CHAPTER 29

QoS の設定

この章では、Automatic QoS（Auto-QoS）コマンド、または標準の QoS コマンドを使用して 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、Catalyst 2950 または Catalyst 2955 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。

この章で説明した機能を使用するには、スイッチに Enhanced software Image（EI; 拡張ソフトウェア イメージ）をインストールする必要があります。

スイッチに Standard software Image（SI; 標準ソフトウェア イメージ）がインストールされている場合は、一部の機能を設定できません。表 29-1 に、設定可能な機能の説明がある項を示します。

表 29-1　　標準ソフトウェア機能の説明があるセクション

トピック	セクション
出力ポートでのキューイングとスケジューリング	「キューイングおよびスケジューリング」（P.29-8）
QoS の設定	「標準 QoS の設定」（P.29-17）
	「標準 QoS のデフォルト設定」（P.29-18）
	「ポートの信頼状態を使用した分類の設定」（P.29-20）
	「出力キューの設定」（P.29-36）

（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*に対応するコマンド リファレンスを参照してください。

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、次の URL にある『Modular Quality of Service Command Line Interface Overview』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd909.html

QoS は Network Assistant または Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して設定できます。設定の手順については、Network Assistant のオンライン ヘルプを参照してください。

また、EI を実行している場合のみ、次のウィザードを使用して、QoS を設定することもできます。

- プライオリティ データ ウィザード：TCP ポートまたは UDP ポートに基づいて、データ アプリケーションにプライオリティ レベルを割り当てることができます。アプリケーションの標準リストから、優先させるアプリケーション、プライオリティ レベル、プライオリティ処理が発生するインターフェイスを選択します。このウィザードの使用手順については、プライオリティ データ ウィザードのオンライン ヘルプを参照してください。
- ビデオ ウィザード：指定されたビデオ サーバから開始されるトラフィックに、データ トラフィックよりも高いプライオリティを指定します。このウィザードは、ビデオ サーバがクラスタ内の単一のデバイスに接続されていることを前提としています。このウィザードの使用手順については、ビデオ ウィザードのオンライン ヘルプ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

ここでは、スイッチで QoS を実装する手順について説明します。スイッチに SI がインストールされている場合は、このセクションの一部の概念および機能が該当しません。使用できる機能のリストについては、表 29-1（P.29-1）を参照してください。

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。輻輳が発生した場合に、廃棄される可能性についても、すべてのトラフィックで同じです。

QoS 機能を設定すると、特定のネットワーク トラフィックを選択し、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 の実装は、DiffServ アーキテクチャに基づきます。これは、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）による規格です。このアーキテクチャでは、ネットワーク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 Type of Service（ToS; サービス タイプ）フィールドの 6 ビットを使用して、分類（クラス）情報として伝達されます。

分類情報はレイヤ 2 フレームでも伝達できます。レイヤ 2 フレームまたはレイヤ 3 パケット内のこれらの特殊ビットについて説明します（図 29-1 を参照）。

- レイヤ 2 フレーム内のプライオリティ値

  レイヤ 2 IEEE 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 Class of Service（CoS; サービス クラス）値が伝達されます。レイヤ 2 IEEE 802.1Q トランクとして設定されたインターフェイスでは、ネイティブ VLAN のトラフィックを除くすべてのトラフィックが IEEE 802.1Q フレームに収められます。

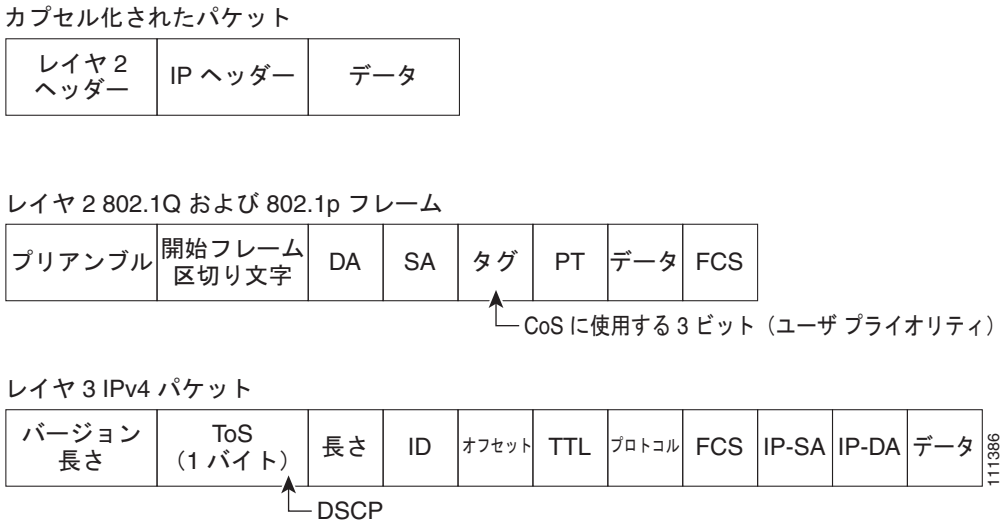
  他のフレーム タイプでレイヤ 2 CoS 値を伝達することはできません。

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 Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を伝達できます。サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。

図 29-1　　フレームおよびパケットにおける QoS 分類レイヤ



インターネット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。パケットの詳しい検証は、コア スイッチおよびルータが過負荷にならないように、ネットワーク エッジに近い位置で行われることが前提になります。

パス上のスイッチおよびルータは、クラス情報を使用して、個々のトラフィック クラスに割り当てるリソースの量を制限できます。DiffServ アーキテクチャでトラフィックを処理するときの、各デバイスの動作をホップ単位動作といいます。パス上のすべてのデバイスに一貫性のある Per-Hop Behavior を実行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

図 29-2 に、QoS の基本モデルを示します。入力インターフェイスでのアクションには、トラフィックの分類、ポリシング、およびマーキングが含まれます。

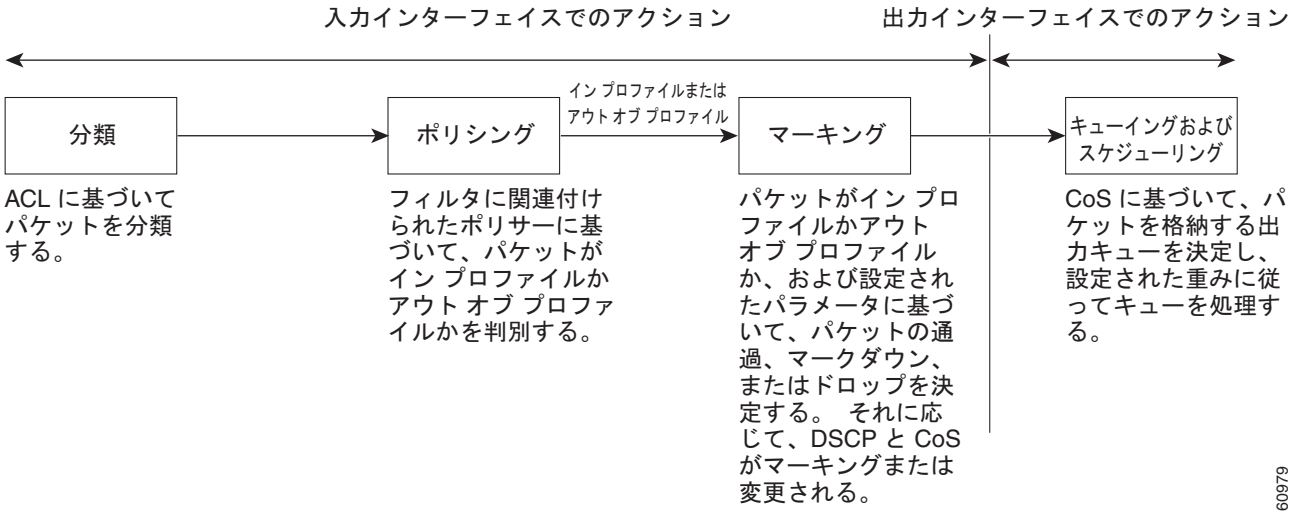
（注） スイッチに SI がインストールされている場合、キューイング機能とスケジューリング機能のみを使用できます。

- 分類は、トラフィックの種類を区別します。詳細については、「分類」（P.29-4）を参照してください。
- ポリシングは、設定されたポリサーに基づいてパケットがイン プロファイルまたはアウト オブ プロファイルのどちらであるかを判別し、ポリサーによってトラフィックのフローで消費される帯域幅が制限されます。この判別の結果が、マーカーに引き渡されます。詳細については、「ポリシングおよびマーキング」（P.29-7）を参照してください。
- マーキングでは、パケットがアウト オブ プロファイルの場合の対処法に関して、ポリサーおよび設定情報を評価し、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 DSCP 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.29-7）を参照してください。

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

- キューイングは、CoS 値を評価し、4 つの出力キューのどれにパケットを入れるかを決定します。
- スケジューリングでは、設定されている Weighted Round Robin（WRR; 重み付けラウンド ロビン）の重みに基づいて、4 つの出力キューを処理します。

図 29-2　QoS の基本モデル



分類

（注）　この機能は、スイッチが EI を実行している場合のみ使用可能です。

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。

分類は物理インターフェイス単位でのみ発生します。VLAN レベルでのパケットの分類はサポートされません。

着信トラフィックの分類に、フレームまたはパケットのどのフィールドを使用するかは、ユーザ側で指定します。

IP 以外のトラフィックについては、次の分類オプションがあります。

- ポート デフォルトを使用します。フレームに CoS 値が含まれない場合、スイッチは着信フレームにデフォルト ポートの CoS 値を割り当てます。

- 着信フレームの CoS 値を信頼します（ポートが CoS を信頼するように設定します）。レイヤ 2 IEEE 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。

  Trust DSCP の設定は、IP 以外のトラフィックに対しては無意味です。このオプションでポートを設定した場合、IP 以外のトラフィックを受信すると、スイッチはデフォルトのポート CoS 値を割り当て、CoS 値に基づいてトラフィックを分類します。

IP トラフィックについては、次の分類オプションがあります。

- 着信パケットの IP DSCP 値を信頼します（ポートが DSCP を信頼するように設定します）。スイッチは内部使用のため同じ DSCP 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。サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。
- 着信パケットの CoS 値を信頼します（存在する場合）。スイッチは CoS/DSCP マップを使用して、DSCP を生成します。

（注）　CoS または DSCP のいずれかを信頼するようにインターフェイスを設定できますが、両方を同時に信頼するように設定することはできません。

QoS ACL に基づく分類

IP 標準 Access Control List（ACL; アクセス コントロール リスト）、IP 拡張 ACL、およびレイヤ 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。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（最初の一致の原則）、指定の QoS 関連アクションが実行されます。
- 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 の照合が済んだ場合は、パケットに対して QoS 処理が行われません。
- インターフェイス上で複数の ACL が設定されている場合は、パケットが許可アクションのある ACL と最初に一致すると、QoS 処理が開始されます。
- スイッチの QoS ACL では拒否アクションの設定がサポートされません。
- システム定義のマスクは、クラス マップで次の制限付きで許可されます。
  - システム定義のマスクとユーザ定義のマスクの組み合わせは、ポリシー マップの一部である複数のクラス マップには使用できません。
  - ポリシー マップの一部であるシステム定義のマスクはすべて、システム マスクと同じタイプを使用する必要があります。たとえば、ポリシー マップに **permit tcp any any** ACE を使用するクラス マップと、**permit ip any any** ACE を使用するクラス マップを含めることはできません。
  - ポリシー マップには、すべてが同じユーザ定義マスクまたは同じシステム定義マスクを使用する複数のクラス マップを含めることができます。

（注）　システム定義のマスクの詳細については、「アクセス コントロール パラメータについて」（P.28-4）を参照してください

ACL 制限の詳細については、「ACL の設定」（P.28-7）を参照してください。

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 を実装してレイヤ 2 トラフィックを分類する場合は、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

クラス マップおよびポリシー マップに基づく分類

クラス マップは、特定のトラフィック フロー（またはクラス）を、他のすべてのトラフィックから切り離して名前を付けるためのメカニズムです。クラス マップでは、さらに細かく分類するために、特定のトラフィック フローと照合するために使用される条件を定義します。この条件には、ACL によって定義されたアクセス グループの一致が含まれます。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。アクションには、トラフィック クラス内の特定の DSCP 値の設定や、トラフィックの帯域幅制限の指定や、トラフィックがアウト オブ プロファイルの場合に実行するアクションが含まれる可能性があります。ポリシー マップを有効にするには、インターフェイスにポリシー マップを付加する必要があります。

クラス マップを作成するには、**class-map** グローバル コンフィギュレーション コマンドまたは **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 コマンドを使用する必要があります。**class-map** グローバル コンフィギュレーション コマンドを入力すると、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。

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** ポリシー マップ コンフィギュレーション コマンド、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 マップを有効にするには、**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシー マップをインターフェイスに付加します。

ポリシー マップには、ポリサーを定義するコマンド、トラフィックの帯域幅制限、および制限を超過した場合に実行するアクションを含めることもできます。詳細については、「ポリシングおよびマーキング」（P.29-7）を参照してください。

ポリシー マップには、次の特性もあります。

- 1 つのポリシー マップに複数のクラス ステートメントを指定できます。
- インターフェイス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。
- ポリシー マップ設定の状態は、インターフェイスの信頼状態に応じたアクションよりも優先されます。

設定情報については、「QoS ポリシーの設定」（P.29-25）を参照してください。

ポリシングおよびマーキング

（注）　この機能は、スイッチが EI を実行している場合のみ使用可能です。

ポリシングには、トラフィックの帯域幅限度を指定するポリサーの作成が伴います。制限を超えるパケットは、「*アウト オブ プロファイル*」または「*不適合*」になります。各ポリサーは、イン プロファイルまたはアウト オブ プロファイル パケットに対して実行するアクションを指定します。マーカーによって実行されるアクションには、パケットのドロップや新しいユーザ定義の値でのパケットのマークダウンなどが含まれます。

個別のポリサーを作成できます。QoS では、一致する各トラフィック クラスに、ポリサー内で指定された帯域幅制限が個別に適用されます。このタイプのポリサーは、**policy-map** コンフィギュレーション コマンドを使用して、ポリシー マップ内で設定します。

ポリシングおよびポリサーを設定する場合、次の点に注意してください。

- デフォルトで設定されるポリサーはありません。
- ポリサーは物理ポートのみで設定できます。VLAN レベルでのポリシングはサポートされません。
- 入力方向で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。
- ポリシングは入力インターフェイスで発生します。
  - 入力ギガビット対応イーサネット ポートでは、60 のポリサーがサポートされます。
  - 入力 10/100 イーサネット ポートでは、6 つのポリサーがサポートされます。
  - ギガビット イーサネット ポートの平均バースト レートの精細度は 8 Mbps です。
- QoS を設定したインターフェイス上では、そのインターフェイス経由で受信されるすべてのトラフィックが、インターフェイスに付加されたポリシー マップに従って、分類、ポリシング、およびマーク付けされます。QoS 対応として設定されているトランク インターフェイスの場合、インターフェイスを介して受信したすべての VLAN のトラフィックは、そのインターフェイスに付加されたポリシー 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。

（注）　出力インターフェイス上ではポリサーを設定できません。

マッピング テーブル

（注）　この機能は、スイッチが EI を実行している場合のみ使用可能です。

分類の実行中に、QoS は設定可能な CoS/DSCP マップを使用して、受信した CoS 値から内部 DSCP 値を取得します。この DSCP 値はトラフィックのプライオリティを表します。

トラフィックがスケジューリング段階に達する前に、QoS は設定可能な DSCP/CoS マップを使用して、内部 DSCP 値から CoS 値を取得します。CoS 値は 4 つの出力キューのいずれかを選択するために使用されます。

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

設定情報については、「CoS マップの設定」（P.29-33）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

（注）　SI と EI の両方でこの機能がサポートされます。

スイッチは QoS ベースの IEEE 802.1p CoS 値を指定します。QoS は、分類およびスケジューリングを使用して、スイッチからのネットワーク トラフィックを予測可能な方法で送信します。QoS は、プライオリティが指定された CoS 値をフレームに割り当てることによって分類し、通話呼などの高いプライオリティのトラフィックを優先します。

サービス クラスの動作原理

Catalyst 6000 ファミリ スイッチと連動する で IEEE 802.1p CoS を設定する前に、Catalyst 6000 のマニュアルを参照してください。IEEE 802.1p の実装には相違点があり、互換性を確保するにはそれを理解しておく必要があります。

ポート プライオリティ

管理上定義された VLAN でユーザから受信したフレームは、他のデバイスへの伝送のために、分類されるかタグが付けられます。転送される前に、定義したルールに基づいて、固有識別子（タグ）が各フレーム ヘッダーに挿入されます。他のスイッチ、ルータ、またはエンド ステーションへのブロードキャストまたは伝送の前に、各デバイスがタグを調べて理解します。フレームがターゲットのエンド ステーションに送信される前に、フレームが最後のスイッチまたはルータに達すると、タグが削除されます。ID やタグなしでトランクまたはアクセス ポートに割り当てられた VLAN は、ネイティブ フレームまたはタグなしフレームと呼ばれます。

タグ情報付きの IEEE 802.1Q フレームの場合、ヘッダー フレームのプライオリティ値が使用されます。ネイティブ フレームの場合、入力ポートのデフォルト プライオリティが使用されます。

ポートのスケジューリング

スイッチの各ポートには、着信トラフィックのための単一受信キュー バッファ（*入力*ポート）があります。タグなしフレームが着信すると、ポートの値がそのポートのデフォルト プライオリティとして割り当てられます。この値は CLI または を使用して割り当てます。タグ付きフレームは、入力ポートを介して渡された場合、引き続き関連付けられた CoS 値を使用します。

CoS では、フレーム タグまたはポートの情報に基づいて、標準プライオリティの送信キューおよび高いプライオリティの送信キューとともに各送信ポート（出力ポート）を設定します。標準プライオリティのキュー内のフレームは、高いプライオリティのキュー内のフレームが転送された後に転送されます。

スイッチ（IEEE 802.1P ユーザのプライオリティ）には 4 つのプライオリティ キューがあります。定義したプライオリティとキューのマッピングに基づいて、フレームが適切なキューに転送されます。

出力 CoS キュー

スイッチでは、出力ポートごとに 4 つの CoS がサポートされます。キューごとに、次のタイプのスケジューリングを指定できます。

- 絶対優先スケジューリング

絶対優先スケジューリングは、キューのプライオリティに基づきます。常に高いプライオリティ キュー内のパケットが最初に送信され、標準プライオリティ キュー内のパケットは、すべての高いプライオリティ キューが空になるまで送信されません。

デフォルトのスケジューリング方法は絶対優先です。

- Weighted Round-Robin（WRR; 重み付けラウンドロビン）スケジューリング

  WRR スケジューリングでは、他の CoS キューと相対的なキューの重要度（重み）を示す数値を指定する必要があります。WRR スケジューリングでは、高いプライオリティのトラフィック中に低いプライオリティのキューが完全に無視されることを防止します。WRR スケジューラは、代わりに各キューから一部のパケットを送信します。送信するパケット数は、キューの相対的な重要度に対応します。たとえば、1 つのキューの重みが 3 で、別のキューの重みが 4 の場合、2 番めのキューから 4 つのパケットが送信される間に、最初のキューから 3 つのパケットが送信されます。このスケジューリングを使用して、高いプライオリティのキューが空でない場合でも、低いプライオリティのキューからパケットが送信されるようにします。

- 絶対優先および WRR スケジューリング

  絶対優先キューイングとも呼ばれる、絶対優先および WRR スケジューリングは、出力キューの 1 つを緊急キュー（キュー 4）として使用します。残りのキューは WRR に参加します。緊急キューが設定される場合、これはプライオリティ キューとなり、空になるまでサービスを提供され、その後、その他のキューが WRR スケジューリングでサービスを提供されます。

  出力緊急キューをイネーブルにして、WRR の重みを他のキューに割り当てるには、**wrr-queue bandwidth** *weight1 weight2 weight3* **0** 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。

自動 QoS の設定

（注）　この機能は、スイッチが EI を実行している場合のみ使用可能です。

自動 QoS 機能を使用して、既存の QoS 機能の配置を容易にできます。自動 QoS ではネットワーク設計を想定し、その結果、スイッチは複数のトラフィック フローのプライオリティ処理を行い、デフォルトの QoS 動作を使用する代わりに、出力キューを適切に使用します（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、単一のキューから送信する）。

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。

自動 QoS コマンドを使用して Cisco IP Phone、および Cisco SoftPhone アプリケーションを実行するデバイスに接続するポートを指定します。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。

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

ここでは、スイッチ上で自動 QoS を設定する手順について説明します。

- 「生成される自動 QoS 設定」（P.29-10）
- 「コンフィギュレーションにおける自動 QoS の影響」（P.29-12）
- 「設定時の注意事項」（P.29-12）

- 「旧版のソフトウェア リリースからのアップグレード」（P.29-13）
- 「VoIP 用自動 QoS のイネーブル化」（P.29-13）

生成される自動 QoS 設定

自動 QoS がイネーブルの場合は、表 29-2 に示すように、入力パケット ラベルを使用してトラフィックを分類し、出力キューを設定します。

表 29-2　トラフィック タイプ、パケット ラベル、出力キュー

	VoIP[1] データ トラフィック	VoIP コントロールトラフィック	ルーティング プロトコル トラフィック	STP[2] BPDU トラフィック	リアルタイム ビデオ トラフィック	その他のトラフィック	
DSCP	46	24、26	48	56	34	–	
CoS	5	3	6	7	4		
CoS/ キュー マップ	5	3、6、7			4	2	0、1
出力キュー	1% WRR（キュー 4）	70% WRR（キュー 3）			20% WRR（キュー 2）	20% WRR（キュー 2）	10% WRR（キュー 1）

1. VoIP = Voice over IP
2. BPDU = ブリッジ プロトコル データ ユニット

表 29-3 に、出力キューに対して生成される自動 QoS の設定を示します。

表 29-3　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/ キュー マップ	キューの重み
1% WRR	4	5	1%
70% WRR	3	3、6、7	70%
20% WRR	2	2、4	20%
10% WRR	1	0、1	10%

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

- Cisco IP Phone に接続されたネットワーク エッジのポートで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチは信頼境界の機能をイネーブルにします。スイッチは、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone が存在するかしないかを検出します。Cisco IP Phone が検出されると、インターフェイスの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。Cisco IP Phone が存在しない場合、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼しないように設定されます。スイッチは、表 29-3 の設定値に従ってポートの出力キューを設定します。
- **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 を稼動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の内部または外部にいるかを判断し、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 の DSCP 値がない場合、またはパケットがアウト オブ プロファイルの場合は、スイッチで DSCP 値が 0 に変更されます。スイッチは、表 29-3 の設定値に従ってポートの出力キューを設定します。

- 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 コマンドを入力すると、スイッチは入力パケットで CoS 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 29-3 の設定値に従ってポートの出力キューを設定します。

  信頼境界機能の詳細については、「信頼境界の設定」（P.29-22）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 29-4 にリストされているコマンドをインターフェイスに適用します。

表 29-4　生成される自動 QoS 設定

説明	等価な自動的に生成される QoS コマンド
表 29-2（P.29-10）に示すように、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 map cos-dscp 0 8 16 26 32 46 48 56`
auto qos voip trust コマンドを入力すると、スイッチは自動的に、インターフェイスの入力分類がパケット内の CoS 値を信頼するように設定します。	`Switch(config-if)# mls qos trust cos`
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)# class-map match-all AutoQoS-VoIP-RTP-Trust`
	`Switch(config-cmap)# match ip dscp 46`
	`Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust`
	`Switch(config-cmap)# match ip dscp 24 26`
	`Switch(config)# policy-map AutoQoS-Police-SoftPhone`
	`Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust`
	`Switch(config-pmap-c)# set ip dscp 46`
	`Switch(config-pmap-c)# police 1000000 4096 exceed-action drop`
	`Switch(config-pmap)# class AutoQoS-VoIP-Control-Trust`
	`Switch(config-pmap-c)# set ip dscp 24`
	`Switch(config-pmap-c)# police 1000000 4096 exceed-action drop`

表 29-4　生成される自動 QoS 設定（続き）

説明	等価な自動的に生成される QoS コマンド
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**
スイッチは自動的にこのインターフェイス上の出力キューの使用状況を割り当てます（表 29-3（P.29-10）を参照）。 一部のネットワーク トラフィックで緊急転送が必要な場合、キュー 4 を緊急キューとして設定します。キューの WRR の重みが 0 に設定される場合、このキューは緊急キューになります。緊急キューにできるのはキュー 4 だけです。 スイッチは、CoS と出力キューのマップを設定します。 • CoS 値 0 ～ 1 はキュー 1 を選択します。 • CoS 値 2 ～ 4 はキュー 2 を選択します。 • CoS 値 3 ～ 6、および 7 はキュー 3 を選択します。 • CoS 値 5 はキュー 4 を選択します。	Switch(config)# **wrr-queue bandwidth 10 20 70 1** Switch(config)# **no wrr-queue cos-map** Switch(config)# **wrr-queue cos-map 1 0 1** Switch(config)# **wrr-queue cos-map 2 2 4** Switch(config)# **wrr-queue cos-map 3 3 6 7** Switch(config)# **wrr-queue cos-map 4 5**

コンフィギュレーションにおける自動 QoS の影響

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

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。既存のユーザ設定により、生成コマンドのアプリケーションに障害が発生したり、生成コマンドによってユーザ設定が上書きされたりする可能性があります。これらの動作は警告なしに発生します。すべての生成コマンドが正常に適用された場合、上書きされていないユーザ入力設定が実行コンフィギュレーションに残ります。上書きされたユーザ入力設定は、現在の設定をメモリに保存することなく、スイッチをリロードすることで取得できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

設定時の注意事項

自動 QoS を設定する前に、次の事項を確認してください。

- Cisco IOS Release 12.1(20)EA2 よりも前のリリースでは、自動 QoS は Cisco IP Phone を搭載したスイッチでのみ VoIP を設定します。
- Cisco IOS Release 12.1(20)EA2 以降では、自動 QoS は Cisco IP Phone を搭載した VoIP のスイッチ、および Cisco SoftPhone アプリケーションを実行しているデバイスを搭載した VoIP のスイッチを設定します。

（注）　Cisco SoftPhone を稼動するデバイスが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。

- 自動 QoS のデフォルト設定を利用する場合、他の QoS コマンドを実行する前に自動 QoS をイネーブルに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.29-12）を参照してください。
- 自動 QoS をイネーブルにしたら、名前に *AutoQoS* が含まれているポリシー マップまたは集約ポリサーを変更しないでください。ポリシー マップまたは集約ポリサーを変更する必要がある場合、これらをコピーしてから、コピーしたポリシー マップまたは集約ポリサーを変更してください。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成されたポリシー マップをインターフェイスから削除し、新しいポリシー マップを適用します。
- 自動 QoS は、スタティック アクセス、ダイナミックアクセス、音声 VLAN アクセス、およびトランク ポートでイネーブルにできます。
- デフォルトでは、CDP はすべてのインターフェイス上でイネーブルになっています。自動 QoS が適切に動作するために、CDP をディセーブルにしないでください。
- Cisco SoftPhone が搭載された VoIP に対して自動 QoS がイネーブルになっている場合、スイッチは自動 QoS 設定に対して 1 つのマスクを使用します。
- 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。
- 接続したデバイスは、Cisco Call Manager バージョン 4 以降を使用する必要があります。

旧版のソフトウェア リリースからのアップグレード

Cisco IOS Release 12.2(20)EA2 では、旧リリースから自動 QoS の実装が変更されています。生成された自動 QoS 設定が変更され、Cisco SoftPhone 機能のサポートが追加されました。

自動 QoS がスイッチ上に設定され、スイッチが Cisco IOS Release12.2(20)EA2 よりも前のリリースを実行している状態で、Cisco IOS Release 12.2(20)EA2 以降のリリースにアップグレードする場合、コンフィギュレーション ファイルに新しい設定が含まれないため、自動 QoS は動作しません。コンフィギュレーション ファイルで自動 QoS 設定をアップグレードするには、次の手順を実行します。

1. スイッチを Cisco IOS Release 12.2(20)EA2 以降のリリースにアップグレードします。
2. 自動 QoS がイネーブルであるポートすべてに対して、自動 QoS をディセーブルにします。
3. **no** コマンドを使用して、グローバル自動 QoS 設定すべてをデフォルト値に戻します。
4. ステップ 2 で自動 QoS をディセーブルにしたポートで、自動 QoS をイネーブルに戻します。その場合、前と同じ自動 QoS 設定でポートを設定します。

VoIP 用自動 QoS のイネーブル化

QoS ドメイン内で VoIP 用の自動 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。

	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*	Cisco IP Phone に接続するインターフェイスを指定し、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。また、ネットワーク内部の別の信頼できるスイッチまたはルータに接続されているアップリンク インターフェイスを指定することもできます。

	コマンド	目的
ステップ 3	**auto qos voip** {cisco-phone | trust}	自動 QoS をイネーブルにします。 キーワードの意味は次のとおりです。 • **cisco-phone**：インターフェイスが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは IP Phone が検出された場合だけ信頼されます。 • **trust**：信頼できるスイッチまたはルータにアップリンク インターフェイスが接続されていて、入力パケット内の VoIP 分類が信頼されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show 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。

スイッチで自動 QoS をディセーブルにして、ポートの信頼状態をデフォルト設定（untrusted）に戻すには、次の手順を実行します。

1. 自動 QoS がイネーブルになっているすべてのインターフェイスで **no auto qos voip** インターフェイス コンフィギュレーション コマンドを使用します。複数のインターフェイスで同時に自動 QoS をディセーブルにするには、**interface range** 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。
2. 自動 QoS がイネーブルになっているすべてのインターフェイスで自動 QoS をディセーブルにした後、次のグローバル コンフィギュレーション コマンドを使用して、出力キューと CoS/DSCP マップをデフォルト設定に戻します。
   - **no wrr-queue bandwidth**
   - **no wrr-queue cos-map**
   - **no mls qos map cos-dscp**

自動 QoS がイネーブルまたはディセーブルの場合に自動生成される QoS コマンドを表示するには、**debug auto qos** 特権 EXEC コマンドを入力してから、自動 QoS をイネーブルにします。詳細については、「debug auto qos コマンドの使用」（P.31-21）を参照してください。

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

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

次の例では、インターフェイスに接続されているスイッチまたはルータが信頼できるデバイスである場合に、自動 QoS をイネーブルにし、着信パケット内の QoS ラベルを信頼する方法を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip trust
```

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 map cos-dscp**
- **show wrr-queue bandwidth**
- **show wrr-queue cos-map**

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。

自動 QoS の設定例

（注）　次の例は、スイッチが EI を実行している場合だけ適用されます。

ここでは、自動 QoS をネットワークに実装する方法について説明します（図 29-3 を参照）。QoS パフォーマンスを最適にするには、ネットワーク内部のデバイスすべてで自動 QoS をイネーブルにします。

図 29-3　ネットワークでの自動 QoS の設定例

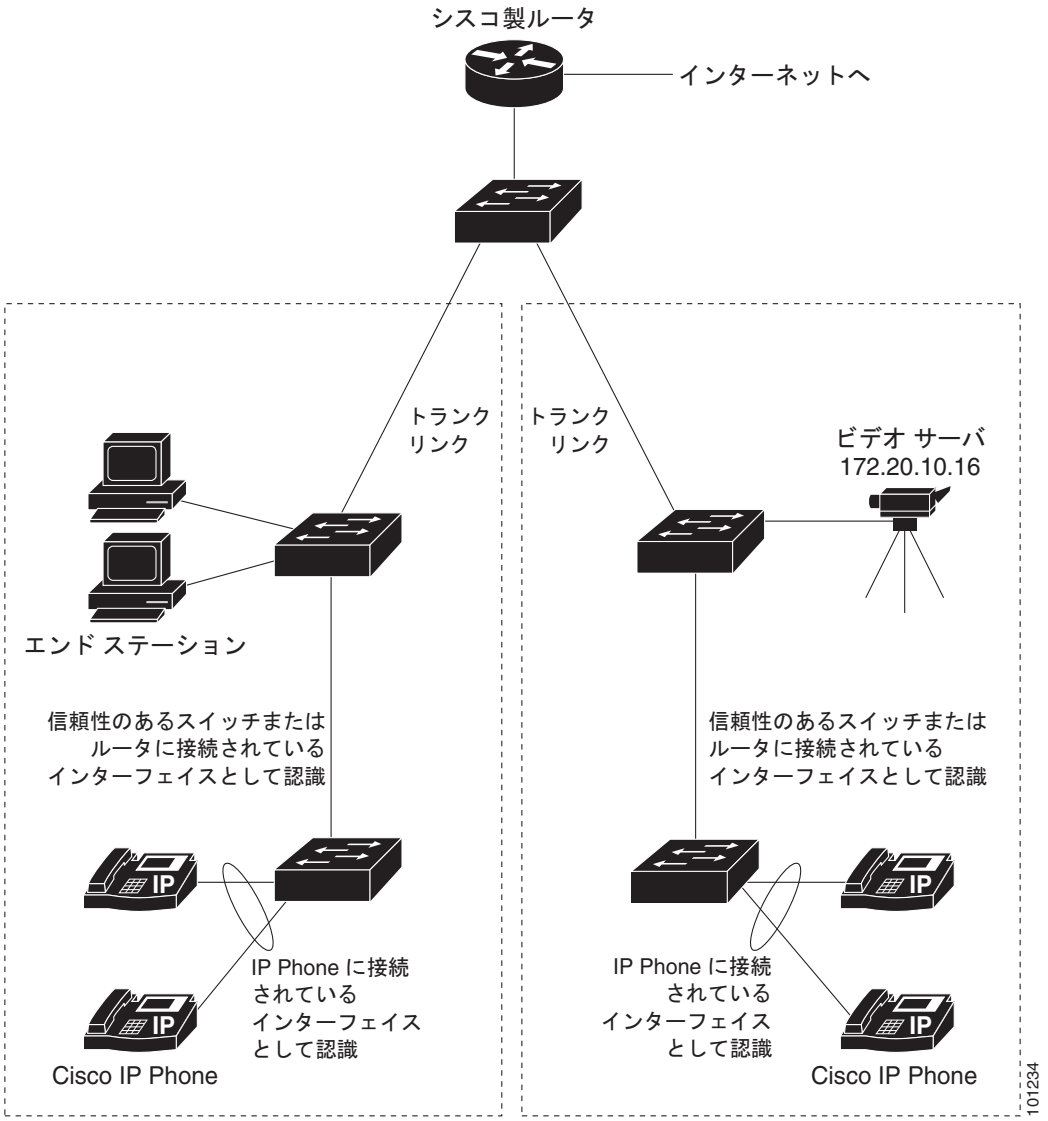


図 29-3 のインテリジェントなワイヤリング クローゼットは、EI を実行している Catalyst 2950 スイッチおよび Catalyst 3550 スイッチで構成されます。この例では、VoIP トラフィックを他のすべてのトラフィックよりも優先させることを目的としています。これを実行するには、ワイヤリング クローゼット内の QoS ドメインのエッジにあるスイッチ上で自動 QoS をイネーブルにします。

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

QoS ドメインのエッジにあるスイッチで VoIP トラフィックを他のトラフィックより優先させるように設定するには、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	debug auto qos	自動 QoS のデバッグをイネーブルにします。デバッグをイネーブルにすると、スイッチは、自動 QoS がイネーブルである場合に自動的に生成される QoS 設定を表示します。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cdp enable**	CDP をグローバルにイネーブルにします。デフォルトではイネーブルに設定されています。
ステップ 4	**interface** *interface-id*	Cisco IP Phone に接続するスイッチ 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 5	**auto qos voip** cisco-phone	インターフェイス上で自動 QoS をイネーブルにし、そのインターフェイスが Cisco IP Phone に接続されるように指定します。 着信パケット内の QoS ラベルは、IP Phone が検出された場合にだけ信頼されます。
ステップ 6	exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7		Cisco IP Phone に接続されているポートの数だけ、ステップ 4 ～ 6 を繰り返します。
ステップ 8	**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。図 29-3 を参照してください。
ステップ 9	**auto qos voip trust**	インターフェイス上で自動 QoS をイネーブルにし、そのインターフェイス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 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show auto qos**	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 によって影響される QoS 設定の詳細については、「自動 QoS 情報の表示」（P.29-15）を参照してください。
ステップ 12	**copy running-config startup-config**	**auto qos voip** インターフェイス コンフィギュレーション コマンドおよび生成された自動 QoS 設定をコンフィギュレーション ファイル内に保存します。

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、スイッチに標準 QoS を設定する方法について説明します。

（注）　スイッチが SI を実行している場合、「ポートの信頼状態を使用した分類の設定」および「出力キューの設定」で説明する機能だけを設定できます。また、「標準 QoS 情報の表示」で説明するように、QoS 情報を表示することもできます。

標準 QoS のデフォルト設定

これはデフォルトの標準 QoS 設定です。

（注）　スイッチが EI を実行している場合だけ、ポリシー マップ、ポリサー、および DSCP/CoS マップを設定できます。

- デフォルトのポート CoS 値は 0 です。
- CoS 値 0 はすべての着信パケットに割り当てられます。
- ポートのデフォルトの信頼状態は、untrusted です。
- ポリシー マップは設定されません。
- 設定されるポリサーはありません。
- デフォルトの CoS/DSCP マップは、表 29-7 のとおりです。
- デフォルトの DSCP/CoS マップは、表 29-8 のとおりです。
- 出力キューのデフォルトのスケジューリング方法は絶対優先です。
- デフォルトの CoS 値および WRR 値の詳細については、「出力キューの設定」（P.29-36）を参照してください。

（注）　Cisco IOS Release 12.1(11)EA1 よりも前のソフトウェア リリースでは、スイッチが DSCP 値を変更せずに着信パケットの CoS 値を使用します。ポートで pass-through モードをイネーブルにすると、このように設定できます。詳細については、「Pass-Through モードのイネーブル化」（P.29-24）を参照してください。

設定時の注意事項

（注）　次のガイドラインは、スイッチが EI を実行している場合だけ適用されます。

QoS の設定を始める前に、次の点を理解する必要があります。

- スイッチで QoS をイネーブルにする前に、すべてのポートで IEEE 802.3x フロー制御をディセーブルにする必要があります。ディセーブルにするには、**flowcontrol receive off** および **flowcontrol send off** インターフェイス コンフィギュレーション コマンドを使用します。
- スイッチ上で 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。
- 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トラフィック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。
- すべての入力 QoS 処理アクションは、スイッチが受信するトラフィック（スパニング ツリー Bridge Protocol Data Unit（BPDU）やルーティング アップデート パケットなど）を制御するために適用されます。
- 物理インターフェイスのために作成された ACL だけをクラス マップに付加できます。
- クラス マップごとにサポートされる ACL と **match** コマンドは 1 つだけです。ACL には複数のアクセス コントロール エントリを含めることができます。これは、フィールドをパケットの内容と照合するコマンドです。
- 出方向の ACL 分類付きのポリシー マップはサポートされず、**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 コマンドを使用してインターフェイスに付加することもできません。
- ポリシー マップでは、*class-default* という名前のクラスがサポートされます。スイッチは、**class class-default** ポリシー マップ コンフィギュレーション コマンドで定義されたポリシー マップに基づいてトラフィックをフィルタリングしません。
- ACL の設定のガイドラインについては、「QoS ACL に基づく分類」（P.29-5）を参照してください。
- ACL の物理インターフェイスへの適用については、「物理インターフェイスへの ACL 適用のガイドライン」（P.28-6）を参照してください。
- システム定義のマスク付きのポリシー マップおよびユーザ定義のマスク付きのセキュリティ ACL がインターフェイスで設定されている場合、スイッチはポリシー マップで指定されたアクションを無視し、ACL で指定されたアクションだけを実行します。マスクについては、「アクセス コントロール パラメータについて」（P.28-4）を参照してください。
- ユーザ定義のマスク付きのポリシー マップおよびユーザ定義のマスク付きのセキュリティ ACL がインターフェイスで設定されている場合は、表 29-5 に示すいずれかのアクションを実行します。マスクについては、「アクセス コントロール パラメータについて」（P.28-4）を参照してください。

表 29-5　ポリシー マップとセキュリティ ACL の相互動作

ポリシー マップ条件	セキュリティ ACL 条件	アクション
パケットがイン プロファイルの場合。	指定されたパケットを許可します。	トラフィックが転送されます。
パケットがアウト オブ プロファイルで、out-of-profile アクションが DSCP 値のマークダウンの場合。	指定されたパケットをドロップします。	トラフィックがドロップされます。
パケットがアウト オブ プロファイルで、out-of-profile アクションがパケットのドロップの場合。	指定されたパケットを許可します。	トラフィックがドロップされます。
	指定されたパケットをドロップします。	トラフィックがドロップされます。

ポートの信頼状態を使用した分類の設定

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

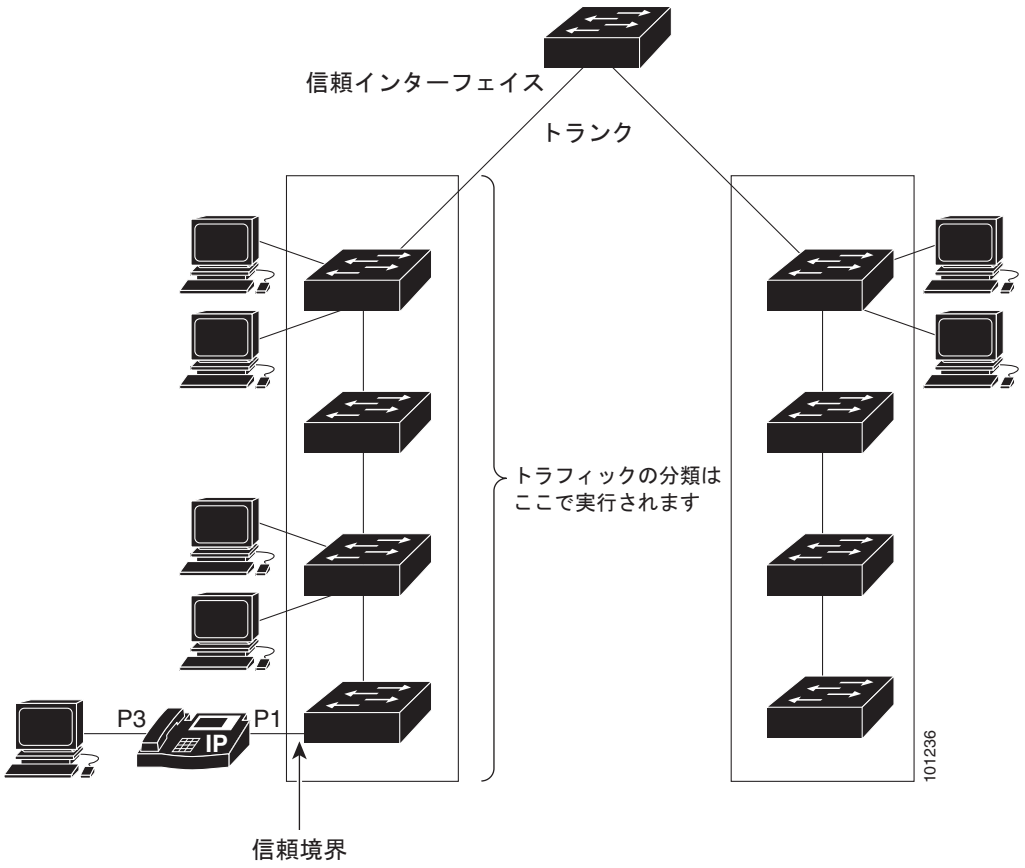
- 「QoS ドメイン内のポートの信頼状態の設定」（P.29-20）
- 「インターフェイスの CoS 値の設定」（P.29-21）
- 「信頼境界の設定」（P.29-22）
- 「Pass-Through モードのイネーブル化」（P.29-24）

（注）　SI と EI の両方でこの機能がサポートされます。

QoS ドメイン内のポートの信頼状態の設定

QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。パケットがエッジで分類されると、QoS ドメイン内の各スイッチでパケットを分類する必要がないので、QoS ドメイン内のスイッチ ポートをいずれか 1 つの信頼状態に設定できます。図 29-4 に、ネットワーク トポロジの例を示します。

図 29-4　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*	信頼するインターフェイスを指定し、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は物理インターフェイスなどです。
ステップ 3	**mls qos trust** [**cos** | **dscp**]	ポートの信頼状態を設定します。 デフォルトでは、ポートは trusted ではありません。 キーワードの意味は次のとおりです。 **cos**：パケットの CoS 値で入力パケットを分類します。タグ付き IP パケットの場合、パケットの DSCP 値が CoS/DSCP マップに基づいて変更されます。パケットに割り当てられる出力キューは、パケットの CoS 値に基づきます。 **dscp**：パケットの DSCP 値で入力パケットを分類します。非 IP パケットの場合、パケットの CoS 値はタグ付きパケットに対して 0 に設定されます。デフォルトのポート CoS はタグなしパケットに使用されます。スイッチは内部的に DSCP/CoS マップを使用して、CoS 値を変更します。 **（注）** Cisco IOS Release 12.1(11)EA1 よりも前のソフトウェア リリースでは、スイッチが EI を実行している場合だけ **mls qos trust** コマンドを使用できます。 ネットワークがイーサネット LAN で構成される場合、**cos** キーワードを使用します。 ネットワークがイーサネット LAN のみで構成されるわけではなく、高度な QoS 機能や実装に関する知識がある場合、**dscp** キーワードを使用します。 このコマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。
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*] [**policers**]	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.29-21）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.29-34）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*	信頼するインターフェイスを指定し、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は物理インターフェイスなどです。
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。 • *default-cos* には、ポートに割り当てるデフォルトの CoS 値を指定します。ポートが CoS を信頼していて、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。CoS 値に指定できる範囲は 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上書きし、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も高いプライオリティを与える場合は、**override** キーワードを使用します。ポートがすでに DSCP 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、出力ポートで、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。

信頼境界の設定

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 29-4（P.29-20）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 IEEE 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。

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。

信頼境界機能をスイッチ ポート上で設定にするには、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 enable**	CDP をグローバルにイネーブルにします。デフォルトではイネーブルに設定されています。
ステップ 3	**interface** *interface-id*	信頼するインターフェイスを指定し、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は物理インターフェイスなどです。
ステップ 4	**cdp enable**	インターフェイスで CDP をイネーブルにします。デフォルトでは、CDP がイネーブルに設定されています。
ステップ 5	**mls qos trust device cisco-phone**	Cisco IP Phone をインターフェイスの信頼済みデバイスとして設定します。 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 6	**mls qos trust cos**	ポートの信頼状態を、入力パケットの CoS 値を信頼するように設定します。 デフォルトでは、ポートは trusted ではありません。 **（注）** Cisco IOS Release 12.1(11)EA1 よりも前のソフトウェア リリースでは、スイッチが EI を実行している場合だけ **mls qos trust cos** コマンドを使用できます。 このコマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。
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** [*interface-id*] [**policers**]	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。

no mls qos trust インターフェイス コンフィギュレーション コマンドを入力しても、信頼境界はディセーブルになりません。このコマンドが入力され、ポートが Cisco IP Phone に接続されている場合、このポートは受信したトラフィックの分類を信頼しません。信頼境界をディセーブルにするには、**mls qos trust cose** 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。

mls qos cos override インターフェイス コンフィギュレーション コマンドを入力した場合、Cisco IP Phone に接続されている場合でも、ポートは受信したトラフィックの分類を信頼しません。

自動 QoS がすでにイネーブルになっている場合、信頼境界をイネーブルにすることはできません。また、ディセーブルになっている場合はディセーブルにできません。自動 QoS がイネーブルになっていて、ポートに Cisco IP Phone が存在していない場合、このポートは受信したトラフィックの分類を信頼しません。

表 29-6 に、IP Phone が存在している場合と存在していない場合のポート設定を示します。

表 29-6　信頼境界がイネーブルの場合のポート設定

ポート設定	Cisco IP Phone が存在する場合	Cisco IP Phone が存在しない場合
ポートは着信パケットの CoS 値を信頼します。	パケットの CoS 値は信頼されます。	パケットの CoS 値にデフォルトの CoS 値が割り当てられます。
ポートは着信パケットの DSCP 値を信頼します。	パケットの DSCP 値は信頼されます。	タグ付き非 IP パケットの場合、パケットの CoS 値は 0 に設定されます。 タグなし非 IP パケットの場合、パケットの CoS 値にデフォルトの CoS 値が割り当てられます。
ポートは着信パケットにデフォルトの CoS 値を割り当てます。	パケットの CoS 値にデフォルトの CoS 値が割り当てられます。	パケットの CoS 値にデフォルトの CoS 値が割り当てられます。

Pass-Through モードのイネーブル化

Cisco IOS Release 12.1(11)EA1 よりも前のソフトウェア リリースでは、スイッチが pass-through モードになっています。DSCP 値を変更せずに着信パケットの CoS 値を使用し、4 つの出力キューのいずれかのパケットを送信します。スイッチが Cisco IOS Release 12.1(11)EA1 よりも前のソフトウェア リリースを実行している場合、pass-through をイネーブルまたはディセーブルにできません。

Cisco IOS Release 12.1(11)EA1 移行のソフトウェア リリースでは、スイッチがパケットを変更せずに CoS 0 をすべての着信パケットに割り当てます。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、単一出力キューからパケットを送信します。

特権 EXEC モードから、次の手順に従って pass-through モードをイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	pass-through モードをイネーブルに設定するインターフェイスを指定し、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は物理インターフェイスなどです。
ステップ 3	**mls qos trust cos pass-through dscp**	Pass-Through モードをイネーブルにします。インターフェイスは着信パケットの CoS 値を信頼するように設定され、DSCP 値を変更せずに送信します。
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*]	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。

pass-through モードをディセーブルにするには、**no mls qos trust pass-through dscp** インターフェイス コンフィギュレーション コマンドを使用します。

pass-through モードがイネーブルの場合に **mls qos cos override** and the **mls qos trust** [**cos** | **dscp**] インターフェイス コマンドを入力すると、pass-through モードがディセーブルになります。

mls qos cos override および **mls qos trust** [**cos** | **dscp**] インターフェイス コマンドがすでに設定されている場合に **mls qos trust cos pass-through dscp** インターフェイス コンフィギュレーション コマンドを入力すると、pass-through モードがディセーブルになります。

QoS ポリシーの設定

（注）　この機能は、スイッチが EI を実行している場合のみ使用可能です。

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、ポリシーをインターフェイスに適用する必要があります。

基本情報については、「分類」（P.29-4）および「ポリシングおよびマーキング」（P.29-7）を参照してください。

ここでは、次の設定情報について説明します。

- 「ACL によるトラフィックの分類」（P.29-25）
- 「クラス マップによるトラフィックの分類」（P.29-29）
- 「ポリシー マップ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.29-30）

ACL によるトラフィックの分類

IP 標準 ACL または IP 拡張 ACL を使用すると、IP トラフィックを分類できます。レイヤ 2 のトラフィックは、レイヤ 2 MAC ACL を使用することで分類できます。

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	**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* {**permit** | **remark**} {*source source-wildcard* | **host** *source* | **any**}	IP 標準 ACL を作成し、必要な回数だけコマンドを繰り返します。 *access-list-number* には、ACL 番号を入力します。有効範囲は 1 ～ 99 および 1300 ～ 1999 です。 条件が満たされている場合にアクセスを許可するかどうかを指定するには、**permit** を入力します。 最大 100 文字の ACL エントリ コメントを指定するには、**remark** を入力します。 **（注）** QoS ACL には拒否ステートメントがサポートされません。詳細については、「QoS ACL に基づく分類」（P.29-5）を参照してください。 *source* には、パケットの送信元となるネットワークまたはホストのアドレスを、次の 3 つの形式のいずれかで指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • *source* および *source-wildcard* の 0.0.0.0 255.255.255.255 の省略形を意味するキーワード **any**。source-wildcard を入力する必要はありません。 • *source* 0.0.0.0 の *source* および *source-wildcard* の省略形としてのキーワード **host**。 （任意）*source-wildcard* 変数は、送信元にワイルドカード ビットを適用します（箇条書きの最初の項目を参照）。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP 標準 ACL の作成の詳細については、「物理インターフェイスへの ACL 適用のガイドライン」（P.28-6）を参照してください。

ACL 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 2 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。ACL 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 36.0.0.0 0.0.0.255
```

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	**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* {**permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [**operator** *port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*] [**dscp** *dscp-value*] [**time-range** *time-range-name*]	IP 拡張 ACL を作成し、必要な回数だけコマンドを繰り返します。 *access-list-number* には、ACL 番号を入力します。有効範囲は 100 ～ 199 および 2000 ～ 2699 です。 条件が満たされている場合にアクセスを許可するには、**permit** を入力します。 最大 100 文字の ACL エントリ コメントを指定するには、**remark** を入力します。 **（注）** QoS ACL には拒否ステートメントがサポートされません。詳細については、「QoS ACL に基づく分類」（P.29-5）を参照してください。 *protocol* には、IP プロトコルの名前または番号を入力します。疑問符（**?**）を使用すると、使用できるプロトコル キーワードのリストが表示されます。 *source* には、パケットの送信元となるネットワークまたはホストを指定します。*source-wildcard* では、無視するビット位置に 1 を入力することによって、ワイルドカード ビットを指定します。*source* および *source-wilcard* を指定するには、ドット付き 10 進表記を使用するか、*source* 0.0.0.0 *source-wildcard* 255.255.255.255 の短縮形として **any** キーワードを使用したり、*source* 0.0.0.0 を表す **host** キーワードを使用します。 *destination* には、パケットの宛先となるネットワークまたはホストを指定します。*destination および destination-wildcard* には、*source* および *source-wildcard* での説明と同じオプションを使用できます。 宛先または送信元のポートを定義します。 • *operator* には **eq**（等号）のみ使用できます。 • *operator* が *source source-wildcard* の後にある場合、送信元ポートが定義済みポートと一致したときに条件が満たされます。 • *operator* が *destination destination-wildcard* の後にある場合、宛先ポートが定義済みポートと一致したときに条件が満たされます。 • *port* は TCP ポートまたは UDP ポートの 10 進数または名前です。番号は、0 ～ 65535 です。 • TCP のポート名は TCP トラフィックにのみ使用します。 • UDP のポート名は UDP トラフィックにのみ使用します。 **dscp** と入力して、サポートされる 13 の DSCP 値のいずれか（0、8、10、16、18、24、26、32、34、40、46、48、および 56）とパケットを照合することを指定するか、または疑問符（**?**）を使用して、使用できる値のリストを表示します。 **time-range** キーワードはオプションです。このコマンドの詳細については、「ACL への時間範囲の適用」（P.28-14）を参照してください。

	コマンド	目的
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IP 拡張 ACL の作成の詳細については、「物理インターフェイスへの ACL 適用のガイドライン」（P.28-6）を参照してください。

ACL 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、TCP ポート番号 25 の宛先 IP アドレス 128.88.1.2 からの TCP トラフィックだけを許可する ACL を作成する例を示します。

```
Switch(config)# access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq
25
```

レイヤ 2 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** {**any** | **host** *source MAC address*} {**any** | **host** *destination MAC address*} [**aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**]	条件が満たされている場合にアクセスを許可するには、**permit** を入力します。 **（注）** QoS ACL には拒否ステートメントがサポートされません。詳細については、「QoS ACL に基づく分類」（P.29-5）を参照してください。 *source MAC address* 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。これを指定するには、**any** キーワードを使用してすべての送信元 MAC アドレスを拒否するか、**host** キーワードおよび 16 進数形式（H.H.H）の送信元を使用します。 *destination MAC address* 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。これを指定するには、**any** キーワードを使用してすべての宛先 MAC アドレスを拒否するか、**host** キーワードおよび 16 進数形式（H.H.H）の宛先を使用します。 （任意）次のオプションを入力することもできます。 **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**（IP 以外のプロトコル）。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	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。

MAC 拡張 ACL の作成の詳細については、「名前付き MAC 拡張 ACL の作成」（P.28-17）を参照してください。

ACL を削除するには、**no mac access-list extended** *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、permit（許可）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。こ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。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit host 0001.0000.0001 host 0002.0000.0001
```

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。照合ステートメントには ACL のみを含めることができます。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 マップによるトラフィックの分類、ポリシング、およびマーキング」（P.29-30）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* **permit** {*source source-wildcard* | **host** *source* | **any**} または **access-list** *access-list-number* {**permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port*] [**dscp** *dscp-value*] [**time-range** *time-range-name*] または **mac access-list extended** *name* **permit** {**any** | **host** *source MAC address*} {**any** | **host** *destination MAC address*} [**aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**]	IP トラフィック用の IP 標準または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「物理インターフェイスへの ACL 適用のガイドライン」（P.28-6）および「ACL によるトラフィックの分類」（P.29-25）を参照してください。 **mac access-list extended** *name* コマンドの詳細については、「名前付き MAC 拡張 ACL の作成」（P.28-17）を参照してください。 （注）　QoS ACL には拒否ステートメントがサポートされません。詳細については、「QoS ACL に基づく分類」（P.29-5）を参照してください。

	コマンド	目的
ステップ 3	**class-map** *class-map-name*	クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。 デフォルトでは、クラス マップは定義されていません。 *class-map-name* には、クラス マップ名を指定します。
ステップ 4	**match** {**access-group** *acl-index* | **access-group name** *acl-name* | **ip dscp** *dscp-list*}	トラフィックを分類するための一致条件を定義します。 デフォルトでは、一致条件がサポートされていません。 クラス マップごとにサポートされる一致条件は 1 つだけです。また、クラス マップごとにサポートされる ACL は 1 つだけです。 **access-group** *acl-index* or **access-group name** *acl-name* には、ステップ 3 で作成した ACL の番号または名前をしています。 **ip dscp** *dscp-list* には、着信パケットと照合する IP DSCP 値を 8 つまで入力します。各値はスペースで区切ります。サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 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** [*class-map-name*]	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。

既存のクラス マップを削除するには、**no class-map** *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* | **name** *acl-name* | **ip dscp**} 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、1 つの一致条件があり、*103* という名前の ACL です。

```
Switch(config)# access-list 103 permit any any tcp eq 80
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

ポリシー マップ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

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。アクションには、トラフィック クラス内の特定の DSCP 値の設定や、一致するトラフィック クラスごとのトラフィックの帯域幅制限の指定や（ポリサー）、トラフィックがアウト オブ プロファイルの場合に実行するアクション（マーキングまたはドロップ）が含まれる可能性があります。

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。
- インターフェイス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。

入力方向でインターフェイスごとに適用できるポリシー マップは 1 つだけです。

特権 EXEC モードを開始して、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	**access-list** *access-list-number* **permit** {*source source-wildcard* | **host** *source* | **any**} または **access-list** *access-list-number* {**permit** | **remark**} *protocol* {*source source-wildcard* | **host** *source* | **any**} [*operator port*] {*destination destination-wildcard* | **host** *destination* | **any**} [*operator port] [dscp dscp-value*] [**time-range** *time-range-name*] または **mac access-list extended** *name* **permit** {**any** | **host** *source MAC address*} {**any** | **host** *destination MAC address*} [**aarp** | **amber** | **appletalk** |**dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**]	IP トラフィック用の IP 標準または IP 拡張 ACL、または非 IP トラフィック用のレイヤ 2 MAC ACL を作成し、必要な回数だけコマンドを繰り返します。 詳細については、「ACL によるトラフィックの分類」（P.29-25）を参照してください。 **（注）** QoS ACL には拒否ステートメントがサポートされません。詳細については、「QoS ACL に基づく分類」（P.29-5）を参照してください。 **mac access-list extended** *name* コマンドの詳細については、「名前付き MAC 拡張 ACL の作成」（P.28-17）を参照してください。
ステップ 3	**policy-map** *policy-map-name*	ポリシー マップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。
ステップ 4	**class** *class-map-name* [**access-group name** *acl-index-or-name*]	トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップ クラス マップは定義されていません。 すでに **class-map** グローバル コンフィギュレーション コマンドを使用してトラフィック クラスが定義されている場合は、このコマンドで *class-map-name* にその名前を指定します。 **access-group name** *acl-index-or-name* には、ステップ 2 で作成した ACL の番号または名前を指定します。 **（注）** ポリシー マップでは、*class-default* という名前のクラスがサポートされます。スイッチは、**class class-default** ポリシー マップ コンフィギュレーション コマンドで定義されたポリシー マップに基づいてトラフィックをフィルタリングしません。

	コマンド	目的
ステップ 5	**set** {**ip dscp** *new-dscp*}	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。 **ip 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。サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。
ステップ 6	**police** *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value*}]	分類したトラフィックにポリサーを定義します。 入力ギガビット対応イーサネット ポートでは、最大 60 個のポリサーを設定できます。 *rate-bps* には、平均トラフィック レートをビット/秒（bps）で指定します。範囲は 10/100 イーサネット ポートの場合は 1 ～ 100 Mbps、入力ギガビット対応イーサネット ポートの場合は 8 ～ 1000 Mbps です。 *burst-byte* には、標準バースト サイズをバイト数で指定します。10/100 ポートでサポートされる値は 4096、8192、16384、32768、および 65536 です。ギガビット対応イーサネット ポートでサポートされる値は 4096、8192、16348、32768、65536、131072、262144 および 524288 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。DSCP 値をマーク ダウンし、パケットを送信するには、**exceed-action dscp** *dscp-value* キーワードを使用します。
ステップ 7	**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 8	**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 9	**interface** *interface-id*	ポリシー マップを適用するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは物理インターフェイスなどです。
ステップ 10	**service-policy input** *policy-map-name*	指定されたポリシー マップを特定のインターフェイスの入力に適用します。 方向ごとのインターフェイスごとに適用できるポリシー マップは 1 つだけです。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show policy-map** [*policy-map-name* class *class-name*]	設定を確認します。
ステップ 13	**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。割り当てられた DSCP 値を削除するには、**no set ip dscp** *new-dscp* 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* | dscp-value}] 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 マップとインターフェイスの関連付けを解除するには、**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。

同じインターフェイスでのポリシー マップとセキュリティ ACL の設定の詳細については、表 29-5（P.29-19）を参照してください。

次に、ポリシー マップを作成し、入力インターフェイスに付加する例を示します。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（5000000 bps）および標準バースト サイズ（8192 バイト）を超えた場合、DSCP が値 10 に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)# police 5000000 8192 exceed-action dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
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、入力インターフェイスに付加する例を示します。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。

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit host 0001.0000.0001 host 0002.0000.0001
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit host 0001.0000.0003 host 0002.0000.0003
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group name maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set ip dscp 56
Switch(config-pmap-c)# exit
Switch(config-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set ip dscp 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

CoS マップの設定

（注）　この機能は、スイッチが EI を実行している場合のみ使用可能です。

ここでは、CoS マップを設定する例を示します。

- 「CoS/DSCP マップの設定」（P.29-34）
- 「DSCP/CoS マップの設定」（P.29-35）

マップはすべてグローバルに定義されています。

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 29-7 に、デフォルトの CoS/DSCP マップを示します。

表 29-7　デフォルトの CoS/DSCP マップ

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

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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map cos-dscp** *dscp1...dscp8*	CoS/DSCP マップを変更します。 *dscp1...dscp8* には、CoS 値 0 ～ 7 に対応する 8 つの DSCP 値を入力します。各 DSCP 値はスペースで区切ります。 サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show mls qos maps cos-dscp**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）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 cos-dscp** グローバル コンフィギュレーション コマンドを使用します。

次に、CoS/DSCP マップを変更して表示する例を示します。

```
Switch# configure terminal
Switch(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
Switch(config)# end
Switch# show mls qos maps cos-dscp

Cos-dscp map:
        cos:  0  1  2  3  4  5  6  7
     --------------------------------
       dscp:  8  8  8  8 24 32 56 56
```

DSCP/CoS マップの設定

DSCP/CoS マップを使用し着信パケットの DSCP 値を CoS 値にマッピングします。これは 4 つの出力キューのいずれかを選択するために使用されます。

スイッチでサポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。

表 29-8 に、デフォルトの DSCP/CoS マップを示します。

表 29-8　デフォルトの DSCP/CoS マップ

DSCP 値	CoS 値
0	0
8、10	1
16、18	2
24、26	3
32、34	4
40、46	5
48	6
56	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。

DSCP/CoS 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。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mls qos map dscp-cos** *dscp-list* **to** *cos*	DSCP/CoS マップを変更します。 *dscp-list* には、最大 13 個の DSCP 値をスペースで区切って入力します。さらに、**to** キーワードを入力します。 *cos* には、DSCP 値と対応する CoS 値を入力します。 サポートされる DSCP 値は、0、8、10、16、18、24、26、32、34、40、46、48、および 56 です。CoS 値に指定できる範囲は 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 dscp-cos**	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 map 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 26 および 48 を CoS 値 7 にマッピングする例を示します。残りの DSCP 値については、DSCP/CoS マッピングがデフォルトです。

```
Switch(config)# mls qos map dscp-cos 26 48 to 7
Switch(config)# exit

Switch# show mls qos maps dscp-cos

Dscp-cos map:
```

```
dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
-------------------------------------------
cos:   0  1  1  2  2  3  7  4  4  5  5  7  7
```

出力キューの設定

（注）　この機能は SI と EI の両方でサポートされます。

ここでは、出力キューを設定する方法を説明します。

- 「CoS プライオリティ キューの設定」（P.29-36）
- 「WRR のプライオリティの設定」（P.29-37）
- 「緊急キューのイネーブル化と WRR プライオリティの設定」（P.29-37）

出力キューの詳細については、「出力 CoS キュー」（P.29-8）を参照してください。

CoS プライオリティ キューの設定

CoS 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。

	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	**wrr-queue cos-map** *qid cos1...cosn*	CoS プライオリティ キューのキュー ID を指定します（範囲は 1 ～ 4 で、1 は最も低い CoS プライオリティ キュー）。 このキュー ID にマッピングされる CoS 値を指定します。 デフォルト値は次のとおりです。 CoS 値CoS プライオリティ キュー 0、11 2、32 4、53 6、74
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	**show wrr-queue cos-map**	CoS プライオリティ キューのマッピングを表示します。

新しい CoS 設定をディセーブルにして、デフォルト設定に戻すには、**no wrr-queue 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。

WRR のプライオリティの設定

WRR のプライオリティを設定するには、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	**wrr-queue bandwidth** *weight1...weight4*	WRR の重みを 4 つの CoS キューに割り当てます。 次に、WRR の値の範囲を示します。 • *weight1*、*weight2*、および *weight3* の範囲は 1 ～ 255 です。 • *weight4* の範囲は 0 ～ 255 です。weight4 が 0 に設定された場合は、キュー 4 が緊急キューとして設定されます。 （注）　Cisco IOS Release 12.1(12c)EA1 よりも前のソフトウェア リリースでは、すべてのキューの範囲が 1 ～ 255 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 wrr-queue bandwidth	CoS プライオリティ キューの WRR 帯域幅の割り当てを表示します。

WRR スケジューリングをディセーブルにして、絶対優先スケジューリングをイネーブルにするには、**no wrr-queue 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。

キューのいずれかを緊急キューとしてイネーブルにし、残りのキューの WRR スケジューリングをイネーブルにする方法については、「緊急キューのイネーブル化と WRR プライオリティの設定」（P.29-37）を参照してください。

緊急キューのイネーブル化と WRR プライオリティの設定

Cisco IOS Release 12.1(12c)EA1 以降で、緊急キュー（キュー 4）をイネーブルにして残りのキューに WRR プライオリティを割り当てるには、特権 EXEC モードで次の手順を実行します。

	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	**wrr-queue bandwidth** *weight1 weight2 weight3* **0**	キュー 4 を緊急キューとして設定し、WRR の重みを残りの出力キューに割り当てます。 *weight1*、*weight2*、および *weight3* の WRR の重みの範囲は 1 ～ 255 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 wrr-queue bandwidth	CoS プライオリティ キューの WRR 帯域幅の割り当てを表示します。

標準 QoS 情報の表示

標準 QoS 情報を表示するには、表 29-9 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 29-9　QoS 情報を表示するためのコマンド

コマンド	目的
show class-map [*class-map-name*]	トラフィックを分類するための一致条件を定義した QoS クラス マップを表示します。
show policy-map [*policy-map-name* [**class** *class-name*]]	着信トラフィックの分類条件を定義した QoS ポリシー マップを表示します。
show mls qos maps [**cos-dscp** | **dscp-cos**]	QoS マッピング情報を表示します。マップは、トラフィックのプライオリティを表す内部 DSCP 値を生成するために使用します。
show mls qos interface [*interface-id*] [**policers**]	インターフェイス レベルで QoS 情報を表示します。これには、出力キューおよび CoS-to-egress-queue マップの設定が含まれ、このインターフェイスでポリサー、入力統計情報が設定されています。
show mls masks [**qos** | **security**]	QoS およびセキュリティ ACL に使用される[1]マスクに関する情報を表示します。
show wrr-queue cos-map	CoS プライオリティ キューのマッピングを表示します。
show wrr-queue bandwidth	CoS プライオリティ キューの WRR 帯域幅の割り当てを表示します。

1. EI を実行しているスイッチだけで使用できます。
2. アクセス コントロール パラメータは、スイッチの CLI コマンドおよび出力でマスクと呼ばれます。

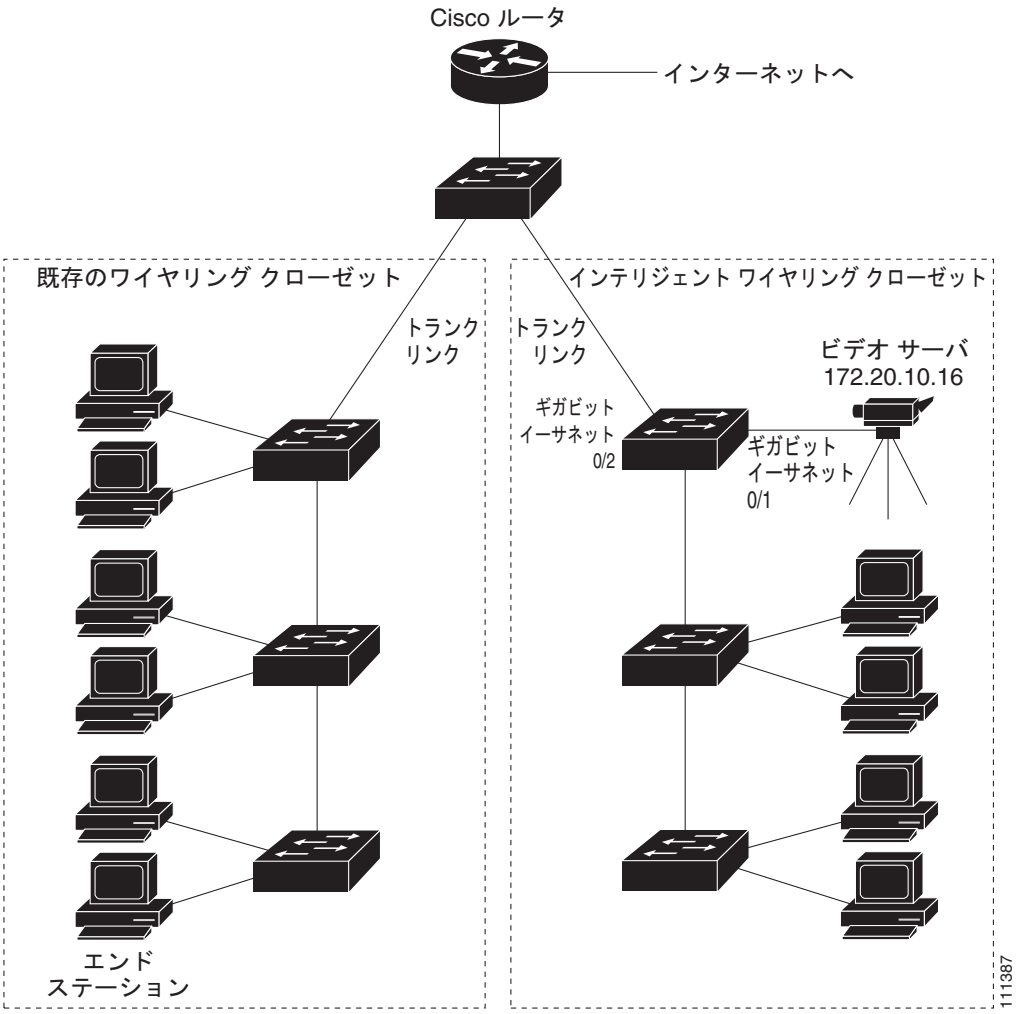
標準 QoS の設定例

（注）　次の例は、スイッチが EI を実行している場合だけ適用されます。

ここでは、図 29-5 に示すように、既存のネットワークとネットワークへの計画済み変更内容に基づき、QoS 機能の導入を簡単に行うために役立つ QoS 移行パスについて説明します。具体的な内容は次のとおりです。

- 「既存のワイヤリング クローゼット用の QoS 設定」（P.29-39）
- 「インテリジェントなワイヤリング クローゼット用の QoS 設定」（P.29-40）

図 29-5　ネットワークでの QoS の設定例



既存のワイヤリング クローゼット用の QoS 設定

図 29-5 に、Catalyst 2900 XL スイッチおよび 3500 XL スイッチでの既存のワイヤリング クローゼットの例を示します。これらのスイッチは Cisco IOS Release 12.0(5)XP 以降を実行し、QoS ベースの IEEE 802.1p CoS 値がサポートされます。QoS は、プライオリティが指定された CoS 値をフレームに割り当てることによって分類し、高いプライオリティのトラフィックを優先します。

Catalyst 2900 スイッチおよび 3500 XL スイッチでは、各ポートにデフォルト CoS プライオリティ（**switchport priority default** *default-priority-id* インターフェイス コンフィギュレーション コマンド）を設定して、入力ポートでタグなし（ネイティブ）イーサネット フレームを分類できます。タグ情報付きの IEEE 802.1Q フレームの場合、ヘッダー フレームのプライオリティ値が使用されます。Catalyst 3524-PWR XL スイッチおよび 3548 XL スイッチでは、**switchport priority default override** インターフェイス コンフィギュレーション コマンドを使用して、このプライオリティのデフォルト値を上書きできます。上書き機能のない Catalyst 2950 スイッチと Catalyst 2900 XL スイッチおよびその他の 3500 XL モデルの場合、配信層の Catalyst 3550-12T スイッチが **mls qos cos override** インターフェイス コンフィギュレーション コマンドを使用して、IEEE 802.1p CoS 値を上書きできます。

Catalyst 2900 スイッチおよび 3500 XL スイッチの場合、CoS では、フレーム タグまたはポートの情報に基づいて、標準プライオリティの送信キューおよび高いプライオリティの送信キューとともに各送信ポート（出力ポート）を設定します。標準プライオリティのキュー内のフレームは、高いプライオリティのキュー内のフレームが転送された後に転送されます。IEEE 802.1p CoS 値が 0 ～ 3 のフレームは標準プライオリティの送信キューに配置され、CoS 値が 4 ～ 7 のフレームは緊急（高いプライオリティの）キューに配置されます。

インテリジェントなワイヤリング クローゼット用の QoS 設定

図 29-5 に、Catalyst 2950 スイッチでのインテリジェントなワイヤリング クローゼットの例を示します。スイッチの 1 つが、IP アドレスが 172.20.10.16 のビデオ サーバに接続されます。

この例では、ビデオ トラフィックを他のすべてのトラフィックよりも優先させることを目的としています。これを行うには、DSCP 46 をビデオ トラフィックに割り当てます。このトラフィックはキュー 4 に保存されます。キュー 4 には他のキューよりも頻繁にサービスが提供されます。

他のすべてのトラフィックを介したビデオ パケットを優先するようにスイッチを設定するには、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	**access-list 1 permit 172.20.10.16**	IP 標準 ACL を定義し、172.20.10.16 のビデオ サーバからのトラフィックを許可します。
ステップ 3	**class-map videoclass**	*videoclass* という名前のクラス 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。
ステップ 4	**match access-group 1**	ACL 1 で指定されたトラフィックと照合する一致条件を定義します。
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map videopolicy**	*videopolicy* という名前のポリシー 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。
ステップ 7	**class videoclass**	動作させるクラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**set ip dscp 46**	ACL 1 と一致するトラフィックに対して、着信パケットの DSCP を 46 に設定します。
ステップ 9	**police 5000000 8192 exceed-action drop**	分類されたビデオ トラフィックのポリサーを定義し、5 Mbps の平均トラフィック レートおよび 8192 バイトのバースト サイズを超えるトラフィックをドロップします。
ステップ 10	**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 11	**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 12	**interface** *interface-id*	ビデオ サーバに接続するスイッチの入力インターフェイスを指定し、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 13	**service-policy input videopolicy**	ポリシーを入力インターフェイスに適用します。
ステップ 14	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**wrr-queue bandwidth 1 2 3 4**	より高い WRR の重みをキュー 4 に割り当てます。
ステップ 16	**wrr-queue cos-map 4 6 7**	CoS 値 6 および 7 でキュー 4 が選択されるように CoS-to-egress-queue を設定します。

	コマンド	目的
ステップ 17	**end**	特権 EXEC モードに戻ります。
ステップ 18	**show class-map videoclass** **show policy-map videopolicy** **show mls qos maps** [**cos-dscp** | **dscp-cos**]	設定を確認します。
ステップ 19	**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。