37-5) および「[ポリシングおよびマーキング](#)」(P.37-9) を参照してください。設定時の注意事項については、「[標準 QoS 設定時の注意事項](#)」(P.37-38) を参照してください。

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

- 「[ACL によるトラフィックの分類](#)」(P.37-50)
- 「[クラス マップによるトラフィックの分類](#)」(P.37-55)
- 「[クラス マップの使用と IPv6 トラフィックのフィルタリングによるトラフィックの分類](#)」(P.37-59)
- 「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-60)
- 「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-66)
- 「[集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-74)

ACL によるトラフィックの分類

入力 IP トラフィックを分類するには、IP 標準または IP 拡張 ACL を使用します。Cisco IOS Release 12.2(52)SE 以降のリリースでは、IPv6 ACL を使用できます。非 IP トラフィックの分類はレイヤ 2 MAC ACL でできます。

IP トラフィック用に IP 標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>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。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、アクセス リスト番号を入力します。有効範囲は 1 ~ 99 および 1300 ~ 1999 です。 <code>permit</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。<code>deny</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 <code>source</code> には、パケットの送信元となるネットワークまたはホストを指定します。<code>any</code> キーワードは 0.0.0.0 255.255.255.255 の省略形として使用できます。 (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show access-lists</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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。ネットワーク アドレスのホスト部分にワイルドカード ビットが適用されます。アクセス リストのステートメントと一致しない送信元アドレスのホストはすべて拒否されます。

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

IP トラフィック用に IP 拡張 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	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	<code>access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard</code>	<p>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。</p> <ul style="list-style-type: none"> <code>access-list-number</code> には、アクセス リスト番号を入力します。有効範囲は 100 ~ 199 および 2000 ~ 2699 です。 <code>permit</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを許可します。<code>deny</code> キーワードを使用すると、条件が一致した場合に特定のトラフィック タイプを拒否します。 <code>protocol</code> には、IP プロトコルの名前または番号を入力します。疑問符 (?) を使用すると、使用できるプロトコル キーワードのリストが表示されます。 <code>source</code> には、パケットの送信元となるネットワークまたはホストを指定します。ネットワークまたはホストを指定するには、ドット付き 10 進表記を使用したり、<code>source 0.0.0.0 source-wildcard 255.255.255.255</code> の短縮形として <code>any</code> キーワードを使用したり、<code>source 0.0.0.0</code> を表す <code>host</code> キーワードを使用します。 <code>source-wildcard</code> では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。ワイルドカードを指定するには、ドット付き 10 進表記を使用したり、<code>source 0.0.0.0 source-wildcard 255.255.255.255</code> の短縮形として <code>any</code> キーワードを使用したり、<code>source 0.0.0.0</code> を表す <code>host</code> キーワードを使用します。 <code>destination</code> には、パケットの宛先となるネットワークまたはホストを指定します。<code>destination</code> および <code>destination-wildcard</code> には、<code>source</code> および <code>source-wildcard</code> での説明と同じオプションを使用できます。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show access-lists</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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 に設定されている任意の宛先への IP トラフィックを許可する ACL を作成する例を示します。

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

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

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

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

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

IP トラフィック用の IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ1	<code>configure terminal</code>	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	<code>ipv6 access-list <i>access-list-name</i></code>	IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 アクセス リスト名にはスペースまたは引用符を含めることはできません。また、数字で開始することもできません。

コマンド	目的
ステップ 3 {deny permit} protocol {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length any host destination-ipv6-address} [operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence value] [time-range name]	<p>条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。</p> <ul style="list-style-type: none"> <i>protocol</i> には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ~ 255 の整数を使用できます。 <p>(注) ICMP、TCP、および UDP の具体的なパラメータについては、「IPv6 ACL の作成」(P.36-5) を参照してください。</p> <ul style="list-style-type: none"> <i>source-ipv6-prefix/prefix-length</i> または <i>destination-ipv6-prefix/prefix-length</i> は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロンの区切りの 16 ビット値を使用した 16 進形式で指定します (RFC 2373 を参照)。 IPv6 プレフィックス <i>::/0</i> の短縮形として、any を入力します。 host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホストアドレスを入力します。アドレスはコロンの区切りの 16 ビット値を使用した 16 進形式で指定します。 (任意) <i>operator</i> には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt (より小さい)、gt (より大きい)、eq (等しい)、neq (等しくない)、range (包含範囲) があります。 <p><i>source-ipv6-prefix/prefix-length</i> 引数のあとの <i>operator</i> は、送信元ポートに一致する必要があります。<i>destination-ipv6-prefix/prefix-length</i> 引数のあとの <i>operator</i> は、宛先ポートに一致する必要があります。</p> <ul style="list-style-type: none"> (任意) <i>port-number</i> は、0 ~ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 (任意) dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コードポイント値を照合します。指定できる範囲は 0 ~ 63 です。 (任意) fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 (任意) log を指定すると、エン트리と一致するパケットに関するログメッセージがコンソールに送信されます。log-input を指定すると、ログ エントリーに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 (任意) routing を入力して、IPv6 パケットのルーティングを指定します。 (任意) sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ~ 4294967295 です。 (任意) time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。

	コマンド	目的
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 access-list	アクセス リストの設定を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、**no ipv6 access-list access-list-number** グローバル コンフィギュレーション コマンドを使用します。

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

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

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

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

非 IP トラフィック用にレイヤ 2 MAC ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	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	リスト名を指定し、レイヤ 2 MAC ACL を作成します。 このコマンドを入力すると、拡張 MAC ACL コンフィギュレーション モードに切り替わります。
ステップ 3	{permit deny} {host src-MAC-addr mask any host dst-MAC-addr dst-MAC-addr mask} [type mask]	条件が一致した場合に許可または拒否するトラフィック タイプを指定します。必要な回数だけコマンドを入力します。 <ul style="list-style-type: none"> src-MAC-addr には、パケットの送信元となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記 (H.H.H) を使用したり、source 0.0.0、source-wildcard ffff.ffff.ffff の短縮形として any キーワードを使用したり、source 0.0.0 を表す host キーワードを使用します。 mask では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。 dst-MAC-addr には、パケットの宛先となるホストの MAC アドレスを指定します。MAC アドレスを指定するには、16 進表記 (H.H.H) を使用したり、source 0.0.0、source-wildcard ffff.ffff.ffff の短縮形として any キーワードを使用したり、source 0.0.0 を表す host キーワードを使用します。 (任意) type mask には、Ethernet II または SNAP でカプセル化されたパケットの Ethertype 番号を指定して、パケットのプロトコルを識別します。type の範囲は 0 ~ 65535 です。通常は 16 進数で指定します。mask には、一致をテストする前に Ethertype に適用される don't care ビットを入力します。 <p>(注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。</p>

	コマンド	目的
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show access-lists [access-list-number access-list-name]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アクセス リストを削除するには、`no mac access-list extended access-list-name` グローバル コンフィギュレーション コマンドを入力します。

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

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

クラス マップによるトラフィックの分類

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



(注)

`class` ポリシー マップ コンフィギュレーション コマンドを使用することによって、ポリシー マップの作成時にクラス マップを作成することもできます。詳細については、「[ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-60) および「[階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング](#)」(P.37-66) を参照してください。

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条件を定義するには、特権 EXEC モードで次の手順を実行します。

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 ipv6 access-list access-list-name {deny permit} protocol {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length any host destination-ipv6-address} [operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence value] [time-range name] 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 標準または IP 拡張 ACL または IPv6 ACL、あるいは非 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 によるトラフィックの分類 」(P.37-50) を参照してください。 (注) アクセス リストを作成するときは、アクセス リストの末尾に暗黙の拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致が見つからなかったすべてのパケットに適用されることに注意してください。

コマンド	目的
ステップ 3 class-map [match-all match-any] <i>class-map-name</i>	<p>クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <i>class-map-name</i> には、クラス マップ名を指定します。 <p>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。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。match-all および match-any キーワードを使用した場合の制限については、「名前付き標準 ACL および名前付き拡張 ACL の作成」(P.35-16) を参照してください。</p>
ステップ 4 match protocol [<i>ip</i> <i>ipv6</i>]	<p>(任意) クラス マップを適用する IP プロトコルを指定します。</p> <ul style="list-style-type: none"> • IPv4 トラフィックを指定するには引数 <i>ip</i>、IPv6 トラフィックを指定するには <i>ipv6</i> をそれぞれ指定します。 • match protocol コマンドを使用する場合、class-map コマンドでは match-all キーワードのみがサポートされます。 <p>(注) このコマンドは、デュアル IPv4 および IPv6 SDM テンプレートが設定されている場合のみ使用できます。</p> <p>match protocol コマンドは match ip dscp または match precedence コマンドとは併用できますが、match access-group コマンドとは併用できません。</p> <p>match protocol コマンドの詳細については、『Cisco IOS Quality of Service Solutions Command Reference』を参照してください。</p>

	コマンド	目的
ステップ 5	<code>match {access-group acl-index-or-name ip dscp dscp-list ip precedence ip-precedence-list}</code>	<p>トラフィックを分類するための一致条件を定義します。</p> <p>デフォルトでは、一致条件は定義されていません。</p> <p>クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。</p> <ul style="list-style-type: none"> <code>access-group acl-index-or-name</code> には、ステップ 2 で作成した ACL の番号または名前を指定します。 IPv6 トラフィックを <code>match access-group</code> コマンドでフィルタリングするには、ステップ 2 の手順で IPv6 ACL を作成します。 <code>ip dscp dscp-list</code> には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。 <code>ip precedence ip-precedence-list</code> には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show class-map</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、`no policy-map policy-map-name` グローバル コンフィギュレーション コマンドを使用します。既存のクラス 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。一致条件を削除するには、`no match {access-group acl-index-or-name | ip dscp | ip precedence}` クラス マップ コンフィギュレーション コマンドを使用します。

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

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

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

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

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

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

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

Cisco IOS Release 12.2(52)SE 以降のリリースでは、スイッチは、デュアル IPv4/IPv6 SDM テンプレートが設定されている場合、IPv4 および IPv6 QoS の両方のトラフィックがサポートされます。デュアル IP SDM テンプレートが設定されている場合、**match ip dscp** 分類と **match ip precedence** 分類は IPv4 と IPv6 の両方に一致します。**match protocol** コマンドを使用すると、IP のバージョン (IPv4 または IPv6) を基準にトラフィックを分類するためのセカンダリ一致分類を設定できます。

プライマリ一致基準を IPv4 トラフィックに対してのみ適用するには、**match protocol** コマンドで **ip** キーワードを使用します。プライマリ一致基準を IPv6 トラフィックに対してのみ適用するには、**match protocol** コマンドで **ipv6** キーワードを使用します。**match protocol** コマンドの詳細については、『[Cisco IOS Quality of Service Solutions Command Reference](#)』を参照してください。

クラス マップを作成し、トラフィックを分類し、IPv6 トラフィックをフィルタリングするための一致条件を定義するには、特権 EXEC モードで次の手順を実行します。

	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} class-map-name	<p>クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <p>match protocol コマンドを使用する場合、match-all キーワードのみがサポートされます。</p> <ul style="list-style-type: none"> class-map-name には、クラス マップ名を指定します。 <p>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。</p>
ステップ 3	match protocol [ip ipv6]	<p>(任意) クラス マップを適用する IP プロトコルを指定します。</p> <ul style="list-style-type: none"> IPv4 トラフィックを指定するには引数 ip、IPv6 トラフィックを指定するには ipv6 をそれぞれ指定します。 match protocol コマンドを使用する場合、class-map コマンドでは match-all キーワードのみがサポートされます。 <p>(注) このコマンドは、デュアル IPv4 および IPv6 SDM テンプレートが設定されている場合のみ使用できます。</p> <p>match protocol コマンドの詳細については、『Cisco IOS Quality of Service Solutions Command Reference』を参照してください。</p>
ステップ 4	match {ip dscp dscp-list ip precedence ip-precedence-list}	<p>トラフィックを分類するための一致条件を定義します。</p> <p>デフォルトでは、一致条件は定義されていません。</p> <ul style="list-style-type: none"> ip dscp dscp-list には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。 ip precedence ip-precedence-list には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。
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) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map *policy-map-name*** グローバル コンフィギュレーション コマンドを使用します。既存のクラス 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。一致条件を削除するには、**no match {*access-group acl-index-or-name* | *ip dscp* | *ip precedence*}** クラス マップ コンフィギュレーション コマンドを使用します。

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

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

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

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

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

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

ポリシー マップには、次の特性もあります。

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

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

- 入力ポートごとに付加できるポリシー マップは、1 つだけです。
- **mls qos map ip-prec-dscp dscp1...dscp8** グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。ポリシー マップでは、**set ip precedence new-precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- **set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。
- **set ip precedence** または **set precedence** ポリシーマップ クラス コンフィギュレーション コマンドを使用すると、パケット IP Precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- ポートに定義したクラスごとに第 2 レベル ポリシー マップを別々に設定できます。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作業を指定します。階層型のポリシー マップの設定については、「階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング」(P.37-66) を参照してください。
- **class class-default** ポリシーマップ コンフィギュレーション コマンドを使用してデフォルトのトラフィック クラスを設定すると、未分類トラフィック (トラフィック クラスで指定された一致基準に一致しないトラフィック) はデフォルトのトラフィック クラス (**class-default**) として処理されます。

非階層型ポリシー マップを作成するには、特権 EXEC モードで次の手順を実行します。

	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] <i>class-map-name</i>	<p>クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> （任意）このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 （任意）このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 <i>class-map-name</i> には、クラス マップ名を指定します。 <p>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。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。match-all および match-any キーワードを使用した場合の制限については、「名前付き標準 ACL および名前付き拡張 ACL の作成」(P.35-16) を参照してください。</p>
ステップ 3	policy-map policy-map-name	<p>ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されていません。</p> <p>ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。</p>
ステップ 4	class [class-map-name class-default]	<p>トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシー マップ クラス マップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p> <p>class-default トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシー マップの最後に配置されます。暗黙の match any が class-default クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは class-default と一致します。</p>

コマンド	目的
ステップ 5 <code>trust [cos dscp ip-precedence]</code>	<p>CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。</p> <p>(注) このコマンドと <code>set</code> コマンドは、同じポリシー マップ内で相互に排他的になります。<code>trust</code> コマンドを入力する場合は、ステップ 6 へ進んでください。</p> <p>デフォルトでは、ポートは <code>trusted</code> ではありません。キーワードを指定せずにコマンドを入力した場合、デフォルトは <code>dscp</code> です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • <code>cos</code> : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • <code>dscp</code> : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • <code>ip-precedence</code> : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 <p>詳細については、「CoS/DSCP マップの設定」(P.37-77) を参照してください。</p>
ステップ 6 <code>set {dscp new-dscp ip precedence new-precedence}</code>	<p>パケットに新しい値を設定することによって、IP トラフィックを分類します。</p> <ul style="list-style-type: none"> • <code>dscp new-dscp</code> には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。 • <code>ip precedence new-precedence</code> には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ~ 7 です。

	コマンド	目的
ステップ 7	<code>police rate-bps burst-byte [exceed-action {drop policed-dscp-transmit}]</code>	<p>分類したトラフィックにポリサーを定義します。</p> <p>デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.37-38)を参照してください。</p> <ul style="list-style-type: none"> • <i>rate-bps</i> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 10000000000 です • <i>burst-byte</i> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • (任意) レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.37-79)を参照してください。
ステップ 8	<code>exit</code>	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	<code>exit</code>	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	<code>interface interface-id</code>	<p>ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>有効なインターフェイスには、物理ポートが含まれます。</p>
ステップ 11	<code>service-policy input policy-map-name</code>	<p>ポリシーマップ名を指定し、入力ポートに適用します。</p> <p>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。</p>
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>show policy-map [policy-map-name [class class-map-name]]</code>	入力を確認します。
ステップ 14	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

既存のポリシー マップを削除するには、**no policy-map policy-map-name** グローバル コンフィギュレーション コマンドを使用します。既存のクラス 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。**untrusted** ステートに戻すには、**no trust** ポリシーマップ コンフィギュレーション コマンドを使用します。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 マップとポートの対応付けを削除するには、**no service-policy input policy-map-name** インターフェイス コンフィギュレーション コマンドを使用します。

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

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
```

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

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

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

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

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

階層型ポリシー マップによる SVI のトラフィックの分類、ポリシング、およびマーキング

階層型ポリシー マップは SVI に設定できますが、他のタイプのインターフェイスには設定できません。階層型のポリシングは、VLAN レベルおよびインターフェイス レベルのポリシー マップで構成された、1 つのポリシー マップとして作成されます。

SVI では、VLAN レベルのポリシー マップに実行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、IP precedence 値の信頼、またはトラフィック クラスの特定の DSCP、IP precedence 値の設定が含まれます。個々のポリサーで作用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。

Cisco IOS Release 12.2(52)SE 以降では、IPv4 トラフィックと IPv6 トラフィックをフィルタリングする階層型のポリシー マップを設定できます。

階層型のポリシー マップを設定するときには、次の注意事項に従ってください。

- 階層型のポリシー マップを設定する前に、インターフェイス レベルのポリシー マップで指定した物理ポートの 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 ごとに付加できるポリシー マップは、1 つだけです。
- 1 つのポリシー マップに、それぞれ異なる一致条件とアクションを指定した複数のクラス ステートメントを指定できます。
- SVI で受信されたトラフィック タイプごとに、別々のポリシー マップ クラスを設定できます。
- mls qos map ip-prec-dscp dscpl...dscp8** グローバル コンフィギュレーション コマンドを使用して IP-precedence/DSCP マップを設定する場合、その設定は IP precedence 値を信頼するよう設定されている入力インターフェイス上のパケットにのみ影響を与えます。ポリシー マップでは、**set ip precedence new-precedence** ポリシー マップ クラス コンフィギュレーション コマンドを使用してパケット IP precedence 値を新しい値に設定する場合、出力 DSCP 値は IP-precedence/DSCP マップによる影響を受けません。出力 DSCP 値を入力値とは異なる値に設定する場合、**set dscp new-dscp** ポリシー マップ クラス コンフィギュレーション コマンドを使用します。
- set ip dscp** コマンドを入力または使用すると、スイッチは設定内で、このコマンドを **set dscp** に変更します。**set ip dscp** コマンドを入力した場合、スイッチ コンフィギュレーションでは **set dscp** の設定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 コマンドを使用すると、パケット IP Precedence 値を変更できます。スイッチ コンフィギュレーションではこの設定は **set ip precedence** として表示されます。
- VLAN ベースの QoS がイネーブルの場合、階層型のポリシー マップは直前に設定したポートベースのポリシー マップを優先します。
- 階層型ポリシー マップが SVI に付加され、VLAN 内の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、その SVI のトラフィックに影響しません。ポート レベルのポリシー マップのポリシングアクションは、影響のある物理インターフェイスの入力トラフィックに影響します。
- トランク ポートの階層型のポリシー マップを設定する場合、VLAN の範囲と重ならないようにしてください。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は、重なっている VLAN の着信トラフィックおよび発信トラフィックにも作用します。
- 集約ポリサーは階層型のポリシー マップではサポートされません。
- VLAN ベースの QoS がイネーブルになると、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。
- 階層型のポリシー マップは、プライベート VLAN のプライマリ VLAN 上にだけ設定できます。

- VLAN ベース QoS をイネーブルにして、スイッチ スタックに階層型ポリシー マップを設定する場合に、スタックの設定を変更すると、次のアクションが自動的に実行されます。
 - 新しいスタック マスターが選択されると、スタック マスターは自身の適用可能なすべてのインターフェイス上でこれらの機能を再度イネーブルにして、再設定します。
 - 新しいスタック メンバーが追加されると、スタック マスターはスタック メンバーの適用可能なすべてのポート上でこれらの機能を再度イネーブルにして、再設定します。
 - スイッチ スタックをマージすると、新しいスタック マスターは新しいスタック上のスイッチでこれらの機能を再度イネーブルにして、再設定します。
 - スイッチ スタックが 2 つ以上のスイッチ スタックに分割されると、各スイッチ スタックのスタック マスターは、スタック マスターを含むスタック メンバーの適用可能なすべてのインターフェイス上でこの機能を再度イネーブルにして、再設定します。
- **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のトラフィック クラスを設定すると、未分類トラフィック（トラフィック クラスで指定された一致基準に一致しないトラフィック）はデフォルトのトラフィック クラス (**class-default**) として処理されます。

特権 EXEC モードを開始して、階層型ポリシー マップを作成するには、次の手順を実行します。

コマンド	目的
ステップ1 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	<p>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 モードを開始します。クラス マップについては、「クラス マップによるトラフィックの分類」(P.37-55) を参照してください。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • class-map-name には、クラス マップ名を指定します。 <p>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。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。match-all および match-any キーワードを使用した場合の制限については、「名前付き標準 ACL および名前付き拡張 ACL の作成」(P.35-16) を参照してください。</p>

コマンド	目的
ステップ 3 match { access-group <i>acl-index-or-name</i> ip dscp <i>dscp-list</i> ip precedence <i>ip-precedence-list</i> }	<p>トラフィックを分類するための一致条件を定義します。</p> <p>デフォルトでは、一致条件は定義されていません。</p> <p>クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。</p> <ul style="list-style-type: none"> • access-group <i>acl-index-or-name</i> には、ACL の番号または名前を指定します。 • ip dscp <i>dscp-list</i> には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 63 です。 • ip precedence <i>ip-precedence-list</i> には、着信パケットと照合する IP precedence 値を 8 つまで入力します。各値はスペースで区切ります。指定できる範囲は 0 ~ 7 です。
ステップ 4 match protocol [<i>ip</i> <i>ipv6</i>]	<p>(任意) クラス マップを適用する IP プロトコルを指定します。</p> <ul style="list-style-type: none"> • IPv4 トラフィックを指定するには引数 <i>ip</i>、IPv6 トラフィックを指定するには <i>ipv6</i> をそれぞれ指定します。 • match protocol コマンドを使用する場合、第 1 レベルのクラス マップでは match-all キーワードのみがサポートされます。 <p>(注) このコマンドは、デュアル IPv4 および IPv6 SDM テンプレートが設定されている場合のみ使用できます。</p> <p>match protocol コマンドは match ip dscp または match precedence コマンドとは併用できますが、match access-group コマンドとは併用できません。</p> <p>match protocol コマンドの詳細については、『Cisco IOS Quality of Service Solutions Command Reference』を参照してください。</p>
ステップ 5 exit	<p>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。</p>
ステップ 6 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>

コマンド	目的
ステップ 7 class-map [match-all match-any] <i>class-map-name</i>	<p>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 モードを開始します。</p> <p>デフォルトでは、クラス マップは定義されていません。</p> <ul style="list-style-type: none"> • (任意) このクラス マップ配下のすべての一致ステートメントの論理 AND を実行するには、match-all キーワードを使用します。この場合は、クラス マップ内のすべての一致条件と一致する必要があります。 • (任意) このクラス マップ配下のすべての一致ステートメントの論理 OR を実行するには、match-any キーワードを使用します。この場合は、1 つまたは複数の一致条件と一致する必要があります。 • <i>class-map-name</i> には、クラス マップ名を指定します。 <p>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。</p> <p>(注) クラス マップごとにサポートされる match コマンドは 1 つだけなので、match-all でも match-any でもキーワードの機能は変わりません。match-all および match-any キーワードを使用した場合の制限については、「名前付き標準 ACL および名前付き拡張 ACL の作成」(P.35-16) を参照してください。</p>
ステップ 8 match input-interface <i>interface-id-list</i>	<p>インターフェイス レベルのクラス マップを実行する物理ポートを指定します。次の方法で、最大 6 つ指定できます。</p> <ul style="list-style-type: none"> • 単一のポート (1 つのエントリとしてカウントされます) • 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ます) • 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ます) <p>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。</p>
ステップ 9 exit	<p>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。</p>
ステップ 10 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 11 policy-map <i>policy-map-name</i>	<p>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 モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されておらず、ポリサーも実行されていません。</p>
ステップ 12 class-map <i>class-map-name</i>	<p>インターフェイス レベルのトラフィック分類を定義し、ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシーマップのクラスマップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p>

コマンド	目的
ステップ 13 police rate-bps burst-byte [exceed-action {drop policed-dscp-transmit}]	<p>分類したトラフィックにそれぞれポリサーを定義します。</p> <p>デフォルトでは、ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.37-38)を参照してください。</p> <ul style="list-style-type: none"> • <i>rate-bps</i> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 10000000000 です • <i>burst-byte</i> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • (任意) レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.37-79)を参照してください。
ステップ 14 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 15 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 16 policy-map policy-map-name	<p>ポリシー マップ名を入力することによって 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 モードを開始します。</p> <p>デフォルトでは、ポリシー マップは定義されていません。</p> <p>ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。</p>
ステップ 17 class [class-map-name class-default]	<p>VLAN レベルのトラフィック分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。</p> <p>デフォルトでは、ポリシーマップのクラスマップは定義されていません。</p> <p>すでに class-map グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで <i>class-map-name</i> にその名前を指定します。</p> <p>class-default トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシー マップの最後に配置されます。暗黙の match any が class-default クラスに含まれている場合、他のトラフィック クラスと一致していないすべてのパケットは class-default と一致します。</p>

コマンド	目的
ステップ 18 trust [cos dscp ip-precedence]	<p>CoS ベースまたは DSCP ベースの QoS ラベルを生成するために QoS が使用する信頼ステートを設定します。</p> <p>(注) このコマンドと set コマンドは、同じポリシー マップ内で相互に排他的になります。trust コマンドを入力する場合は、ステップ 18 を省略してください。</p> <p>デフォルトでは、ポートは trusted ではありません。キーワードを指定せずにコマンドを入力した場合、デフォルトは dscp です。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • cos : QoS は受信した CoS 値やデフォルトのポート CoS 値、および CoS/DSCP マップを使用して、DSCP 値を抽出します。 • dscp : QoS は入力パケットの DSCP 値を使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 • ip-precedence : QoS は入力パケットの IP precedence 値および IP precedence/DSCP マップを使用して、DSCP 値を抽出します。タグ付きの非 IP パケットの場合、QoS は受信した CoS 値を使用して DSCP 値を抽出します。タグなしの非 IP パケットの場合、QoS はデフォルトのポート CoS 値を使用して DSCP 値を抽出します。いずれの場合も、DSCP 値は CoS/DSCP マップから抽出されます。 <p>詳細については、「CoS/DSCP マップの設定」(P.37-77) を参照してください。</p>
ステップ 19 set { dscp new-dscp ip precedence new-precedence }	<p>パケットに新しい値を設定することによって、IP トラフィックを分類します。</p> <ul style="list-style-type: none"> • dscp new-dscp には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ~ 63 です。 • ip precedence new-precedence には、分類されたトラフィックに割り当てる新しい IP precedence 値を入力します。指定できる範囲は 0 ~ 7 です。
ステップ 20 service-policy <i>policy-map-name</i>	<p>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 を参照)、VLAN レベルのポリシー マップと連動させます。</p> <p>VLAN レベルのポリシー マップで複数のクラスが指定されている場合、各クラスで別々の service-policy policy-map-name コマンドを使用できます。</p>
ステップ 21 exit	<p>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。</p>
ステップ 22 exit	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 23 interface <i>interface-id</i>	<p>階層型のポリシー マップを適用する SVI を指定し、インターフェイス コンフィギュレーション モードを開始します。</p>

	コマンド	目的
ステップ 24	service-policy input <i>policy-map-name</i>	VLAN レベルのポリシーマップ名を指定し、SVI にそれを適用します。前のステップとこのコマンドを使用して、他の SVI にポリシーマップを適用します。 階層型 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、すべてのクラスが service-policy <i>policy-map-name</i> コマンドで指定されている同じ VLAN レベルのポリシーマップに設定されている必要があります。
ステップ 25	end	特権 EXEC モードに戻ります。
ステップ 26	show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]] または show mls qos vlan-based	入力を確認します。
ステップ 27	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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

インターフェイス レベルのポリシーマップの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。階層型のポリシーマップとポートの対応付けを削除するには、**no service-policy input** *policy-map-name* インターフェイス コンフィギュレーション コマンドを使用します。

次に、階層型のポリシーマップの作成方法を示します。

```
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#
Switch#
```

次に、SVI に新しいマップを割り当てる例を示します。

```
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 gigabitethernet3/0/1 - gigabitethernet3/0/2
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)# set dscp 10
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

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

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

次に、デフォルト トラフィック クラスをポリシー マップに設定する例を示します。

```
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-c)# exit
Switch(config-pmap)# exit
```

次の例では、class-default が最初に設定された場合でも、デフォルトのトラフィック クラスをポリシー マップ pm3 の終わりに自動的に配置する方法を示します。

```
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#
```

集約ポリサーによるトラフィックの分類、ポリシング、およびマーキング

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

集約ポリサーは、物理ポートの非階層型ポリシー マップにだけ設定できます。

集約ポリサーを作成するには、特権 EXEC モードで次の手順を実行します。

	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 <i>aggregate-policer-name rate-bps burst-byte</i> exceed-action {drop policed-dscp-transmit}	<p>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。</p> <p>デフォルトでは、集約ポリサーは定義されていません。サポートされているポリサー数については、「標準 QoS 設定時の注意事項」(P.37-38) を参照してください。</p> <ul style="list-style-type: none"> • <i>aggregate-policer-name</i> には、集約ポリサーの名前を指定します。 • <i>rate-bps</i> には、平均トラフィック レートをビット/秒 (bps) で指定します。指定できる範囲は 8000 ~ 10000000000 です。 • <i>burst-byte</i> には、標準バースト サイズをバイト数で指定します。指定できる範囲は 8000 ~ 1000000 です。 • レートを超過した場合に実行するアクションを指定します。パケットをドロップする場合は、exceed-action drop キーワードを使用します。(ポリシング済み DSCP マップを使用して) DSCP 値をマークダウンし、パケットを送信するには、exceed-action policed-dscp-transmit キーワードを使用します。詳細については、「ポリシング済み DSCP マップの設定」(P.37-79) を参照してください。
ステップ3	class-map [match-all match-any] <i>class-map-name</i>	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 マップによるトラフィックの分類」(P.37-55) および「名前付き標準 ACL および名前付き拡張 ACL の作成」(P.35-16) を参照してください。
ステップ4	policy-map <i>policy-map-name</i>	<p>ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。</p> <p>詳細については、「ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング」(P.37-60) を参照してください。</p>
ステップ5	class [<i>class-map-name</i> class-default]	<p>トラフィックの分類を定義し、ポリシーマップ クラス コンフィギュレーション モードを開始します。</p> <p>詳細については、「ポリシー マップによる物理ポートのトラフィックの分類、ポリシング、およびマーキング」(P.37-60) を参照してください。</p>
ステップ6	police aggregate <i>aggregate-policer-name</i>	<p>同じポリシー マップ内の複数のクラスに集約ポリサーを適用します。</p> <p><i>aggregate-policer-name</i> には、ステップ 2 で指定した名前を入力します。</p>
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 <i>interface-id</i>	<p>ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。</p> <p>有効なインターフェイスには、物理ポートが含まれます。</p>

	コマンド	目的
ステップ 9	service-policy input <i>policy-map-name</i>	ポリシーマップ名を指定し、入力ポートに適用します。 サポートされるポリシー マップは、入力ポートに 1 つだけです。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show mls qos aggregate-policer [<i>aggregate-policer-name</i>]	入力を確認します。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

指定された集約ポリサーをポリシー マップから削除するには、**no police aggregate aggregate-policer-name** ポリシー マップ コンフィギュレーション モードを使用します。集約ポリサーおよびそのパラメータを削除するには、**no mls qos 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、集約ポリサーを作成して、ポリシー マップ内の複数のクラスに結合する例を示します。この設定では、IP ACL はネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィックを許可します。ネットワーク 10.1.0.0 から着信するトラフィックの場合は、着信パケットの DSCP が信頼されます。ホスト 11.3.1.1 から着信するトラフィックの場合、パケットの DSCP は 56 に変更されます。ネットワーク 10.1.0.0 およびホスト 11.3.1.1 からのトラフィック レートには、ポリシングが設定されます。トラフィックが平均レート (48000 bps)、および標準バースト サイズ (8000 バイト) を超過している場合は、(ポリシング済み DSCP マップに基づいて) DSCP がマークダウンされて、送信されます。ポリシー マップは入力ポートに結合されます。

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

DSCP マップの設定

ここでは、次の設定について説明します。

- 「CoS/DSCP マップの設定」(P.37-77) (任意)
- 「IP precedence/DSCP マップの設定」(P.37-78) (任意)
- 「ポリシング済み DSCP マップの設定」(P.37-79) (任意、マップのヌル設定が不適切な場合以外)
- 「DSCP/CoS マップの設定」(P.37-80) (任意)
- 「DSCP/DSCP 変換マップの設定」(P.37-81) (任意、マップのヌル設定が不適切な場合以外)

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、すべてのポートに適用されます。

CoS/DSCP マップの設定

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

表 37-12 に、デフォルトの CoS/DSCP マップを示します。

表 37-12 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

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

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	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	<code>mls qos map cos-dscp dscp1...dscp8</code>	CoS/DSCP マップを変更します。 <i>dscp1...dscp8</i> には、CoS 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ~ 63 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show mls qos maps cos-dscp</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマッピングに戻すには、**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 マッピングを変更して表示する例を示します。

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

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

IP precedence/DSCP マッピングの設定

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

表 37-13 に、デフォルトの IP precedence/DSCP マッピングを示します。

表 37-13 デフォルトの IP Precedence/DSCP マッピング

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

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

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

	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 <i>dscp1...dscp8</i>	IP precedence/DSCP マッピングを変更します。 <i>dscp1...dscp8</i> には、IP precedence 値 0 ~ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 DSCP の範囲は 0 ~ 63 です。
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) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマッピングに戻すには、**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。

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

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

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

ポリシング済み DSCP マップの設定

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

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

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

	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 <i>dscp-list</i> to <i>mark-down-dscp</i>	ポリシング済み DSCP マップを変更します。 <ul style="list-style-type: none"> <i>dscp-list</i> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、to キーワードを入力します。 <i>mark-down-dscp</i> 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) コンフィギュレーション ファイルに設定を保存します。

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

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



(注)

このポリシング済み DSCP マップでは、マークダウンされる DSCP 値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点にある値が、マークダウンされる値です。たとえば、元の DSCP 値が 53 の場合、マークダウンされる DSCP 値は 0 です。

DSCP/CoS マップの設定

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

表 37-14 に、デフォルトの DSCP/CoS マップを示します。

表 37-14 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

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

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	<code>configure terminal</code>	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	<code>mls qos map dscp-cos dscp-list to cos</code>	DSCP/CoS マップを変更します。 <ul style="list-style-type: none"> <code>dscp-list</code> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、<code>to</code> キーワードを入力します。 <code>cos</code> には、DSCP 値と対応する CoS 値を入力します。 DSCP の範囲は 0 ~ 63、CoS の範囲は 0 ~ 7 です。
ステップ3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show mls qos maps dscp-to-cos</code>	設定を確認します。
ステップ5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、`no 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、および 50 を CoS 値 0 にマッピングして、マップを表示する例を示します。

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



(注)

上記の DSCP/CoS マップでは、CoS 値が表形式で示されています。d1 列は DSCP の最上位桁、d2 行は DSCP の最下位桁を示します。d1 と d2 の交点にある値が CoS 値です。たとえば、この DSCP/CoS マップでは、DSCP 値が 08 の場合、対応する CoS 値は 0 です。

DSCP/DSCP 変換マップの設定

2 つの QoS ドメインで異なる DSCP 定義が使用されている場合は、一方のドメインの一連の DSCP 値を変換して、もう一方のドメインの定義に一致させる DSCP/DSCP 変換マップを使用します。

DSCP/DSCP 変換マップは、QoS 管理ドメインの境界にある受信ポートに適用します (入力変換)。

入力変換により、パケットの DSCP 値が新しい DSCP 値で上書きされ、QoS はこの新しい値を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。

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

	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 <i>dscp-mutation-name in-dscp to out-dscp</i>	DSCP/DSCP 変換マップを変更します。 <ul style="list-style-type: none"> <i>dscp-mutation-name</i> 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。 <i>in-dscp</i> には、最大 8 つの DSCP 値をスペースで区切って入力します。さらに、to キーワードを入力します。 <i>out-dscp</i> には、1 つの DSCP 値を入力します。 DSCP の範囲は 0 ~ 63 です。
ステップ 3	interface interface-id	マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	mls qos trust dscp	DSCP trusted ポートとして入力ポートを設定します。デフォルトでは、ポートは trusted ではありません。
ステップ 5	mls qos dscp-mutation <i>dscp-mutation-name</i>	指定された DSCP trusted 入力ポートにマップを適用します。 <i>dscp-mutation-name</i> 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。
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) コンフィギュレーション ファイルに設定を保存します。

デフォルトのマップに戻すには、**no 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すべてのエントリは変更されません (空のマップで指定された値のままです)。

```
Switch(config)# mls qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
mutation1:
d1 : d2 0 1 2 3 4 5 6 7 8 9
-----
0 : 00 00 00 00 00 00 00 00 10 10
1 : 10 10 10 10 14 15 16 17 18 19
2 : 20 20 20 23 24 25 26 27 28 29
3 : 30 30 30 30 30 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
```



(注)

上記の DSCP/DSCP 変換マップでは、変換される値が表形式で示されています。d1 列は元の DSCP の最上位桁、d2 行は元の DSCP の最下位桁を示します。d1 と d2 の交点の値が、変換される値です。たとえば、DSCP 値が 12 の場合、対応する変換される値は 10 です。

入力キューの特性の設定

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

- 各キューに (DSCP 値または CoS 値によって) 割り当てるパケット
- 各キューに適用されるドロップしきい値、および各しきい値にマッピングされる CoS または DSCP 値
- 各キュー間に割り当てられる空きバッファ スペースの量
- 各キュー間に割り当てられる使用可能な帯域幅の量
- ハイ プライオリティを設定する必要があるトラフィック (音声など) の有無

ここでは、次の設定について説明します。

- 「入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定」(P.37-84) (任意)
- 「入力キュー間のバッファ スペースの割り当て」(P.37-85) (任意)
- 「入力キュー間の帯域幅の割り当て」(P.37-86) (任意)
- 「入力プライオリティ キューの設定」(P.37-86) (任意)

入力キューへの DSCP または CoS 値のマッピングおよび WTD しきい値の設定

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

DSCP または CoS 値を入力キューにマッピングして、WTD しきい値を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

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 値を入力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ~ 39 および 48 ~ 63 はキュー 1 およびしきい値 1 にマッピングされます。DSCP 値 40 ~ 47 はキュー 2 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 ~ 4、6、および 7 はキュー 1 およびしきい値 1 にマッピングされます。CoS 値 5 はキュー 2 およびしきい値 1 にマッピングされます。 <ul style="list-style-type: none"> • <i>queue-id</i> で指定できる範囲は 1 ~ 2 です。 • <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいつぱいの状態に対して設定されます。 • <i>dscp1...dscp8</i> には、最大 8 つの値を入力し、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。 • <i>cos1...cos8</i> 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	入力キューに 2 つの WTD しきい値の割合 (しきい値 1 および 2 用) を割り当てます。デフォルトでは、両方のしきい値が 100% に設定されています。 <ul style="list-style-type: none"> • <i>queue-id</i> で指定できる範囲は 1 ~ 2 です。 • <i>threshold-percentage1 threshold-percentage2</i> の範囲は、1 ~ 100 です。各値はスペースで区切ります。 <p>各しきい値は、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。</p>
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 maps	設定を確認します。 DSCP 入力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1 (02-01) のようになります。 CoS 入力キューしきい値マップでは、先頭行に CoS 値、2 番目の行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2 (2-2) のようになります。
ステップ 6 copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの CoS 入力キューしきい値マップまたはデフォルトの DSCP 入力キューしきい値マップに戻すには、**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 しきい値の割合に戻すには、**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 とドロップしきい値 50% のしきい値 1 にマッピングする方法を示します。DSCP 値 20～26 は、入力キュー 1 とドロップしきい値 70% のしきい値 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
```

この例では、50% の WTD しきい値が DSCP 値 (0～6) に割り当てられており、70% の WTD しきい値が割り当てられた DSCP 値 (20～26) よりも先にドロップされます。

入力キュー間のバッファ スペースの割り当て

2 つのキュー間で入力バッファを分割する比率を定義します (スペース量を割り当てます)。バッファ割り当てと帯域幅割り当てにより、パケットがドロップされる前にバッファに格納できるデータ量が制御されます。

入力キュー間にバッファを割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	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、バッファの 90% がキュー 1 に、残りの 10% がキュー 2 に割り当てられます。 <i>percentage1 percentage2</i> の範囲は、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。
ステップ 4	show mls qos interface buffer または show mls qos input-queue	入力内容を確認します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**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
```

入力キュー間の帯域幅の割り当て

入力キュー間に割り当てられる使用可能な帯域幅の量を指定する必要があります。重みの比率は、SRR スケジューラが各キューからパケットを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により、パケットがドロップされる前にバッファに格納できるデータ量を制御できます。入力キューで SRR が動作するのは、共有モードの場合のみです。

入力キュー間に帯域幅を割り当てるには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>mls qos srr-queue input bandwidth weight1 weight2</code>	入力キューに共有ラウンド ロビン重みを割り当てます。 <i>weight1</i> および <i>weight2</i> のデフォルト設定は 4 です (帯域幅の 1/2 が 2 つのキューで等しく共有されます)。 <i>weight1</i> および <i>weight2</i> の範囲は、1 ~ 100 です。各値はスペースで区切ります。 SRR は、 <code>mls qos srr-queue input priority-queue queue-id bandwidth weight</code> 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 <code>mls qos srr-queue input bandwidth weight1 weight2</code> グローバル コンフィギュレーション コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、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.37-86) を参照してください。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos interface queuing</code> または <code>show mls qos input-queue</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no mls qos 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限り使用してください (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、オーバーサブスクリプトリングに激しいネットワーク トラフィックが発生している状況で (バックプレーンが伝達できるトラフィックよりも多くのトラフィックが発生し、キューがいっぱいになって、フレームがドロップされている場合)、遅延およびジッタを軽減するように帯域幅の一部が保証されています。

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 コマンドによって設定された重みに従い、残りの帯域幅を両方の入力キューと共有し、キューを処理します。

プライオリティ キューを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>mls qos srr-queue input priority-queue queue-id bandwidth weight</code>	<p>キューをプライオリティ キューとして割り当て、スタックまたは内部リングが輻輳している場合にリングの帯域幅を保証します。</p> <p>デフォルトのプライオリティ キューはキュー 2 です。このキューには帯域幅の 10% が割り当てられています。</p> <ul style="list-style-type: none"> <code>queue-id</code> で指定できる範囲は 1 ~ 2 です。 <code>bandwidth weight</code> には、スタックまたは内部リングの帯域幅に対する割合を割り当てます。指定できる範囲は 0 ~ 40 です。値が大きい場合はリング全体に影響が及び、スイッチまたはスタックのパフォーマンスが低下することがあるため、保証できる帯域幅は制限されています。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show mls qos interface queueing</code> または <code>show mls qos input-queue</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、`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` を入力します。

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 および 2 に割り当てられている帯域幅比率は $4/(4+4)$ 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。その後、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

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

- DSCP 値または CoS 値によって各キューおよびしきい値 ID にマッピングされるパケット
- キューセット (ポートごとの 4 つの出力キュー) に適用されるドロップしきい値の割合、およびトラフィック タイプに必要なメモリの確保量および最大メモリ
- キューセットに割り当てる固定バッファ スペースの量

- ポートの帯域幅に関するレート制限の必要性
- 出力キューの処理頻度、および使用する技術（シェーピング、共有、または両方）

ここでは、次の設定について説明します。

- 「設定時の注意事項」(P.37-88)
- 「出力キューセットに対するバッファ スペースの割り当ておよび WTD しきい値の設定」(P.37-88) (任意)
- 「出力キューおよび ID への DSCP または CoS 値のマッピング」(P.37-90) (任意)
- 「出力キューでの SRR シェーピング重みの設定」(P.37-92) (任意)
- 「出力キューでの SRR 共有重みの設定」(P.37-93) (任意)
- 「出力緊急キューの設定」(P.37-94) (任意)
- 「出力インターフェイスの帯域幅の制限」(P.37-94) (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で、SRR シェーピング重みが設定されていない場合、SRR はこのキューを共有モードで処理します。

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

バッファの可用性の保証、WTD しきい値の設定、およびキューセットの最大メモリ割り当ての設定を行うには、`mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` グローバル コンフィギュレーション コマンドを使用します。

各しきい値はキューに割り当てられたメモリの割合です。このパーセント値を指定するには、`mls qos queue-set output qset-id buffers allocation1 ... allocation4` グローバル コンフィギュレーション コマンドを使用します。キューは WTD を使用して、トラフィック クラスごとに異なるドロップ割合をサポートします。



(注)

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

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

	コマンド	目的
ステップ1	<code>configure terminal</code>	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	<code>mls qos queue-set output <i>qset-id</i> buffers <i>allocation1</i> ... <i>allocation4</i></code>	<p>キューセットにバッファを割り当てます。</p> <p>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。</p> <ul style="list-style-type: none"> • <i>qset-id</i> 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。 • <i>allocation1</i> ... <i>allocation4</i> には、キューセット内のキューごとに 1 つずつ、合計 4 つのパーセンテージを指定します。<i>allocation1</i>、<i>allocation3</i>、<i>allocation4</i> の場合、使用可能な範囲は 0 ~ 99 です。<i>allocation2</i> の場合、範囲は 1 ~ 100 です (CPU バッファを含める)。 <p>トラフィックの重要度に応じてバッファを割り当てます。たとえば、最高プライオリティのトラフィックを持つキューには多くの割合のバッファを与えます。</p>
ステップ3	<code>mls qos queue-set output <i>qset-id</i> threshold <i>queue-id</i> <i>drop-threshold1</i> <i>drop-threshold2</i> <i>reserved-threshold</i> <i>maximum-threshold</i></code>	<p>WTD を設定し、バッファのアベイラビリティを保証し、キューセット (ポートごとに 4 つの出力キュー) の最大メモリ割り当てを設定します。</p> <p>デフォルトでは、キュー 1、3、および 4 の WTD は 100% に設定されています。キュー 2 の WTD は 200% に設定されています。キュー 1、2、3、および 4 の専用は 50% に設定されています。すべてのキューの最大は 400% に設定されています。</p> <ul style="list-style-type: none"> • <i>qset-id</i> 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。 • <i>queue-id</i> には、コマンドの実行対象となるキューセット内の特定のキューを入力します。指定できる範囲は 1 ~ 4 です。 • <i>drop-threshold1</i> <i>drop-threshold2</i> には、キューの割り当てメモリの割合として表される 2 つの WTD しきい値を指定します。指定できる範囲は 1 ~ 3200% です。 • <i>reserved-threshold</i> には、割り当てメモリの割合として表されるキューに保証 (確保) されるメモリ サイズを入力します。指定できる範囲は 1 ~ 100% です。 • <i>maximum-threshold</i> を指定すると、いっぱいになったキューが確保量を超えるバッファを取得できるようになります。この値は、共通プールが空でない場合に、パケットがドロップされるまでキューが使用できるメモリの最大値です。指定できる範囲は 1 ~ 3200% です。
ステップ4	<code>interface <i>interface-id</i></code>	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ5	<code>queue-set <i>qset-id</i></code>	<p>キューセットにポートをマッピングします。</p> <p><i>qset-id</i> 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。</p>
ステップ6	<code>end</code>	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 interface <i>[interface-id]</i> buffers	入力内容を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no mls qos queue-set output *qset-id* buffers** グローバル コンフィギュレーション コマンドを使用します。デフォルトの WTD の割合に戻すには、**no mls qos queue-set output *qset-id* threshold [*queue-id*]** グローバル コンフィギュレーション コマンドを使用します。

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

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

出力キューおよび ID への DSCP または CoS 値のマッピング

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



(注)

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

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

	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 <i>queue-id</i> threshold <i>threshold-id</i> <i>dscp1...dscp8</i> または mls qos srr-queue output cos-map queue <i>queue-id</i> threshold <i>threshold-id</i> <i>cos1...cos8</i>	DSCP または CoS 値を出力キューおよびしきい値 ID にマッピングします。 デフォルトでは、DSCP 値 0 ~ 15 はキュー 2 およびしきい値 1 に、DSCP 値 16 ~ 31 はキュー 3 およびしきい値 1 に、DSCP 値 32 ~ 39 および 48 ~ 63 はキュー 4 およびしきい値 1 に、DSCP 値 40 ~ 47 はキュー 1 およびしきい値 1 にマッピングされます。 デフォルトでは、CoS 値 0 および 1 はキュー 2 およびしきい値 1 に、CoS 値 2 および 3 はキュー 3 およびしきい値 1 に、CoS 値 4、6、および 7 はキュー 4 およびしきい値 1 に、CoS 値 5 はキュー 1 およびしきい値 1 にマッピングされます。 <ul style="list-style-type: none"> • <i>queue-id</i> で指定できる範囲は 1 ~ 4 です。 • <i>threshold-id</i> で指定できる範囲は 1 ~ 3 です。しきい値 3 のドロップしきい値 (%) は事前に定義されています。パーセンテージはキューがいっぱいの状態に対して設定されます。 • <i>dscp1...dscp8</i> には、最大 8 つの値を入力し、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。 • <i>cos1...cos8</i> 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。
ステップ4	show mls qos maps	入力内容を確認します。 DSCP 出力キューしきい値マップは、表形式で表示されます。d1 列は DSCP 値の最上位桁、d2 行は DSCP 値の最下位桁を示します。d1 および d2 値の交点がキュー ID およびしきい値 ID です。たとえば、キュー 2 およびしきい値 1 (02-01) のようになります。 CoS 出力キューしきい値マップでは、先頭行に CoS 値、2 番目の行に対応するキュー ID およびしきい値 ID が示されます。たとえば、キュー 2 およびしきい値 2 (2-2) のようになります。
ステップ5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの DSCP 出力キューしきい値マップまたはデフォルトの CoS 出力キューしきい値マップに戻すには、**no mls qos srr-queue output dscp-map** または **no mls qos srr-queue output cos-map** グローバル コンフィギュレーション コマンドを使用します。

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

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

出力キューでの SRR シェーピング重みの設定

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

出力キューにシェーピング重み、共有重み、またはその両方を設定できます。バースト性のあるトラフィックをスムーズにする、または長期にわたって出力をスムーズにする場合に、シェーピングを使用します。シェーピング重みの詳細については、「[SRR のシェーピングおよび共有](#)」(P.37-15) を参照してください。共有重みの詳細については、「[出力キューでの SRR 共有重みの設定](#)」(P.37-93) を参照してください。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	発信トラフィックのポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>srr-queue bandwidth shape weight1 weight2 weight3 weight4</code>	出力キューに SRR 重みを割り当てます。 デフォルトでは、weight1 は 25、weight2、weight3、および weight4 は 0 に設定されています。これらのキューは共有モードです。 <code>weight1 weight2 weight3 weight4</code> には、シェーピングされるポートの割合を制御する重みを入力します。このキューのシェーピング帯域幅は、インバース比率 ($1/\text{weight}$) 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 を設定した場合は、対応するキューが共有モードで動作します。 srr-queue bandwidth shape コマンドで指定された重みは無視され、 srr-queue bandwidth share インターフェイス コンフィギュレーション コマンドで設定されたキューの重みが有効になります。シェーピングおよび共有の両方に対して同じキューセットのキューを設定した場合は、必ず番号が最も小さいキューにシェーピングを設定してください。 シェーピング モードは、共有モードを無効にします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface interface-id queuing</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no srr-queue bandwidth shape` インターフェイス コンフィギュレーション コマンドを使用します。

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

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

出力キューでの SRR 共有重みの設定

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



(注)

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

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

	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 モードを開始します。
ステップ 3	srr-queue bandwidth share weight1 weight2 weight3 weight4	出力キューに SRR 重みを割り当てます。 デフォルトでは、4 つの重みがすべて 25 です（各キューに帯域幅の 1/4 が割り当てられています）。 <i>weight1 weight2 weight3 weight4</i> には、SRR スケジューラがパケットを送信する頻度の比率を制御する重みを入力します。各値はスペースで区切ります。指定できる範囲は 1 ~ 255 です。
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 queuing	入力内容を確認します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**no srr-queue bandwidth share** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、出力ポートで稼働する SRR スケジューラの重み比を設定する方法を示します。4 つのキューが使用され、共有モードで各キューに割り当てられる帯域幅の比率は、キュー 1、2、3、および 4 に対して $1/(1+2+3+4)$ 、 $2/(1+2+3+4)$ 、 $3/(1+2+3+4)$ 、および $4/(1+2+3+4)$ になります（それぞれ、10、20、30、および 40%）。キュー 4 はキュー 1 の帯域幅の 4 倍、キュー 2 の帯域幅の 2 倍、キュー 3 の帯域幅の 1 と 1/3 倍であることを示します。

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

出力緊急キューの設定

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

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

	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	スイッチ上で 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 モードを開始します。
ステップ 4	priority-queue out	デフォルトでディセーブルに設定されている出力緊急キューをイネーブルにします。 このコマンドを設定すると、SRR に参加するキューは 1 つ少なくなるため、SRR 重みおよびキュー サイズの比率が影響を受けます。つまり、 srr-queue bandwidth shape または srr-queue bandwidth share コマンドの <i>weight1</i> が無視されます（比率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) コンフィギュレーション ファイルに設定を保存します。

出力緊急キューをディセーブルにするには、**no priority-queue out** インターフェイス コンフィギュレーション コマンドを使用します。

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

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

出力インターフェイスの帯域幅の制限

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



(注)

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

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	レートを制限するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>srr-queue bandwidth limit weight</code>	ポートの上限となるポート速度の割合を指定します。指定できる範囲は 10 ~ 90 です。 デフォルトでは、ポートのレートは制限されず、100% に設定されています。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show mls qos interface [interface-id] queuing</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、`no srr-queue bandwidth limit` インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートの帯域幅を 80% に制限する例を示します。

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

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

標準 QoS 情報の表示

Cisco IOS Release 12.2(52)SE 以降のリリースでは、表 37-15 にリストされているコマンドは、デュアル IPv4/IPv6 SDM テンプレートが使用されている場合、IPv4 および IPv6 の両方のトラフィックに適用されます。

標準 QoS 情報を表示するには、表 37-15 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 37-15 標準 QoS 情報を表示するためのコマンド

コマンド	目的
<code>show class-map [class-map-name]</code>	トラフィックを分類するための一致条件を定義した QoS クラス マップを表示します。
<code>show mls qos</code>	グローバル QoS コンフィギュレーション 情報を表示します。
<code>show mls qos aggregate-policer [aggregate-policer-name]</code>	集約ポリサーの設定を表示します。
<code>show mls qos input-queue</code>	入力キューの QoS 設定を表示します。
<code>show mls qos interface [interface-id] [buffers policers queuing statistics]</code>	バッファ割り当て、ポリサーが設定されるポート、キューイング方式、入出力統計情報など、ポート レベルの QoS 情報が表示されます。

表 37-15 標準 QoS 情報を表示するためのコマンド (続き)

コマンド	目的
<code>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]</code>	QoS マッピング情報を表示します。
<code>show mls qos queue-set [qset-id]</code>	出力キューの QoS 設定を表示します。
<code>show mls qos vlan vlan-id</code>	指定の SVI に適用されたポリシー マップを表示します。
<code>show policy-map [policy-map-name [class class-map-name]]</code>	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。 (注) 着信トラフィックの分類情報を表示する場合は、 show policy-map interface 特権 EXEC コマンドを使用しないでください。 control-plane および interface キーワードはサポートされていません。表示される統計情報は無視してください。
<code>show running-config include rewrite</code>	透過的な DSCP 設定を表示します。