Catalyst 6000ファミリスイッチのQoSについて

内容

概要

この文書では、Catalyst 6000 ファミリ スイッチで使用できる Quality of Service（QoS）機能について説明します。この文書では、QoS の設定機能について説明するほか、QoS の実装方法についていくつかの例を紹介しています。

この文書は設定ガイドではありません。Catalyst 6000 ファミリのハードウェアおよびソフトウェアの QoS 機能の説明を容易にするために、このドキュメント全体で設定例が使用されています。QoS コマンド構造の構文については、以下の Catalyst 6000 ファミリ用の設定およびコマンド ガイドを参照してください。

- Catalyst 6500 ファミリ スイッチ

レイヤ 2 QoS の定義

レイヤ 2（L2）スイッチでの QoS は、単にイーサネット フレームの優先順位付けであると考えられがちで、実際にはもっと豊富な機能を提供していることは、あまり理解されていません。L2 QoS には以下が含まれます。

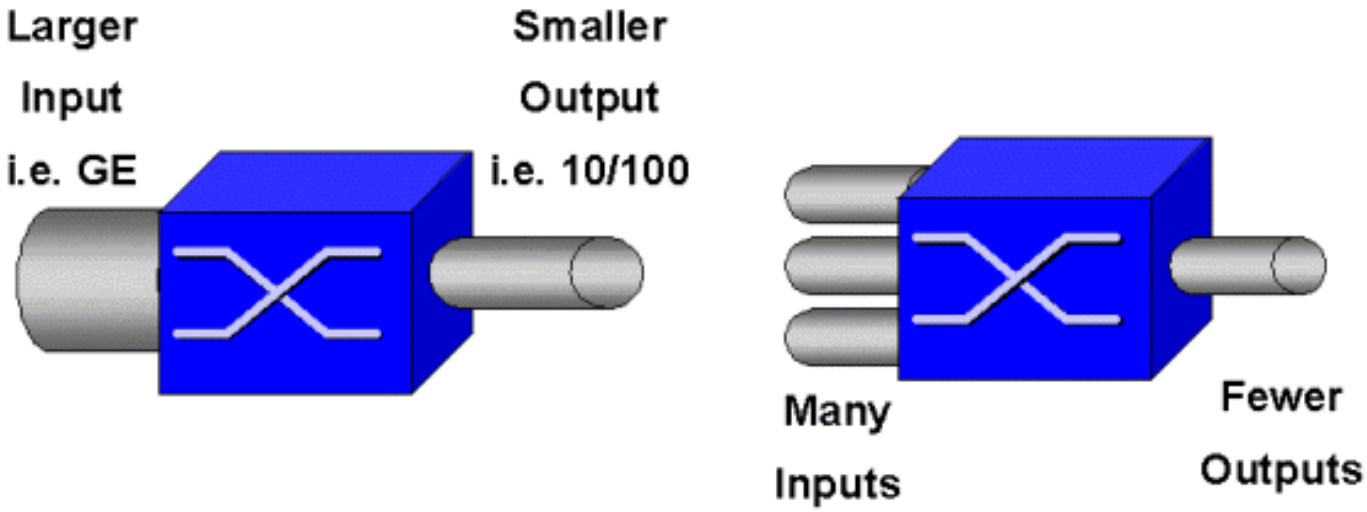
1. **入力キューのスケジューリング**：フレームがポートに着信すると、出力ポートへのスイッチングのスケジューリングに先立ち、ポートベースの複数のキューのいずれかへの割り当てが可能です。トラフィックによって異なるサービス レベルが必要な場合や、スイッチによる遅延を最小に抑える必要がある場合は、通常は複数のキューが使用されます。たとえば、IP ベースのビデオおよび音声データは低遅延であることが求められるため、ファイル転送プロトコル（FTP）、Web、電子メール、Telnet などその他のデータを切り替える前に、このデータを切り替える必要がある場合があります。

2. **分類**：分類のプロセスでは、イーサネットL2ヘッダーのさまざまなフィールド、およびIPヘッダー(レイヤ3(L3))とTransmission Control Protocol/User Datagram Protocol(TCP/UDP)ヘッダー(レイヤ4(L4))のフィールドを検査して、スイッチを通過するフレームに適用する
3. **ポリシング**：ポリシングとは、イーサネット フレームを検査して、一定のタイムフレーム内でトラフィックが事前に定義されているレートを超過していないかどうかを確認するプロセスです（通常、スイッチでは、このタイムフレームは固定値として設定されています）。 そのフレームがプロファイル外である（つまり、事前定義されたレートの制限を超過したデータ ストリームの一部である）場合、廃棄されるか、またはサービス クラス（CoS）値がマークダウンされます。
4. **リライト**：リライト処理とは、イーサネット ヘッダー内の CoS や、IPV4 ヘッダー内の Type of Service（ToS）ビットを変更するというスイッチの機能です。
5. **出力キューのスケジューリング**：リライト処理の後、イーサネット フレームはスイッチングのために適切な発信（出力）キューに置かれます。スイッチは、このキュー上でバッファがオーバーフローしないようにバッファ管理を行います。これは通常、ランダムなフレームがキューから削除（廃棄）されるランダム初期廃棄（RED）アルゴリズムを利用して実行されます。Weighted RED（WRED; 重み付けランダム早期検出）は、REDから派生したもので、廃棄するフレームを決定するために CoS 値を検査します。これは、Catalyst 6000 ファミリの一部のモジュールで使用されています。バッファが事前に定義されているしきい値に達すると、通常は優先順位の低いフレームが廃棄され、優先順位の高いフレームはキューに残されます。

この文書では、これに続くセクションで、上記の各メカニズムの詳細と、Catalyst 6000 ファミリとの関係について説明します。

スイッチにおける QoS の必要性

今日、膨大なバックプレーン、毎秒数百万のパケットのスイッチング、ノンブロッキング スイッチはすべて、大容量のスイッチングと同義です。QoS が必要とされる理由は何でしょうか。その答えは、輻輳にあります。



スイッチは世界最速のスイッチとなる可能性がありますが、上記の図に示されている 2 つのシナリオのいずれかが生じると、そのスイッチで輻輳が発生します。輻輳時に、輻輳管理機能が設けられていなければ、パケットは廃棄されます。パケットが廃棄されると、再送信が行われます。再送信が行われると、ネットワークの負荷が増大します。すでに輻輳しているネットワークでは、このような負荷が既存のパフォーマンスの問題に加わり、さらにパフォーマンスを低下させる恐れがあります。

集約型ネットワークの場合には、輻輳管理はさらに重要になります。音声やビデオなど遅延の影響を受けやすいトラフィックでは、遅延が発生すると、重大な影響を受ける可能性があります。単にスイッチのバッファを大きくするだけでは、輻輳問題の解決には不十分です。遅延の影響を受けやすいトラフィックは、できるだけ早く切り替える必要があります。まず、分類技術を活用してこの重要なトラフィックを特定し、その後にバッファ管理技術を実装して、輻輳時に優先度の高いトラフィックが廃棄されないようにする必要があります。最後に、スケジューリング技術を組み込んで、できるだけすばやくキューから重要なパケットを切り替える必要があります。このドキュメントを読み進めるとご理解いただけると思いますが、Catalyst 6000 ファミリではこれらの技術すべてが実装されており、この QoS サブシステムは業界で最も包括的なシステムの 1 つとなっています。

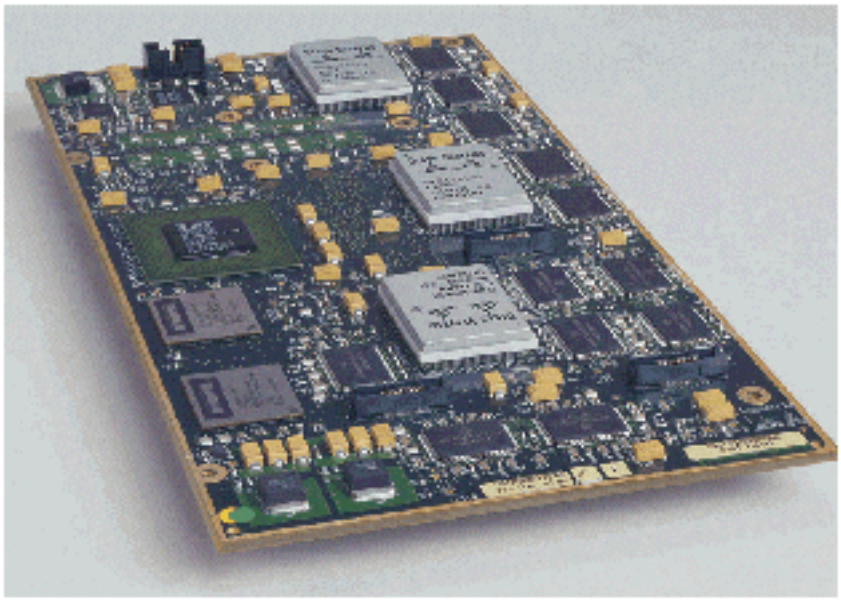
前のセクションで説明した QoS 技術のすべてを、このドキュメント全体で詳しく説明します。

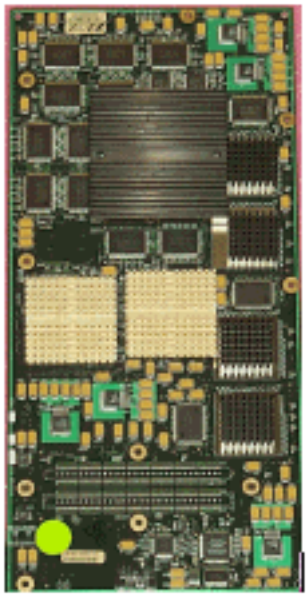
Catalyst 6000 ファミリにおける QoS のハードウェア サポート

Catalyst 6000 ファミリで QoS をサポートするには、ハードウェアによるサポートが必要です。QoS をサポートするハードウェアには、Multilayer Switch Feature Card (MSFC)、Policy Feature Card (PFC)、およびこのラインカード上のポート Application Specific Integrated Circuit (ASIC; 特定用途集積回路) などがあります。この文書では、MSFC の QoS 機能については説明していませんが、PFC とラインカード上の ASIC の QoS 機能に絞って説明を行います。

PFC

PFC バージョン 1 は、Catalyst 6000 ファミリのスーパーバイザ I (SupI) およびスーパーバイザ IA (SupIA) に装着されるドーター カードです。PFC2 は、PFC1 を再設計したもので、新型のスーパーバイザ II (SupII) と、新しいオンボード ASIC と一緒に出荷されています。PFC1 と PFC2 は、主に L3 スイッチングでのハードウェア アクセラレーションとしての機能が知られていますが、QoS もその目的とする機能の 1 つです。PFC を次に示します。





PFC1 と PFC2 は基本的には同じものですが、QoS 機能に関してはいくつかの相違点があります。つまり、PFC2 は以下を追加します。

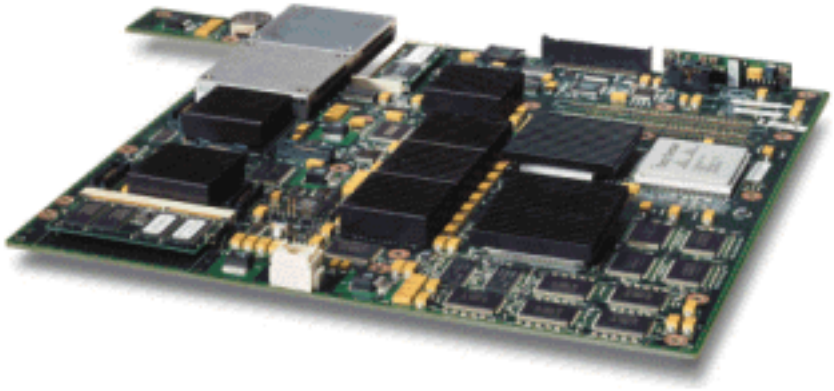
1. QoS ポリシーを Distributed Forwarding Card（DFC）に送出する機能。
2. ポリシング判定が、わずかに異なっています。PFC1 と PFC2 の両方は、集約ポリシーまたはマイクロフロー ポリシーがプロファイル外の決定を返す場合に、フレームが廃棄またはマークダウンされるという通常のポリシングをサポートしています。ただし、PFC2 では、レートの超過に対する処理もサポートされており、ポリシーのアクションが実行される 2 番目のポリシング レベルを指定できます。

超過レート ポリサーを定義すると、パケットが超過レートを超えた場合に、そのパケットは廃棄またはマークダウンされます。超過ポリシング レベルを設定すると、超過 DSCP マッピングを使用して、元の DSCP 値がマークダウンされる値に置き換えられます。標準ポリシング レベルだけを設定すると、標準 DSCP マッピングが使用されます。両方のポリシー レベルが設定されていると、マッピング ルールの選択には超過ポリシング レベルが優先されます。

すでに言及された ASIC によって実行される、このドキュメントで説明されている QoS 機能は、高いレベルのパフォーマンスを生み出すことに注目してください。基本的な Catalyst 6000 ファミリでの QoS のパフォーマンス（スイッチ ファブリック モジュールなし）は、15 MPPS になります。DFC が使用される場合、QoS のさらに高いパフォーマンスが実現されます。

DFC

DFC は、WS-X6516-GBIC にオプションとして装着できます。ただし、WS-X6816-GBIC カードでは標準装備されています。また、最近導入されたファブリック 10/100（WS-X6548-RJ45）ラインカード、ファブリック RJ21 ラインカード（WS-X6548-RJ21）、100FX ラインカード（WS-X6524-MM-FX）など、今後のファブリック ラインカードでもサポートされます。 DFC を次に示します。



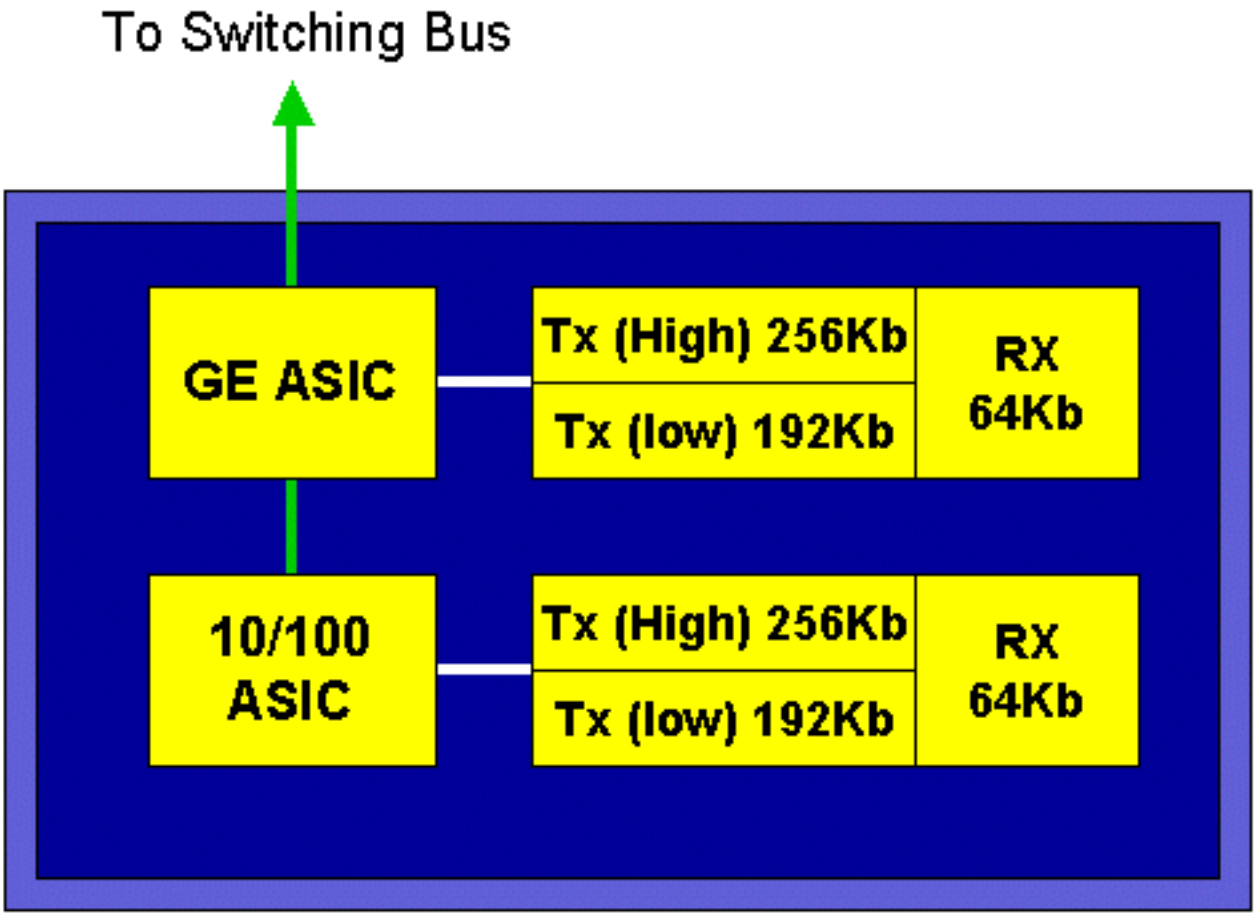
DFC を装着すると、そのファブリック（クロスバー接続）ラインカードでローカル スイッチングが行えるようになります。これを実行するには、スイッチについて定義したすべての QoS ポリシーをサポートする必要があります。管理者は、DFC を直接設定することはできません。これは、アクティブ スーパーバイザのマスター MSFC/PFC で制御されます。プライマリ PFC から Forwarding Information Base（FIB）テーブルがプッシュされ、これにより DFC に L2 および L3 フォワーディング テーブルが付与されます。また、QoS ポリシーのコピーもプッシュされ、それらのコピーはラインカード固有のものとなります。これより後は、ローカル スイッチングの判断は QoS ポリシーのローカル コピーを参照して行われます。その結果、ハードウェアの QoS 処理速度が向上し、分散型スイッチングによる高いレベルのパフォーマンスが提供されます。

ポートベースのASIC

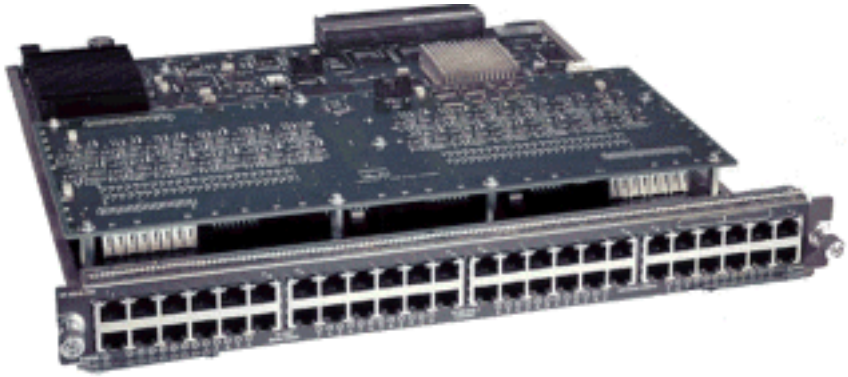
ハードウェアの機能を補完するために、各ラインカードには多数の ASIC が実装されています。これらの ASIC には、フレームがそのスイッチを通過する際の一時的な保存領域として使用されるキュー、バッファリング、しきい値が実装されています。10/100 カードでは、ASIC の組み合わせにより、10/100 ポートが 48 ポート提供されています。

基本的な 10/100 ラインカード（WS-X6348-RJ45）

10/100 の ASIC では、それぞれの 10/100 ポートごとに、一連の受信（Rx）キューと送信（Tx）キューが用意されています。またこの ASIC では、10/100 の 1 ポートあたり 128 K のバッファリングが備わっています。各ラインカードで使用できるポート バッファリングごとの操作の詳細については、リリース ノートを参照してください。このラインカード上の各ポートは、1 つの Rx キューと高低が示された 2 の Tx キューをサポートします。これを次の図で示します。



上記の図では、各 10/100 ASIC は 12 個の 10/100 ポートに対して 1 つのブレークアウトを提供します。各 10/100 ポートでは、128 K のバッファが提供されます。このバッファの 128 K は、3 つのキューに分割されています。上の図で示しているキューはデフォルトの設定ではありませんが、設定される代表的な例を表しています。1 つの Rx キューが 16 K を使用し、残りの 112 K のメモリは 2 つの Tx キューで分割されています。デフォルト（CatOS）では、高キューはこのスペースの 20 パーセントを取得し、低キューは 80 パーセントを取得します。Catalyst IOS では、デフォルトで高キューは 10 パーセント、低キューは 90 パーセントを取得します。

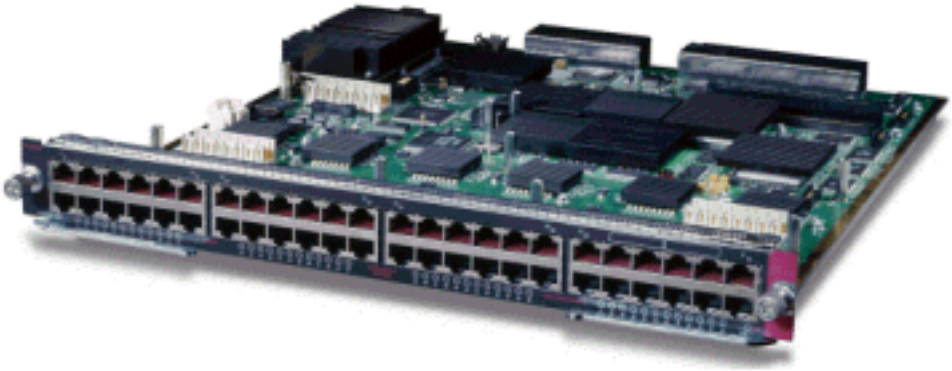


このカードでは、2 段階のバッファリングを行いますが、QoS 設定の際に操作できるのは 10/100 ASIC ベースのバッファリングだけです。

ファブリック 10/100 ラインカード（WS-X6548-RJ45）

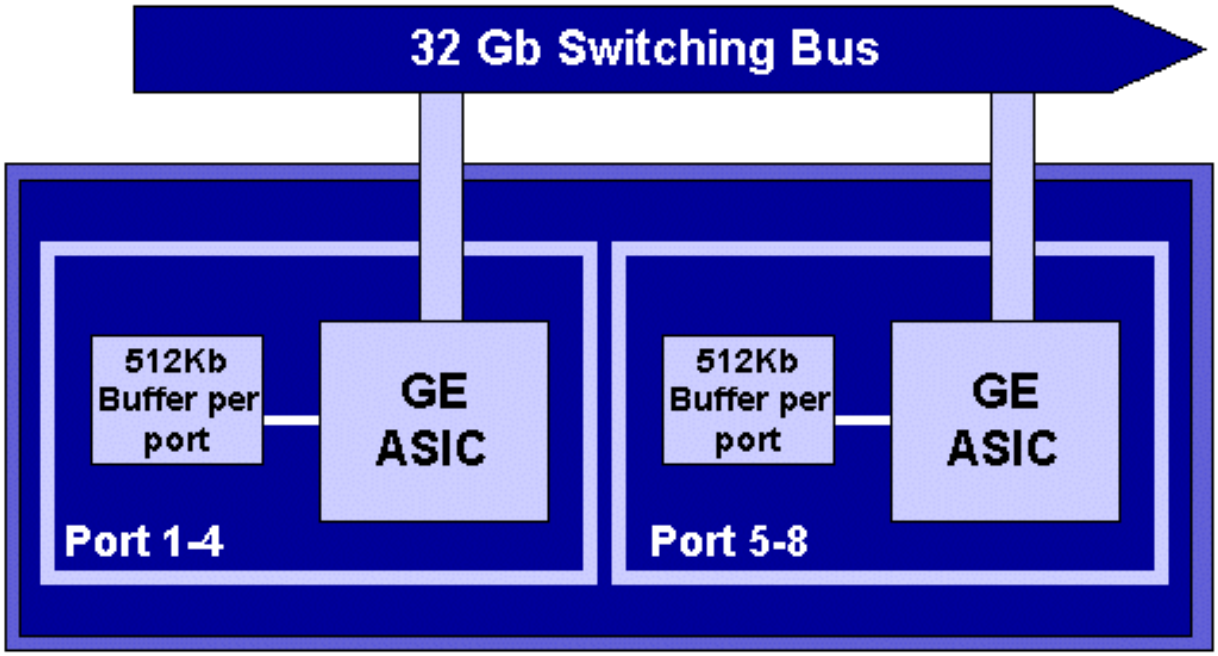
新型の 10/100 の ASIC では、それぞれの 10/100 ポートごとに、一連の Rx キューと Tx キューが用意されています。この ASIC では、10/100 ポート全体で使用できるメモリの共有プールが提供されています。各ラインカードで使用できるポート バッファリングごとの操作の詳細については、リリース ノートを参照してください。このラインカード上の各ポートは、2 つの Rx キューと

3 の Tx キューをサポートします。1 つの Rx キューと 1 つの Tx キューは、絶対的に優先されるキューとされています。これらは、低遅延キューとして動作し、Voice over IP (VoIP) トラフィックなどの遅延の影響を受けやすいトラフィックに最適です。

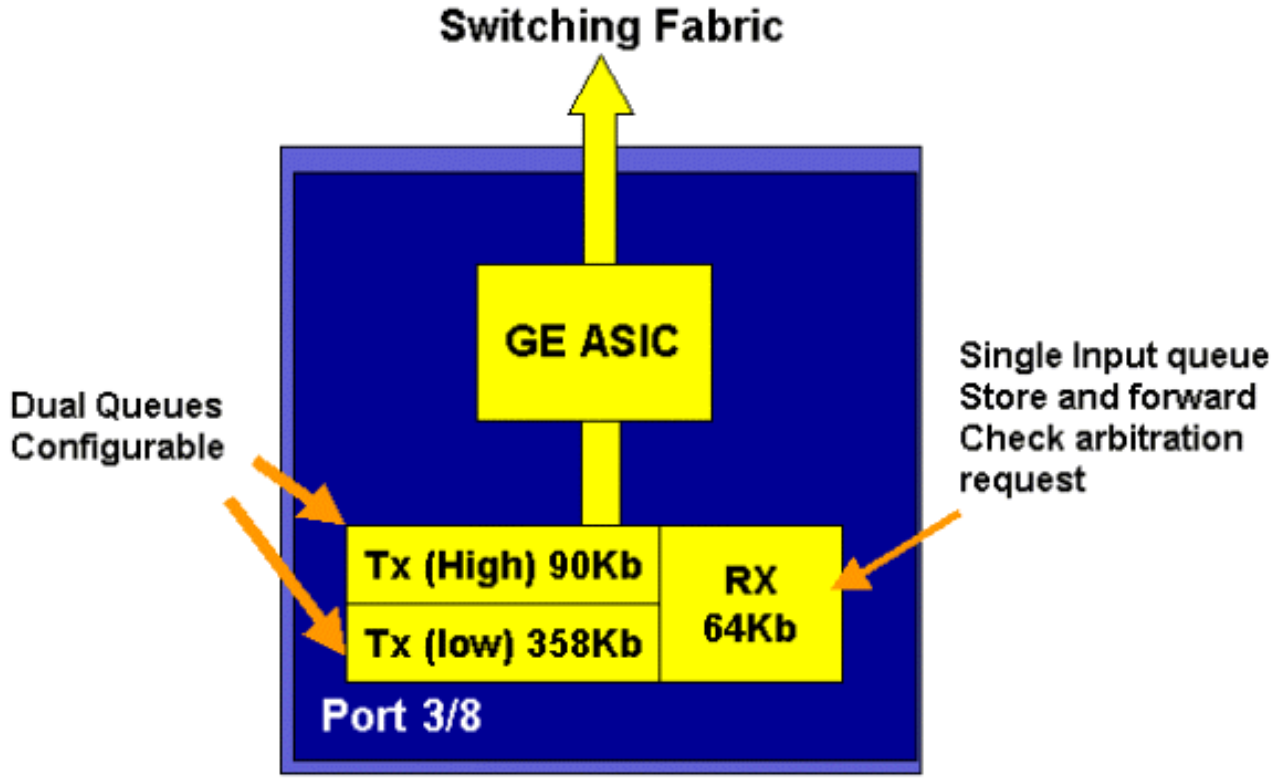


GE ラインカード (WS-X6408A、WS-X6516、WS-X6816)

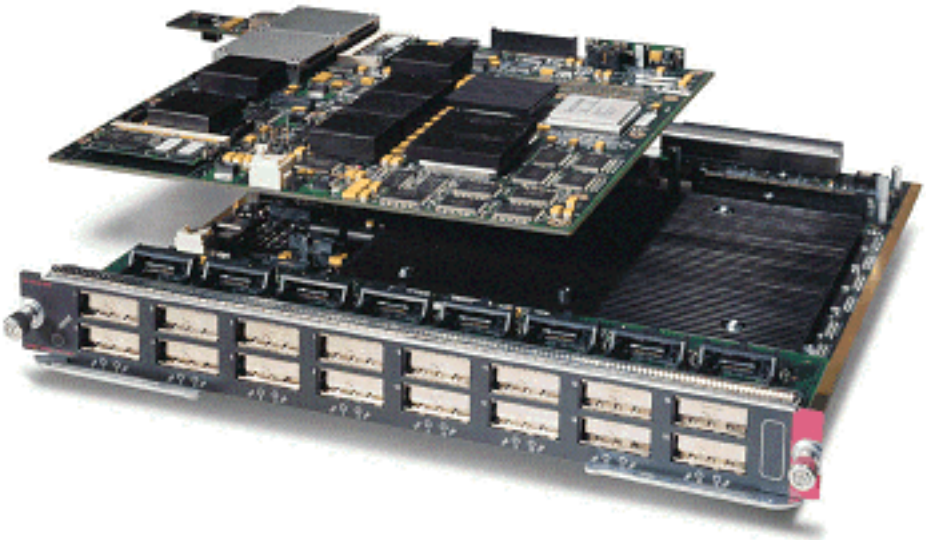
GE ラインカードでは、ASIC はポート バッファリングごとに 512 K を提供します。次の図に 8 個のポートを持つ GE ラインカードを示します。



10/100 ポートと同様に、各 GE ポートに 3 つのキュー (1 つの Rx キューと 2 つの Tx キュー) があります。これは WS-X6408-GBIC ラインカードのデフォルトであり、次の図で説明します。



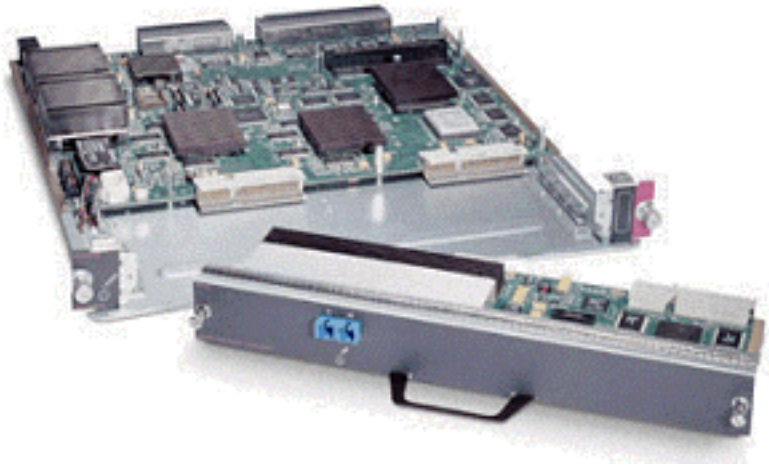
さらに新しい 16 ポートの GE カード、スーパーバイザ IA とスーパーバイザ II の GBIC ポート、および WS-X6408A-GBIC 8 ポート GE カードでは、Strict Priority (SP; 完全優先) キューが 2 つ追加装備されています。SP キューの 1 つが Rx キューに割り当てられ、もう 1 つの SP キューが Tx キューに割り当てられます。この SP キューは、主として音声などの遅延の影響を受けやすいトラフィックのキューイングに使用されます。SP キューを使用すると、このキューに置かれたあらゆるデータは、高優先キューと低優先キューにあるデータよりも先に処理されます。高優先キューと低優先キューの内容が処理されるのは、SP キューが空の場合だけです。



10 GE ラインカード (WS-X6502-10GE)

2001 年の後半に、シスコはラインカードあたり 10 GE の 1 つのポートを備えた一連の 10 GE ラインカードを導入しました。このモジュールは、6000 シャーシの 1 つのスロットを使用します。この 10 GE ラインカードでは、QoS がサポートされています。10 GE ポートでは、2 つの Rx キューと 3 の Tx キューを提供します。1 つの Rx キューと 1 つの Tx キューは、それぞれ SP キ

ユー専用です。ポートに対してバッファリングも提供され、合計で 256 K の Rx バッファリングと 64 MB の Tx バッファリングが提供されます。このポートには、Rx 側に 1p1q8t のキュー構造、Tx 側に 1p2q1t のキュー構造が実装されています。キュー構造については、この文書の後の方で説明します。



Catalyst 6000 ファミリーQoS ハードウェアの概要

次の表に、Catalyst 6000 ファミリで前述の QoS 機能を実行するハードウェア コンポーネントの詳細が記載されています。

QoS Process	Catalyst 6500 Component that performs function
Input Scheduling	Performed by port ASIC's L2 only with or without the PFC
Classification	Performed by Supervisor or PFC L2 only is done by Supervisor L2/3 is done by PFC
Policing	Done by PFC via L3 forwarding Engine
Packet Re-write	Done by port ASIC's L2/L3 based on classification done in point 2 above
Output Scheduling	Done by port ASIC's L2/L3 based on classification done in point 2 above

Catalyst 6000 ファミリ ソフトウェアの QoS サポート

Catalyst 6000 ファミリでは、2 つのオペレーティング システムがサポートされています。元来のソフトウェア プラットフォームである CatOS は、Catalyst 5000 プラットフォームで使用されていたコード ベースに由来するものです。最近、シスコでは、シスコ ルータの IOS から派生したコード ベースを使用する統合 Cisco IOS ® (ネイティブ モード) を導入しました。両方のOSプラットフォーム(CatOSおよび統合Cisco IOS (ネイティブモード))では、前のセクションで説明したハードウェアを使用して、Catalyst 6000スイッチファミリプラットフォームでQoSを有効にするソフトウェアサポートが実装されています。

注：この文書では、両方の OS プラットフォームの設定例を使用しています。

IP およびイーサネットの優先メカニズム

データに適用されるすべての QoS サービスには、IP パケットまたはイーサネット フレームにタグを付けるか、優先順位を付ける手段が必要です。ToS および CoS のフィールドは、このために使用されます。

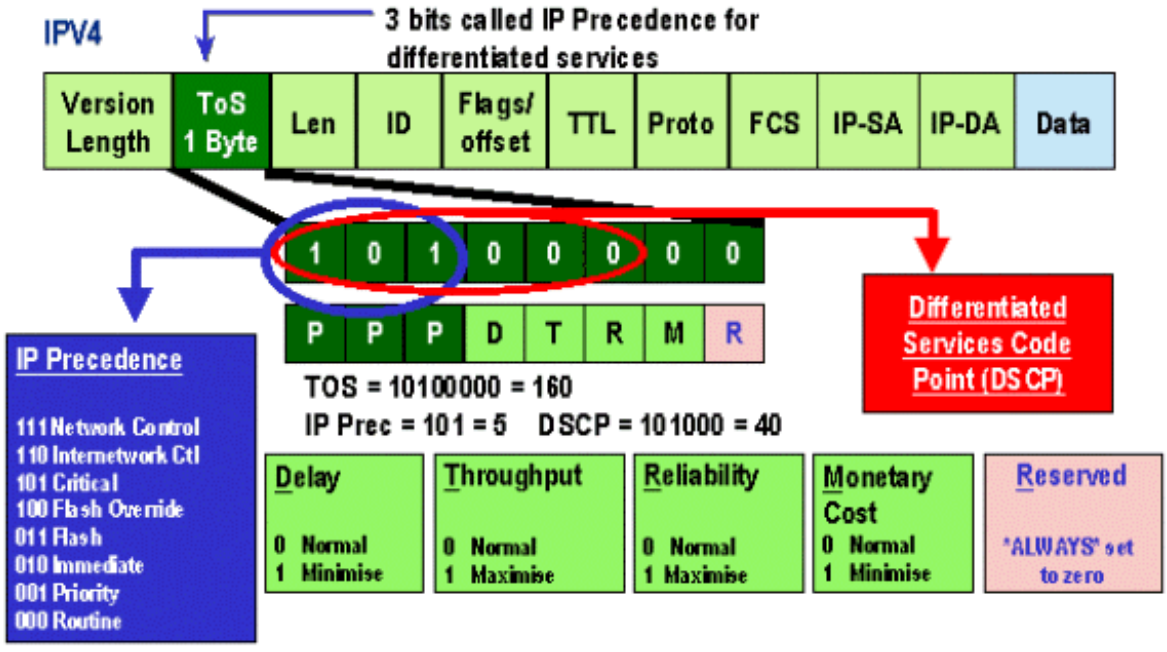
ToS

ToS は IPV4 ヘッダーにある 1 バイトのフィールドです。ToS フィールドは 8 ビットで構成されており、そのうちの最初の 3 ビットが IP パケットの優先順位を示すために使用されます。この 3 ビットは、IP 優先順位ビットと呼ばれます。これらのビットで 0 から 7 までの値を設定でき、0 が最低の優先度、7 が最高の優先度を表します。IP 優先順位を設定する機能は、IOS で長年に渡ってサポートされてきました。IP 優先順位を再設定する機能は、MSFC または PFC (MSFC とは無関係) によりサポートされています。信頼できない信頼設定によって、着信フレームの IP 優先順位設定が消去される可能性があります。

IP 優先順位に設定できる値は、次のとおりです。

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

次の図では、ToS ヘッダー内の IP 優先順位ビットの例を表しています。MSB (先頭) の 3 ビットが、IP 優先順位として解釈されます。



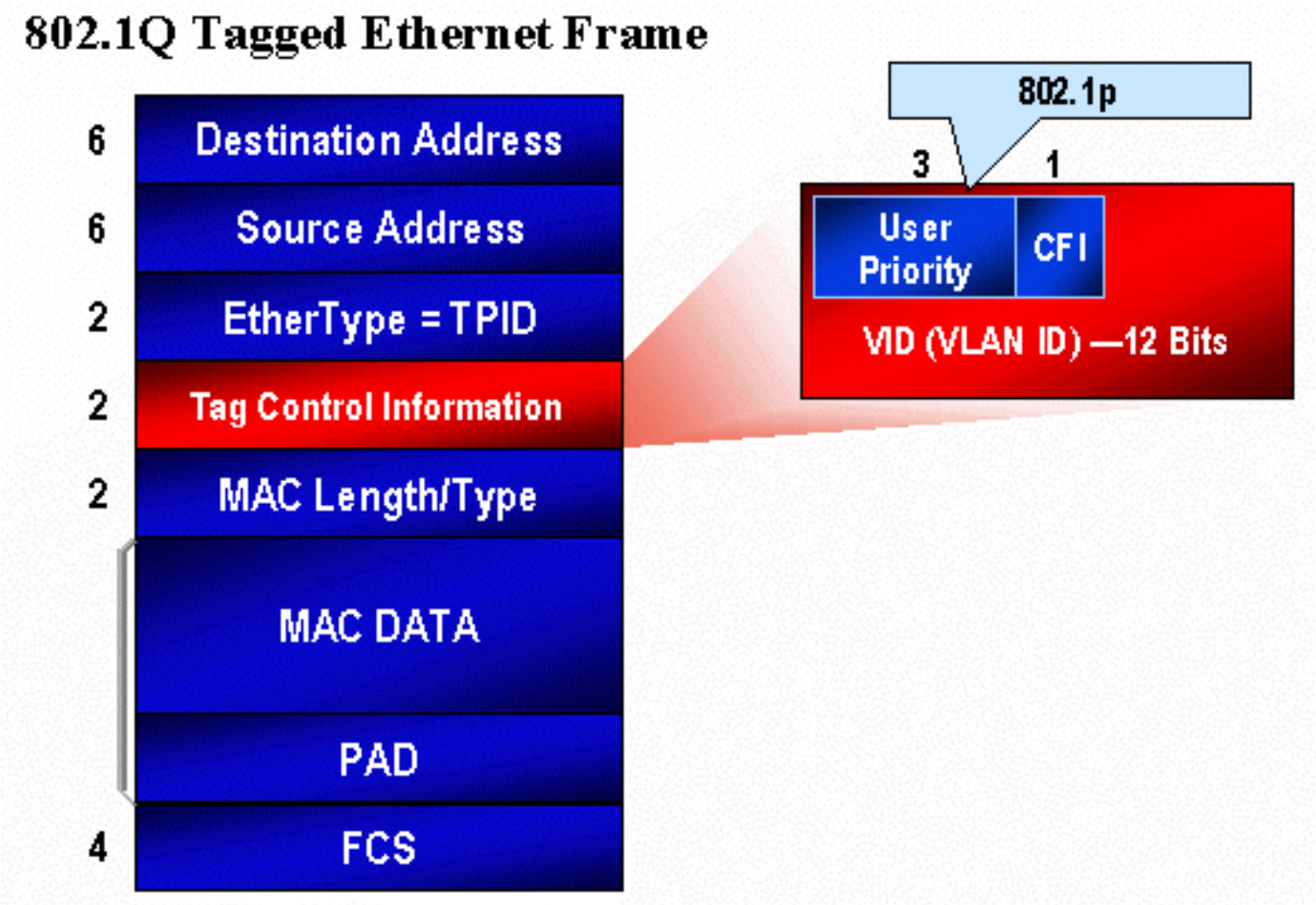
最近、ToS フィールドの使用が拡張され、6 MSB を含むようになりました。これを DSCP と呼びます。DSCP では、64 個のプライオリティ値 (2 の 6 乗) を IP パケットに割り当てることができるようになりました。

Catalyst 6000 ファミリでは、ToS の処理が可能です。この処理には、PFC と MSFC のいずれかまたは両方を使用します。フレームがスイッチに着信すると、DSCP 値が割り当てられます。この DSCP 値は、管理者が定義したサービス レベル (QoS ポリシー) を割り当てるために、スイッチの内部で使用されるものです。DSCP は、すでにフレーム内にあってそれが使用されることもあり、また既存の CoS、IP 優先順位、またはフレーム内の DSCP から得られる場合もあります (そのポートが信頼されている場合)。DSCP を取得するためにスイッチでマップが内部的に使用されます。デフォルトのマップでは、8 段階の CoS/IP 優先順位値と 64 段階の DSCP 値を使用して、CoS/IP 優先順位の 0 を DSCP の 0 に、CoS/IP 優先順位の 1 を DSCP の 7 に、CoS/IP 優先順位の 2 を DSCP の 15 にというようにマップします。管理者は、このデフォルトのマッピングを書き換えることができます。フレームがある発信ポートにスケジュールされている場合は、その CoS を書き換えし、その DSCP 値を元にして新しい CoS 値を設定できます。

CoS

CoS は、スイッチド ネットワークを通過するときにイーサネット フレームのプライオリティを示す ISL ヘッダーまたは 802.1Q ヘッダーどちらかの 3 ビットのことです。このドキュメントの目的に従い、ここでは 802.1Q ヘッダーの使用にのみ言及します。802.1Q ヘッダーの CoS ビットは、一般的には 802.1p ビットと呼ばれます。当然ながら、IP の優先順位に使用されるビット数に一致する 3 つの CoS ビットがあります。多くのネットワークでは、エンドツーエンドで QoS を維持するために、パケットは L2 と L3 の両方のドメインを通過できます。QoS を維持するためには、ToS を CoS にマップすることも、CoS を ToS をマップすることもできます。

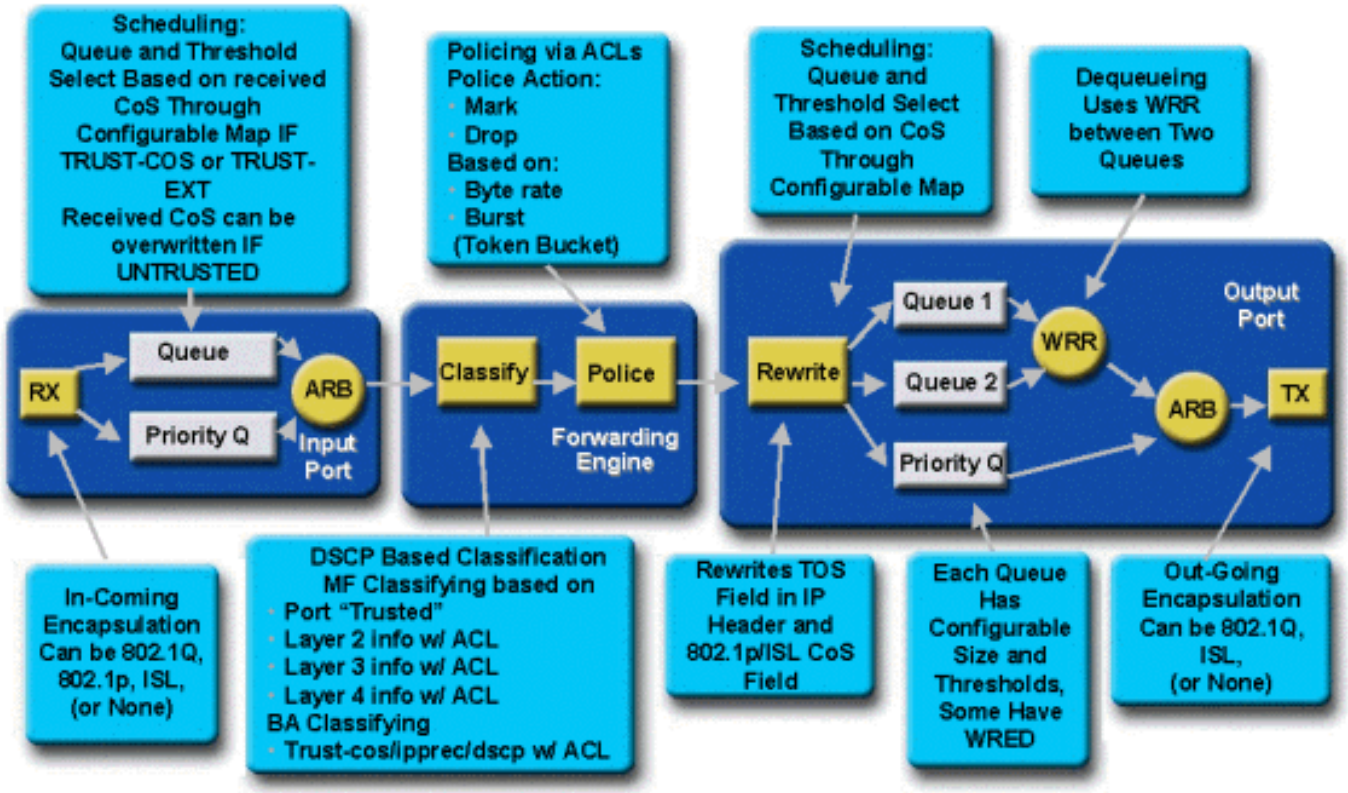
次の図は、802.1Q フィールドでタグ付けがされたイーサネット フレームを表しています。これは、2 バイトのイーサタイプと、2 バイトのタグで構成されています。2 バイトのタグの内容は、ユーザ プライオリティ ビット (802.1p) です。



Catalyst 6000 ファミリの QoS フロー

Catalyst 6000 ファミリでの QoS は、現在の Cisco Catalyst スイッチの中でも、QoS の最も包括的な実装です。次のセクションでは、フレームがスイッチを通過する際に、さまざまな QoS プロセスがどのように適用されるかについて説明します。

このドキュメントの前の箇所ですでに言及しましたが、複数の L2 および L3 スイッチが提供できる QOS 要素は多数存在します。これらの要素には、分類、入力キューのスケジューリング、ポリシング、リライト、および出力キューのスケジューリングが含まれています。Catalyst 6000 ファミリとの違いは、これらの QoS 要素が L2 エンジンによって適用されることです。この L2 エンジンでは、単に L2 ヘッダー情報だけでなく、L3 および L4 の詳細も考慮されます。次の図は、Catalyst 6000 ファミリでこれらの要素が実装されている仕組みを要約したものです。



フレームがスイッチに入り、フレームを受信したポート ASIC によって最初に処理されます。フレームが Rx キューに配置されます。Catalyst 6000 ファミリ ラインカードによっては、1 つか 2 つの Rx キューが存在します。

ポート ASIC では、CoS ビットを指標として使用し、フレームをどのキューに置くかを判定します（入力キューが複数ある場合）。 ポートが信頼できないとして分類された場合、ポート ASIC は事前定義された値に基づいて既存の CoS ビットを上書きできます。

その後、フレームは L2/L3 フォワーディング エンジン（PFC）に渡されます。ここでは、フレームを分類し、オプションでポリシング（レート制限）を適用します。分類とは、フレームに DSCP 値を割り当てるプロセスで、この値はフレームを処理するためスイッチによって内部的に使用されます。DSCP の値は次のいずれかで求められます。

1. フレームがスイッチに入る前に設定された既存の DSCP 値。
2. IPv4 ヘッダーにすでに設定されている、受信した IP 優先順位ビット。64 個の DSCP 値がありますが、IP 優先順位の値は 8 個しかないので、管理者はスイッチが DSCP を取得するためのマッピングを設定します。管理者がマップを設定しない場合は、デフォルト マッピングが使用されます。
3. フレームがスイッチに着信するより前に設定されていた CoS ビット。IP 優先順位と同様に、CoS 値には 8 段階の値しかないため、それぞれを 64 段階の DSCP 値にマップする必要があります。このマップは設定することもできますが、スイッチが、すでに存在するデフォルト マップを使用することもできます。
4. Access Control List（ACL; アクセス コントロール リスト）のエントリで通常割り当てられている DSCP のデフォルト値を使用して、フレームに DSCP 値を設定。

DSCP 値がフレームに割り当てられたら、ポリシング（レート制限）が適用されます。そのため、ポリシング設定が存在している必要があります。ポリシングとは、PFC を通過するデータのフローを制限するもので、プロファイル外のトラフィックは廃棄またはマークダウンされます。プロファイル外という用語は、トラフィックが管理者によって定義されている制限値を超えたことを意味します。この制限値は、PFC が送信する 1 秒当たりのビット数で表されます。プロファイ

ル外のトラフィックは、廃棄されるか、CoS の値がマークダウンされます。PFC1 と PFC2 では、現在、入力ポリシング（レート制限）だけがサポートされています。 入出力ポリシングのサポートは、新しい PFC のリリースで使用可能になる予定です。

その後、PFC によりそのフレームが出力ポートに渡され、処理されます。この時点で、フレームの CoS 値および IPV4 ヘッダーの ToS 値を修正するために、リライト処理が呼び出されます。これは内部の DSCP に基づいて行われます。次に、フレームは CoS 値に基づいて送信キューに置かれて、転送できる状態になります。フレームがキュー内にある間、ポート ASIC はそのバッファを監視し、オーバーフローを防ぐために WRED を実行します。出力ポートからフレームをスケジュールして送信するために、WRR スケジューリング アルゴリズムが使用されます。

次の各セクションでは、上記で説明された各手順の設定例を提供しつつ、このフローの詳細を説明します。

キュー、バッファ、しきい値およびマッピング

QoS 設定の詳細を説明する前に、スイッチの QoS 設定機能を完全に理解していただくため、特定の用語について説明する必要があります。

キュー

スイッチの各ポートには、データの一時ストレージ領域として使用される一連の入力および出力キューがあります。Catalyst 6000 ファミリ ラインカードは、各ポートに対して異なる数のキューを実装します。通常、キューは各ポート用のハードウェア ASIC の中に実装されています。Catalyst 6000 ファミリのラインカードの最初の世代では、入力キューが 1 つと、出力キューが 2 つという構成が一般的でした。新しいラインカード（10/100 および GE）では、ASIC によってさらに 2 つのキューの組（入力キューが 1 つと、出力キューが 1 つ）が追加され、合計で 2 つの入力キューと 3 つの出力キューが実装されています。これらの新しい 2 つのキューは、VoIP のような遅延の影響を受けやすいトラフィックのために使用される特別な SP（完全優先）キューです。これらは SP 方式で処理されます。つまり、SP キューにフレームが到達すると、低優先キューからのフレームのスケジューリングが停止され、SP キューにあるフレームが処理されます。SP キューが空の場合にだけ、低優先キューからのパケットのスケジューリングが再開されます。

輻輳時にポート（入力ポートまたは出力ポート）にフレームが到達すると、そのフレームはキューに置かれます。フレームをどのキューに置くかの決定は、通常、着信フレームのイーサネット ヘッダー内の CoS 値に基づいて行われます。

出力の場合、スケジューリング アルゴリズムを使用して、Tx（出力）キューが空にされます。WRR は、このために使用される技術です。各キューでは、次のキューに移る前に、どれほどのデータがキューから取り出されるか示すために、重みが使用されます。管理者によって割り当てられる重み付けは、1 から 255 までの数値で、各 Tx キューに割り当てられます。

バッファ

各キューには、送信データを保管するために一定量のバッファ スペースが割り当てられます。ポート ASIC にはメモリがあり、分割されてポートごとに割り当てられます。各 GE ポートでは、GE ASIC が 512 K のバッファ スペースを割り当てます。10/100 ポートでは、ポート ASIC によって、ポート バッファリングごとに 64 K または 128 K（ラインカードに応じる）が予約されます。このバッファ領域は、さらに Rx（入力）キュー用と Tx（出力）キュー用に分割されます。

しきい値

通常のデータ送信では、パケットが廃棄されると、そのパケットは再送信されます（TCP フロー）。 輻輳時には、これがネットワークの負荷を増大させ、バッファがさらにオーバーロードになる可能性があります。バッファがオーバーフローしないようにする手段として、Catalyst 6000 ファミリ スイッチでは、この発生を回避するためのさまざまな技術が利用されています。

しきい値は、スイッチ（または管理者）によって設定される予測値で、輻輳管理アルゴリズムがキューからのデータの廃棄を開始できる適用水準を定義するものです。Catalyst 6000 ファミリのポートでは、通常は入力キューに対応付けられた 4 つのしきい値が用意されています。通常、出力キュー用には、2 つのしきい値が設定されています。

また、QoS 上、これらのしきい値は、さまざな優先順位を持ったフレームを割り当てる手段としても配置されています。バッファがいっぱいになり始め、しきい値を超えるようになると、管理者はさまざまな優先順位をそれぞれ異なるしきい値にマップすることにより、しきい値を超えたときに、どのフレームを廃棄するかスイッチに対して指示を出すことができます。

マッピング

上記の「キュー」と「しきい値」セクションでは、どのキューをフレームに配置するか、どの時点でバッファがいっぱいになりフレームを廃棄すべきか判断するため、イーサネット フレームの CoS 値が使用されることが説明されました。これがマッピングの目的です。

Catalyst 6000 ファミリで QoS が設定されている場合は、デフォルト マッピングがイネーブルになり、次のことが定義されます。

- ある CoS 値を持ったフレームが廃棄されるようになるしきい値
- フレームが配置されるキュー（CoS 値が基準）

デフォルト マッピングがある場合、管理者はそれらのマッピングを上書きできます。次のようなマッピングが存在します。

- DSCP 値への着信フレームの CoS 値
- DSCP 値への着信フレームの IP 優先順位の値
- 発信フレームの CoS 値に対する DSCP 値
- 受信キューでの廃棄しきい値の CoS 値
- 送信キューでの廃棄しきい値の CoS 値
- ポリシング ステートメントを超えるフレームの DSCP マークダウン値
- 特定の宛先 MAC アドレスを持つフレームに対する CoS 値

WRED およびWRR

WRED と WRR は、Catalyst 6000 ファミリに搭載されている 2 つのきわめて強力なアルゴリズムです。WRED および WRR は両方とも、拡張バッファ管理と発信スケジューリングを提供するために、イーサネット フレーム内のプライオリティ タグ（CoS）を使用します。B

WRED

WRED は、Catalyst 6000 ファミリで使用されているバッファ管理アルゴリズムであり、輻輳発生時の、高優先度トラフィック廃棄への影響を最小限にするものです。WRED は、RED アルゴリズムをベースとしています。

RED および WRED については、TCP フロー管理の概念を復習してください。フロー管理によって、TCP 送信元がネットワークに負荷をかけ過ぎないようにすることができます。TCP スロースタート アルゴリズムは、これに対する解決策の一環です。このアルゴリズムでは、フローが開始すると、確認応答を待機する前に、1 つのパケットが送信されるようにします。さらに、ACK を受信する前にパケットを 2 つ送信します。こうして、段階的に各 ACK を受信する前に送信するパケットの数を増やして行きます。輻輳を発生させる負荷を生じさせずにネットワークで処理できる送信レベルに達するまで、これが続けられます（つまり *x 個のパケットが送信されます*）。輻輳が発生すると、スロースタート アルゴリズムはウィンドウ サイズ（確認応答を待つ前に送信されるパケット数）を抑制し、その TCP セッション（フロー）の全体的なパフォーマンスを低減します。

RED は、キューの開始から、満杯になるのを監視します。あるしきい値を超過すると、パケットはランダムに廃棄され始めます。特定のフローはまったく考慮されません。むしろ、ランダムにパケットが廃棄されます。これらのパケットは、高優先度のフローである場合も、低優先度のフローの場合もあります。廃棄されたパケットは、1 つのフローまたは複数の TCP フローの一部である可能性があります。複数のフローが影響を受ける場合、前述のように、各フローのウィンドウ サイズに大きな影響を及ぼす可能性があります。

RED とは異なり、WRED では、ランダムなフレームの廃棄は行われません。WRED では、フレームの優先順位が考慮されます（Catalyst 6000 ファミリでは、CoS 値が使用されます）。WRED では、管理者が、ある CoS 値を持つフレームを特定のしきい値に割り当てます。これらのしきい値を超過すると、そのしきい値にマップされた CoS 値を持つフレームは廃棄対象になります。より高いしきい値に割り当てられた CoS 値を持つフレームは、キューの中で維持されます。この処理により、高い優先順位を持つフローはそのまま保持され、その大きなウィンドウ サイズもそのまま維持されます。送信元から受信先へ送られるパケットの遅延も最小限に留まります。

ラインカードが WRED をサポートするかどうかはどうすればわかりますか。次のコマンドを発行します。出力で、そのポートの WRED をサポートしていることを示すセクションを確認します。

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------------
```

```
1         40% 100%
2         40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
--------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ------------------------------------ 1 100 2 255 Console> (enable)
```

ポートで WRED が使用できない場合、ポートはバッファ管理のテール ドロップ方式を使用します。テール ドロップ方式とは、その名前が示しているように、バッファが完全に使用中の状態になったときに、着信したフレームを単純に廃棄するというものです。

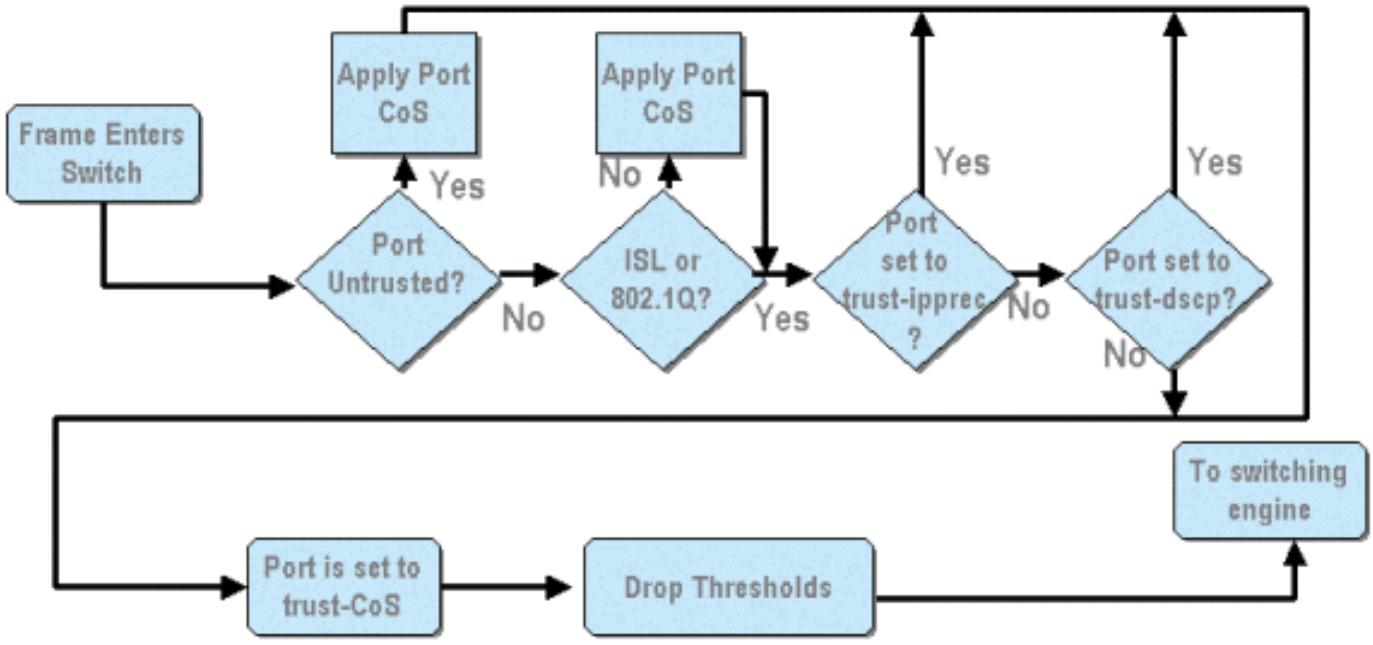
WRR

WRR は、Tx キューからの出力トラフィックのスケジューリングに使用されます。通常のラウンドロビン アルゴリズムでは、次のキューに移る前に各キューから同じ数のパケットを送信する Tx キューを交互に使用します。WRR の重み付け機能により、キューに適用されている重みの値をチェックするスケジューリング アルゴリズムが実現されます。これによって、定義されたキューが帯域幅をより多く使用できるようになります。WRR スケジューリング アルゴリズムでは、指定したキューで、他のキューよりも多くのデータを空にすることができます。これによって、選択したキューを優先することができます。

WRR の設定と上記の内容のその他の面については、続くセクションで説明します。

Catalyst 6000 ファミリ上でポート ASIC ベースの QoS を設定する方法

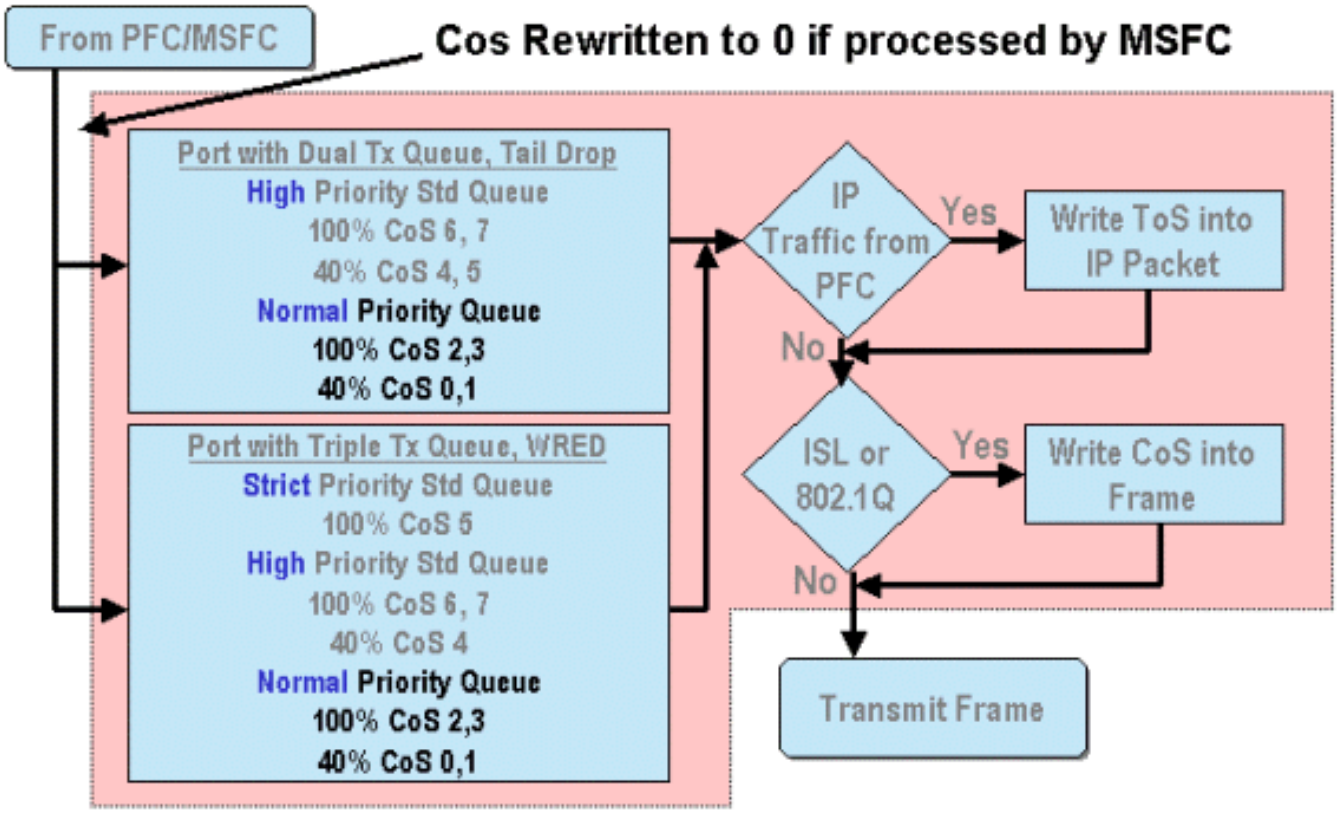
QoS の設定により、ポート ASIC あるいは PFC に対して QoS アクションの実行が指示されます。次のセクションでは、これら両方の処理に対する QoS の設定について説明します。ポート ASIC の場合、QoS の設定は、着信トラフィックと発信トラフィックの両方に影響します。



上記の図から、以下の QoS 設定プロセスが適用されることが分かります。

1. ポートの信頼状態

2. ポート ベースの CoS の適用
3. Rx 側の廃棄しきい値の割り当て
4 CoS の Rx ドロップしきい値へのマップ



フレームが MSFC または PFC で処理される場合、フレームはその後の処理のために発信側のポート ASIC に渡されます。MSFC によって処理されるフレームは、CoS 値がゼロにリセットされます。これは、発信側ポートでの QoS 処理を受けるために必要です。

上の図は、ポート ASIC によって発信トラフィックに対して行われる QoS の処理を表しています。発信側での QoS 処理で実行される処理には、次のようなものがあります。

1. TX 側のテール ドロップおよび WRED しきい値の割り当て

2. CoS の Tx テール ドロップおよび WRED へのマップ
また、上記の図には示されていませんが、発信フレームへの CoS の再割り当てプロセスは、DSCP の CoS へのマップを使用しています。

次のセクションでは、ポート ベース ASIC の QoS 設定機能を、さらに詳しく検証します。

注：重要な点として、CatOS を使用して QoS コマンドが実行する場合、通常指定したキュー タイプを持つすべてのポートに適用されることに注意してください。たとえば、WRED 廃棄しきい値がキュー タイプ 1p2q2t のポートに適用される場合、この WRED 廃棄しきい値はこのキュー タイプをサポートするすべてのラインカード上のすべてのポートに適用されます。IOS を使用している場合は、通常は QoS コマンドはインターフェイス レベルで適用されます。

QoS の有効化

Catalyst 6000 ファミリで QoS 設定を行うには、その前にスイッチで QoS を有効にする必要があります。これを行うには、次のコマンドを発行します。

CatOS

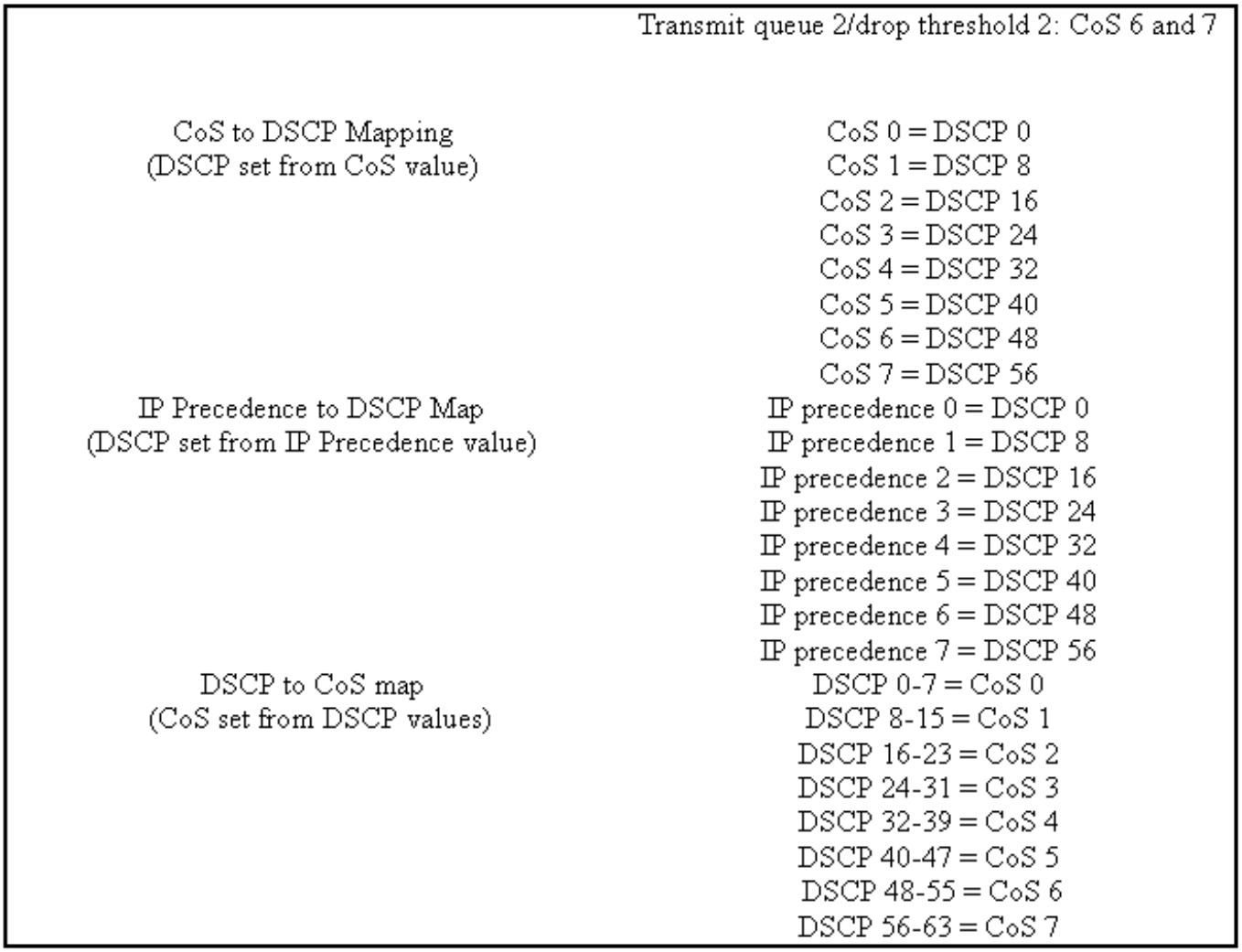
```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

統合 Cisco IOS (ネイティブ モード)

```
Cat6500(config)# mls qos
```

Catalyst 6000 ファミリで QoS をイネーブルにすると、そのスイッチでは、一連の QoS デフォルト値に設定されます。これらのデフォルトには次の設定が含まれます。

QoS Feature	Default setting
Trust state of each port	Un-trusted
Receive Queue drop threshold percentages	Threshold 1 – 50% Threshold 2 – 60% Threshold 3 – 80% Threshold 4 – 100%
Transmit Queue drop threshold percentages	Low priority queue threshold 1 – 80% Low priority queue threshold 2 – 100% High priority queue threshold 1 – 80% High priority queue threshold 2 – 100%
CoS value to Drop threshold mapping	Receive queue 1/drop threshold 1: CoS 0 and 1 Transmit queue 1/drop threshold 1: CoS 0 and 1 Receive queue 1/drop threshold 2: CoS 2 and 3 Transmit queue 1/drop threshold 2: CoS 2 and 3 Receive queue 1/drop threshold 3: CoS 4 and 5 Transmit queue 2/drop threshold 1: CoS 4 and 5 Receive queue 1/drop threshold 4: CoS 6 and 7



信頼されるポートと信頼されないポート

Catalyst 6000 ファミリの特定のポートを、信頼されるポートまたは信頼できないポートとして設定できます。ポートの信頼状態によって、スイッチを通過するときの、フレームのマーク付け、分類、スケジュールの方法を示します。デフォルトでは、すべてのポートが信頼できない状態になっています。

信頼できないポート（ポートのデフォルト設定）

ポートが信頼できないポートとして設定されている場合、フレームが最初にポートに着信した時点で、そのフレームの CoS 値と ToS 値はポート ASIC によってゼロにリセットされます。これは、このフレームがスイッチを通過するパスでは、最低の優先順位のサービスが与えられることを意味します。

別の方法として、管理者は、信頼できないポートに入るイーサネット フレームの CoS 値を、事前定義された値にリセットできます。この設定については、後のセクションで説明します。

ポートを信頼できないとして設定することは、スイッチには輻輳回避を何も行わないように指示することになります。輻輳回避は、そのキューに対して定義されたしきい値を超えると、CoS 値に基づいてフレームを廃棄するために使用される方法です。このポートに入るすべてのフレームは、バッファが 100 パーセントに達すると、等しく廃棄される対象になります。

CatOS では、次のコマンドを発行することによって、10/100 または GE ポートを信頼できないとして設定できます。

CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

このコマンドでは、モジュール 3 のポート 16 を信頼できないとして設定します。

注：統合 Cisco IOS (ネイティブ モード) では、ソフトウェアは現在 GE ポートに関して信頼の設定のみをサポートしています。

統合 Cisco IOS (ネイティブ モード)

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

上記の例では、IOS であるため、インターフェイス設定を入力し、**no 形式のコマンドを適用して、信頼できないとしてポートを設定しています。**

信頼できるポート

また、スイッチに入るイーサネット フレームに、フレームがスイッチを通過するときに管理者がスイッチで維持させたいと思う CoS または ToS のいずれかの設定がある場合があります。このようなトラフィックの場合、管理者は、そのトラフィックが信頼できる状態としてスイッチに入ってくるポートの信頼状態を設定できます。

前述のように、スイッチはそのフレームに事前に設定したレベルのサービスを割り当てるために DSCP 値を内部的に使用します。フレームが信頼できるポートに入ってくる際に、管理者は、既存の CoS、IP 優先順位、または DSCP 値のいずれかを確認して内部 DSCP 値を設定するように、ポートを設定できます。別の方法として、管理者は、ポートに入ってくるすべてのパケットに対して事前定義された DSCP 値を設定することもできます。

ポートの信頼状態を信頼できると設定するには、次のコマンドを使用します。

CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

このコマンドは、WS-X6548-RJ45 ラインカードに適用され、ポート 3/16 の信頼状態を信頼できるとして設定します。このスイッチでは、着信フレームで設定されている CoS 値の設定を使用して、内部 DSCP が設定されます。DSCP 値は、そのスイッチで QoS がイネーブルにされたときに作成されたデフォルト マップか、管理者によって定義されたマップから取得されます。管理者は、trust-COs キーワードの代わりに、trust-dscp または trust-ipprec キーワードを使用することもできます。

以前の 10/100 ラインカード (WS-X6348-RJ45 および WS-X6248-RJ45) の場合は、**set qos acl コマンドを実行して、ポートの信頼状態を設定する必要があります。**このコマンドでは、信頼状態は **set qos acl コマンドのサブ パラメータで割り当てることができます。**また、これらのラインカードでは、次に示すとおり、trust CoS というポート設定はサポートされていません。

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to
turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so
port is set to untrusted.
```

上記のコマンドでは、入力キューのスケジューリングをイネーブルにする必要があります。そのため、WS-X6248-RJ45 および WS-X6348-RJ45 ラインカードの 10/100 ポートの場合は、信頼状態の設定にも **set port qos x/y trust trust-COs コマンドを設定して、ACL を使用する必要があります。**

統合 Cisco IOS (ネイティブ モード) の場合は、新しい WS-X6548-RJ45 ラインカードの GE インターフェイスおよび 100/100 ポートに信頼状態を設定できます。

統合 Cisco IOS (ネイティブ モード)

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

この例では、GE ポート 5/4 の信頼状態を信頼できると設定しています。DSCP 値の決定には、フレームの IP 優先順位値が使用されます。

入力分類および設定ポートベースのCoS

イーサネット フレームがスイッチのポートに着信したとき、次の 2 つの基準のいずれかを満たしている場合は、このフレームの CoS を変更できます。

1. ポートが信頼できないとして設定されている
2. そのイーサネット フレームに CoS 値が設定されていない

入力イーサネット フレームの CoS を再設定する場合、次のコマンドを発行する必要があります。

CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

このコマンドは、モジュール 3 のポート 16 に着信したイーサネット フレームの CoS を、フレームに CoS の設定がない場合や、ポートが信頼できないと設定されていた場合に、3 という値に設定します。

統合 Cisco IOS (ネイティブ モード)

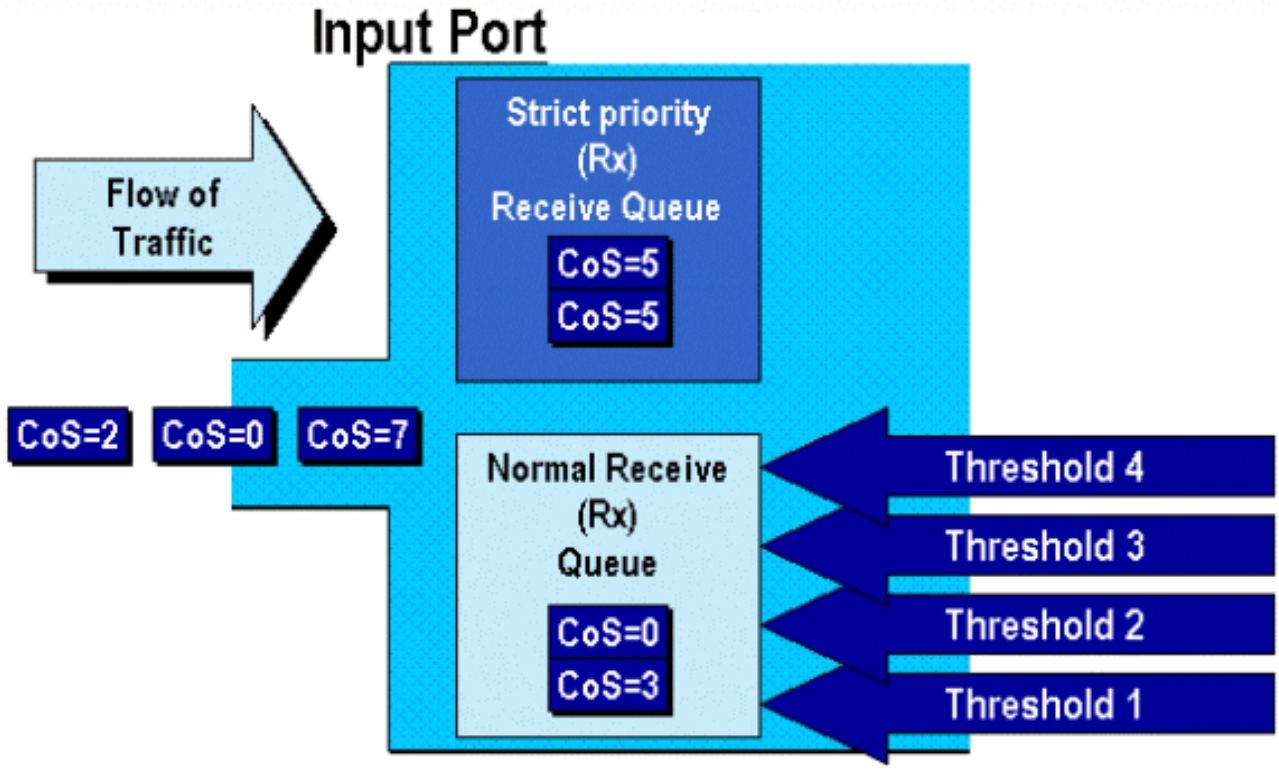
```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

このコマンドは、モジュール 5 のポート 13 に着信したイーサネット フレームの CoS を、フレー

ムに CoS の設定がない場合や、ポートが信頼できないと設定されていた場合に、4 という値に設定します。

Rx ドロップしきい値の設定

フレームは、スイッチのポートに着信すると、Rx キューに置かれます。バッファのオーバーフローを防ぐために、ポート ASIC には各 Rx キューに 4 つのしきい値が実装されており、これらのしきい値により、超過時に廃棄するフレームが決定されます。ポート ASIC では、フレームにセットされた CoS 値を使用して、しきい値の超過が生じたときに廃棄するフレームを決定します。この機能によって、輻輳が発生したときには、優先順位が高いフレームほど、バッファに長く留まるようになります。



上記の図では、フレームが届き、キューに置かれます。キューがいっぱいになり始めると、しきい値がポート ASIC によって監視されます。しきい値に達すると、管理者が特定した CoS 値を持つフレームは、キューからランダムに廃棄されます。1q4t キュー（WS-X6248-RJ45 および WS-X6348-RJ45 ラインカードで使用されるキュー）に対するデフォルトのしきい値マッピングは、次のとおりです。

- しきい値 1 の設定は 50%、CoS の値 0 および 1 がこのしきい値にマップされる
- しきい値 2 の設定は 60%、CoS の値 2 および 3 がこのしきい値にマップされる
- しきい値 3 の設定は 80%、CoS の値 4 および 5 がこのしきい値にマップされる
- しきい値 4 の設定は 100 %、CoS の値 6 および 7 がこのしきい値にマップされる

1P1q4t（GE ポートで検出）キューでは、デフォルトのマッピングは次のようになります。

- しきい値 1 の設定は 50%、CoS の値 0 および 1 がこのしきい値にマップされる
- しきい値 2 の設定は 60%、CoS の値 2 および 3 がこのしきい値にマップされる
- しきい値 3 の設定は 80 %、CoS の値 4 がこのしきい値にマップされる
- しきい値 4 の設定は 100 %、CoS の値 6 および 7 がこのしきい値にマップされる
- 5 の CoS 値は、完全優先キューにマップされる

1p1q0t（WS-X6548-RJ45 ラインカードの 10/100 ポートで検出）では、デフォルトのマッピングは次のようになります。

- CoS が 5 のフレームは SP Rx キュー（キュー 2）に入ります。ここで、SP 受信キューのバッファが 100% 満たされている場合だけ、スイッチは着信フレームを廃棄します。
- CoS が 0、1、2、3、4、6、または 7 のフレームは、Rx キューに入ります。この場合、Rx キューのバッファの使用率が 100 % に達したときに着信フレームが廃棄されます。

これらの廃棄しきい値は、管理者が変更することもできます。また、各しきい値にマップされているデフォルトの CoS 値も変更できます。タイプの異なるラインカードは、それぞれ異なる Rx キューを実装します。キュー タイプの概要を次に示します。

CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

このコマンドでは、1 つのキューと 4 つのしきい値を持つ入力ポート（1q4t）すべての受信廃棄しきい値を、20 %、40 %、75 %、および 100 % に設定しています。

統合 Cisco IOS（ネイティブ モード）では、次のコマンドを実行します。

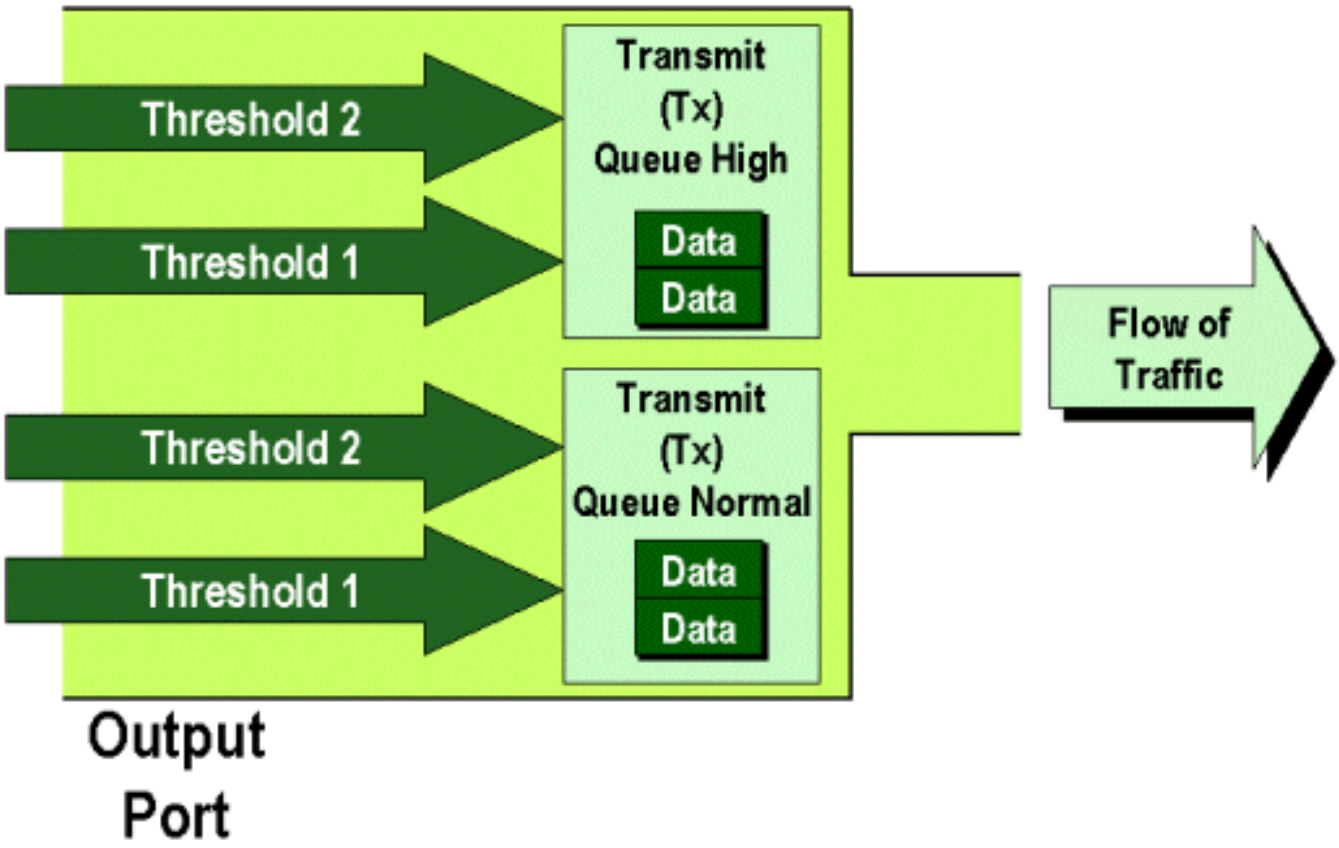
統合 Cisco IOS（ネイティブ モード）

```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

Rx の廃棄しきい値は、管理者がイネーブルにする必要があります。現在、**set port qos x/y trust trust-COs コマンドは、Rx 廃棄しきい値をアクティブにするために使用する必要があります（ここで、*x にはモジュール番号を指定し、y はそのモジュールのポートになります*）。**

Tx ドロップしきい値の設定

出力ポートでは、輻輳回避メカニズムの一部として、キュー 1 とキュー 2 という 2 つの Tx しきい値が使用されます。キュー 1 は標準の低優先キュー、キュー 2 は標準の高優先キューになります。使用されているラインカードに応じて、テール ドロップまたは WRED しきい値管理アルゴリズムを利用します。両方のアルゴリズムは、各 Tx キューの 2 つのしきい値を使用します。



管理者は、これらのしきい値を次のように設定できます。

CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

このコマンドでは、2 つのキューと 2 つのしきい値（2q2t）を持つすべての出力ポートのキュー 1 の Tx 廃棄しきい値を、40 % および 100 % に設定しています。

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

このコマンドでは、1 つの SP キューと 2 つの通常キューと 2 つのしきい値（1p2q2t）を持つすべての出力ポートのキュー 1 の WRED 廃棄しきい値を、60 % および 100 % に設定しています。キュー 1 は通常の低優先キューとして定義されており、その優先順位は最低になります。キュー 2 は通常の高優先キューであり、キュー 1 よりも高い優先順位を持ちます。キュー 3 は SP キューであり、そのポートでは他のどのキューよりも先にサービスを受けます。

統合 Cisco IOS（ネイティブ モード）では、これと同等のコマンドを次のように実行します。

統合 Cisco IOS（ネイティブ モード）

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
Cat6500(config-if)#
```

これにより、1p2q2t ポートのキュー 1 の WRED 廃棄しきい値として、しきい値 1 (Tx) が 40 %、しきい値 2 (Tx) が 100 % に設定されます。

統合 Cisco IOS (ネィティブ モード) では、WRED を必要に応じてディセーブルにすることもできます。 これを実行するには、このコマンドの **n" 形式を使用します。**WRED を無効にする例を次に示します。

統合 Cisco IOS (ネイティブ モード)

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

CoS 値への MAC アドレスのマップ

グローバル ポート定義に基づいて CoS を設定することに加えて、スイッチによって管理者は宛先 MAC アドレスと VLAN ID に基づいて CoS 値を設定することができます。これにより、事前に決定された CoS 値で特定のターゲット宛てのフレームにタグ付けすることができます。この設定には、次のコマンドを実行します。

CatOS

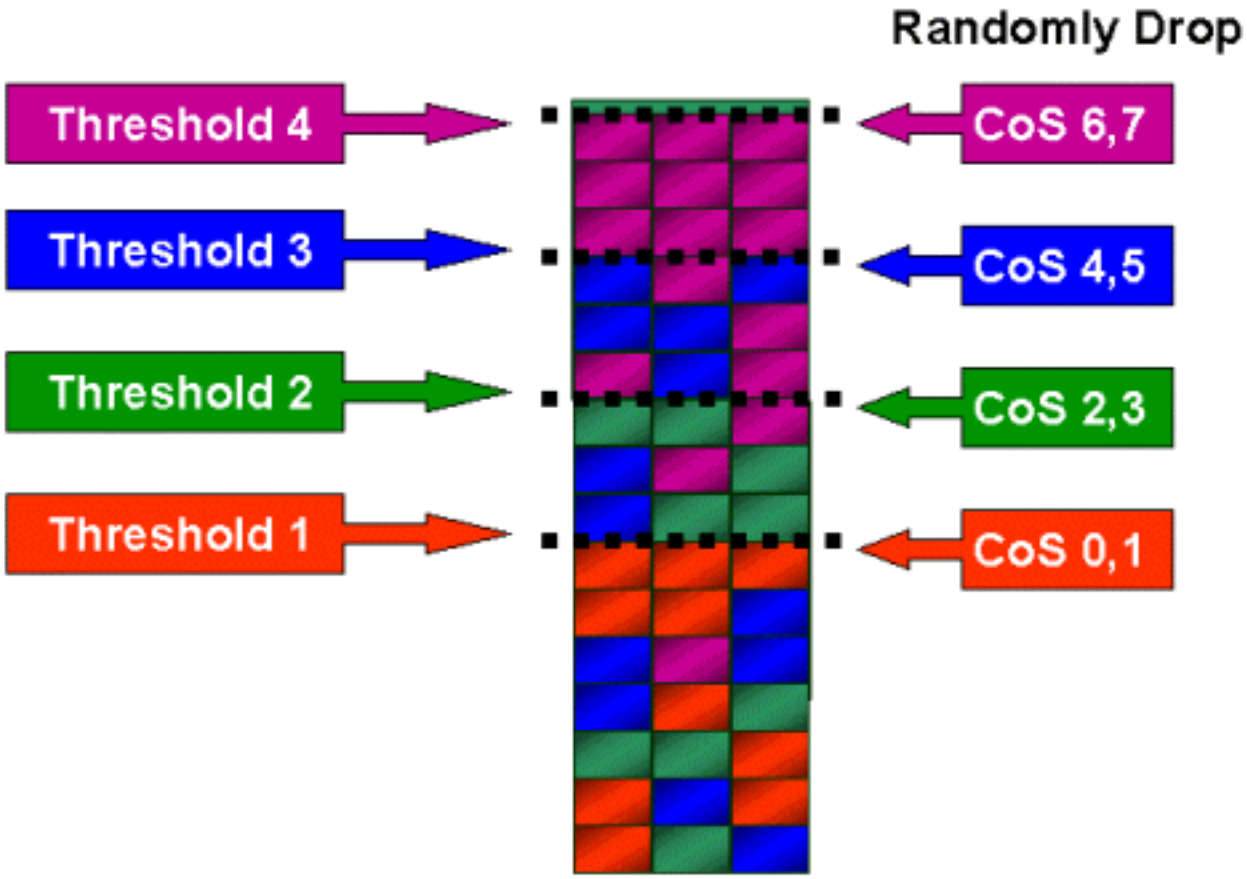
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

このコマンドでは、宛先 MAC アドレスが 00-00-0c-33-2a-4e で、VLAN 200 から送られたフレームすべてに対して、CoS として 5 を設定しています。

統合 Cisco IOS (ネイティブ モード) には、これに相当するコマンドはありません。 これは、このコマンドは PFC がまだ存在しなかった時期に限ってサポートされていたものであり、統合 Cisco IOS (ネイティブ モード) では実行に PFC を必要とするためです。

しきい値への CoS のマップ

しきい値を設定した後、そのしきい値を超えたときに、特定の CoS 値を持つフレームを廃棄できるよう、管理者はそのしきい値に CoS 値を割り当てることができます。通常は、低い優先順位を持つフレームを低いしきい値に割り当てるため、輻輳が発生したときには高い優先順位を持つトラフィックがキュー内に維持されます。



上の図では、4 つのしきい値を持つ入力キューと、CoS 値がどのように各しきい値に割り当てられたかが示されています。

次の出力では、CoS 値がどのようにしきい値に割り当てられるかが示されています。

CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

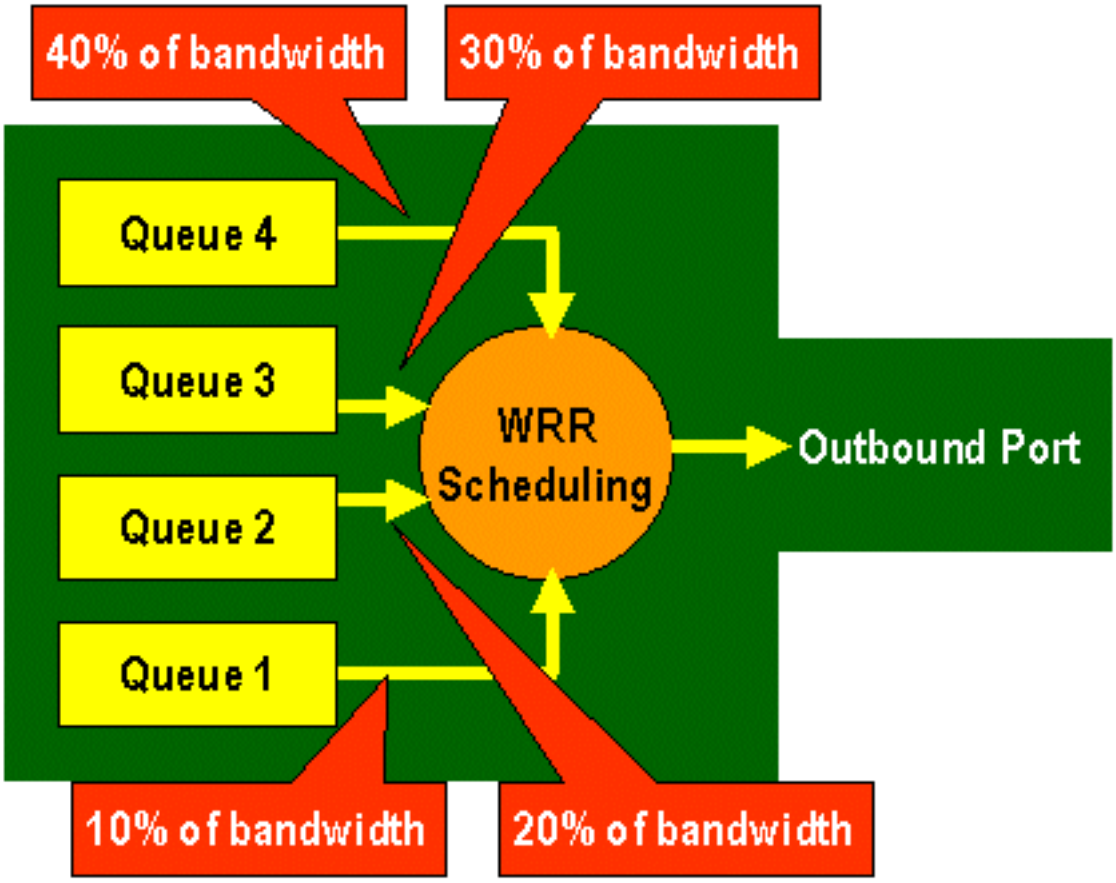
このコマンドは、0と1のCO値をqueue 1、threshold 1に割り当てます。統合Cisco IOS（ネイティブモード）での同等のコマンドを次に示します。

統合 Cisco IOS（ネイティブ モード）

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

Tx キューの帯域幅の設定

フレームが出力キューに配置された場合、そのフレームは出力スケジューリング アルゴリズムを使用して送信されます。この出力スケジューラの処理では、フレームを出力キューから送信するために WRR が使用されます。使用しているラインカードのハードウェアに応じて、ポートごとに 2、3、または 4 個の送信キューがあります。



WS-X6248 および WS-X6348 ラインカード（キュー構造は 2q2t）では、WRR メカニズムによって 2 つの Tx キューがスケジューリングに使用されます。WS-X6548 ラインカード（キュー構造は 1p3q1t）には、4 つの Tx キューがあります。これらの 4 つの Tx キューのうち、3 つの Tx キューは WRR アルゴリズムによって処理されます（最後の Tx キューは SP キューです）。 GE ラインカードには、3 つの Tx キューがあります（1p2q2t キュー構造を使用）。これらのキューの 1 つは SP キューで、WRR アルゴリズムは 2 つの Tx キューのみを処理します。

通常、管理者は Tx キューに重みを割り当てます。WRR は、ポートのキューに割り当てられた重みを調べて動作します。この重みはスイッチの内部において、次のキューに移る前に、どれだけのトラフィックが送信されるかを判断するために使用されます。1 から 255 の間の重みの値を、それぞれのポート キューに割り当てることができます。

CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

このコマンドは、キュー1に40の重み付けを割り当て、キュー2に80の重み付けを割り当てます。これは、実質的に、2つのキュー間に割り当てられた帯域幅の2対1の比率（80 ~ 40 = 2対1）を意味します。このコマンドは、2 つのキューと 2 つのしきい値を持つすべてのポートに有効です。

統合 Cisco IOS（ネイティブ モード）では、これと同等のコマンドを次のように実行します。

統合 Cisco IOS（ネイティブ モード）

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

ここでは、2 つのキュー間の 3 対 1 の比率が示されています。このコマンドの Cisco IOS バージョンは、特定の 1 つのインターフェイスだけに適用されます。

DSCP の CoS へのマッピング

フレームが出力ポートに置かれると、ポート ASIC により、割り当てられた CoS を使用して、輻輳回避（つまり WRED）が実行されます。さらに、その CoS を使用して、フレームのスケジューリングが決定されます（フレームの送信）。 この時点では、スイッチはデフォルトのマップを使用して、割り当てられている DSCP を取得し、CoS 値にその値をマップします。デフォルトのマップは、前出のこの表で示されています。

別の方法として、管理者は、スイッチが使用するマップを作成し、割り当てられた内部 DSCP 値を取得してフレームの新しい CoS 値を作成することができます。これを実現するため CatOS と統合 Cisco IOS（ネイティブ モード）を使用する方法の例を次に示します。

CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

上記のコマンドは、DSCP値20 ~ 30をCOs値5、DSCP値10 ~ 15をCOs値3に、DSCP値45 ~ 52をCOs値7にマップします。他のすべてのDSCP値は、スイッチで有効にされたときに作成されます。

統合 Cisco IOS（ネイティブ モード）では、これと同等のコマンドを次のように実行します。

統合 Cisco IOS（ネイティブ モード）

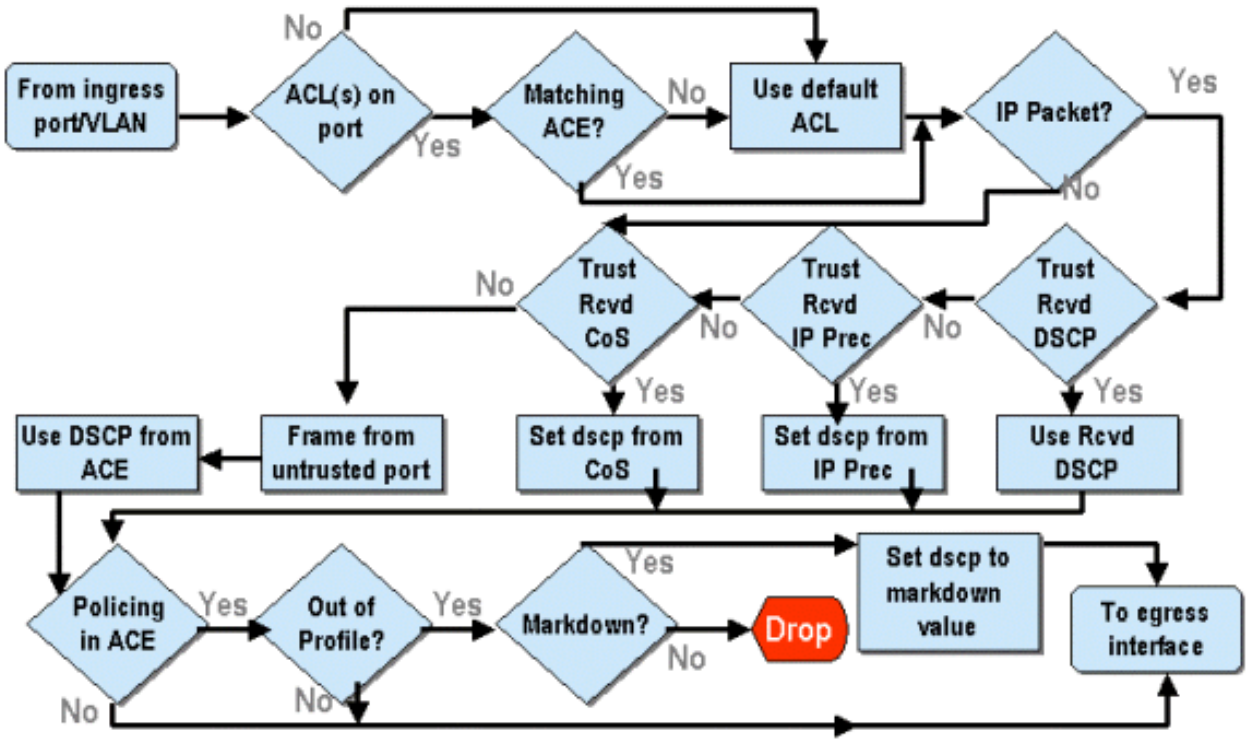
```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

ここでは、DSCP 値の 20、30、40、50、52、10、および 1 が CoS 値の 3 に設定されています。

PFC の分類およびポリシング

PFC では、フレームの分類とポリシングがサポートされています。分類は、優先順位（DSCP）を付けて着信フレームを割り当てる（マーキング）ために ACL を使用できます。 またポリシングを行うことで、トラフィックの流れを帯域幅の一定量に制限できます。

次のセクションでは、この PFC の機能について、CatOS と統合 Cisco IOS（ネイティブ モード）の両 OS プラットフォームの観点から説明します。PFC によって実行される処理を次の図に示します。



CatOS を実行するCatalyst 6000 ファミリーのポリシングの設定

ポリシングの機能は、CatOS と統合 Cisco IOS (ネイティブ モード) の 2 つのセクションに分けて説明します。 両方とも同じ結果が得られますが、異なる方法で設定および実装されます。

ポリシング

PFC では、スイッチに着信したトラフィックのレート制限 (またはポリシング) を行って、トラフィックのフローを事前に定義した制限まで減らすことができる機能をサポートしています。この制限を超えたトラフィックは、廃棄されるか、フレームの DSCP 値が低い値にマークダウンされます。

出力 (出力) レート制限は、現在PFC1またはPFC2のいずれでもサポートされていません。これは、出力 (または出力) ポリシングをサポートする2002年後半に予定されているPFCの新しいリビジョンで追加されます。

ポリシングは、CatOS と新しい統合 Cisco IOS (ネイティブ モード) の両方でサポートされていますが、機能の設定方法は大きく異なっています。次のセクションでは、両方の OS プラットフォームでのポリシングの設定について説明します。

集約とマイクロフロー (CatOS)

集約とマイクロフローは、PFC が実行するポリシングの範囲を定義するために使用される条件です。

マイクロフローは、単一フローのポリシングを定義します。フローは、一意の SA/DA MAC アドレス、SA/DA IP アドレス、および TCP/UDP ポート番号を持つセッションによって定義されます。VLAN のポートを介して開始される新しい各フローに対して、スイッチがそのフローのために受信するデータ量を制限するためにマイクロフローを使用できます。マイクロフローの定義では、所定のレート制限を超過したパケットを廃棄するか、またはそれらのパケットの DSCP 値をマーク ダウンすることができます。

マイクロフローと同様に、集約も、トラフィックをレート制限するために使用できます。ただし

、集約レートは、指定した QoS ACL に一致するポートまたは VLAN に着信するすべてのトラフィックに適用されます。集約は、Access Control Entry（ACE; アクセス コントロール エントリ）のプロファイルに一致する累積的なトラフィックのポリシングであると見なすことができます。

集約とマイクロフローの両方は、スイッチに受け入れ可能なトラフィック量を定義します。集約とマイクロフローの両方をポートまたは VLAN に同時に割り当てることができます。

マイクロフローを定義するときには最大 63 件まで、また集約は 1023 件まで定義できます。

アクセス コントロール エントリおよび QoS ACL（CatOS）

QoS ACL は、着信フレームを処理するために PFC が使用する一連の QoS ルールを定義する ACE のリストで構成されます。ACE は、ルータ アクセス コントロール リスト（RACL）に似ています。 ACE では、着信フレームに対する分類、マーキング、ポリシングの基準を定義します。着信フレームが、ACE で設定された条件と一致すると、QoS エンジンはフレームを処理します（ACE の判断に従います）。

すべての QoS 処理はハードウェアで行われるため、QoS ポリシングを有効にしても、スイッチのパフォーマンスには影響しません。

現在、PFC2 では、最大 500 の ACL をサポートしています。また、その ACL は最大 32000 の ACE（総計）で構成できます。 実際の ACE の数は、定義されている他のサービスや PFC で使用可能なメモリによって異なります。

定義できる ACE には 3 つのタイプがあります。これらは IP、IPX、および MAC です。IP と IPX の両方の ACE は L3 ヘッダーの情報を確認します。一方、MAC ベースの ACE は L2 ヘッダーの情報のみを確認します。また、MAC ACE は非 IP および非 IPX のトラフィックにしか適用できないことに注意してください。

ポリシング ルールの作成

ポリシング ルールを作成するには、集約（またはマイクロフロー）を作成した後、この集約（またはマイクロフロー）を ACE にマップする処理が必要です。

たとえば、要件がポート 5/3 に着信するすべての IP トラフィックを最大 20 MB に制限するというものである場合、前述の 2 つの手順を設定する必要があります。

最初に、この例では、着信するすべての IP トラフィックを制限することを要求しています。これは、集約ポリサーを定義する必要があることを意味しています。この例を示すと、次のようになります。

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

ここでは、test-flow という集約を作成しました。これは、20000 KBPS(20 Mbps)のレートと13のバーストを定義します。policed-dscpキーワードは、このポリシーを超えるデータのDSCP値がDSCPマークダウンマップで指定されているようにマークダウンされることを示します（デフォルト値が存在か、管理者変更です）。 policed-dscp キーワードを使用する代わりに、drop キーワードを使用することもできます。キーワード drop を定義すると、プロファイル外のトラフィック（割り当てられているバースト値を外れたトラフィック）は単純に廃棄されます。

ポリシング機能は、リーキー トークン バケット方式で動作しています。この方式では、まずバー

スト（所定の時間間隔内で受容できるデータの総量をビット/秒で定義したもの）を定義し、さらにレート（1 秒間にバケットを空にできるデータの総量を定義したもの）を定義します。 このバケットをオーバーフローするすべてのデータは、廃棄されるか、その DSCP がマークダウンされます。上で説明した所定の時間間隔とは、0.00025 秒（1/4000 秒）で固定されています（つまり、この数値を変更するコマンドは使用できません）。

上の例で使用されている値 13 は、1/4000 秒ごとに最大 13,000 ビットのデータを受容できるバケットを意味しています。これは毎秒に換算すると、52 MB（13K × ((1 / 0.00025）あるいは 13K × 4000）になります。 設定するバースト値を送出するデータのレートと同等か、それ以上に設定する必要があることには、常に注意してください。つまり、バースト値は一定期間に送信したいデータの最小量と同じか、それより多い必要があります。バースト値がレートとして指定した値より低い値になると、レート制限はバーストと同じになります。つまり、20 Mbps のレートと 15 Mbps まで計算するバーストを定義した場合、レートは 15 Mbps で制限することになります。次に疑問となるのは、なぜバースト値が 13 であるかということでしょう。バーストは、トークン バケットの深さ、つまり 1/4000 秒ごとの着信データの受信に使用されるバケットの深さを定義していることを思い出してください。よって、バースト値は、1 秒間に 20 MB 以上の着信データ レートをサポートするいずれかの数値になります。20 MB のレート制限に使用できる最小のバースト値は、20000 / 4000 = 5 になります。

ポリサーを処理する場合、トークン バケットがトークンでいっぱいになると、ポリシング アルゴリズムが始動します。このトークン数は、バースト値と同じになります。したがって、バースト値が13の場合、バケット内のトークンの数は13,000になります。1/4000秒ごとに、ポリシングアルゴリズムは定義されたレートを4000で割ったデータ量を送信します。送信済みデータのビット（2 進数）ごとに、バケットから 1 つのトークンが消費されます。そのインターバルの終わりに、新たなトークンのセットでバケットは再度いっぱいになります。交換されるトークン数は、レート / 4000 で定義されます。次の例を理解するために、上記の例を考慮しましょう。

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

これは 100 Mbps のポートであり、ポートに 100 Mbps の一定のストリームで送信していると仮定します。これは、100,000,000 ビット/秒の着信レートに相当します。パラメータは20000のレートと13のバーストです。時間間隔t0では、バケット内にトークンの完全な補完(13,000)があります。 時間間隔 t0 で、データの最初のセットがポートに届きます。この時間間隔の場合、到達レートは 100,000,000 / 4000 = 25,000 ビット/秒です。トークン バケットには 13,000 トークンの深さしかないため、この間隔ではポートに着信する 25,000 ビットのうち 13,000 ビットのみが送信される対象となり、12,000 ビットは破棄されます。

指定したレートでは、20,000,000 ビット/秒のフォワーディング レートを定義しています。これは 1/4000 秒に換算すると 5,000 ビットになります。送信される 5,000 ビットごとに、消費される 5,000 トークンが存在します。時間間隔 T1 では、別の 25,000 ビットのデータが到着しますが、バケットは 12,000 ビットを廃棄します。バケットは、レートを 4000 で除した数のトークン（5,000 個の新しいトークン）で再度いっぱいになります。 そして、次の 5,000 ビットに相当するデータが送出され（新たに 5,000 トークンを消費）、これが各時間間隔ごとに繰り返されます。

基本的に、バケットの深さ（定義されたバースト）を超過して到達するすべてのデータが廃棄されます。データが送信された後に残るデータ（規定とレートは一致します）も廃棄され、到着データの次のセットに移行します。不完全なパケットは、時間間隔内に完全に受信されなかったパケットで、廃棄されませんが、ポートに完全に受信されるまで保持されます。

このバースト値は、トラフィックのフローが一定であると仮定しています。ただし、実際のネットワークでは、データは一定ではなく、そのフローは TCP ウィンドウ サイズ（これは TCP 確認応答を送信シーケンスに組み込みます）によって決まります。TCP ウィンドウ サイズの問題を考慮するには、バースト値を 2 倍にすることを推奨します。上記の例では、13 の推奨値は実際には

26 として設定されました。

もう 1 つの重要なポイントは、時間間隔 0 (つまり、ポリシング サイクルの開始時点) で、トークン バケットはトークンでいっぱいになる点です。

現在、この集約ポリシーは QoS ACE に組み込む必要があります。ACE は、着信フレームに対する一連の基準を満たすように、仕様を作成する場所です。次の例について考えます。上で定義した集約をすべての IP トラフィック、特にサブネット 10.5.x.x を発信元とし、サブネット 203.100.45.x を宛先とするトラフィックに適用するものとします。このときの ACE は次のようになります。

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

上記のコマンドでは、IP ACE (**set qos acl ip コマンドを使用したことで判明) を作成し、test-acl という QoS ACL に関連付けています。**この後に作成されて ACL test-acl に関連付けられる ACE は、この ACE リストの末尾に追加されます。ACE エントリには、集約 test-flow が関連付けられています。10.5.0.0 の送信元サブネットと 203.100.45.0 の宛先サブネットを持つ TCP フローに、このポリシーが適用されます。

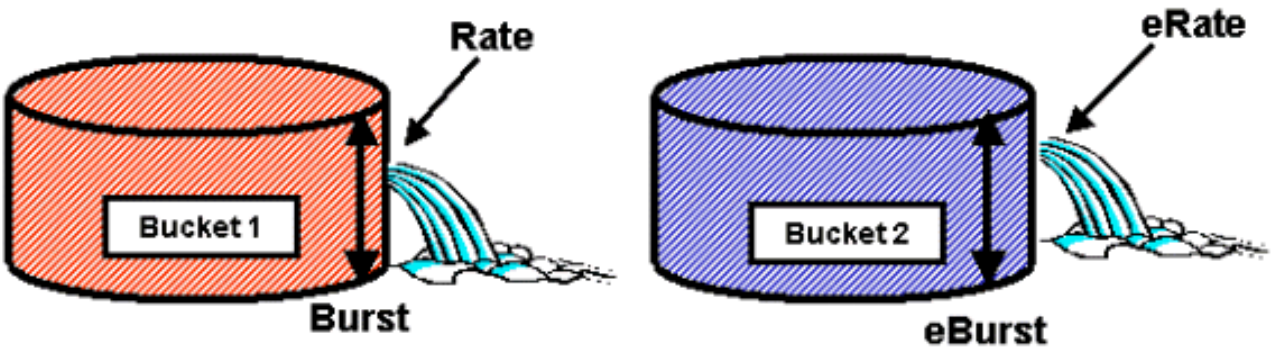
ACL (および関連 ACE) によって、管理者は柔軟に非常にきめ細かいレベルで設定することができます。ACL は 1 つまたは複数の ACE で構成され、ポリシングする必要がある特定のフローを識別するために、送信元および/または宛先アドレスと L4 ポート値を使用できます。

ただし、ポリシングが実際に発生する前に、ACL を物理ポートまたは VLAN にマップする必要があります。

PFC2 ポリシングの決定

PFC2 は、CatOS 7.1 および CatOS 7.2 で変更されています。ポリシングのデュアル リーキー バケット アルゴリズムが導入されました。この新しいアルゴリズムにより、次に示す 2 つのレベルが新しく追加されました。

1. **ポリシング通常レベル**これは最初のバケットに相当し、バケットの深さ (バースト) とバケットからデータが送出されるときのレート (レート) を指定するパラメータを定義します。
2. **ポリシング超過レベル**これは 2 番目のバケットに相当し、バケットの深さ (eburst) とバケットからデータが送出されるときのレート (erate) を指定するパラメータを定義します。



この処理が動作する方式は、最初のバケットにデータが入り始めるということになります。PFC2

では、最初のバケットの深さ（バースト値）以下の着信データ ストリームを受け入れます。最初のバケットからオーバーフローしたデータはマークダウンされ、2 番目のバケットに渡されます。2 番目のバケットでは、1 番目のバケットからオーバーフローしたデータを、eburst 値以下の着信レートで、受け入れることができます。2 番目のバケットからのデータは、erate パラメータから rate パラメータを引いたレートで送信されます。2 番目のバケットからオーバーフローしたデータは、マークダウンされるか、廃棄されます。

デュアル リーキー バケット ポリサーの例を次に示します。

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

この例では、10 Mbps を超えるトラフィック レートを持つ集約 AGG1 を設定し、ポリシングした DSCP マップに基づいてマークダウンを行います。erate（12 Mbps に設定）を超えるトラフィックは、キーワード drop が指定されているため、廃棄されます。

集約ポリサーの DFC 対応のモジュールへの適用

6000がフォワーディングトラフィックのために中央集中型フォワーディングエンジン(PFC)を使用することから、非DFCラインカードのアグリゲートポリサーのアプリケーションを取得できることに注目してください。中央集中型フォワーディング エンジンの実装により、所定の VLAN のトラフィック統計を追跡することが可能になりました。この処理は、集約ポリサーを VLAN に適用するために使用できます。

ただし、DFC 対応のラインカードでは、転送の決定はそのラインカードに伝達されます。DFC は直近のラインカード上のポートのみを認識し、他のラインカードのトラフィックの移動は認識しません。そのため、複数の DFC モジュールにわたってメンバー ポートが存在する VLAN に集約ポリサーが適用される場合、ポリサーは一貫性のない結果を生じさせる可能性があります。これは、DFC で追跡するのはローカルのポートの統計値だけであり、他のラインカード上のポートの統計値は対象にされていないためです。このため、集約ポリサーが DFC 対応ラインカードのメンバー ポートを使用する VLAN に適用されることによって、DFC は DFC ラインカードのみに存在する VLAN ポートのレート制限までトラフィックをポリシングすることになります。

DSCP マークダウン マップ（CatOS）

DSCP マークダウン マップは、プロファイル外のトラフィックを廃棄せずにマークダウンするようにポリサーを定義するときに使用します。プロファイル外のトラフィックとは、定義されたバースト設定を超過したトラフィックです。

QoS が有効なときに、デフォルトの DSCP マークダウン マップが設定されます。デフォルトのマークダウン マップは、前出のこの表で示されています。管理者は、コマンドライン インターフェイス（CLI）で **set qos policed-dscp-map コマンドを発行すると、デフォルトのマークダウン マップを変更できます。**次にこの例を示します。

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

この例では、ポリシングされている DSCP マップを変更し、20 から 25 の DSCP 値を 7 に、33 から 38 の DSCP 値を 3 にマークダウンしています。

VLAN とポート（CatOS）へのポリシーのマッピング

ACL を作成したら、その ACL を適用するポートまたは VLAN にマップする必要があります。

関係するコマンドの 1 つであり、あまり気付かれていないものに、すべての QoS をポート ベースにするデフォルトの QoS 設定があります。VLAN に集約（またはマイクロフロー）を適用して

も、ポートが VLAN ベースの QoS に対して設定されていない限り、そのポートでは有効になりません。

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

ポート ベースの QoS を VLAN ベースの QoS に変更すると、そのポートに割り当てられたすべての ACL が切り離され、そのポートに VLAN ベースの ACL が割り当てられます。

次のコマンドを発行して、ポート（または VLAN）に ACL をマップします。

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

ACL をポート（または VLAN）にマップしても、ACL がハードウェアにコミットされるまでその ACL は有効にはなりません。このことについては、次のセクションで説明します。この時点で、ACL はメモリ内の一時的なエディット バッファに置かれます。ACL がこのバッファにある間は変更を加えることができます。

エディット バッファに存在するコミットされていない ACL を削除する場合、**rollback コマンドを発行します。**このコマンドにより、ACL がエディット バッファから削除されます。

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

ACL のコミット（CatOS）

上で定義した QoS ACL を適用するには、この ACL がハードウェアにコミットされる必要があります。コミット処理では、ACL が一時的なバッファから PFC ハードウェアにコピーされます。PFC メモリに読み込まれると、この QoS ACL で定義されているポリシーが、ACE の条件を満たすすべてのトラフィックに適用されます。

設定を簡単にするため、ほとんどの管理者は **commit all コマンドを発行します。**ただし、エディット バッファに現在存在している可能性のある特定の ACL（1 つまたは複数）をコミットすることもできます。commit コマンドの例を、次に示します。

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

ポート（VLAN）から ACL を削除する場合、次のコマンドを発行して、その ACL をそのポート（VLAN）に関連付けているマップをクリアする必要があります。

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

統合Cisco IOS (ネイティブモード) を実行するCatalyst 6000 ファミリーのポリシングの設定

ポリシングは統合 Cisco IOS (ネイティブ モード) でもサポートされています。 ただし、ポリシング機能の設定と実装はポリシー マップを使用して実行します。それぞれのポリシー マップで複数のポリシー クラスを使用してポリシー マップを作成し、これらのポリシー クラスを異なるタイプのトラフィック フローに定義できます。

ポリシー マップ クラスでは、フィルタリングの際に IOS ベースの ACL とクラス マッチ文を使用して、トラフィックをポリシングするかどうかが判定されます。ポリシングを受けるトラフィックが識別されると、ポリシー クラスが集約またはマイクロフロー ポリサーを使用して、ポリシング用ポリシーをそのトラフィックに適用します。

次のセクションでは、統合 Cisco IOS (ネイティブ モード) でのポリシングの設定について、詳しく説明します。

集約とマイクロフロー (統合 Cisco IOS (ネイティブ モード))

集約とマイクロフローは、PFC が実行するポリシングの範囲を定義するために使用される条件です。CatOS の場合と同様に、統合 Cisco IOS (ネイティブ モード) でも集約とマイクロフローが使用されます。

マイクロフローは、単一フローのポリシングを定義します。フローは、一意の SA/DA MAC アドレス、SA/DA IP アドレス、および TCP/UDP ポート番号を持つセッションによって定義されます。VLAN のポートを介して開始される新しい各フローに対して、スイッチがそのフローのために受信するデータ量を制限するためにマイクロフローを使用できます。マイクロフローの定義では、所定のレート制限を超過したパケットを廃棄するか、またはそれらのパケットの DSCP 値をマーク ダウンすることができます。マイクロフローは、ポリシー マップ クラスの一部を形成する police flow コマンドを使用して適用します。

統合 Cisco IOS (ネイティブ モード) でマイクロフロー ポリシングをイネーブルにするには、スイッチ上でグローバルにイネーブルにする必要があります。これには、次のコマンドを実行します。

```
Cat6500(config)# mls qos flow-policing
```

マイクロフロー ポリシングは、L3 スイッチドではないトラフィックのブリッジド トラフィックにも適用できます。スイッチでブリッジ トラフィックに対するマイクロフロー ポリシングがサポートされるようにするには、次のコマンドを実行します。

```
Cat6500(config)# mls qos bridged
```

このコマンドは、マルチキャスト トラフィックに対するマイクロフロー ポリシングもイネーブルにします。マイクロフロー ポリサーが適用される必要のあるマルチキャスト トラフィックは、**mls qos bridged** コマンドを有効にする必要があります。

マイクロフローと同様に、集約も、トラフィックをレート制限するために使用できます。ただし、集約レートは、指定した QoS ACL に一致するポートまたは VLAN に着信するすべてのトラフィックに適用されます。集約は、定義されたトラフィック プロファイルに一致する累積的なトラフィックのポリシングであると見なすことができます。

統合 Cisco IOS (ネイティブ モード) では、次の 2 つの形式の集約を定義できます。

- インターフェイス単位の集約ポリサー

- 名前付き集約ポリサー

インターフェイス単位の集約は、ポリシー マップ クラスで **police コマンドを発行することにより、個々のインターフェイスに適用されます。**これらのマップ クラスは、複数のインターフェイスにマップできますが、ポリサーは各インターフェイスに個別に適用されます。名前付き集約は、ポートのグループに適用され、すべてのインターフェイスのトラフィックを累積方式でポリシングします。名前付き集約は、**mls qos aggregate policer コマンドを発行して適用します。**

マイクロフローを定義するときには最大 63 件まで、また集約は 1023 件まで定義できます。

ポリシング ルールの作成（統合 Cisco IOS（ネイティブ モード））

ポリシング ルールを作成するには、ポリシー マップで集約（またはマイクロフロー）を作成した後、このポリシー マップをインターフェイスに関連付ける処理が必要です。

CatOS 用に作成したのと同じ例を考慮します。要件は、ポート 5/3 に着信するすべての IP トラフィックを、最大 20 Mbps に制限することです。

最初に、ポリシー マップを作成する必要があります。limit-traffic という名前のポリシー マップを作成します。これは、次の手順で実行します。

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

スイッチのプロンプトが変わり、マップ クラスを作成する設定モードに入ったことがすぐに分かります。ポリシー マップには複数のクラスを含めることができることを思い出してください。各クラスには、異なるトラフィック ストリームに適用できるポリシー アクションの別個のセットが含まれます。

ここでは、着信トラフィックを 20 Mbps に制限するトラフィック クラスを作成します。このクラスをlimit-to-20と呼びます。次に示します。

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

再びプロンプトが変わり、マップ クラスを設定中であることが示されます（プロンプトの末尾に -c と表示されています）。 レート制限を適用して特定の着信トラフィックに一致させる場合、ACL を設定し、それをクラス名に適用することができます。20 Mbps の制限をネットワーク 10.10.1.x から送信されるトラフィックに適用する場合、次の ACL を発行します。

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

この ACL をこのクラス名に追加するには、次のようにします。

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

クラス マップを定義すると、このクラスに個々のポリサーを定義できるようになり、集約（キー

ワード police を使用）またはマイクロフロー（キーワード police flow を使用）を作成できます。次に示すように、集約を作成します。

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上記の class 文では、（**police コマンド）で 20,000 K（20 Mbps）のレート制限を 52 Mbps（13000 × 4000 = 52 MB）のバースト値とともに設定しています。** トラフィックがプロファイルに一致し、それがレート制限内である場合、confirm-action ステートメントで設定し、プロファイル内のトラフィックを送信します。トラフィックがプロファイル外である（つまりこの例では、20 MB の制限を超えている）場合、トラフィックを廃棄するように exceed-action ステートメントを設定します（つまりこの例では、20 MB を超えるすべてのトラフィックは廃棄されます）。

マイクロフローの定義には、同様の操作を行います。特定のクラス マップに一致するポートへのすべてのフローにレート制限（それぞれ 200 K）を適用する場合、そのフローの設定は次のようになります。

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

DSCP マークダウン マップ

DSCP マークダウン マップは、プロファイル外のトラフィックを廃棄せずにマークダウンするようにポリサーを定義するときに使用します。プロファイル外のトラフィックとは、定義されたバースト設定を超過したトラフィックです。

QoS が有効なときに、デフォルトの DSCP マークダウン マップが確立されます。このデフォルト マークダウン マップは、前出のこの表で示されています。CLI を使用して、**set qos policed-dscp-map コマンドを発行すると、デフォルトのマークダウン マップを変更できます。**次にこの例を示します。

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

この例では、DSCP値32がDSCP値16にマークダウンされるデフォルトのポリシングされたDSCPマップの変更を定義します。このポリサーが定義されているポートでは、指定されたバーストを超えるデータブロックの一部である着信データは、DSCP値11116に16。

ポリシーの VLAN とポートへのマップ（統合 Cisco IOS（ネイティブ モード））

ポリシーを作成したら、そのポリシーを有効にするために、適用するポートまたは VLAN にマッ

プする必要があります。CatOS でのコミット処理とは異なり、統合 Cisco IOS (ネイティブ モード) には、これに相当する処理はありません。 ポリシーがインターフェイスにマップされると、そのポリシーは有効になります。上記のポリシーをインターフェイスにマップするには、次のコマンドを使用します。

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

ポリシーを VLAN にマップする場合、VLAN ポリシーを適用したい VLAN の各ポートに対し、**mls qos vlan-based コマンドを発行することによって、インターフェイスに QoS が VLAN ベースであるであることを通知する必要があります。**

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

インターフェイス 3/5 が VLAN 100 の一部であること、また VLAN 100 に適用される limit-traffic という名前のポリシーがインターフェイス 3/5 に適用されることが想定されています。

CatOS を使用するCatalyst 6000 ファミリーでの分類の設定

PFC には、L2、L3、および L4 ヘッダー情報を調べられる ACL を使用する、データの分類のサポートを導入されています。SupI または IA (PFC なし) では、分類はポートでの trust キーワードの使用に限定されます。

次のセクションでは、CatOS で PFC が分類に使用する QoS の設定要素について説明します。

CoS の DSCP へのマップ (CatOS)

スイッチにフレームが着信する際には、スイッチによってフレームに DSCP 値が設定されます。ポートが信頼できない状態にあり、管理者が trust-COs キーワードを使用した場合、フレームに設定された DSCP 値を判別するため、フレームで設定された CoS 値が使用されます。前述のように、スイッチは、内部 DSCP 値に基づいてスイッチを通過する際にサービス レベルをフレームに割り当てることができます。

初期の 10/100 モジュール (WS-X6248 および WS-X6348) では、このキーワードはサポートされていません。これらのモジュールでは、受信データの CoS 設定を適用するために、ACL を使用することが推奨されています。

QoS をイネーブルにすると、スイッチではデフォルト マップが作成されます。このマップは、CoS 値に基づいて設定される DSCP 値を指定するために使用されます。このマップについては、前出のこの表で示しています。別の方法として、管理者は固有のマップを設定できます。次にこの例を示します。

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

上記のコマンドでは、次のようなマップを設定しています。

CoS	0	1	0	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

上記のマップが、実際のネットワークで使用されることはまずありませんが、このコマンドで実行できることの説明のために提示してあります。

IP 優先順位の DSCP へのマップ (CatOS)

CoS から DSCP へのマッピングと同様に、フレームの DSCP 値を着信パケットの IP 優先順位の設定から決めることもできます。これは、ポートが管理者によって信頼できると設定された場合にだけ行われ、これにはキーワード trust-ipprec を使用します。

QoS をイネーブルにすると、スイッチではデフォルト マップが作成されます。このマップについては、前出のこの表を参照できます。このマップは、IP 優先順位の値に基づいて設定される DSCP 値を指定するために使用されます。別の方法として、管理者は固有のマップを設定できます。次に例を示します。

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

上記のコマンドでは、次のようなマップを設定しています。

IP Precedence	0	1	0	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

上記のマップが、実際のネットワークで使用されることはまずありませんが、このコマンドで実行できることの説明のために提示してあります。

分類 (CatOS)

フレームが PFC に渡されると、そのフレームに対する分類の処理が行われます。PFC では、事前に定義された ACL (またはデフォルト ACL) を使用して、フレームに DSCP 値を割り当てます。ACE の内部では、DSCP 値の割り当てに、4 つのキーワードのいずれかを使用します。あります。

1. TRUST-DSCP (IP ACL だけ)
2. TRUST-IPPREC (IP ACL だけ)
3. TRUST-COS (PFC2 の IPX および MAC を除くすべての ACL)
4. DSCP

キーワード TRUST-DSCP では、PFC に到達したフレームには、スイッチに着信する前にすでに DSCP 値が設定されているものと仮定されています。スイッチでは、この DSCP 値が維持されます。

TRUST-IPPREC では、PFC が DSCP 値を、ToS フィールドにある既存の IP 優先順位値を元にして設定します。PFC は、IP 優先順位から DSCP へのマップを使用して、正しい DSCP 値を割り当てます。QoS がスイッチで有効な場合に、デフォルト マップが作成されます。または、管理者によって作成されたマップを使用して、DSCP 値を取得することもできます。

TRUST-IPPREC と同様に、キーワード TRUS-COS でも、PFC に対して DSCP 値をフレーム ヘッダーの CoS を元にして設定するように指示されます。この場合も CoS から DSCP へのマップがあり (デフォルトまたは管理者が割り当てたもの)、PFC が DSCP を決定するために使用されます。

DSCP キーワードは、フレームが信頼できないポートから着信した場合に使用されます。これは、DSCP 値の設定に関する興味深い状況を表しています。この時点で、set qos acl ステートメントに設定されている DSCP を使用して、DSCP を取得します。しかし、ACE で設定された分類基準に基づいてトラフィックの DSCP を取得するために ACL を使用できるのは、この時点です。このことは、ACE では、トラフィックの識別に、発信元と宛先の IP アドレス、TCP/UDP ポート番号、ICMP コード、IGMP タイプ、IPX ネットワーク番号およびプロトコル番号、発信元および宛先の MAC アドレス、イーサタイプ（非 IP および非 IPX のトラフィックに限定）などの分類基準を使用できることを意味しています。これはつまり、FTP トラフィック上の HTTP トラフィックなどに特定の DSCP 値を割り当てるように、ACE を設定できることになります。

以下のようになります。

```
Console> (enable) set port qos 3/5 trust untrusted
```

ポートを信頼できないとして設定することにより、PFC には、ACE を使用してフレームに DSCP を設定するように指示されます。分類基準を使用して ACE が設定された場合、そのポートからの個々のフローは、別の優先順位で分類することができます。次の ACE はこれを表しています。

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

この例では、2 つの ACE ステートメントがあります。最初のACEは、ポート番号が80(80 = HTTP)でDSCP値が32に割り当てられるTCPフロー（送信元と宛先のトラフィックを識別するためにキーワードanyを使用）を識別します。2番目のACEは、DSCP値11611111116。

統合Cisco IOS (ネイティブモード) を実行するCatalyst 6000 ファミリーの分類の設定

次のセクションでは、統合 Cisco IOS（ネイティブ モード）により、PFC での分類のサポートに使用される QoS の設定要素について説明します。

CoS の DSCP へのマップ（統合 Cisco IOS（ネイティブ モード））

スイッチにフレームが着信する際には、スイッチによってフレームに DSCP 値が設定されます。ポートが信頼できない状態にあり、管理者が mls qos trust-COs キーワードを使用した（WS-X6548 ラインカード上の GE ポートまたは 10/100 ポートで）場合、フレームに設定された DSCP 値を判別するため、フレームで設定された CoS 値が使用されます。前述のように、スイッチは、内部 DSCP 値に基づいてスイッチを通過する際にサービス レベルをフレームに割り当てることができます。

QoS をイネーブルにすると、スイッチではデフォルト マップが作成されます。デフォルト設定については、前出のこの表を参照してください。このマップは、CoS 値に基づいて設定される DSCP 値を指定するために使用されます。別の方法として、管理者は固有のマップを設定できます。次にこの例を示します。

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

上記のコマンドでは、次のようなマップを設定しています。

CoS	0	1	0	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

上記のマップが、実際のネットワークで使用されることはまずありませんが、このコマンドで実行できることの説明のために提示してあります。

IP 優先順位の DSCP へのマップ (統合 Cisco IOS (ネイティブ モード))

CoS から DSCP へのマッピングと同様に、フレームの DSCP 値を着信パケットの IP 優先順位の設定から決めることもできます。これは、ポートが管理者によって信頼できると設定された場合にだけ行われ、これにはキーワード mls qos trust-ipprec を使用します。このキーワードは、WS-X6548 ラインカードの GE ポートおよび 10/100 ポートでだけサポートされています。WS-X6348 および WS-X6248 ラインカード上の 10/100 ポートでは、IP 優先順位の信頼を受信データに割り当てるため ACL を使用する必要があります。

QoS をイネーブルにすると、スイッチではデフォルト マップが作成されます。デフォルト設定については、前出のこの表を参照してください。 このマップは、IP 優先順位の値に基づいて設定される DSCP 値を指定するために使用されます。別の方法として、管理者は固有のマップを設定できます。次にこの例を示します。

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

上記のコマンドでは、次のようなマップを設定しています。

IP Precedence	0	1	0	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

上記のマップが、実際のネットワークで使用されることはまずありませんが、このコマンドで実行できることの説明のために提示してあります。

分類 (統合 Cisco IOS (ネイティブ モード))

フレームが PFC に渡されると、分類処理を実行して、着信フレームに新しい優先順位を割り当てられます。ここでの重要な点は、この処理はフレームが信頼できないポートから送られたものであるか、フレームが信頼できないとして分類されている場合にだけ行われることです。

ポリシー マップ クラスのアクションを使用できます。

1. TRUST COs
2. TRUST IP-PRECEDENCE
3. TRUST DSCP
4. NO TRUST

キーワード TRUST DSCP では、PFC に到達したフレームには、スイッチに着信する前にすでに DSCP 値が設定されているものと仮定されています。スイッチでは、この DSCP 値が維持されます。

TRUST IP-PRECEDENCE では、PFC が DSCP 値を ToS フィールドにある既存の IP 優先順位値を元にして設定します。PFC では IP 優先順位から DSCP へのマップを使用して、正しい DSCP 値を割り当てます。QoS がスイッチで有効な場合に、デフォルト マップが作成されます

。または、管理者によって作成されたマップを使用して、DSCP 値を取得することもできます。

TRUST IP-PRECEDENCE と同様に、キーワード TRUST COs でも、PFC に対して DSCP 値をフレーム ヘッダーの CoS を元にして設定するように指示されます。この場合も CoS から DSCP へのマップがあり（デフォルトまたは管理者が割り当てたもの）、PFC が DSCP を決定するために使用されます。

既存の優先順位（DSCP、IP 優先順位、または CoS）から DSCP 取得する例を以下に示します。

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上のクラス マップでは、イーサネット ヘッダーの CoS から DSCP 値を得ています。

キーワード NO TRUST は、フレームが信頼できないポートから着信したときに使用されます。これによって、ポリシング処理の際にフレームに DSCP 値を割り当てることができるようになります。

以下のポリシー定義を使用して PFC に入ってくる別のフローに新しい優先順位（DSCP）を割り当てる方法を示す次の例について考えます。

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

上の例では、次のことが示されています。

1. ポートに入ってくる http フローを識別するために作成された ACL。
2. new-dscp-for-flow と呼ばれるポリシー マップ。
3. このクラス マップがアクションを実行する対象となるトラフィックを識別するためにアクセス リスト 102 を使用するクラス マップ（名前は test）。
4. クラス マップ test は、着信フレームの信頼状態を信頼できないとして設定し、そのフローに DSCP 値 24 を割り当てる。
5. さらに、このクラス マップは、すべての http フローの集約を最大 1 MB に制限。

Common Open Policy Server (COPS)

COPS は、Catalyst 6000 ファミリでリモート ホストから QoS を設定できるようにするプロトコルです。COPS は、QoS の intserv アーキテクチャの一部で、現在 CatOS の使用のみをサポートしています。現在（この文書の作成時点）、統合 Cisco IOS（ネイティブ モード）を使用している場合には、COPS はサポートされていません。 COPS プロトコルは QoS 設定情報をスイッチに搬送するものであり、QoS 設定情報の発信元ではありません。COPS プロトコルを使用するに

は、スイッチ向けの QoS 情報をホスティングする外部 QoS マネージャが必要です。外部 QoS マネージャは、COPS プロトコルを使用して、設定情報のスイッチへの送出を起動します。シスコの QoS Policy Manager（QPM）は、外部 QoS マネージャの一例です。

QPM の機能について説明することはこのドキュメントの目的ではありませんが、外部 QoS 設定をサポートするために、QPM を使用するスイッチに必要な設定について説明しています。

COPSの設定

デフォルトでは、COPS のサポートは無効になっています。スイッチで COPS を使用するには、これをイネーブルにする必要があります。これには、次のコマンドを実行します。

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

このコマンドが起動されると、所定のデフォルトの QoS 設定値が COPS サーバから送られます。これらは、以下の内容を含みます：

1. CoS のキューへのマップ
2. 入力および出力キューのしきい値の割り当て
3. WRR 帯域幅の割り当て
4. 集約およびマイクロフローのポリシー
5. 出力トラフィック用の DSCP の CoS へのマップ
6. ACL
7. デフォルトのポート CoS 割り当て

COPS を使用して QoS 設定を行う場合には、これらの設定の適用方法が他とは異なることを理解しておくことが重要です。COPS は、ポートを直接設定するよりも、ポート ASIC の設定に使用されます。通常、ポート ASIC はポートのグループを制御するため、COPS による設定は、同時に多数のポートに適用されます。

設定されるポート ASIC は、GE ASIC です。GE ラインカードには、GE ごとに 4 つのポート（1 ~ 4、5 ~ 8、9 ~ 12、13 ~ 16）があります。 これらのラインカードでは、COPS の設定はポートの各グループに対して効力があります。このドキュメントですでに説明したように、10/100 ラインカードには、GE と 10/100 ASIC という 2 つの ASIC のグループが存在します。10/100 ASIC 4 つに対して GE ASIC が 1 つあります。各 10/100 ASIC は 12 個の 10/100 ポートをサポートします。COPS は GE ASIC を設定します。したがって、COPS を使用して QoS 設定を 10/100 ラインカードに適用すると、その設定は 48 個の 10/100 ポートすべてに適用されます。

set qos policy-source cops コマンドを発行して COPS のサポートを有効にすると、COPS による QoS 設定が、スイッチのシャーシにあるすべての ASIC に適用されます。特定の ASIC に COPS 設定を適用することができます。これには、次のコマンドを使用します。

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

上のコマンドを実行することで、このコマンドは GE モジュールに対して発行され、4 つのポートがこのコマンドの影響を受けることが分かります。

Policy Decision Pointサーバ およびドメイン名

Policy Decision Point Server（PDPS）は、スイッチへ送出する QoS 設定の詳細を保存するため

に使用される外部ポリシー マネージャです。スイッチで COPS を有効にする場合、QoS 設定の詳細をスイッチに提供する外部マネージャの IP アドレスを使用してスイッチを設定する必要があります。これは、SNMP をイネーブルにしている場合に、SNMP マネージャの IP アドレスを指定するようなものです。

外部 PDPS を指定するコマンドは、次のように実行します。

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```

上記のコマンドでは、デバイス 192.168.1.1 をプライマリの PDPS として指定しています。

スイッチが PDPS と通信する際には、PDPS で定義されているドメインに属している必要があります。PDPS は、定義されているドメインに参加しているスイッチとしか通信しないため、スイッチは PDPS が属している COPS ドメインを識別するよう設定する必要があります。この作業を行うには、次のコマンドを発行します。

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

上のコマンドは、スイッチが remote-cat6k という名前のドメインに属すように設定されていることを示しています。このドメインは QPM で定義されている必要があり、スイッチもこのドメインに属している必要があります。

関連情報

- スイッチ製品に関するサポート ページ
- LAN スイッチング テクノロジーに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems
