CHAPTER 42

PFC QoS の設定

この章では、Catalyst 6500 シリーズ スイッチの Policy Feature Card（PFC; ポリシー フィーチャ カード）および Distributed Forwarding Card（DFC）に実装された Quality of Service（QoS; サービス品質）機能を設定する方法について説明します。

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の URL の『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』Release 12.2SX を参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm
- QoS および MPLS の詳細については、第 43 章「PFC3BXL または PFC3B モード MPLS QoS の設定」を参照してください。
- Catalyst 6500 シリーズ スイッチの QoS（PFC QoS）では、Cisco IOS のモジュール型 QoS CLI（MQC）をいくつか使用します。PFC QoS はハードウェアに実装されているため、一部の MQC 構文のみがサポートされます。
- PFC3 は、Network-Based Application Recognition（NBAR）をサポートしていません。
- Supervisor Engine 2、PFC2、および Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を使用すると、レイヤ 3 インターフェイスに、PFC QoS の代わりに NBAR を設定できます。
  - PFC2 は、NBAR を設定したポートで、入力 Access Control List（ACL; アクセス制御リスト）をハードウェアでサポートします。
  - PFC QoS がイネーブルの場合、NBAR を設定しているポートを通過するトラフィックは、入力キュー、出力キューおよび廃棄スレッシュホールドを通過します。
  - PFC QoS がイネーブルの場合、MSFC2 は、NBAR トラフィック内の出力 IP precedence と等しくなるように出力 CoS を設定します。
  - 入力キューの通過後、すべてのトラフィックは、NBAR を設定したインターフェイス上の MSFC2 ソフトウェアで処理されます。
  - NBAR を設定するには、次のマニュアルを参照してください。
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

この章で説明する内容は、次のとおりです。

- PFC QoS の機能概要（p.42-2）
- PFC QoS のデフォルト設定（p.42-29）
- PFC QoS 設定時の注意事項および制約事項（p.42-50）
- PFC QoS の設定（p.42-56）

- 一般的な QoS のシナリオ（p.42-113）
- PFC QoS の用語（p.42-124）

PFC QoS の機能概要

「PFC QoS」という用語は、Catalyst 6500 シリーズ スイッチに実装された QoS を意味します。PFC QoS は PFC やすべての DFC のほか、さまざまなスイッチ コンポーネントに実装されます。ここでは、PFC QoS の機能について説明します。

- PFC QoS によってサポートされるポート タイプ（p.42-2）
- 概要（p.42-2）
- コンポーネントの概要（p.42-6）
- 分類とマーキングの概要（p.42-16）
- ポートベースのキュー タイプの概要（p.42-22）

PFC QoS によってサポートされるポート タイプ

PFC は、FlexWAN モジュール ポートに対して QoS を提供しません。FlexWAN モジュール の QoS 機能については、次の資料を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/flexport/combo/index.htm

すべてのリリースで、PFC QoS は *LAN ポート*をサポートします。LAN ポートとは、4 ポート ギガビット イーサネット WAN（GBIC）モジュール（OSM-4GE-WAN および OSM-2+4GE-WAN+）を除く、イーサネット スイッチング モジュール上のイーサネット ポートです。一部の OSM は、WAN ポートのほかに 4 つのイーサネット LAN ポートを備えています。

Release 12.2(17b)SXA 以降のリリースでは、PFC QoS は OSM（オプティカル サービス モジュール）ポートをサポートします。*OSM ポート*とは、OSM 上の WAN ポートです。その他の OSM QoS 機能については、次の資料を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm

概要

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

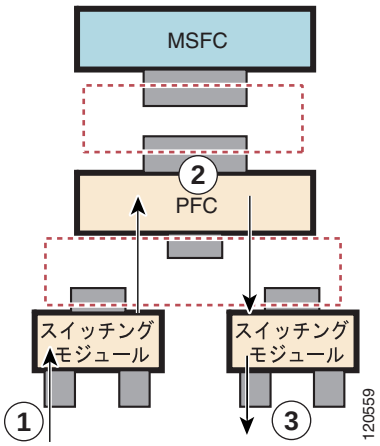
QoS を実装すると、ネットワーク パフォーマンスが予測可能になり、帯域幅をより効率的に利用できます。QoS 機能は、ネットワーク トラフィックを選択（分類）し、プライオリティを示す QoS ラベルを割り当て、使用します。これにより、パケットは設定されたリソース使用制限に従い（トラフィックのポリシングとマーキング）、リソースの競合が生じた場合に輻輳回避が行われます。

PFC QoS 分類、ポリシング、マーキング、および輻輳回避は、PFC、DFC、および LAN スイッチング モジュール ポートの Application Specific Integrated Circuit（ASIC; 特定用途向け IC）のハードウェアに実装されます。

（注）　Catalyst 6500 シリーズ スイッチでは、レイヤ 3 またはレイヤ 2 でハードウェアによってスイッチングされたトラフィックに対し、一部の MQC 機能（Committed Access Rate [CAR; 専用アクセス レート] など）がサポートされません。キューイングはポートの ASIC に実装されるため、Catalyst 6500 シリーズ スイッチでは、MQC によって設定したキューイングはサポートされません。

図 42-1 は、Catalyst 6500 シリーズ スイッチにおける QoS 処理の概要を示します。

図 42-1　PFC QoS 機能による処理の概要



各 PFC QoS 機能は、次の順序で適用されます。

1. 入力ポートの PFC QoS 機能：
   - ポートの信頼状態 — PFC QoS における *信頼* とは、有効なポートとして受け入れられ、初期内部 DSCP 値の基準として使用されることを意味します。デフォルトではポートは信頼されず（untrusted）、初期内部 DSCP 値は 0 に設定されます。各ポートは、受信する CoS、IP precedence、または DSCP を信頼するように設定できます。
   - レイヤ 2 の CoS 再マーキング — PFC QoS は、レイヤ 2 CoS の再マーキングを適用します。この機能では、次の状況において、受信フレームにポートの CoS 値がマークされます。
     — トラフィックの形式が ISL、802.1Q、または 802.1p フレームではない場合
     — ポートが非信頼ポートとして設定されている場合
     OSM ATM および POS ポートでは、PFC QoS は入力 CoS を常に 0 に設定します。
   - 輻輳回避 — イーサネット LAN ポートを CoS または DSCP を信頼するように設定している場合は、QoS はレイヤ 2 CoS 値またはレイヤ 3 DSCP 値に基づきトラフィックを分類し、入力キューに割り当てることで、輻輳回避を行います。レイヤ 3 DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートのみで有効です。
2. PFC および DFC QoS 機能：
   - 内部 DSCP — PFC および DFC 上で、QoS はすべてのトラフィックに内部 DSCP 値を関連付け、システム内で処理できるように分類します。トラフィックの信頼状態に基づいて生成される初期内部 DSCP 値、および最終内部 DSCP 値が存在します。最終内部 DSCP は、初期値と同じである場合も、MQC ポリシー マップによって別の値に設定される場合もあります。
   - MQC ポリシー マップ — MQC ポリシー マップでは、次の 1 つまたは複数の処理が実行されます。

— トラフィックの信頼状態の変更（内部 DSCP 値を別の QoS ラベルに基づいて設定）
— 初期内部 DSCP 値の設定（信頼できないポートからのトラフィックのみ）
— トラフィックのマーキング
— トラフィックのポリシング

3. 出力イーサネット LAN ポートの QoS 機能：
   - 最終内部 DSCP によるレイヤ 3 DSCP マーキング（PFC2 では標準、PFC3 ではオプション）
   - 最終内部 DSCP からのマッピングによるレイヤ 2 CoS マーキング
   - レイヤ 2 CoS ベース、およびレイヤ 3 DSCP ベースの輻輳回避（レイヤ 3 DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートのみで有効）

次の図は、QoS とスイッチ コンポーネント間の関係の詳細を示します。

- 図 42-2、PFC3 でのトラフィック フローおよび PFC QoS 機能
- 図 42-3、PFC2 でのトラフィック フローおよび PFC QoS 機能
- 図 42-4、PFC QoS 機能とコンポーネントの概要

図 42-2 は、PFC3 でのトラフィック フローと PFC QoS 機能を示します。

図 42-2　PFC3 でのトラフィック フローおよび PFC QoS 機能

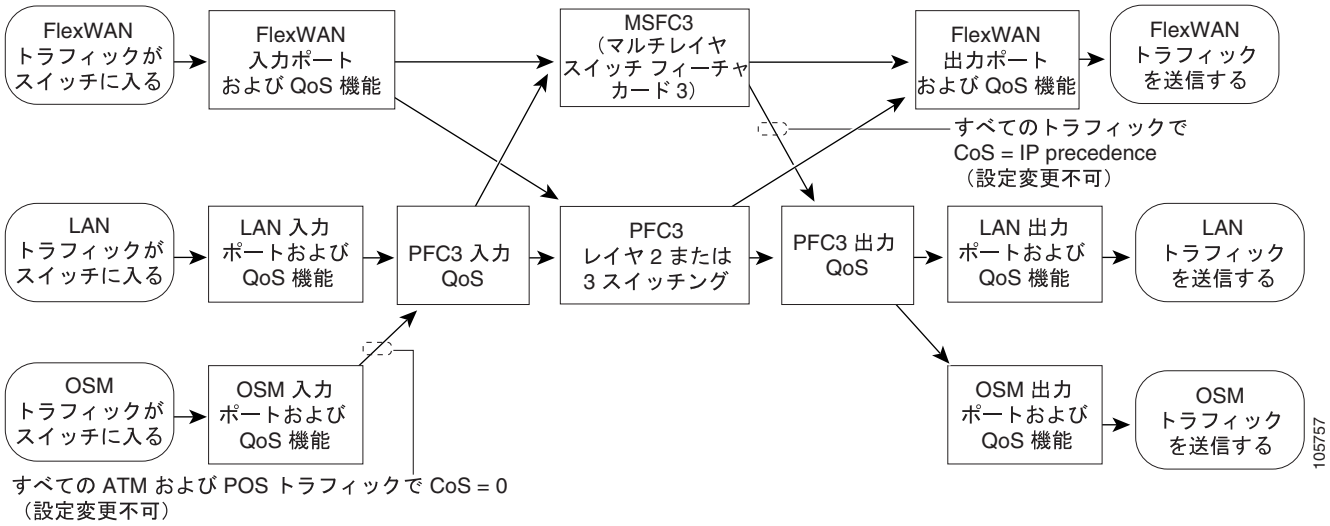


図 42-2 は、PFC3 の PFC QoS 機能間のトラフィック フローを示します。

- トラフィックは、どのタイプのポートからも入力および出力が可能です。
- DFC は、スイッチング モジュール上にローカルに PFC QoS を実装します。
- FlexWAN モジュール トラフィックの場合：
  - 入力 FlexWAN QoS 機能は、FlexWAN 入力トラフィックに適用できます。
  - 入力 FlexWAN トラフィックは、PFC3 によってレイヤ 3 スイッチングすることも、MSFC によってソフトウェアでルーティングすることも可能です。
  - 出力 PFC QoS は、FlexWAN 入力トラフィックには適用されません。
  - 出力 FlexWAN QoS は、FlexWAN 出力トラフィックに適用できます。
- LAN ポート トラフィックの場合：
  - 入力 LAN ポート QoS 機能は、LAN ポート入力トラフィックに適用できます。
  - 入力 PFC QoS は、LAN ポート入力トラフィックに適用できます。

- 入力 LAN ポート トラフィックは、PFC3 によってレイヤ 2 またはレイヤ 3 スイッチングすることも、MSFC によってソフトウェアでルーティングすることも可能です。
- 出力 PFC QoS および出力 LAN ポート QoS は、LAN ポート出力トラフィックに適用できます。

- OSM トラフィックの場合：
  - 入力 OSM ポート QoS 機能は、OSM ポート入力トラフィックに適用できます。
  - 入力 PFC3 QoS は、OSM ポート入力トラフィックに適用できます。
  - 入力 OSM ポート トラフィックは、PFC3 によってレイヤ 3 スイッチングすることも、MSFC によってソフトウェアでルーティングすることも可能です。
  - 出力 PFC3 QoS および出力 OSM ポート QoS は、OSM ポート出力トラフィックに適用できます。

図 42-3 は、PFC2 でのトラフィック フローと PFC QoS 機能を示します。

図 42-3　PFC2 でのトラフィック フローおよび PFC QoS 機能

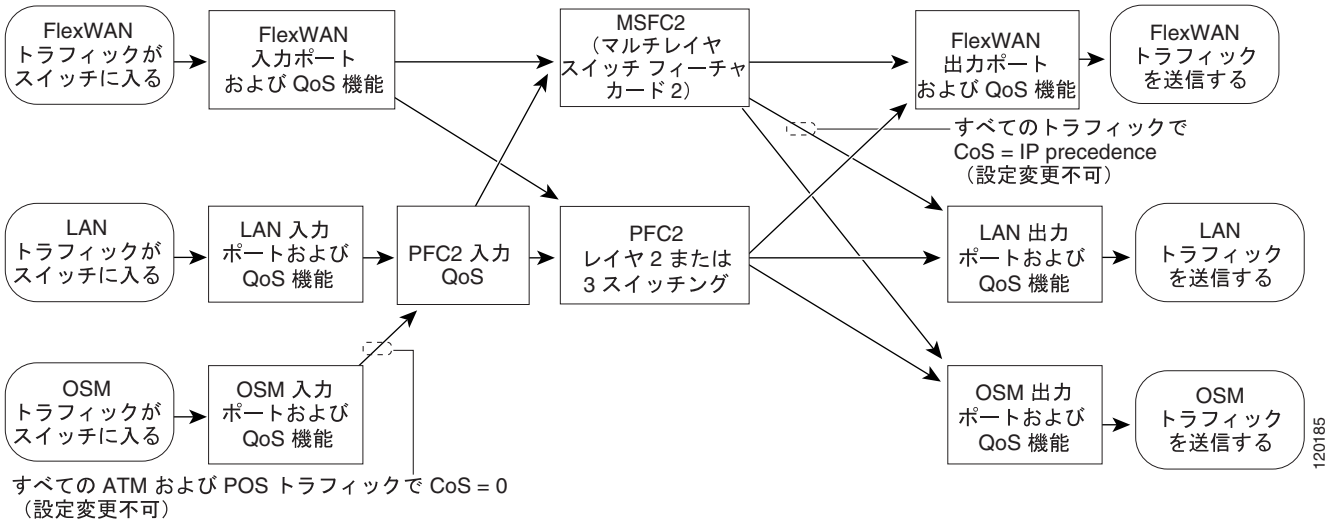
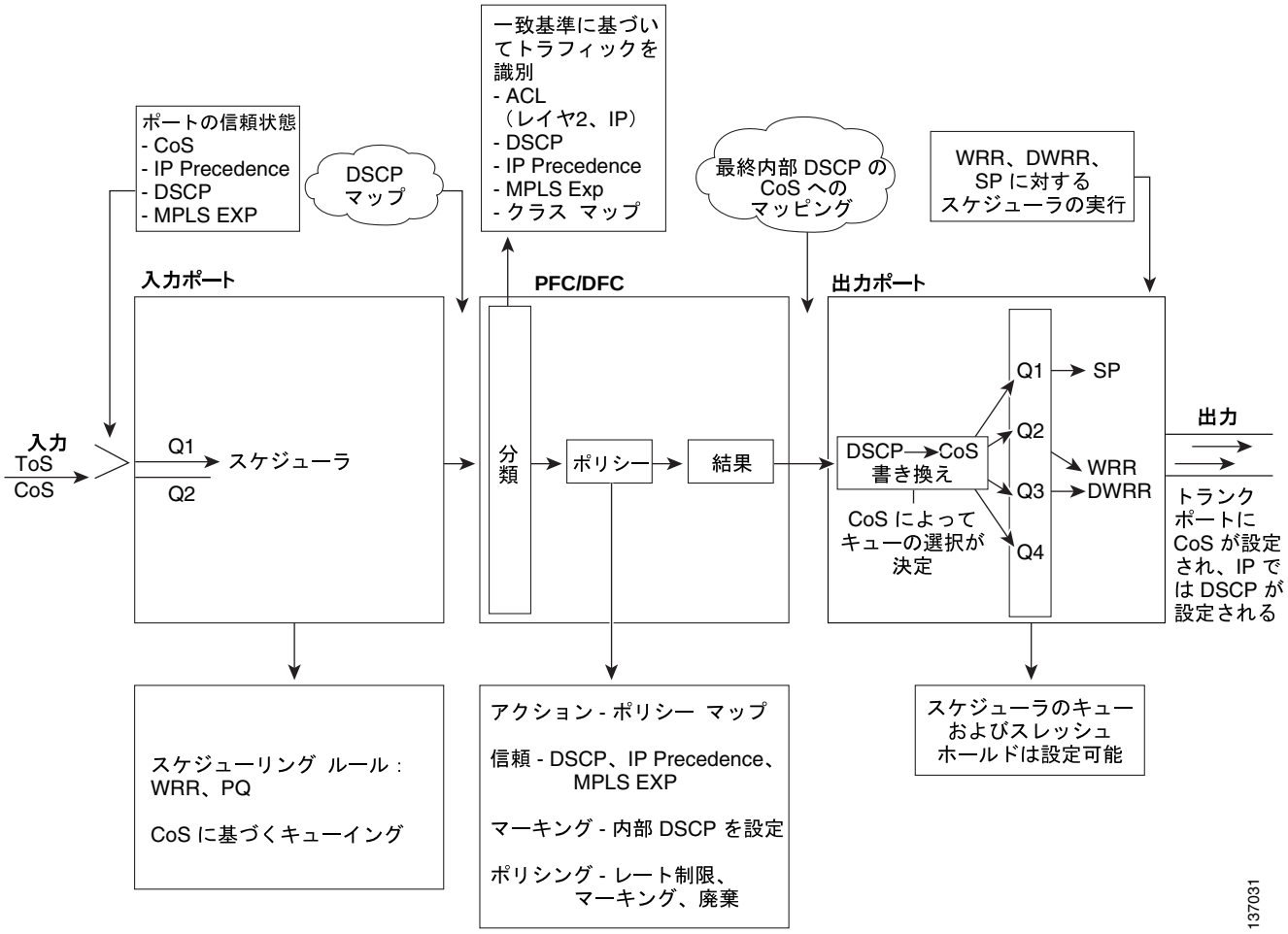


図 42-3 は、PFC2 での PFC QoS 機能間のトラフィック フローを示します。

- トラフィックは、どのタイプのポートからも入力および出力が可能です。
- DFC は、スイッチング モジュール上にローカルに PFC QoS を実装します。
- FlexWAN モジュール トラフィックの場合：
  - 入力 FlexWAN QoS 機能は、FlexWAN 入力トラフィックに適用できます。
  - 入力 FlexWAN トラフィックは、PFC2 によってレイヤ 3 スイッチングすることも、MSFC2 によってソフトウェアでルーティングすることも可能です。
  - 出力 FlexWAN QoS は、FlexWAN 出力トラフィックに適用できます。
- LAN ポート トラフィックの場合：
  - 入力 LAN ポート QoS 機能は、LAN ポート入力トラフィックに適用できます。
  - 入力 LAN ポート トラフィックは、PFC2 によってレイヤ 2 またはレイヤ 3 スイッチングすることも、MSFC2 によってソフトウェアでルーティングすることも可能です。
  - 出力 LAN ポート QoS は、LAN ポート出力トラフィックに適用できます。

- OSM トラフィックの場合：
  - OSM ポート QoS 機能は、OSM ポート入力トラフィックに適用できます。
  - 入力 PFC2 QoS は、OSM ポート入力トラフィックに適用できます。
  - OSM ポート入力トラフィックは、PFC2 によってレイヤ 3 スイッチングすることも、MSFC2 によってソフトウェアでルーティングすることも可能です。
  - 出力 OSM ポート QoS は、OSM ポート出力トラフィックに適用できます。

図 42-4　PFC QoS 機能とコンポーネントの概要



コンポーネントの概要

ここでは、PFC QoS の決定とプロセスにおける、次の各コンポーネントの役割について詳しく説明します。

- 入力 LAN ポートの PFC QoS 機能（p.42-7）
- PFC および DFC の QoS 機能（p.42-9）
- PFC QoS の出力ポート機能（p.42-12）

入力 LAN ポートの PFC QoS 機能

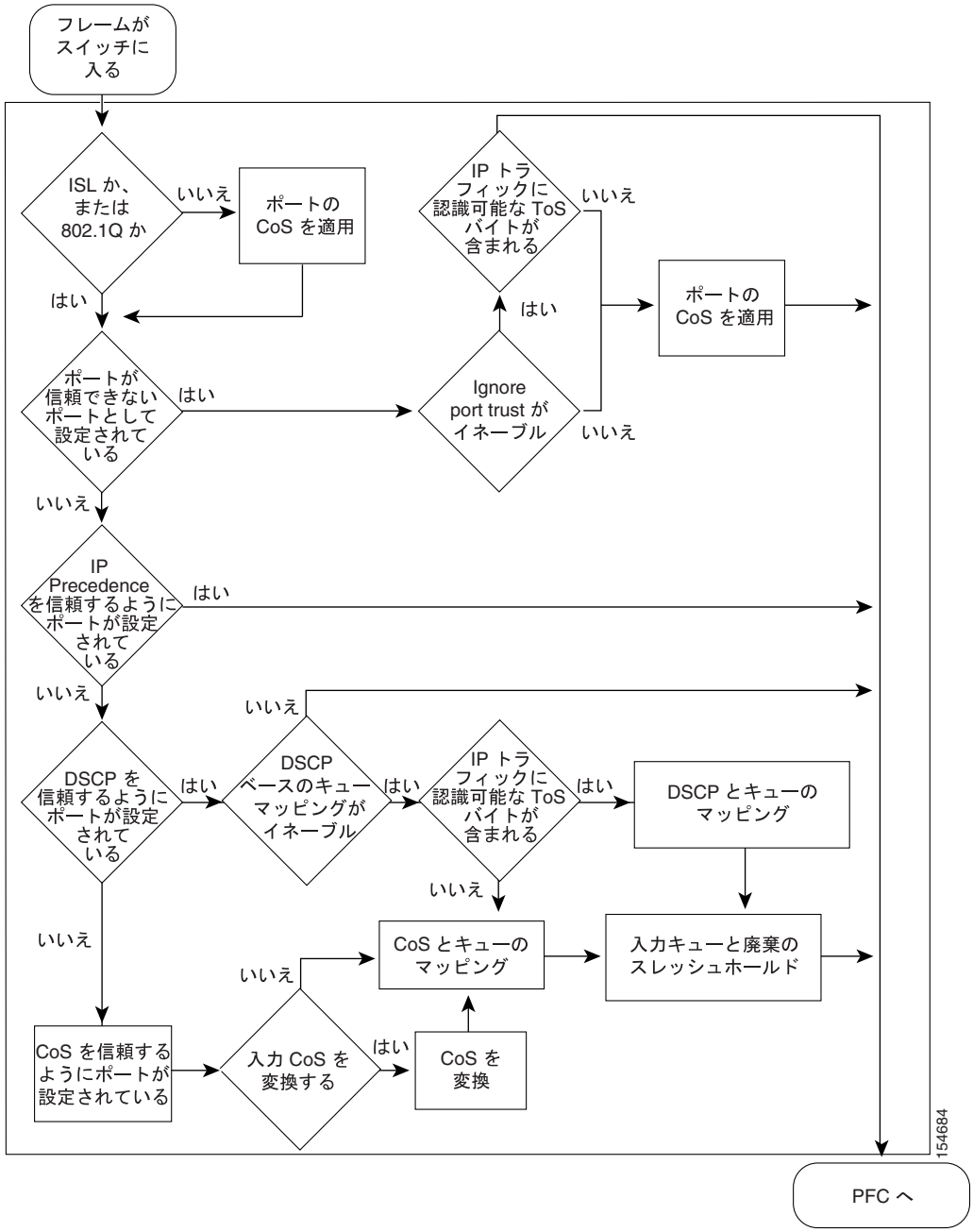
ここでは、入力ポートの QoS 機能の概要について説明します。

- 入力 LAN ポート PFC QoS 機能のフローチャート（p.42-7）
- ポートの信頼状態（p.42-8）
- 入力側の輻輳回避（p.42-8）

入力 LAN ポート PFC QoS 機能のフローチャート

図 42-5 は、入力 LAN ポートの PFC QoS 機能間のトラフィック フローを示します。

図 42-5　入力 LAN ポートの PFC QoS 機能



（注）
- 入力 CoS 変換は、802.1Q トンネル ポートのみでサポートされます。
- Release 12.2(18)SXF5 以降のリリースでは、ignore port trust 機能がサポートされます。
- DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートのみでサポートされます。

ポートの信頼状態

PFC QoS における*信頼*とは、有効なポートとして受け入れられ、初期内部 DSCP 値の基準として使用されることを意味します。ポートは、信頼できないポート（untrusted）として設定することも、次の QoS 値を信頼するように設定することもできます。

- レイヤ 2 CoS
  - CoS を信頼するように設定されたポートを、信頼できる CoS ポートと呼びます。
  - 信頼できる CoS ポートから受信するトラフィック、またはポリシー マップによって CoS を信頼するように設定されたトラフィックを、信頼できる CoS トラフィックと呼びます。

（注）すべてのトラフィックに CoS 値が含まれるわけではありません。CoS 値を伝送するのは、ISL、802.1Q、および 802.1P トラフィックのみです。PFC QoS は、CoS 値を伝送しないすべてのトラフィックに対し、ポートの CoS 値を適用します。信頼できないポートでは、PFC QoS はすべてのトラフィックにポートの CoS 値を適用し、受信したすべての CoS 値を上書きします。

- IP precedence
  - IP precedence を信頼するように設定されたポートを、信頼できる IP precedence ポートと呼びます。
  - 信頼できる IP precedence ポートから受信するトラフィック、またはポリシー マップによって IP precedence を信頼するように設定されたトラフィックを、信頼できる IP precedence トラフィックと呼びます。
- DSCP
  - DSCP を信頼するように設定されたポートを、信頼できる DSCP ポートと呼びます。
  - 信頼できる DSCP ポートから受信するトラフィック、またはポリシー マップによって DSCP を信頼するように設定されたトラフィックを、信頼できる DSCP トラフィックと呼びます。

信頼できないポートから受信したトラフィックを、信頼できないトラフィックと呼びます。

入力側の輻輳回避

PFC QoS は、信頼できる CoS ポートに輻輳回避を実装します。信頼できる CoS ポートでは、QoS はレイヤ 2 の CoS 値に基づきトラフィックを分類して入力キューに割り当て、輻輳回避を行います。Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE の信頼できる DSCP ポートを設定して、受信する DSCP 値を使用して輻輳回避を行うことができます。入力側の輻輳回避の詳細については、「信頼できる CoS LAN 入力ポートでの分類とマーキング」（p.42-17）を参照してください。

PFC および DFC の QoS 機能

ここでは、PFC および DFC の QoS 関連事項について説明します。

- サポートされる PFC（p.42-9）
- サポートされる DFC（p.42-9）
- PFC および DFC の QoS 機能リストおよびフローチャート（p.42-9）
- 内部 DSCP 値（p.42-11）

サポートされる PFC

Policy Feature Card（PFC; ポリシー フィーチャ カード）は、スーパーバイザ エンジンに搭載されるドータカードです。PFC は、他の機能とともに QoS 機能を提供します。Catalyst 6500 シリーズ スイッチでは、次の PFC がサポートされます。

- PFC2（Supervisor Engine 2）
- PFC3A（Supervisor Engine 720）
- PFC3B（Supervisor Engine 720 および Supervisor Engine 32）
- PFC3BXL（Supervisor Engine 720）

サポートされる DFC

PFC は QoS ポリシーのコピーを Distributed Forwarding Card（DFC）に送信することで、QoS ポリシーがローカルにサポートされるようにします。これにより、DFC では、PFC がサポートしているものと同じ QoS 機能をサポートできるようになります。

Catalyst 6500 シリーズ スイッチでは、次の DFC がサポートされます。

- WS-F6K-DFC（Supervisor Engine 2 とともに dCEF256 および CEF256 モジュールで使用）
- WS-F6K-DFC3A、WS-F6K-DFC3B、WS-F6K-DFC3BXL（Supervisor Engine 720 とともに dCEF256 および CEF256 モジュールで使用）
- WS-F6700-DFC3A、WS-F6700-DFC3B、WS-F6700-DFC3BXL（Supervisor Engine 720 とともに CEF720 モジュールで使用）

PFC および DFC の QoS 機能リストおよびフローチャート

表 42-1 は、PFC および DFC の各バージョンでサポートされる QoS 機能の一覧を示します。

表 42-1　PFC および DFC でサポートされる QoS 機能

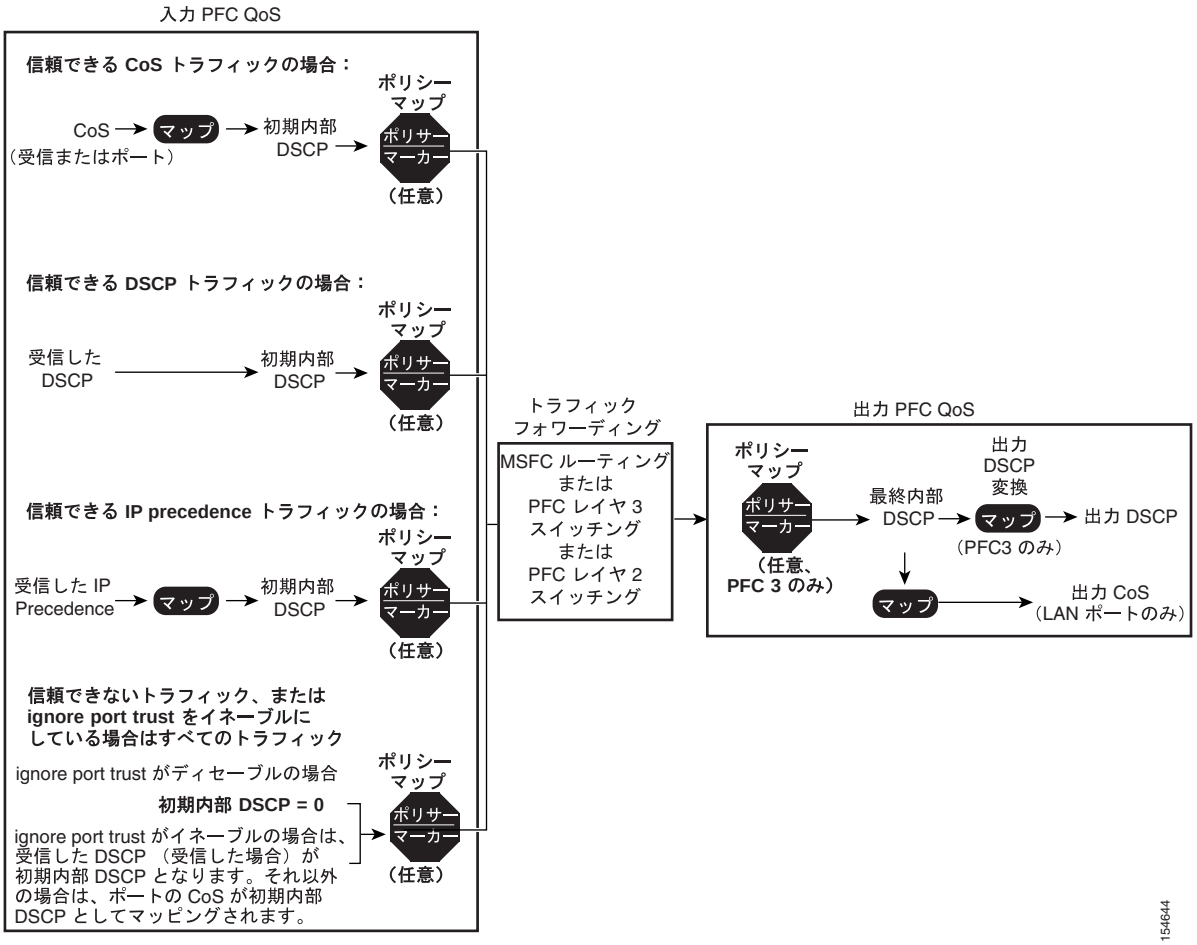
機能	PFC2/DFC	PFC3A/DFC3A	PFC3B/DFC3B	PFC3BXL/ DFC3BXL
DFC のサポート	あり	あり	あり	あり
フローの粒度	完全なフロー	送信元宛先	送信元宛先	送信元宛先
QoS ACL	IP、IPX、MAC	IP、MAC	IP、MAC	IP、MAC
DSCP の透過性 （注）　DSCP の透過性をイネーブルにすると、出力 ToS の書き換えがディセーブルになります。	なし	任意	任意	任意
出力 ToS 書き換え	必須	任意	任意	任意

表 42-1　PFC および DFC でサポートされる QoS 機能（続き）

機能	PFC2/DFC	PFC3A/DFC3A	PFC3B/DFC3B	PFC3BXL/ DFC3BXL
ポリシング：				
入力 aggregate ポリサー	あり	あり	あり	あり
出力 aggregate ポリサー	なし	あり	あり	あり
aggregate ポリサーの数	1022	1022	1022	1022
microflow ポリサー	64 レート	64 レート	64 レート	64 レート
microflow ポリサーあたりのフロー数	32,000	64,000	110,000	240,000
ポリサーによる統計の計測単位	パケット	バイト	バイト	バイト
ポリサー処理の基準	レイヤ 3 の長さ	レイヤ 2 の長さ	レイヤ 2 の長さ	レイヤ 2 の長さ

図 42-6 は、PFC および DFC 上の QoS 機能間のトラフィック フローを示します。

図 42-6　PFC および DFC の QoS 機能



（注）　DSCP 透過性機能を使用すると、オプションで出力 DSCP 値をレイヤ 3 ToS バイトに書き込むことができます。

内部 DSCP 値

PFC QoS は処理中、すべてのトラフィック（非 IP トラフィックを含む）のプライオリティを、内部 DSCP 値で表します。

初期内部 DSCP 値

PFC では何らかのマーキングまたはポリシングが行われる前に、PFC QoS によって、次のように初期内部 DSCP 値が導出されます。

- 信頼できないトラフィックにおいて、ignore port trust がイネーブルになっていない場合は、タグ付きおよびタグなしの両方のトラフィックに対し、初期内部 DSCP 値が 0 に設定されます。
- 信頼できないトラフィックにおいて、ignore port trust がイネーブルにされている場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。
  - 認識可能な ToS バイトが含まれないトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。
- 信頼できる CoS トラフィックにおいて、ignore port trust がイネーブルにされている場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。

  （注）　信頼できる CoS トラフィックにおいて、ignore port trust がイネーブルにされている場合は、受信したタグ付き IP トラフィック内の CoS 値は使用されません。

  - 認識可能な ToS バイトが含まれないタグ付きトラフィックの場合は、受信した CoS 値が初期内部 DSCP 値にマッピングされます。
  - 認識可能な ToS バイトが含まれないタグなしトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。
- 信頼できる IP precedence トラフィックの場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した IP precedence 値を初期内部 DSCP 値にマッピングします。
  - 認識可能な ToS バイトが含まれないタグ付きトラフィックの場合は、受信した CoS 値が初期内部 DSCP 値にマッピングされます。
  - 認識可能な ToS バイトが含まれないタグなしトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。
- 信頼できる DSCP トラフィックの場合は、PFC QoS によって次の処理が行われます。
  - IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。
  - 認識可能な ToS バイトが含まれないタグ付きトラフィックの場合は、受信した CoS 値が初期内部 DSCP 値にマッピングされます。
  - 認識可能な ToS バイトが含まれないタグなしトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。

信頼できる CoS トラフィックおよび信頼できる IP precedence トラフィックの場合は、PFC QoS は設定可能なマップを使用して、3 ビット値である CoS または IP precedence から、6 ビットの初期内部 DSCP 値を導出します。

最終内部 DSCP 値

PFC でのポリシー マーキングおよびポリシングでは、初期内部 DSCP 値が最終内部 DSCP 値に変更されることがあります。この値は、これ以降に適用されるすべての QoS 機能で使用されます。

ポートベースの PFC QoS、および VLAN ベースの PFC QoS

各入力 LAN ポートは、物理ポート ベースの PFC QoS（デフォルト）または VLAN ベースの PFC QoS のいずれかに対応するように設定し、選択したインターフェイスにポリシー マップを付加できます。

ポート ベースの PFC QoS を設定するポートの場合、次のように入力 LAN ポートにポリシー マップを付加します。

- 非トランク入力 LAN ポートをポート ベースの PFC QoS 用に設定すると、そのポートを通じて受信するすべてのトラフィックに、ポートに付加されたポリシー マップが適用されます。
- トランク入力 LAN ポートをポート ベースの PFC QoS 用に設定すると、そのポートを通じて受信するすべての VLAN トラフィックに、ポートに付加されたポリシー マップが適用されます。

非トランク入力 LAN ポートを VLAN ベースの PFC QoS 用に設定すると、そのポートを通じて受信するトラフィックに、ポートの VLAN に付加されたポリシー マップが適用されます。

トランク入力 LAN ポートを VLAN ベースの PFC QoS 用に設定すると、そのポートを通じて受信するトラフィックに、トラフィックの VLAN に付加されたポリシー マップが適用されます。

PFC QoS の出力ポート機能

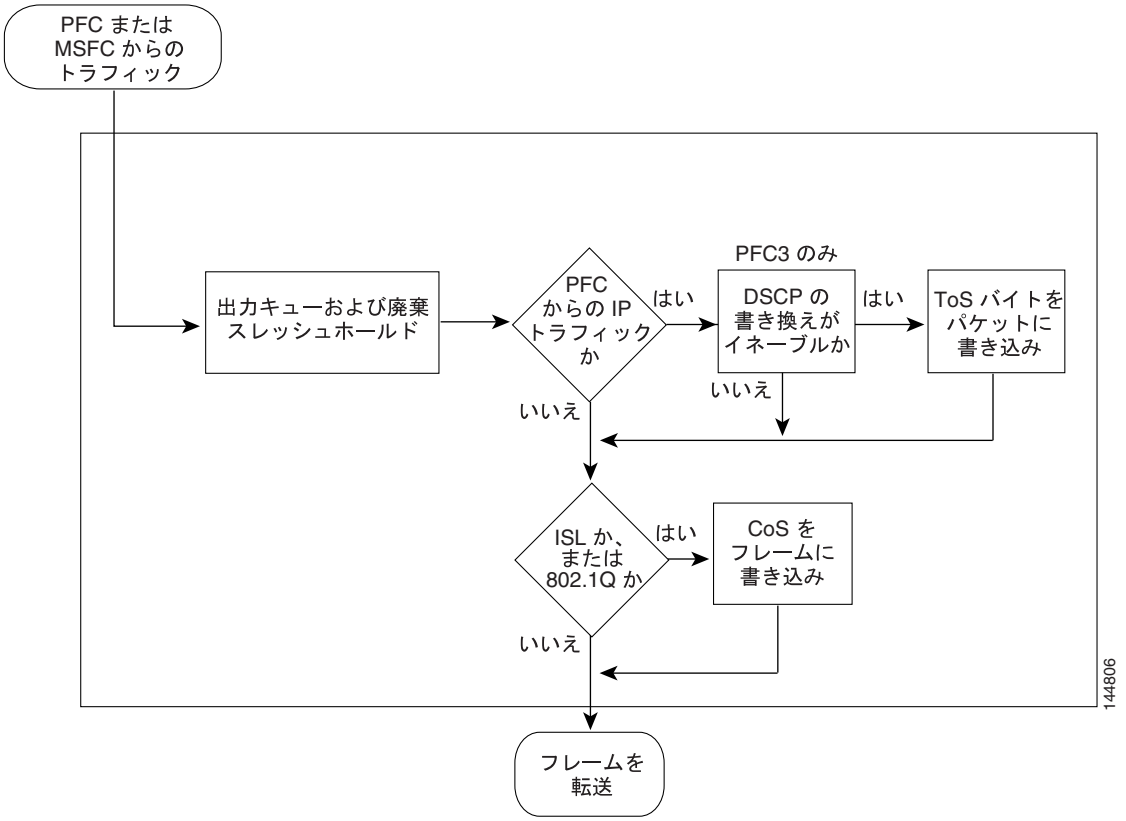
ここでは、PFC QoS の出力ポート機能について説明します。

- PFC QoS の出力 LAN ポート機能のフローチャート（p.42-12）
- 出力 CoS 値（p.42-13）
- PFC3 による出力 DSCP の変換（p.42-13）
- 出力 ToS バイト（p.42-14）
- 出力 PFC QoS インターフェイス（p.42-14）
- 再マーキングされた DSCP に対する出力 ACL のサポート（p.42-14）
- 出力 OSM ポートでのマーキング（p.42-15）

PFC QoS の出力 LAN ポート機能のフローチャート

図 42-7 は、出力 LAN ポートでの QoS 機能間のトラフィック フローを示します。

図 42-7　出力 LAN ポートでのスケジューリング、輻輳回避、およびマーキング



出力 CoS 値

すべての出力トラフィックについて、PFC QoS は設定変更可能なマップを使用して、トラフィックと対応付けられた最終内部 DSCP 値から CoS 値を導出します。導出された CoS 値は出力 LAN ポートに送られます。この値は分類および輻輳回避に使用されるほか、ISL フレームおよび 802.1Q フレームに書き込まれます。

（注）　Release 12.2(18)SXF5 以降のリリースでは、出力 LAN ポートでの分類と輻輳回避に最終内部 DSCP 値が使用されるように、WS-X6708-10GE ポートを設定することができます（「DSCP ベースのキューマッピングの設定」[p.42-99] を参照）。

PFC3 による出力 DSCP の変換

PFC3 の場合、内部 DSCP 値が出力 ToS バイトに書き込まれる前に内部 DSCP 値を変換するには、最大 15 個の出力 DSCP 変換マップを設定できます。出力 DSCP 変換マップは、PFC QoS がサポートする任意のインターフェイスに付加できます。

（注）
- 出力 DSCP 変換を設定する場合は、PFC QoS による、変換された DSCP 値に基づく出力 CoS 値の導出は行われません。
- PFC2 は出力 DSCP 変換をサポートしません。

出力 ToS バイト

DSCP 透過性をイネーブルにしている場合を除き、PFC QoS は最終内部 DSCP 値または変換された DSCP 値を基に、出力 IP トラフィックの ToS バイトを作成します。この ToS バイトは出力ポートに送られ、IP パケット内に書き込まれます。信頼できる DSCP トラフィック、および信頼できない IP トラフィックの場合、ToS バイトには、受信した ToS バイトの元の最下位 2 ビットが含まれます。

内部 DSCP 値または変換された DSCP 値には、IP precedence 値と同じ機能があります（「IP precedence 値と DSCP 値」[p.42-55] を参照）。

出力 PFC QoS インターフェイス

出力ポリシー マップをレイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）に付加することで、ポリシー マップを出力トラフィックに適用できます。

（注）
- 出力ポリシー は microflow ポリシングをサポートしません。
- PFC3 では、microflow ポリシングを ARP トラフィックに適用できません。
- 出力ポリシーで信頼状態を設定することはできません。

再マーキングされた DSCP に対する出力 ACL のサポート

（注）　再マーキングされた DSCP に対する出力 ACL のサポートは、パケット再循環とも呼ばれます。

PFC3 を使用すると、Release 12.2(18)SXE 以降のリリースで、再マーキングされた DSCP を出力 ACL によってサポートできます。これにより、入力 PFC QoS によって行われた IP precedence または DSCP のポリシングまたはマーキングの変更を使用して、IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングが実行されるように設定できます。

再マーキングされた DSCP に対する出力 ACL のサポートがないと、出力 QoS フィルタリングには、受信した IP precedence または DSCP の値が使用されます。ポリシングまたはマーキングの結果として入力 PFC QoS によって行われた、IP precedence または DSCP の変更は使用されません。

PFC3 は、出力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）において、レイヤ 3 でスイッチングおよびルーティングされたトラフィックのみに対して出力 PFC QoS を提供します。

再マーキングされた DSCP に対する出力 ACL サポートは、入力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）上で設定します。

再マーキングされた DSCP に対する出力 ACL サポートを設定したインターフェイス上では、PFC3 は QoS フィルタリングされた各 IP パケットを 2 回ずつ処理します。1 回めは入力 PFC QoS を適用し、2 回めは出力 PFC QoS を適用します。

注意　再マーキングされた DSCP に対する出力 ACL サポートを設定したスイッチが PFC3A モードで動作している場合は、PFC3 はトラフィックを処理して入力 PFC QoS を適用する際、入力 PFC QoS フィルタリングおよび入力 PFC QoS を適用し、入力インターフェイスに設定されたすべての出力 QoS フィルタリングおよび出力 PFC QoS を不正に適用します。この結果、再マーキングされた DSCP に対する出力 ACL サポートがイネーブルになっているインターフェイス上で QoS フィルタリングが設定された場合に、予期しない動作が発生します。この問題は、他の PFC3 モードでは発生しません。

入力 PFC QoS によってパケットが処理され、すべてのポリシングまたはマーキング変更が行われると、このパケットは出力 PFC QoS によって処理される前に、すべての設定済みレイヤ 2 機能（VACL など）によって入力インターフェイス上で再び処理されます。

再マーキングされた DSCP に対する出力 ACL サポートが設定されたインターフェイスで、入力 QoS によって変更された IP precedence または DSCP 値がレイヤ 2 機能と一致すると、一致するパケットはレイヤ 2 機能によってリダイレクトまたは廃棄されます。これにより、このパケットが出力 QoS によって処理されることを防ぎます。

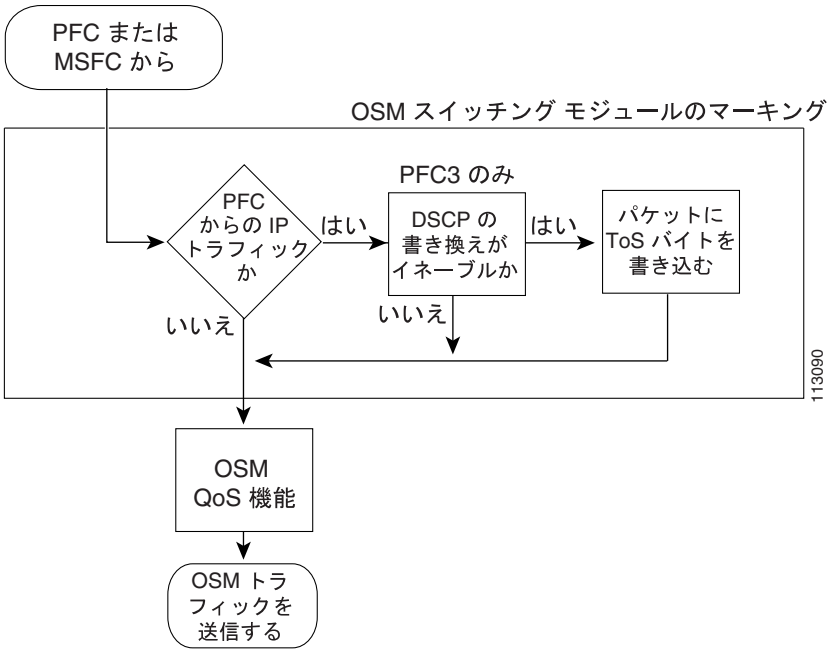
入力 PFC QoS によってパケットが処理され、すべてのポリシングまたはマーキング変更が行われると、このパケットは出力 PFC QoS によって処理される前に、すべての設定済みレイヤ 3 機能（たとえば、入力 Cisco IOS ACL、Policy-Based Routing [PBR; ポリシー ベース ルーティング] など）によって入力インターフェイス上で再び処理されます。

再マーキングされた DSCP に対する出力 ACL サポートが設定されたインターフェイスにレイヤ 3 機能を設定している場合は、入力 PFC QoS によって処理されたパケットはこのレイヤ 3 機能によってリダイレクトまたは廃棄されることがあります。これにより、このパケットが出力 PFC QoS によって処理されることを防ぎます。

出力 OSM ポートでのマーキング

入力 PFC QoS により、OSM 出力 QoS 機能で使用される DSCP 値が設定されます（図 42-8 を参照）。

図 42-8　出力 OSM ポートでのマーキング



分類とマーキングの概要

ここでは、Catalyst 6500 シリーズ スイッチにおいて分類とマーキングが行われる場所、およびその方法について説明します。

- 信頼できる入力ポートおよび信頼できない入力ポートでの分類とマーキング（p.42-16）
- 入力 OSM ポートでの分類とマーキング（p.42-18）
- サービス ポリシーおよびポリシー マップによる PFC での分類およびマーキング（p.42-18）
- MSFC での分類およびマーキング（p.42-19）

信頼できる入力ポートおよび信頼できない入力ポートでの分類とマーキング

入力ポートの信頼状態によって、そのポートが受信したレイヤ 2 フレームをどのようにマーキング、スケジューリング、および分類するか、また、輻輳回避を実行するかどうかが決まります。ポートの信頼状態には、次の種類があります。

- untrusted（デフォルト）
- trust IP precedence
- trust DSCP
- trust CoS

すべてのリリースにおいて、入力 LAN ポートでの分類、マーキング、および輻輳回避ではレイヤ 2 CoS 値が使用可能であり、レイヤ 3 の IP precedence 値または DSCP 値は設定されません。

Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートを設定して、入力 LAN ポートでの分類と輻輳回避に、受信した DSCP 値を使用することができます（「DSCP ベースのキュー マッピングの設定」[p.42-99] を参照）。

Release 12.2(18)SXF5 より前のリリースでは、入力 LAN ポートの分類、マーキング、および輻輳回避には、レイヤ 2 CoS 値のみが使用されます。

ここでは、信頼できる入力ポートおよび信頼できない入力ポートでの、分類およびマーキングについて説明します。

- 信頼できない入力ポートでの分類とマーキング（p.42-16）
- 信頼できる入力ポートでの分類とマーキング（p.42-16）

信頼できない入力ポートでの分類とマーキング

PFC QoS のレイヤ 2 再マーキングでは、信頼できないポートから受信したすべてのフレームに、ポートの CoS 値がマークされます（デフォルト値は 0）。

信頼できない入力トラフィックに適用されたポート CoS 値を初期内部 DSCP 値にマッピングするには、入力トラフィックと一致する、信頼できる CoS ポリシー マップを設定します。

信頼できる入力ポートでの分類とマーキング

ポートを信頼可能として設定する場合は、そのポートが、有効な QoS ラベルを伝送するトラフィックを受信する場合のみにしてください。QoS は受信した QoS ラベルを、初期内部 DSCP 値の基準値として使用します。スイッチに入力後のトラフィックには、ポリシー マップによって、別の信頼状態を適用できます。たとえば、信頼できる CoS ポートからスイッチに入力されたトラフィックに対し、ポリシー マップを使用して、IP precedence または DSCP を信頼するように設定できます。これにより、ポートで信頼された QoS ラベルではなく、この信頼値が初期内部 DSCP 値の基準値として使用されます。

ここでは、信頼できる入力ポートでの分類およびマーキングについて説明します。

- 信頼できる CoS LAN 入力ポートでの分類とマーキング（p.42-17）
- 信頼できる IP Precedence 入力ポートでの分類とマーキング（p.42-17）
- 信頼できる入力 DSCP ポートでの分類とマーキング（p.42-17）

信頼できる CoS LAN 入力ポートでの分類とマーキング

CoS を信頼するように LAN ポートを設定する場合は、そのポートが、有効なレイヤ 2 CoS を伝送するトラフィックを受信する場合のみにしてください。

信頼できる入力 LAN ポートから ISL フレームがスイッチに入ると、PFC QoS はユーザ フィールドの最下位 3 ビットを CoS 値として受け取ります。信頼できる入力 LAN ポートから 802.1Q フレームがスイッチに入ると、PFC QoS はユーザ プライオリティ ビットを CoS 値として受け取ります。PFC QoS のレイヤ 2 再マーキングでは、タグなしフレームで受信したすべてのトラフィックが、入力ポートの CoS 値でマーキングされます。

CoS を信頼するように設定したポートでは、PFC QoS によって次の処理が行われます。

- タグ付きの信頼できる CoS トラフィックによって受信した CoS 値は、初期内部 DSCP 値にマッピングされます。
- タグなしの信頼できるトラフィックに適用された入力ポート CoS 値は、初期内部 DSCP 値にマッピングされます。
- PFC QoS では、CoS ベースの入力キューおよびスレッショルドをイネーブルにすることで、輻輳回避を行うことができます。入力キューおよびスレッショルドの詳細については、「ポートベースのキュー タイプの概要」（p.42-22）を参照してください。

信頼できる IP Precedence 入力ポートでの分類とマーキング

IP precedence を信頼するようにポートを設定する場合は、そのポートが、有効なレイヤ 3 IP precedence を伝送するトラフィックを受信する場合のみにしてください。信頼できる IP precedence ポートからのトラフィックに対し、PFC QoS は受信した IP precedence 値を初期内部 DSCP 値にマッピングします。入力ポートのキューおよびスレッショルドでは、レイヤ 2 CoS が使用されます。したがって PFC QoS は、IP precedence を信頼するように設定されているポートでは、入力ポートの輻輳回避を行いません。PFC は、IP precedence を信頼するように設定されている入力ポートでは、トラフィックのマーキングを行いません。

信頼できる入力 DSCP ポートでの分類とマーキング

DSCP を信頼するようにポートを設定する場合は、そのポートが、有効なレイヤ 3 DSCP を伝送するトラフィックを受信する場合のみにしてください。

Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートで DSCP ベースの入力キューおよびスレッショルドをイネーブルにすることで、輻輳回避を実行できます（「DSCP ベースのキュー マッピングの設定」[p.42-99] を参照）。

Release 12.2(18)SXF5 より前のリリースでは、入力ポートキューおよびスレッショルドでは、レイヤ 2 CoS しか使用されません。したがって、DSCP を信頼するように設定されたポートでは、PFC QoS によるポートの輻輳回避は行われません。

信頼できる DSCP ポートからのトラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。受信する DSCP を信頼するように設定された入力ポートでは、PFC QoS によるトラフィックのマーキングは行われません。

入力 OSM ポートでの分類とマーキング

PFC QoS は、入力 OSM ポートから受信したすべてのトラフィックに、0 の CoS を対応付けます。入力 OSM ポートの信頼状態を設定し、この信頼状態を、PFC が IP precedence 値または DSCP 値、および CoS 値を設定するときに使用させることができます。各入力 OSM ポートの信頼状態を、次のように設定できます。

- untrusted（デフォルト）
- trust IP precedence
- trust DSCP
- trust CoS（POS および ATM OSM ポートではポートの CoS 値を設定できないため、POS および ATM OSM ポートの CoS 値は常に 0）

サービス ポリシーおよびポリシー マップによる PFC での分類およびマーキング

PFC QoS は、サービス ポリシーによる分類およびマーキングをサポートします。これは、次のインターフェイス タイプに 1 つのポリシー マップを付加することで、入力 PFC QoS を適用します。

- 各入力ポート（FlexWAN インターフェイスを除く）
- 各 EtherChannel ポートチャネル インターフェイス
- 各 VLAN インターフェイス

PFC3 では、各レイヤ 3 インターフェイス（FlexWAN インターフェイスを除く）に 1 つのポリシー マップを付加することで、出力 PFC QoS を適用できます。

各ポリシー マップには、複数のポリシー マップ クラスを含めることができます。インターフェイスにより処理されたトラフィックのタイプごとに、個別のポリシー マップ クラスを設定できます。ポリシー マップ クラスのフィルタリングを設定するには、次の 2 つの方法があります。

- Access Control List（ACL; アクセス制御リスト）
- IP precedence および DSCP 値に対するクラス マップの **match** コマンド

ポリシー マップ クラスでは、次のオプション コマンドを使用してアクションを指定します。

- ポリシー マップ **set** コマンド — 信頼できないトラフィックの場合、または ignore port trust をイネーブルにしている場合は、PFC QoS は最終内部 DSCP 値として、設定済みの IP precedence 値または DSCP 値を使用できます。IP precedence および DSCP のビット値については、「IP precedence 値と DSCP 値」（p.42-55）を参照してください。
- ポリシー マップ クラス **trust** コマンド — PFC QoS は一致する入力トラフィックに対し、ポリシー マップ クラスの信頼状態を適用します。この信頼値は、ポートで信頼された QoS ラベル（存在する場合）の代わりに、初期内部 DSCP 値の基準値として使用されます。ポリシー マップでは、CoS、IP precedence、または DSCP を信頼するように設定できます。

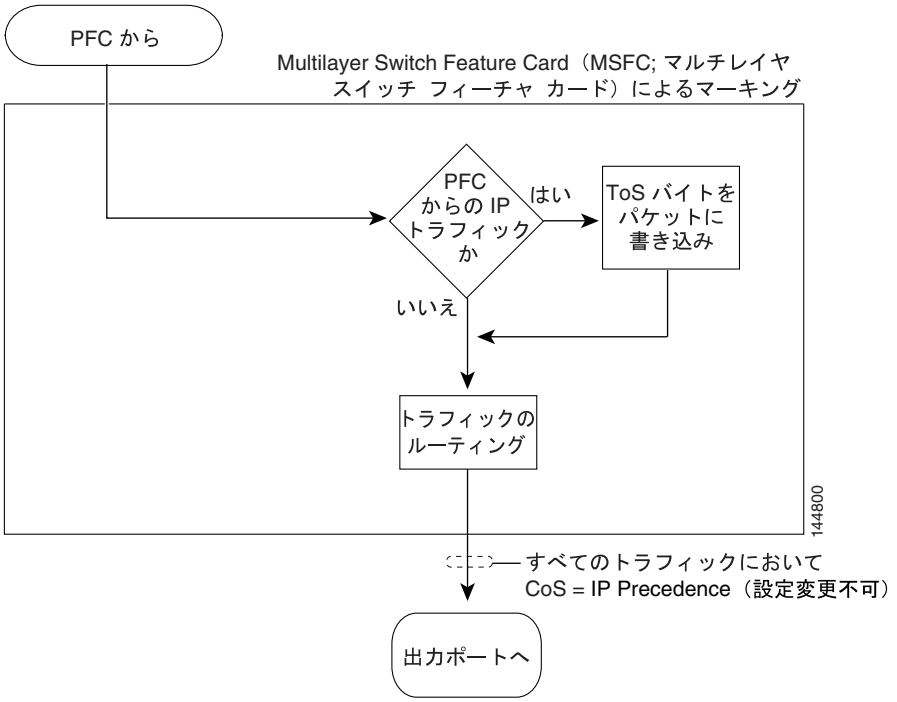
（注）　信頼できる CoS ポリシー マップでは、信頼できないポートからのトラフィックで受信した CoS を元に戻すことはできません。信頼できないポートからのトラフィックには、常にポートの CoS 値が含まれます。

- aggregate ポリサーおよび microflow ポリサー — PFC QoS ではポリサーを使用して、適合するトラフィックと適合しないトラフィックの両方について、マーキングまたは廃棄のいずれかを実行できます。

MSFC での分類およびマーキング

PFC QoS は MSFC に対し、IP トラフィックを最終内部 DSCP 値とともに送信します。MSFC から出力ポートへ送信されるすべてのトラフィックにおいて、CoS は IP precedence と同じ値です。

図 42-9　PFC2/PFC3 および MSFC2/MSFC2A/MSFC3 によるマーキング



（注）　PFC でレイヤ 3 スイッチングされるトラフィックは MSFC を通過せず、PFC によって割り当てられる CoS 値を維持します。

ポリサー

ここでは、各ポリサーについて説明します。

- ポリサーの概要（p.42-19）
- aggregate ポリサー（p.42-20）
- microflow ポリサー（p.42-21）

ポリサーの概要

ポリシングを使用すると、QoS 設定で定義されたトラフィック転送ルールに適合するように、着信および送信トラフィックをレート制限できます。システムにおいてトラフィックが転送される方法を定義した設定済みルールは、契約と呼ばれます。この契約に適合しないトラフィックは、低い DSCP 値にマーク ダウンされるか、または廃棄されます。

ポリシングでは、不適合パケットはバッファに保存されません。したがって、ポリシングが送信遅延に影響することはありません。逆に、トラフィック シェーピングでは不適合トラフィックをバッファに保存することで、トラフィック バーストを緩和します（PFC QoS はシェーピングをサポートしません）。

PFC2 は入力 PFC QoS のみをサポートしますが、これには入力ポリシングが含まれます。PFC3 は入力および出力 PFC QoS の両方をサポートし、これには入力および出力ポリシングが含まれます。トラフィック シェーピングは、一部の WAN モジュールでサポートされます。OSM および FlexWAN モジュールでのトラフィック シェーピングの詳細については、次の URL で、OSM および FlexWAN 関連マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/index.htm

（注）　ポリサーは、ポート単位または VLAN 単位で入力トラフィックに適用されます。PFC3 の出力トラフィックに対するポリシングは、VLAN 単位のみで行われます。

次の処理を行うポリサーを作成できます。

- トラフィックのマーキング
- 帯域幅利用の制限およびトラフィックのマーキング

aggregate ポリサー

PFC QoS は、1 つの aggregate ポリサーで指定される帯域幅限度を、一致するトラフィックのすべてのフローに対して累積方式で適用します。たとえば、VLAN 1 および VLAN 3 上のすべての TFTP トラフィック フローの帯域幅として、1 Mbps を許可するように aggregate ポリサーを設定すると、VLAN 1 および VLAN 3 上のすべての TFTP トラフィック フローは、合計 1 Mbps となるように制限されます。

- ポリシー マップ クラスのインターフェイス別 aggregate ポリサーは、**police** コマンドを使用して定義します。インターフェイス別 aggregate ポリサーを複数の入力ポートに付加すると、各入力ポート上の一致するトラフィックが個別にポリシングされます。
- 名前付き aggregate ポリサーは、**mls qos aggregate-policer** コマンドを使用して作成します。名前付き aggregate ポリサーを複数の入力ポートに付加すると、そのポリサーが付加された全入力ポートからの一致するトラフィックがポリシングされます。
- aggregate ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。aggregate ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。aggregate ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が、影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチングされた仮想インターフェイスに適用されたポリサー
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。

microflow ポリサー

PFC QoS は、microflow ポリサーで指定される帯域幅限度を、一致するトラフィックの各フローに対して個別に適用します。たとえば、VLAN 1 および VLAN 3 で TFTP トラフィックを 1 Mbps に制限するように microflow ポリサーを設定すると、VLAN 1 の各フローに 1 Mbps が、VLAN 3 の各フローに 1 Mbps がそれぞれ許可されます。VLAN 1 に 3 つのフローが含まれ、VLAN 3 に 4 つのフローが含まれる場合は、microflow ポリサーはこの各フローにそれぞれ 1 Mbps を許可します。

microflow ポリサーの帯域幅限度を適用するように、PFC QoS を次のように設定できます。

- microflow ポリサーは、最大 63 通りのレート / バースト パラメータの組み合わせを使用して作成できます。
- ポリシー マップ クラスの microflow ポリサーは、**police flow** コマンドを使用して作成します。
- 送信元アドレスだけを使用するように microflow ポリサーを設定できます。これにより宛先アドレスに関係なく、特定の送信元アドレスからのすべてのトラフィックに microflow ポリサーを適用します。
- 宛先アドレスだけを使用するように microflow ポリサーを設定できます。これにより送信元アドレスに関係なく、特定の宛先アドレスへのすべてのトラフィックに microflow ポリサーを適用します。
- MAC レイヤ microflow ポリシングの場合、PFC QoS はプロトコルおよび送信元と宛先の MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、Ethertype が違っていても、同じフローの一部であるとみなします。PFC3 では、IPX トラフィックをフィルタリングするように MAC ACL を設定できます。
- PFC2 では、IPX トラフィックをフィルタリングするように IPX ACL を設定できます。IPX microflow ポリシングの場合、PFC QoS は、送信元ノードまたは送信元ソケットが異なるトラフィックを含め、同じ送信元ネットワーク、宛先ネットワーク、および宛先ノードを持つ IPX トラフィックは同じフローの一部であるとみなします。
- デフォルトでは、microflow ポリサーは MSFC がルーティングするトラフィックだけに影響します。それ以外のトラフィック（ブリッジ グループのトラフィックも含む）の microflow ポリシングをイネーブルにするには、**mls qos bridged** コマンドを使用します。PFC2 では、ルーティングされたトラフィックに対してブリッジ microflow ポリシングもイネーブルにする必要があります。
- PFC3 では、microflow ポリシングを ARP トラフィックに適用できません。

各ポリシー マップ クラスに aggregate ポリサーおよび microflow ポリサーの両方を含めると、単独の帯域利用率と、他のフローと合算された帯域利用率に基づいて、フローのポリシングを行うことができます。

（注） トラフィックに aggregate ポリシングと microflow ポリシングの両方を実行する場合、aggregate ポリサーおよび microflow ポリサーを同じポリシー マップ クラスに組み込み、各ポリサーで同じ **conform-action** および **exceed-action** キーワード オプションを使用する必要があります（**drop**、**set-dscp-transmit**、**set-prec-transmit**、または **transmit**）。

たとえば、グループの個々のメンバーに適した帯域幅限度を設定して microflow ポリサーを作成し、さらに、グループ全体として適切な帯域幅限度を設定して名前付き aggregate ポリサーを作成できます。グループのトラフィックと一致するポリシー マップ クラスに、この両方のポリサーを含めます。この組み合わせは、個々のフローには別々に作用し、グループには集約的に作用します。

ポリシー マップ クラスに aggregate ポリサーおよび microflow ポリサーの両方が含まれている場合、PFC QoS はどちらかのポリサーに基づいて不適合なステータスに対応し、そのポリサーの指定に従って、新しい DSCP 値を適用するか、またはパケットを廃棄します。両方のポリサーから不適合なステータスが戻された場合には、どちらかのポリサーでパケットの廃棄が指定されていれば、パケットは廃棄されます。指定されていない場合は、マークダウンされた DSCP 値が適用されます。

（注）　矛盾した結果が生じないように、同一の aggregate ポリサーでポリシングするすべてのトラフィックで、信頼状態が同じであることを確認してください。

PFC3 のポリシングでは、レイヤ 2 のフレーム サイズを使用します。PFC2 のポリシングでは、レイヤ 3 のパケット サイズを使用します。帯域幅利用限度は、Committed Information Rate（CIR; 認定情報速度）で指定します。より高い Peak Information Rate（PIR; 最大情報レート）も指定できます。レートを超過するパケットは、「不適合」とみなされます。

ポリサーごとに、不適合なパケットを廃棄するか、または新しい DSCP 値を適用するかを指定します（新しい DSCP 値を適用することを「マークダウン」といいます）。不適合なパケットは、元のプライオリティを維持しないので、適合するパケットが消費した帯域幅の一部としてはカウントされません。

PIR を設定する場合、PIR に不適合な場合のアクションは、CIR に不適合な場合のアクションよりも厳しいものになります。たとえば、CIR に不適合な場合のアクションがトラフィックをマークダウンするというアクションである場合、PIR に不適合な場合のアクションは、トラフィックを送信するというアクションにすることはできません。

PFC QoS はあらゆるポリサーで、設定変更可能なグローバル テーブルを使用して、内部 DSCP 値をマークダウンされた DSCP 値にマッピングします。マークダウンが発生すると、PFC QoS はこのテーブルからマークダウンされた DSCP 値を取得します。ユーザが個々のポリサーでマークダウン後の DSCP 値を指定することはできません。

（注）

- **conform-action transmit** キーワードによるポリシングは、一致するトラフィックの入力 LAN ポート信頼状態（trust DSCP、または **trust** ポリシー マップ クラス コマンドで定義された信頼状態）よりも優先されます。
- デフォルトでは、マークダウン テーブルは、マークダウンが起こらないように設定されています。つまり、マークダウンされた DSCP 値は、元の DSCP 値と同じです。マークダウンをイネーブルにするには、ネットワークに合わせてテーブルを適切に設定します。
- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。

ポートベースのキュー タイプの概要

ポートベースのキュー タイプは、ポートを制御する ASIC によって決定されます。ここでは、Catalyst 6500 シリーズ スイッチの LAN モジュールによってサポートされるキュー タイプ、廃棄スレッシュホールド、およびバッファについて説明します。

- 入力および出力バッファとレイヤ 2 CoS ベース キュー（p.42-23）
- 入力キューのタイプ（p.42-25）
- 出力キューのタイプ（p.42-25）
- モジュールとキュー タイプのマッピング（p.42-26）

入力および出力バッファとレイヤ 2 CoS ベース キュー

イーサネット LAN モジュール ポートの ASIC は、固定数のキューに分割されるバッファを備えています。輻輳回避をイネーブルにすると、PFC QoS はトラフィックのレイヤ 2 CoS 値を使用して、トラフィックを各キューに割り当てます。バッファとキューは、スイッチを通過するフレームを一時的に保管します。PFC QoS はポートの ASIC メモリを、各ポートの各キューに対するバッファとして割り当てます。

Catalyst 6500 シリーズ スイッチの LAN モジュールは、次のキュー タイプをサポートします。

- 標準キュー
- 完全優先キュー

Catalyst 6500 シリーズ スイッチの LAN モジュールは、キュー間で次のスケジューリング アルゴリズムをサポートします。

- Shaped Round Robin（SRR; シェイプド ラウンド ロビン）— SRR を使用すると、1 つのキューは、割り当てられた帯域幅のみの使用が許可されます。
- Deficit Weighted Round Robin（DWRR）— より高いプライオリティのキュー内のトラフィックによってプライオリティを低く設定されている、転送中のすべてのキューを追跡し、次回のラウンドでこの差分を補います。
- Weighted Round-Robin（WRR; 重み付きラウンドロビン）— WRR は、各キューに対して帯域幅を明示的に予約しません。各キューに割り当てられる帯域幅の量は、ユーザが設定できます。キューに割り当てられる割合（重み）は、このキューに割り当てられる帯域幅の量を定義します。
- 完全優先キューイング — 遅延に影響されやすいデータ（音声など）を、他のキュー内のパケットがキューから取り出される前にキューから取り出します。これにより、遅延に影響されやすいデータが、他のトラフィックより優先的に処理されます。スイッチは、完全優先キュー内のトラフィックを処理してから、標準キューを処理します。スイッチは標準キュー内のパケットを送信したあとで、完全優先キュー内のトラフィックを調べます。スイッチは完全優先キュー内でトラフィックを検出すると、標準キューの処理を中断し、先に完全優先キュー内のすべてのトラフィックを処理してから、標準キューに戻ります。

Catalyst 6500 シリーズ スイッチの LAN モジュールは、輻輳回避を実行する際、キュー内で次のタイプのスレッシュホールドを使用します。

- Weighted Random Early Detection（WRED; 重み付きランダム早期検出）— WRED 廃棄スレッシュホールドを設定したポートでは、バッファの輻輳を回避する目的のランダムな確率に基づき、特定の QoS ラベルを持つフレームがキューへの入力を許可されます。特定の QoS ラベルを持つフレームがキューへの入力を許可、または廃棄される確率は、この QoS ラベルに割り当てられた重みとスレッシュホールドに依存します。

  たとえば、スレッシュホールドが 2 のキュー 1 に CoS 2 が割り当てられ、スレッシュホールド 2 のレベルが 40%（ロー）および 80%（ハイ）であるとします。この場合、CoS 2 を持つフレームは、キュー 1 が 40% 以上占有されるまでは廃棄されません。キューの深さが 80% に近づくにつれ、CoS 2 を持つフレームは、キューへの入力が許可される確率よりも、廃棄される確率のほうが高くなります。キューの占有率が 80% を超えると、キューの占有率が 80% 未満となるまで、CoS 2 フレームはすべて廃棄されます。キュー レベルがロー スレッシュホールドとハイ スレッシュホールドの中間にある場合に、スイッチによって廃棄されるフレームは、フロー単位や FIFO 形式ではなく、ランダムに選択されます。この方法は、バックオフや転送ウィンドウ サイズの調整によって、定期的なパケット廃棄に適応することが可能な、TCP などのプロトコルに適します。
- テール廃棄スレッシュホールド — テール廃棄スレッシュホールドを設定したポートでは、特定の QoS ラベルを持つフレームは、この QoS ラベルに関連付けられた廃棄スレッシュホールドが超過するまで、キューへの入力を許可されます。同じ QoS ラベルを持つ以降のフレームは、スレッシュホールドの超過状態が解消するまで廃棄されます。たとえば、スレッシュホールドが 2 のキュー 1 に CoS 1 が割り当てられ、スレッシュホールド 2 の水準が 60% であるとします。この場合、CoS 1 を持つフレームは、キュー 1 が 60% 占有されるまでは廃棄されません。

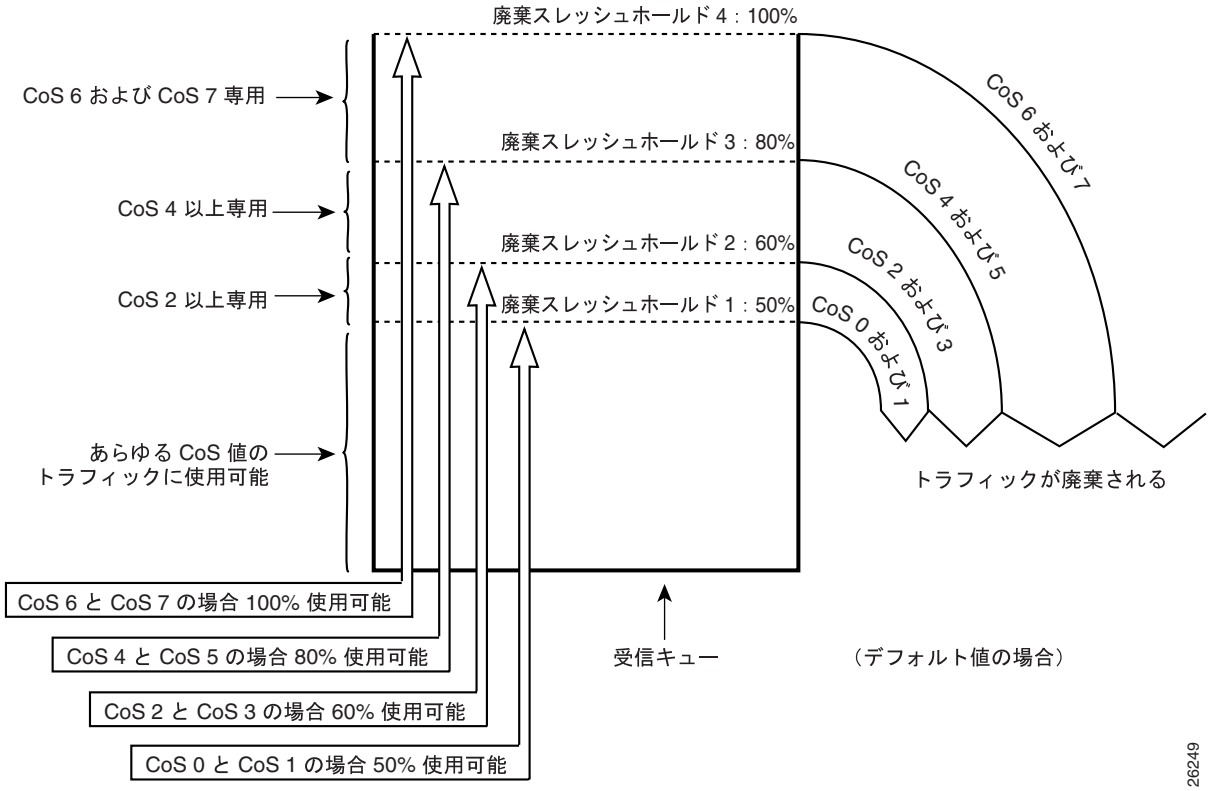
以降のすべての CoS 1 フレームは、キューの占有率が 60 % 未満になるまで廃棄されます。一部のポート タイプでは、テール廃棄スレッシュホールドおよび WRED 廃棄スレッシュホールドの両方を使用するように標準受信キューを設定するには、CoS 値をキューにマッピングするか、またはキューおよびスレッシュホールドにマッピングします。スイッチでは、キューにのみマッピングされている CoS 値を伝送するトラフィックには、テール廃棄スレッシュホールドが使用されます。キューおよびスレッシュホールドにマッピングされている CoS 値を伝送するトラフィックには、WRED 廃棄スレッシュホールドが使用されます。同じタイプの LAN ポートは、すべて同じ廃棄スレッシュホールドの設定を使用します。

（注）　Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートで、DSCP ベースのキューおよびスレッシュホールドをイネーブルにできます（「DSCP ベースのキュー マッピングの設定」[p.42-99] を参照）。

複数のキューを組み合わせ、各キューにスケジューリング アルゴリズムを関連付けることで、スイッチでの輻輳回避を実行できます。

図 42-10 に、**1q4t** 入力 LAN ポートの廃棄スレッシュホールドを示します。他の設定でも、廃棄スレッシュホールドは同様に機能します。

図 42-10　受信キューの廃棄スレッシュホールド



入力キューのタイプ

LAN ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。このコマンドを実行すると、次のいずれかのアーキテクチャが表示されます。

- **1q2t** は、1 つの設定変更可能なテール廃棄スレッシュホールドおよび 1 つの設定変更できないテール廃棄スレッシュホールドがある、1 つの標準キューを意味します。
- **1q4t** は、4 つの設定変更可能なテール廃棄スレッシュホールドがある 1 つの標準キューを意味します。
- **1q8t** は、8 つの設定変更可能なテール廃棄スレッシュホールドがある 1 つの標準キューを意味します。
- **2q8t** は、それぞれ 8 つの設定変更可能なテール廃棄スレッシュホールドがある 2 つの標準キューを意味します。
- **8q4t** は、それぞれ WRED 廃棄またはテール廃棄として設定変更可能な 4 つのスレッシュホールドがある、8 つの標準キューを意味します。
- **8q8t** は、それぞれ WRED 廃棄またはテール廃棄として設定変更可能な 8 つのスレッシュホールドがある 8 つの標準キューを意味します。
- **1p1q4t** は次を意味します。
  - 1 つの完全優先キュー
  - 4 つの設定変更可能なテール廃棄スレッシュホールドがある 1 つの標準キュー
- **1p1q0t** は次を意味します。
  - 1 つの完全優先キュー
  - 設定変更可能なスレッシュホールドがない 1 つの標準キュー（実質的には 100% のテール廃棄スレッシュホールド）
- **1p1q8t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のスレッシュホールドを持つ 1 つの標準キュー：
    - それぞれ WRED 廃棄またはテール廃棄として設定変更可能な 8 つのスレッシュホールド
    - 設定変更できない（100%）1 つの テール廃棄スレッシュホールド

出力キューのタイプ

出力 LAN ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。

このコマンドを実行すると、次のいずれかのアーキテクチャが表示されます。

- **2q2t** は、それぞれ 2 つの設定変更可能なテール廃棄スレッシュホールドがある 2 つの標準キューを意味します。
- **1p2q2t** は次を意味します。
  - 1 つの完全優先キュー
  - それぞれ 2 つの設定変更可能な WRED 廃棄スレッシュホールドがある 2 つの標準キュー
- **1p3q1t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のスレッシュホールドを持つ 3 つの標準キュー：
    - WRED 廃棄またはテール廃棄として設定変更可能な 1 つのスレッシュホールド
    - 設定変更できない（100%）1 つの テール廃棄スレッシュホールド

- **1p2q1t** は次を意味します。
  - 1 つの完全優先キュー
  - 次のスレッシュホールドを持つ 2 つの標準キュー：
    - 1 つの WRED 廃棄スレッシュホールド
    - 設定変更できない（100%）1 つの テール廃棄スレッシュホールド
- **1p3q8t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED　廃棄またはテール廃棄のいずれかとして設定変更可能なスレッシュホールドがそれぞれ 8 つある、3 つの標準キュー
- **1p7q4t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED　廃棄またはテール廃棄のいずれかとして設定変更可能なスレッシュホールドがそれぞれ 4 つある、7 つの標準キュー
- **1p7q8t** は次を意味します。
  - 1 つの完全優先キュー
  - WRED　廃棄またはテール廃棄のいずれかとして設定変更可能なスレッシュホールドがそれぞれ 8 つある、7 つの標準キュー

モジュールとキュー タイプのマッピング

次の表は、モジュールとキュー構造のマッピングを示します。

- スーパーバイザ エンジン モジュールの QoS キュー構造
- イーサネットおよびファスト イーサネット モジュールのキュー構造
- ギガビットおよび 10/100/1000 イーサネット モジュール
- 10 ギガビット イーサネット モジュール

表 42-2　スーパーバイザ エンジン モジュールの QoS キュー構造

スーパーバイザ エンジン	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-SUP720	1p1q4t	WRR	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-SUP720-3B							
WS-SUP720-3BXL							
WS-SUP32-10GE	2q8t	WRR	1p3q8t	DWRR SRR	1.3 MB	166 KB	1.2 MB
WS-SUP32-GE							
WS-X6K-S2U-MSFC2	1p1q4t	WRR	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-X6K-S2-MSFC2							
WS-X6K-S2-PFC2							

表 42-3　イーサネットおよびファスト イーサネット モジュールのキュー構造

モジュール	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6524-100FX-MM	1p1q0t	WRR	1p3q1t	DWRR	1,116 KB	28 KB	1,088 KB
WS-X6548-RJ-21							
WS-X6548-RJ-45							
WS-X6324-100FX-MM	1q4t	WRR	2q2t	WRR	128 KB	16 KB	112 KB
WS-X6324-100FX-SM							
WS-X6348-RJ-45							
WS-X6348-RJ-45V							
WS-X6348-RJ-21V							
WS-X6224-100FX-MT					64 KB	8 KB	56 KB
WS-X6248-RJ-45							
WS-X6248-TEL							
WS-X6248A-TEL					128 KB	16 KB	112 KB
WS-X6148-RJ-45							
WS-X6148-RJ-45V							
WS-X6148-45AF							
WS-X6148-RJ-21							
WS-X6148-RJ-21V							
WS-X6148-21AF							
WS-X6148X2-RJ-45	1p1q0t	WRR	1p3q1t	DWRR	1,116 KB	28 KB	1,088 KB
WS-X6148X2-45AF							
WS-X6024-10FL-MT	1q4t	WRR	2q2t	WRR	64 KB	8 KB	56 KB

表 42-4　ギガビットおよび 10/100/1000 イーサネット モジュール

モジュール	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6816-GBIC	1p1q4t	WRR	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-X6748-GE-TX および DFC3	2q8t	WRR	1p3q8t	DWRR	1.3 MB	166 KB	1.2 MB
WS-X6748-GE-TX および CFC	1q8t	WRR					
WS-X6748-SFP および DFC3	2q8t	WRR					
WS-X6748-SFP および CFC	1q8t	WRR					
WS-X6724-SFP および DFC3	2q8t	WRR					
WS-X6724-SFP および CFC	1q8t	WRR					
WS-X6548-GE-TX	1q2t	WRR	1p2q2t	WRR	1.4 MB	185 KB	1.2 MB
WS-X6548V-GE-TX							
WS-X6548-GE-45AF							

表 42-4　ギガビットおよび 10/100/1000 イーサネット モジュール（続き）

モジュール	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6516-GBIC	1p1q4t	WRR	1p2q2t	WRR	512 KB	73 KB	439 KB
WS-X6516A-GBIC		WRR		WRR	1 MB	135 KB	946 KB
WS-X6516-GE-TX		WRR		WRR	512 KB	73 KB	439 KB
WS-X6408-GBIC	1q4t	WRR	2q2t	WRR		80 KB	432 KB
WS-X6408A-GBIC	1p1q4t	WRR	1p2q2t	WRR		73 KB	439 KB
WS-X6416-GBIC		WRR					
WS-X6416-GE-MT		WRR					
WS-X6316-GE-TX		WRR					
WS-X6148-GE-TX	1q2t	WRR			1.4 MB	185 KB	1.2 MB
WS-X6148V-GE-TX							
WS-X6148-GE-45AF							

表 42-5　10 ギガビット イーサネット モジュール

モジュール	入力キューおよび廃棄スレッシュホールド	入力キュースケジューラ	出力キューおよび廃棄スレッシュホールド	出力キュースケジューラ	合計バッファサイズ	入力バッファサイズ	出力バッファサイズ
WS-X6708-10GE	8q4t	DWRR	1p7q4t	DWRR SRR	198 MB	108 MB	90 MB
WS-X6704-10GE および DFC3	8q8t	WRR	1p7q8t	DWRR	16 MB	2 MB	14 MB
WS-X6704-10GE および CFC	1q8t	WRR					
WS-X6502-10GE	1p1q8t	WRR	1p2q1t	DWRR	64.2 MB	256 KB	64 MB
WS-X6501-10GEX4							

PFC QoS のデフォルト設定

ここでは、PFC QoS デフォルトの設定手順について説明します。

- PFC QoS のグローバルな設定（p.42-29）
- PFC QoS がイネーブルの場合のデフォルト値（p.42-30）
- PFC QoS がディセーブルの場合のデフォルト値（p.42-49）

PFC QoS のグローバルな設定

次のグローバル PFC QoS 設定が適用されます。

機能	デフォルト値
PFC QoS のグローバル イネーブル ステート	ディセーブル
PFC QoS のポート イネーブル ステート	PFC QoS がグローバルにイネーブルの場合、イネーブル
ポートの CoS 値	0
microflow ポリシング	イネーブル
VLAN 内 microflow ポリシング	ディセーブル
ポート ベースまたは VLAN ベースの PFC QoS	ポートベース
受信した CoS と初期内部 DSCP とのマッピング（受信した CoS 値に基づき設定された初期内部 DSCP）	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
受信した IP precedence と初期内部 DSCP とのマッピング（受信した IP precedence 値に基づき設定された初期内部 DSCP）	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
最終内部 DSCP と出力 CoS とのマッピング（最終内部 DSCP 値に基づき設定された出力 CoS）	DSCP 0 ～ 7 = CoS 0 DSCP 8 ～ 15 = CoS 1 DSCP 16 ～ 23 = CoS 2 DSCP 24 ～ 31 = CoS 3 DSCP 32 ～ 39 = CoS 4 DSCP 40 ～ 47 = CoS 5 DSCP 48 ～ 55 = CoS 6 DSCP 56 ～ 63 = CoS 7
DSCP マップからの DSCP のマークダウン	マークダウンされた DSCP 値は元の DSCP 値と等しい（マークダウンなし）
ポリサー	なし
ポリシー マップ	なし

機能	デフォルト値
プロトコル独立型 MAC ACL フィルタリング	ディセーブル
VLAN ベースの MAC ACL QoS フィルタリング	ディセーブル

PFC QoS がイネーブルの場合のデフォルト値

ここでは、PFC QoS がイネーブルである場合に適用されるデフォルト値を示します。

- 受信キューの制限（p.42-30）
- 送信キューの制限（p.42-30）
- 帯域幅割り当て比率（p.42-31）
- デフォルトの廃棄スレッシュホールドの割合および CoS 値マッピング（p.42-31）

（注）　入力 LAN ポート信頼状態は、QoS がイネーブルで untrusted にデフォルト設定されています。

受信キューの制限

機能	デフォルト値
2q8t	ロー プライオリティ：80%
	ハイ プライオリティ：20%
8q4t	ロー プライオリティ：80%
	中間キュー：0%
	ハイ プライオリティ：20%
8q8t	最小プライオリティ：80%
	中間キュー：0%
	最大プライオリティ：20%

送信キューの制限

機能	デフォルト値
2q2t	ロー プライオリティ：80%
	ハイ プライオリティ：20%
1p2q2t	ロー プライオリティ：70%
	ハイ プライオリティ：15%
	完全優先：15%
1p2q1t	ロー プライオリティ：70%
	ハイ プライオリティ：15%
	完全優先：15%
1p3q8t	ロー プライオリティ：50%
	ミディアム プライオリティ：20%
	ハイ プライオリティ：15%
	完全優先：15%

機能	デフォルト値
1p7q4t	標準キュー 1（最小プライオリティ）：50%
	標準キュー 2：20%
	標準キュー 3：15%
	標準キュー 4 ～ 7：0%
	完全優先：15%
1p7q8t	標準キュー 1（最小プライオリティ）：50%
	標準キュー 2：20%
	標準キュー 3：15%
	標準キュー 4 ～ 7：0%
	完全優先：15%

帯域幅割り当て比率

機能	デフォルト値
2q8t	90:10
8q4t	90:0:0:0:0:0:0:10
8q8t	90:0:0:0:0:0:0:10
1p3q8t	22:33:45
1p7q4t	100:150:200:0:0:0:0:0
1p7q8t	22:33:45:0:0:0:0
1p2q1t	100:255
2q2t、**1p2q2t**、および **1p2q1t**	5:255
1p3q1t	100:150:255

デフォルトの廃棄スレッシュホールドの割合および CoS 値マッピング

次のテーブルでは、キュー タイプ別の デフォルトの廃棄スレッシュホールド値および CoS 値マッピングを示します。

- 1q2t 受信キュー（p.42-32）
- 1q4t 受信キュー（p.42-32）
- 1p1q4t 受信キュー（p.42-33）
- 1p1q0t 受信キュー（p.42-33）
- 1p1q8t 受信キュー（p.42-34）
- 1q8t 受信キュー（p.42-35）
- 2q8t 受信キュー（p.42-36）
- 8q4t 受信キュー（p.42-37）
- 8q8t 受信キュー（p.42-41）
- 2q2t 送信キュー（p.42-42）
- 1p2q2t 送信キュー（p.42-42）
- 1p3q8t 送信キュー（p.42-43）
- 1p7q4t 送信キュー（p.42-44）
- 1p7q8t 送信キュー（p.42-48）

- 1p3q1t 送信キュー（p.42-49）
- 1p2q1t 送信キュー（p.42-49）

（注）　ここに示す受信キューの値は、CoS または DSCP を信頼するようにポートを設定した場合に有効です。信頼できないポートの場合は、受信キューの値は、QoS をグローバルにディセーブルにした場合と同じ値となります。

1q2t 受信キュー

機能			デフォルト値
標準受信キュー	スレッショルド 1	CoS	0、1、2、3、4
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッショルド 2	CoS	5、6、7
		テール廃棄	100%（設定はできません）
		WRED 廃棄	サポートされません。

1q4t 受信キュー

機能			デフォルト値
標準受信キュー	スレッショルド 1	CoS	0 および 1
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッショルド 2	CoS	2 および 3
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッショルド 3	CoS	4 および 5
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッショルド 4	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。

1p1q4t 受信キュー

機能			デフォルト値
標準受信キュー	スレッショルド 1	CoS	0 および 1
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッショルド 2	CoS	2 および 3
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッショルド 3	CoS	4
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッショルド 4	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。
完全優先受信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p1q0t 受信キュー

機能		デフォルト値
標準受信キュー	CoS	0、1、2、3、4、6、7
	テール廃棄	100%（設定はできません）
	WRED 廃棄	サポートされません。
完全優先受信キュー	CoS	5
	テール廃棄	100%（設定はできません）

1p1q8t 受信キュー

機能			デフォルト値
標準受信キュー	スレッショルド 1	CoS	0
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッショルド 2	CoS	1
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、 ハイ：70%
	スレッショルド 3	CoS	2
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：50%、 ハイ：80%
	スレッショルド 4	CoS	3
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：50%、 ハイ：80%
	スレッショルド 5	CoS	4
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：60%、 ハイ：90%
	スレッショルド 6	CoS	6
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：60%、 ハイ：90%
	スレッショルド 7	CoS	7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、 ハイ：100%
完全優先受信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1q8t 受信キュー

機能			デフォルト値
標準受信キュー	スレッシュホールド 1	CoS	0
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	なし
		テール廃棄	50%
		WRED 廃棄	サポートされません。
	スレッシュホールド 3	CoS	1、2、3、4
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッシュホールド 4	CoS	なし
		テール廃棄	60%
		WRED 廃棄	サポートされません。
	スレッシュホールド 5	CoS	6 および 7
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 6	CoS	なし
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 7	CoS	5
		テール廃棄	100%
		WRED 廃棄	サポートされません。
	スレッシュホールド 8	CoS	なし
		テール廃棄	100%
		WRED 廃棄	サポートされません。

2q8t 受信キュー

機能			デフォルト値
標準受信キュー 1（ロー プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	70%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	2 および 3
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 3	CoS	4
		テール廃棄	90%
		WRED 廃棄	サポートされません。
	スレッシュホールド 4	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。
	スレッシュホールド 5 ～ 8	CoS	なし
		テール廃棄	100%
		WRED 廃棄	サポートされません。
標準受信キュー 2（ハイ プライオリティ）	スレッシュホールド 1	CoS	5
		テール廃棄	100%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2 ～ 8	CoS	なし
		テール廃棄	100%
		WRED 廃棄	サポートされません。

8q4t 受信キュー

機能			デフォルト値
標準受信キュー 1（最小プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		DSCP	0 ～ 9、11、13、15 ～ 17、19、21、23、25、27、29、31、33、39、41 ～ 45、47
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	2 および 3
		DSCP	
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：80%
	スレッシュホールド 3	CoS	4
		DSCP	
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：90%
	スレッシュホールド 4	CoS	6 および 7
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：100%
標準受信キュー 2（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	14
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	12
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	10
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%

機能			デフォルト値
標準受信キュー 3（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	22
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	20
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	18
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
標準受信キュー 4（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	24 および 30
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	28
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	26
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%

機能			デフォルト値
標準受信キュー 5（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	32、34 ～ 38
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
標準受信キュー 6（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	48 ～ 63
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%

機能			デフォルト値
標準受信キュー 7（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
標準受信キュー 8（ハイ プライオリティ）	スレッシュホールド 1	CoS	5
		DSCP	40 および 46
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%

8q8t 受信キュー

機能			デフォルト値
標準受信キュー 1（最小プライオリティ）	スレッショルド 1	CoS	0 および 1
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッショルド 2	CoS	2 および 3
		テール廃棄	ディセーブル、80%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：80%
	スレッショルド 3	CoS	4
		テール廃棄	ディセーブル、90%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：90%
	スレッショルド 4	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：100%
	スレッショルド 5 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：100%
標準受信キュー 2 ～ 7（ミディアム プライオリティ）	スレッショルド 1 ～ 8	CoS	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
標準受信キュー 8（最大プライオリティ）	スレッショルド 1	CoS	5
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッショルド 2 ～ 8	CoS	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%

2q2t 送信キュー

機能			デフォルト値
標準送信キュー 1（ロー プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	2 および 3
		テール廃棄	100%
		WRED 廃棄	サポートされません。
標準送信キュー 2（ハイ プライオリティ）	スレッシュホールド 1	CoS	4 および 5
		テール廃棄	80%
		WRED 廃棄	サポートされません。
	スレッシュホールド 2	CoS	6 および 7
		テール廃棄	100%
		WRED 廃棄	サポートされません。

1p2q2t 送信キュー

機能			デフォルト値
標準送信キュー 1（ロー プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	2 および 3
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：70%、ハイ：100%
標準送信キュー 2（ハイ プライオリティ）	スレッシュホールド 1	CoS	4
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	6 および 7
		テール廃棄	サポートされません。
		WRED 廃棄	ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p3q8t 送信キュー

機能			デフォルト値
標準送信キュー 1（最小プライオリティ）	スレッショルド 1	CoS	0
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッショルド 2	CoS	1
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッショルド 3	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッショルド 4	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッショルド 5 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：50%、ハイ：100%
標準送信キュー 2（ミディアム プライオリティ）	スレッショルド 1	CoS	2
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッショルド 2	CoS	3 および 4
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッショルド 3 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 3（ハイ プライオリティ）	スレッショルド 1	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッショルド 2 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p7q4t 送信キュー

機能			デフォルト値
標準受信キュー 1（最小プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		DSCP	0 ～ 9、11、13、15 ～ 17、19、21、23、25、27、29、31、33、39、41 ～ 45、47
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	2 および 3
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 3	CoS	4
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 4	CoS	6 および 7
		DSCP	
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準受信キュー 2（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	14
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	なし
		DSCP	12
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	10
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%

機能			デフォルト値
標準受信キュー 3（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	22
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	20
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	18
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準受信キュー 4（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	24 および 30
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	28
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	26
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%

機能			デフォルト値
標準受信キュー 5（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	32、34 ～ 38
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
標準受信キュー 6（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	48 ～ 63
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%

機能			デフォルト値
標準受信キュー 7（ミディアム プライオリティ）	スレッシュホールド 1	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 2	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 3	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
	スレッシュホールド 4	CoS	なし
		DSCP	なし
		テール廃棄	イネーブル、100%
		WRED 廃棄	ディセーブル、ロー：100%、ハイ：100%
完全優先送信キュー		CoS	5
		DSCP	40 および 46
		テール廃棄	100%（設定はできません）

1p7q8t 送信キュー

機能			デフォルト値
標準送信キュー 1（最小プライオリティ）	スレッシュホールド 1	CoS	0
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	1
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 3 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 2（ミディアム プライオリティ）	スレッシュホールド 1	CoS	2
		テール廃棄	ディセーブル、70%
		WRED 廃棄	イネーブル、ロー：40%、ハイ：70%
	スレッシュホールド 2	CoS	3 および 4
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 3 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 3（ミディアム プライオリティ）	スレッシュホールド 1	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
	スレッシュホールド 2 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：100%、ハイ：100%
標準送信キュー 4 ～ 7（ミディアム プライオリティ）	スレッシュホールド 1 ～ 8	CoS	なし
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：100%、ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p3q1t 送信キュー

機能			デフォルト値
標準送信キュー 1（最小プライオリティ）	スレッシュホールド 1	CoS	0 および 1
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 2（ミディアム プライオリティ）	スレッシュホールド 1	CoS	2、3、4
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 3（ハイ プライオリティ）	スレッシュホールド 1	CoS	6 および 7
		テール廃棄	ディセーブル、100%
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

1p2q1t 送信キュー

機能			デフォルト値
標準送信キュー 1（最小プライオリティ）	スレッシュホールド 1	CoS	0、1、2、3
		テール廃棄	サポートされません。
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
標準送信キュー 3（ハイ プライオリティ）	スレッシュホールド 1	CoS	4、6、7
		テール廃棄	サポートされません。
		WRED 廃棄	イネーブル、ロー：70%、ハイ：100%
完全優先送信キュー		CoS	5
		テール廃棄	100%（設定はできません）

PFC QoS がディセーブルの場合のデフォルト値

機能	デフォルト値
入力 LAN ポートの信頼状態	trust DSCP
受信キュー廃棄スレッシュホールドの割合	すべてのスレッシュホールドを 100% に設定
送信キュー廃棄スレッシュホールドの割合	すべてのスレッシュホールドを 100% に設定
送信キュー帯域幅割り当て比率	255:1
送信キュー容量の比率	ロー プライオリティ：100%（他のキューが使用されない場合）
CoS 値および廃棄スレッシュホールドのマッピング	すべての QoS ラベルをロー プライオリティ キューにマッピング

PFC QoS 設定時の注意事項および制約事項

PFC QoS を設定する際に、次の注意事項と制約事項に従ってください。

- 全般的な注意事項（p.42-50）
- PFC3 に関する注意事項（p.42-52）
- PFC2 に関する注意事項（p.42-52）
- クラス マップ コマンドの制約事項（p.42-53）
- ポリシー マップ コマンドの制約事項（p.42-53）
- ポリシー マップ クラス コマンドの制約事項（p.42-53）
- CIR および PIR レート値に対してサポートされる粒度（p.42-54）
- CIR および PIR トークン バケット サイズに対してサポートされる粒度（p.42-54）
- IP precedence 値と DSCP 値（p.42-55）

全般的な注意事項

- **match ip precedence** および **match ip dscp** コマンドは、IPv4 トラフィックのみをフィルタリングします。
- Release 12.2(18)SXE 以降のリリースでは、**match precedence** および **match dscp** コマンドは IPv4 および IPv6 トラフィックをフィルタリングします。
- Release 12.2(18)SXE 以降のリリースでは、**set ip dscp** および **set ip precedence** コマンドは **set dscp** および **set precedence** コマンドとしてコンフィギュレーション ファイルに保存されます。
- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は IPv4 および IPv6 トラフィックに対して **set dscp** および **set precedence** ポリシー マップ クラス コマンドをサポートします。
- QoS、NetFlow、および NetFlow Data Export（NDE; NetFlow データ エクスポート）のフローマスク要件は、特に microflow ポリシングを設定する場合に競合する可能性があります。
- 再マーキングされた DSCP に対する出力 ACL サポート、および VACL キャプチャの両方を 1 つのインターフェイス上に設定すると、VACL キャプチャによって各パケットが 2 コピーずつキャプチャされることがあります。この場合、2 つめのコピーは壊れている可能性があります。
- 再マーキングされた DSCP に対する出力 ACL サポートは、トンネル インターフェイスには設定できません。
- 再マーキングされた DSCP に対する出力 ACL のサポートは、IP ユニキャスト トラフィックをサポートします。
- 再マーキングされた DSCP に対する出力 ACL のサポートは、マルチキャスト トラフィックとは無関係です。PFC QoS は出力 QoS を適用する前に、入力 QoS の変更をマルチキャスト トラフィックに適用します。
- NetFlow および NDE は、再マーキングされた DSCP に対する出力 ACL のサポートが設定されたインターフェイスはサポートしません。
- 再マーキングされた DSCP に対する出力 ACL のサポートをいずれかのインターフェイスに設定している場合に、これを設定していないインターフェイスで NetFlow および NDE のサポートをイネーブルにするには、インターフェイス固有のフローマスクを設定する必要があります。**mls flow ip interface-destination-source**、または **mls flow ip interface-full** のいずれかのグローバル コンフィギュレーション モード コマンドを入力してください。
- 再マーキングされた DSCP に対する出力 ACL のサポートを設定しているインターフェイスでは、インターフェイス カウンタの値が不正確となります。
- 再マーキングされた DSCP に対する出力 ACL のサポートによって許可されたトラフィックには、microflow ポリシングを適用できません。
- 再マーキングされた DSCP に対する出力 ACL のサポートによって許可されたトラフィックには、MPLS トラフィックとしてタグを付けることはできません（このトラフィックは、他のネットワーク装置上では MPLS トラフィックとしてタグ付けできます）。

- 入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません（CSCea23571）。
- トラフィックに aggregate ポリシングと microflow ポリシングを実行する場合、aggregate ポリサーおよび microflow ポリサーを同じポリシー マップ クラスに組み込み、各ポリサーで同じ **conform-action** および **exceed-action** キーワード オプションを使用する必要があります（**drop**、**set-dscp-transmit**、**set-prec-transmit**、または **transmit**）。
- トンネル インターフェイス上では、PFC QoS 機能を設定できません。
- PFC QoS は、トンネル トラフィックのペイロード ToS バイトを書き換えません。
- PFC QoS フィルタリングの基準になるのは、ACL、DSCP 値、または IP precedence 値だけです。
- 次のコマンドに対し、PFC QoS は同一 ASIC によって制御されるすべての LAN ポートに、同じ設定を適用します。
  - **rcv-queue random-detect**
  - **rcv-queue queue-limit**
  - **wrr-queue queue-limit**
  - **wrr-queue bandwidth**（ギガビット イーサネット LAN ポートを除く）
  - **priority-queue cos-map**
  - **rcv-queue cos-map**
  - **wrr-queue cos-map**
  - **wrr-queue threshold**
  - **rcv-queue threshold**
  - **wrr-queue random-detect**
  - **wrr-queue random-detect min-threshold**
  - **wrr-queue random-detect max-threshold**
- これらのコマンドは、物理ポートのみで設定してください。論理インターフェイスでは設定できません。
  - **priority-queue cos-map**
  - **wrr-queue cos-map**
  - **wrr-queue random-detect**
  - **wrr-queue random-detect max-threshold**
  - **wrr-queue random-detect min-threshold**
  - **wrr-queue threshold**
  - **wrr-queue queue-limit**
  - **wrr-queue bandwidth**
  - **rcv-queue cos-map**
  - **rcv-queue bandwidth**
  - **rcv-queue random-detect**
  - **rcv-queue random-detect max-threshold**
  - **rcv-queue random-detect min-threshold**
  - **rcv-queue queue-limit**
  - **rcv-queue cos-map**
  - **rcv-queue threshold**

PFC3 に関する注意事項

- Release 12.2(18)SXE 以降のリリースでは、PFC3 の全バージョンで、IPv6 ユニキャストおよびマルチキャスト トラフィックに対する QoS がサポートされます。
- IPv6 PFC QoS についての情報を表示するには、**show mls qos ipv6** コマンドを入力します。
- ポート ASIC（キュー アーキテクチャおよびデキューイング アルゴリズム）に実装された QoS 機能は、IPv4 および IPv6 トラフィックをサポートします。
- PFC3 は、IPv6 の名前付き拡張 ACL、および名前付き標準 ACL をサポートします。
- Release 12.2(18)SXE 以降のリリースでは、PFC3 は **match protocol ipv6** コマンドをサポートします。
- TCAM 検索のフロー キー ビット要件が競合するため、IPv6 DSCP ベースのフィルタリングとレイヤ 4 範囲ベースのフィルタリングを同一インターフェイス上に設定することはできません。次に、例を示します。
  - 1 つの IPv6 ACE 内に DSCP 値と、レイヤ 4 の greater than（gt）または less than（lt）演算子の両方を設定した場合は、この ACL は PFC QoS フィルタリングには使用できません。
  - 1 つの IPv6 ACL 内に DSCP 値を設定し、別の IPv6 ACL 内にレイヤ 4 の greater than（gt）または less than（lt）演算子を設定した場合は、同一インターフェイス上の異なるクラス マップで両方の ACL を使用して、PFC QoS フィルタリングを行うことはできません。
- Release 12.2(18)SXE 以降のリリースでは、IPv6 トラフィックに aggregate ポリサーおよび microflow ポリサーを適用できます。
- 再マーキングされた DSCP に対する出力 ACL サポートを設定すると、PFC3 は次の機能に対するハードウェア支援を行わなくなります。
  - Cisco IOS 再帰 ACL
  - TCP インターセプト
  - Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）
  - Network Address Translation（NAT; ネットワーク アドレス変換）
- PFC3 では、microflow ポリシングを ARP トラフィックに適用できません。
- PFC3 は、MSFC3 へブリッジされるトラフィックに出力ポリシングを適用しません。
- PFC3 は、MSFC3 からのマルチキャスト トラフィックに出力ポリシングまたは出力 DSCP 変換を適用しません。
- PFC3 では、PFC QoS はブリッジド マルチキャスト トラフィックの ToS バイトを書き換えません。

PFC2 に関する注意事項

- PFC2 は **match protocol** クラス マップ コマンドをサポートしています。これにより、NBAR を設定して、レイヤ 3 インターフェイスの入出力両方のトラフィックをすべて送信し、MSFC2 ソフトウェアで処理できます。NBAR を設定するには、次のマニュアルを参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm
- PFC2 は、次の PFC QoS 機能をサポートしていません。
  - 出力ポリシング
  - 出力 DSCP 変換
  - DSCP の透過性
  - DFC が取り付けられている場合の VLAN ベースの QoS
- PFC2 は、IEEE 802.1Q トンネル ポートでの入力 CoS 変換に対応したモジュールをサポートしていません。

クラス マップ コマンドの制約事項

- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は **match any** クラス マップ コマンドをサポートします。
- PFC QoS は、**match** コマンドが ***1 つだけ***指定されているクラス マップをサポートします。
- PFC QoS では、次のクラス マップ コマンドはサポートされません。
  - **match cos**
  - **match any**
  - **match classmap**
  - **match destination-address**
  - **match input-interface**
  - **match qos-group**
  - **match source-address**

ポリシー マップ コマンドの制約事項

PFC QoS では、次のポリシー マップ コマンドはサポートされません。

- **class** *class_name* **destination-address**
- **class** *class_name* **input-interface**
- **class** *class_name* **protocol**
- **class** *class_name* **qos-group**
- **class** *class_name* **source-address**

ポリシー マップ クラス コマンドの制約事項

PFC QoS では、次のポリシー マップ クラス コマンドはサポートされません。

- **bandwidth**
- **priority**
- **queue-limit**
- **random-detect**
- **set qos-group**
- **service-policy**

CIR および PIR レート値に対してサポートされる粒度

PFC QoS では、CIR および PIR レート値に対し、ハードウェアで次の粒度が使用されます。

CIR および PIR レート値の範囲	粒度
32768 ～ 2097152（2 Mbs）	32768（32 Kb）
2097153 ～ 4194304（4 Mbs）	65536（64 Kb）
4194305 ～ 8388608（8 Mbs）	131072（128 Kb）
8388609 ～ 16777216（16 Mbs）	262144（256 Kb）
16777217 ～ 33554432（32 Mbs）	524288（512 Kb）
33554433 ～ 67108864（64 Mbs）	1048576（1 Mb）
67108865 ～ 134217728（128 Mbs）	2097152（2 Mb）
134217729 ～ 268435456（256 Mbs）	4194304（4 Mb）
268435457 ～ 536870912（512 Mbs）	8388608（8 Mb）
536870913 ～ 1073741824（1 Gps）	16777216（16 Mb）
1073741825 ～ 2147483648（2 Gps）	33554432（32 Mb）
2147483649 ～ 4294967296（4 Gps）	67108864（64 Mb）
4294967296 ～ 8589934592（8 Gps）	134217728（128 Mb）
8589934592 ～ 10000000000（10 Gps）	268435456（256 Mb）

各範囲で、PFC QoS は粒度の倍数に相当するレート値を使用して、PFC をプログラミングします。

CIR および PIR トークン バケット サイズに対してサポートされる粒度

PFC QoS では、CIR および PIR トークン バケット（バースト）サイズに対し、ハードウェアで次の粒度が使用されます。

CIR および PIR トークン バケット サイズの範囲	粒度
1 ～ 32768（32 KB）	1024（1 KB）
32769 ～ 65536（64 KB）	2048（2 KB）
65537 ～ 131072（128 KB）	4096（4 KB）
131073 ～ 262144（256 KB）	8196（8 KB）
262145 ～ 524288（512 KB）	16392（16 KB）
524289 ～ 1048576（1 MB）	32768（32 KB）
1048577 ～ 2097152（2 MB）	65536（64 KB）
2097153 ～ 4194304（4 MB）	131072（128 KB）
4194305 ～ 8388608（8 MB）	262144（256 KB）
8388609 ～ 16777216（16 MB）	524288（512 KB）
16777217 ～ 33554432（32 MB）	1048576（1 MB）

各範囲で、PFC QoS は粒度の倍数に相当するトークン バケット サイズを使用して、PFC をプログラミングします。

IP precedence 値と DSCP 値

3 ビット IP precedence	ToS の MSb 6 ビット[1]						6 ビット DSCP
	8	7	6	5	4	3	
0	0	0	0	0	0	0	0
	0	0	0	0	0	1	1
	0	0	0	0	1	0	2
	0	0	0	0	1	1	3
	0	0	0	1	0	0	4
	0	0	0	1	0	1	5
	0	0	0	1	1	0	6
	0	0	0	1	1	1	7
1	0	0	1	0	0	0	8
	0	0	1	0	0	1	9
	0	0	1	0	1	0	10
	0	0	1	0	1	1	11
	0	0	1	1	0	0	12
	0	0	1	1	0	1	13
	0	0	1	1	1	0	14
	0	0	1	1	1	1	15
2	0	1	0	0	0	0	16
	0	1	0	0	0	1	17
	0	1	0	0	1	0	18
	0	1	0	0	1	1	19
	0	1	0	1	0	0	20
	0	1	0	1	0	1	21
	0	1	0	1	1	0	22
	0	1	0	1	1	1	23
3	0	1	1	0	0	0	24
	0	1	1	0	0	1	25
	0	1	1	0	1	0	26
	0	1	1	0	1	1	27
	0	1	1	1	0	0	28
	0	1	1	1	0	1	29
	0	1	1	1	1	0	30
	0	1	1	1	1	1	31

3 ビット IP precedence	ToS の MSb 6 ビット[1]						6 ビット DSCP
	8	7	6	5	4	3	
4	1	0	0	0	0	0	32
	1	0	0	0	0	1	33
	1	0	0	0	1	0	34
	1	0	0	0	1	1	35
	1	0	0	1	0	0	36
	1	0	0	1	0	1	37
	1	0	0	1	1	0	38
	1	0	0	1	1	1	39
5	1	0	1	0	0	0	40
	1	0	1	0	0	1	41
	1	0	1	0	1	0	42
	1	0	1	0	1	1	43
	1	0	1	1	0	0	44
	1	0	1	1	0	1	45
	1	0	1	1	1	0	46
	1	0	1	1	1	1	47
6	1	1	0	0	0	0	48
	1	1	0	0	0	1	49
	1	1	0	0	1	0	50
	1	1	0	0	1	1	51
	1	1	0	1	0	0	52
	1	1	0	1	0	1	53
	1	1	0	1	1	0	54
	1	1	0	1	1	1	55
7	1	1	1	0	0	0	56
	1	1	1	0	0	1	57
	1	1	1	0	1	0	58
	1	1	1	0	1	1	59
	1	1	1	1	0	0	60
	1	1	1	1	0	1	61
	1	1	1	1	1	0	62
	1	1	1	1	1	1	63

1. MSb = Most Significant bit（最上位ビット）

PFC QoS の設定

ここでは、Catalyst 6500 シリーズ スイッチ上で PFC QoS を設定する手順について説明します。

- PFC QoS のグローバルなイネーブル化（p.42-56）
- ignore port trust のイネーブル化（p.42-57）
- DSCP の透過性の設定（p.42-58）
- queueing-only モードのイネーブル化（p.42-58）
- ブリッジド トラフィックの microflow ポリシングのイネーブル化（p.42-59）
- レイヤ 2 LAN ポートでの VLAN ベース PFC QoS のイネーブル化（p.42-60）
- 再マーキングされた DSCP に対する出力 ACL のサポートのイネーブル化（p.42-61）
- 名前付き aggregate ポリサーの作成（p.42-62）
- PFC QoS ポリシーの設定（p.42-64）
- PFC3 による出力 DSCP 変換の設定（p.42-82）
- IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定（p.42-84）
- DSCP 値マッピングの設定（p.42-86）
- イーサネット LAN ポートおよび OSM ポートの信頼状態の設定（p.42-90）
- 入力 LAN ポート CoS 値の設定（p.42-91）
- 標準キューの廃棄スレッシュホールドの割合設定（p.42-92）
- QoS ラベルのキューおよび廃棄スレッシュホールドへのマッピング（p.42-98）
- 標準送信キュー間での帯域幅の割り当て（p.42-108）
- 受信キューのサイズ比の設定（p.42-110）
- 送信キューのサイズ比の設定（p.42-111）

（注）　PFC QoS は、ユニキャスト トラフィックおよびマルチキャスト トラフィックの両方を処理します。

PFC QoS のグローバルなイネーブル化

PFC QoS をグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos`	スイッチで PFC QoS をグローバルにイネーブルにします。
	`Router(config)# no mls qos`	スイッチで PFC QoS をグローバルにディセーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos [ipv6]`	設定を確認します。

次に、PFC QoS をグローバルにイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# mls qos
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos
  QoS is enabled globally
  Microflow QoS is enabled globally

QoS global counters:
    Total packets: 544393
    IP shortcut packets: 1410
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 467
    IP packets with COS changed by policing: 59998
    Non-IP packets with COS changed by policing: 0

Router#
```

ignore port trust のイネーブル化

Release 12.2(18)SXF5 以降のリリースでは、ignore port trust 機能を使用できます。これにより、入力ポリシーにおいて、設定済みの IP precedence または DSCP 値を、信頼できないトラフィックだけではなくすべてのトラフィックに適用できます。

ignore port trust をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos marking ignore port-trust`	スイッチで ignore port trust をグローバルにイネーブルにします。
	`Router(config)# no mls qos marking ignore port-trust`	スイッチで ignore port trust をグローバルにディセーブルにします（デフォルト）。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos | include ignores`	設定を確認します。

（注）　信頼できないトラフィックにおいて、ignore port trust がイネーブルにされている場合は、PFC QoS によって次の処理が行われます。

- IP トラフィックでは、PFC QoS は受信した DSCP 値を初期内部 DSCP 値として使用します。
- 認識可能な ToS バイトが含まれないトラフィックの場合は、ポートの CoS 値が初期内部 DSCP 値にマッピングされます。

次に、ignore port trust をイネーブルにし、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# mls qos marking ignore port-trust
Router(config)# end
Router# show mls qos | include ignores
  Policy marking ignores port_trust
Router#
```

DSCP の透過性の設定

（注）
- 他の IP トラフィックへのサポートに加え、PFC3B および PFC3BXL は MPLS トラフィック、IP トンネルの IP のトラフィック、GRE トンネルのトラフィックに対して、**no mls qos rewrite ip dscp** コマンドをサポートします。
- PFC3A は、MPLS トラフィック、IP トンネルの IP のトラフィック、GRE トンネルのトラフィック以外の IP トラフィックすべてに対して、**no mls qos rewrite ip dscp** コマンドをサポートします。

DSCP 透過性をイネーブルにして、受信したレイヤ 3 ToS バイトを保持するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# no mls qos rewrite ip dscp`	スイッチで ToS バイトの書き換えをグローバルにディセーブルにします。
	`Router(config)# mls qos rewrite ip dscp`	スイッチで ToS バイトの書き換えをグローバルにイネーブルにします。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos | include rewrite`	設定を確認します。

受信したレイヤ 3 ToS バイトを保持する場合、QoS では出力キューイング用に、およびタグ付き出力トラフィックで、マーキングした CoS 値またはマークダウンした CoS 値が使用されます。

次に、受信したレイヤ 3 ToS バイトを保持し、その設定を確認する例を示します。

```
Router# configure terminal
Router(config)# no mls qos rewrite ip dscp
Router(config)# end
Router# show mls qos | include rewrite
  QoS ip packet dscp rewrite disabled globally
Router#
```

queueing-only モードのイネーブル化

スイッチで queueing-only モードをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos queueing-only`	スイッチで queueing-only モードをイネーブルにします。
	`Router(config)# no mls qos queueing-only`	スイッチで PFC QoS をグローバルにディセーブルにします。 （注）queueing-only モードを個別にディセーブルにすることはできません。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos`	設定を確認します。

queueing-only モードをイネーブルにする場合、スイッチは次の処理を行います。

- マーキングおよびポリシングをグローバルにディセーブルにします。
- すべてのポートがレイヤ 2 CoS を信頼するように設定します。

（注）　スイッチでは、タグなし入力トラフィックと、trust CoS に設定できないポートを介して受信されるトラフィックにポート CoS 値が適用されます。

次に、queueing-only モードをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# mls qos queueing-only
Router(config)# end
Router#
```

ブリッジド トラフィックの microflow ポリシングのイネーブル化

（注）　PFC2 の場合、マルチキャスト トラフィックに microflow ポリシングを適用するには、レイヤ 3 マルチキャスト入力インターフェイスで **mls qos bridged** コマンドを入力する必要があります。

デフォルトでは、microflow ポリサーはルーテッド トラフィックだけに影響します。特定の VLAN 上のブリッジド トラフィックに対して microflow ポリシングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type[1] slot/port}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos bridged`	VLAN 上で、ブリッジド トラフィック（ブリッジ グループも含む）の microflow ポリシングをイネーブルにします。
	`Router(config-if)# no mls qos bridged`	ブリッジド トラフィックの microflow ポリシングをディセーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show mls qos`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、VLAN 3 ～ 5 のブリッジド トラフィックに対して microflow ポリシングをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface range vlan 3 - 5
Router(config-if)# mls qos bridged
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos | begin Bridged QoS
Bridged QoS is enabled on the following interfaces:
    Vl3 Vl4 Vl5
(テキスト出力は省略)
Router#
```

レイヤ 2 LAN ポートでの VLAN ベース PFC QoS のイネーブル化

（注）
- PFC2 では、DFC が搭載されている場合、VLAN ベースの QoS は PFC QoS によってサポートされません。
- PFC3 では、DFC3 が搭載されている場合、VLAN ベースの QoS がサポートされます。
- PFC3 では、出力トラフィックに対する PFC QoS アプリケーション用に、レイヤ 3 インターフェイスにポリシー マップを付加できます。レイヤ 2 ポート上の VLAN ベースまたはポート ベースの PFC QoS は、レイヤ 3 インターフェイス上の出力トラフィックに対する PFC QoS アプリケーションとは関係ありません。

デフォルトでは、PFC QoS は LAN ポートに付加されたポリシー マップを使用します。**switchport** キーワードを使用してレイヤ 2 LAN ポートとして設定されているポートでは、PFC QoS が VLAN に付加されたポリシー マップを使用するように設定できます。**switchport** キーワードを使用せずに設定されたポートは、VLAN に対応付けられません。

レイヤ 2 LAN ポートで VLAN ベース PFC QoS をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{`*type*[1] *slot/port*`} | {port-channel` *number*`}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos vlan-based`	レイヤ 2 LAN ポートまたはレイヤ 2 EtherChannel で VLAN ベース PFC QoS をイネーブルにします。
	`Router(config-if)# no mls qos vlan-based`	VLAN ベース PFC QoS をディセーブルにします。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show mls qos`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート FastEthernet 5/42 で VLAN ベースの PFC QoS をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/42
Router(config-if)# mls qos vlan-based
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show mls qos | begin QoS is vlan-based
  QoS is vlan-based on the following interfaces:
    Fa5/42
(テキスト出力は省略)
```

（注）　レイヤ 2 LAN ポートを VLAN ベースの PFC QoS に設定しても、ポリシー マップに関するポート設定はそのままの状態です。**no mls qos vlan-based** ポート コマンドを使用すると、すでに設定されていたポート コマンドが再びイネーブルになります。

再マーキングされた DSCP に対する出力 ACL のサポートのイネーブル化

再マーキングされた DSCP に対する出力 ACL のサポートを、入力インターフェイスでイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}}	設定する入力インターフェイスを選択します。
ステップ 2	Router(config-if)# **platform ip features sequential** [**access-group** *IP_acl_name_or_number*]	再マーキングされた DSCP に対する出力 ACL のサポートを、入力インターフェイス上でイネーブルにします。
	Router(config-if)# **no platform ip features sequential** [**access-group** *IP_acl_name_or_number*]	再マーキングされた DSCP に対する出力 ACL のサポートを、入力インターフェイス上でディセーブルにします。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show running-config interface** ({*type*[1] *slot/port*} | {**port-channel** *number*}}	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

再マーキングされた DSCP に対する出力 ACL のサポートを入力インターフェイスに設定する場合は、次の点に注意してください。

- 再マーキングされた DSCP に対する出力 ACL のサポートを、特定の標準 ACL、拡張名前付き ACL、または拡張番号付き IP ACL によってフィルタリングしたトラフィックのみに対してイネーブルにするには、IP ACL の名前または番号を入力します。
- IP ACL 名または番号を入力しないと、再マーキングされた DSCP に対する出力 ACL のサポートは、インターフェイス上のすべての IP 入力 IP トラフィックに対してイネーブルになります。

次に、再マーキングされた DSCP に対する出力 ACL のサポートを、ポート FastEthernet 5/36 上でイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# platform ip features sequential
Router(config-if)# end
```

名前付き aggregate ポリサーの作成

名前付き aggregate ポリサーを作成するには、次の作業を行います。

コマンド	目的
`Router(config)# mls qos aggregate-policer` *policer_name bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir** *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit**[1] *dscp_value* | **set-prec-transmit**[1] *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	名前付き aggregate ポリサーを作成します。
`Router(config)# no mls qos aggregate-policer` *policer_name*	名前付き aggregate ポリサーを削除します。

1. **set-dscp-transmit** および **set-prec-transmit** キーワードは、IP トラフィックに対してのみサポートされます。

名前付き aggregate ポリサーを作成する場合、次の点に注意してください。

- aggregate ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。aggregate ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。aggregate ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチングされた仮想インターフェイスに適用されたポリサー
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。
- Release 12.2(18)SXE 以降のリリースでは、IPv6 トラフィックに aggregate ポリサーを適用できます。
- PFC3 のポリシングでは、レイヤ 2 のフレーム サイズを使用します。
- PFC2 のポリシングでは、レイヤ 3 のパケット サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS 設定時の注意事項および制約事項」（p.42-50）を参照してください。
- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 — 32 Kbps（32000 と入力）
  - Release 12.2(18)SXE 以降のリリースでの最大：
    10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE より前のリリースでの最大：
    4 Gbps（4000000000 と入力）
- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。
- *maximum_burst_bytes* パラメータでは、PIR トークン バケット サイズを設定します。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - 最小トークン バケット サイズは 1 KB（1000 と入力）（*maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります）。
  - 最大トークン バケット サイズは 32 MB（32000000 と入力）。

- 特定のレートを維持するには、トークン バケット サイズがレート値を 4000 で割った値よりも大きくなるように設定します。トークンは 1 秒の 4000 分の 1（0.25 ミリ秒）ごとにバケットから削除されるからです。
- トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、パラメータには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
- TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。

- 有効な **pir** *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 **—** 32 Kbps（32000 と入力、CIR *bits_per_second* パラメータより小さい値は使用できません）
  - Release 12.2(18)SXE 以降のリリースでの最大：
    10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE より前のリリースでの最大：
    4 Gbps（4000000000 と入力）
- （任意）一致する適合トラフィックに対応する conform アクションを、次のように指定できます。
  - デフォルトの conform アクションは **transmit** です。このアクションでは、ポリシー マップ クラスに **trust** コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が *trust dscp* に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマークするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマークします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してのみサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 一致したトラフィックをすべて廃棄するには、**drop** キーワードを入力します。

（注）　**drop** を conform アクションとして設定すると、PFC QoS は **drop** を exceed アクションおよび violate アクションとして設定します。

- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

（注）　exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致した不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

（注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- （任意）PIR を超過するトラフィックについて、violate アクションを次のように指定できます。
  - ポリシングを行わずにトラフィックをマーキングするには、**transmit** キーワードを入力して、一致する不適合トラフィックをすべて送信します。
  - デフォルトの violate アクションは、exceed アクションと同じものです。
  - 一致した不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。
  - ポリシングを行わずにマーキングするには、**transmit** キーワードを入力して、一致した不適合トラフィックをすべて送信します。

（注）　入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。

次に、1 Mbps のレート制限および 10 MB のバースト サイズの名前付き aggregate ポリサーを作成し、適合するトラフィックを送信し、不適合トラフィックをマークダウンする例を示します。

```
Router(config)# mls qos aggregate-policer aggr-1 1000000 10000000 conform-action
transmit exceed-action policed-dscp-transmit
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos aggregate-policer aggr-1
ag1 1000000 1000000 conform-action transmit exceed-action policed-dscp-transmit AgId=0
[pol4]
Router#
```

出力では次の情報が表示されます。

- ハードウェア ポリサー ID は、**AgId** パラメータで表示されます。
- ポリサーを使用しているポリシー マップは、角カッコ（[]）で囲まれて表示されます。

PFC QoS ポリシーの設定

ここでは、PFC QoS ポリシーの設定手順について説明します。

- PFC QoS ポリシー設定作業の概要（p.42-65）
- MAC ACL の設定（p.42-66）
- QoS フィルタリングに対する ARP ACL の設定（p.42-69）
- クラス マップの設定（p.42-70）
- クラス マップの設定の確認（p.42-72）
- ポリシー マップの設定（p.42-73）
- ポリシー マップの設定の確認（p.42-80）
- インターフェイスへのポリシー マップの付加（p.42-80）

（注）　PFC QoS ポリシーは、ユニキャスト トラフィックおよびマルチキャスト トラフィックの両方を処理します。

PFC QoS ポリシー設定作業の概要

（注）　帯域幅利用を制限しないでトラフィックをマーキングするには、適合するトラフィックと適合しないトラフィックの両方に対して、**transmit** キーワードを使用するポリサーを作成します。

次に示すコマンドを使用すると、トラフィック クラスおよびトラフィック クラスに適用されるポリシーが設定され、ポートにポリシーが付加されます。

- **access-list**（IP トラフィックの場合は任意です。IP トラフィックは **class-map** コマンドでフィルタリングできます。）
  - PFC QoS は、次の ACL タイプをサポートしています。

プロトコル	番号付き ACL の有無	拡張 ACL の有無	名前付き ACL の有無
IPv4	あり： 1 ～ 99 1300 ～ 1999	あり： 100 ～ 199 2000 ～ 2699	あり
IPv6	—	あり（名前付き）	あり
IPX （PFC2 でのみサポート）	あり：800 ～ 899	あり：900 ～ 999	あり
MAC レイヤ	なし	なし	あり
ARP	なし	なし	あり

  - Release 12.2(18)SXE 以降のリリースでは、PFC3 は IPv6 名前付き拡張 ACL、および名前付き標準 ACL をサポートします。
  - Release 12.2(18)SXD 以降のリリースでは、PFC3 は ARP ACL をサポートします。

（注）
— PFC2 は IP ACL を ARP トラフィックに適用します。
— PFC3 は IP ACL を ARP トラフィックに適用しません。
— PFC3 の場合は、microflow ポリシングを ARP トラフィックに適用できません。

  - PFC3 は IPX ACL をサポートしません。PFC3 では、IPX トラフィックをフィルタリングするように MAC ACL を設定できます。
  - PFC2 の場合、PFC QoS は、*source-network* パラメータ、任意の *destination-network* パラメータ、任意の *destination-node* パラメータを備えた IPX ACL をサポートしています。PFC QoS は、他のパラメータ（*source-node*、*protocol*、*source-socket*、*destination-socket*、または *service-type* など）を備えた IPX ACL をサポートしていません。
  - PFC2 または PFC3 の場合、PFC QoS は時間ベースの Cisco IOS ACL をサポートします。
  - MAC ACL および ARP ACL 以外の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide*』Release 12.2 の「Traffic Filtering and Firewalls」を参照してください。
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/index.htm
  - Catalyst 6500 シリーズ スイッチの ACL の詳細については、第 34 章「ネットワーク セキュリティの設定」を参照してください。
- **class-map**（任意）— **class-map** コマンドを使用してトラフィックの分類基準を指定することにより、1 つまたは複数のトラフィック クラスを定義します。

- **policy-map — policy-map** コマンドを使用して、次の定義を行います。
  - ポリシー マップ クラスの信頼モード
  - aggregate ポリシングおよびマーキング
  - microflow ポリシングおよびマーキング
- **service-policy — service-policy** 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。

MAC ACL の設定

ここでは、MAC ACL の設定手順について説明します。

- プロトコル独立型 MAC ACL フィルタリングの設定（p.42-66）
- VLAN ベースの MAC QoS フィルタリングのイネーブル化（p.42-67）
- MAC ACL の設定（p.42-68）

（注）　VLAN ACL（VACL）で MAC ACL を使用できます。詳細については、第 36 章「VACL の設定」を参照してください。

プロトコル独立型 MAC ACL フィルタリングの設定

Release 12.2(18)SXD 以降のリリースでは、PFC3BXL モードおよび PFC3B モードは、プロトコル独立型 MAC ACL フィルタリングをサポートします。プロトコル独立型 MAC ACL フィルタリングでは、MAC ACL をすべての入力トラフィック タイプ（MAC レイヤ トラフィックのほかに IPv4 トラフィック、IPv6 トラフィック、MPLS トラフィックなど）に適用します。

次のインターフェイス タイプを プロトコル独立型 MAC ACL フィルタリングに設定できます。

- IP アドレスのない VLAN インターフェイス
- EoMPLS をサポートするように設定された物理 LAN ポート
- EoMPLS をサポートするように設定された論理 LAN サブインターフェイス

プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否された入力トラフィックは、出力インターフェイスによって MAC レイヤ トラフィックとして処理されます。プロトコル独立型 MAC ACL フィルタリング用に設定されたインターフェイスの MAC ACL によって許可または拒否されたトラフィックに、出力 IP ACL を適用することはできません。

プロトコル独立型 MAC ACL フィルタリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type[1] slot/port[.subinterface]} | {port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mac packet-classify`	インターフェイス上でプロトコル独立型 MAC ACL フィルタリングをイネーブルにします。
	`Router(config-if)# no mac packet-classify`	インターフェイス上でプロトコル独立型 MAC ACL フィルタリングをディセーブルにします。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

プロトコル独立型 MAC ACL フィルタリングを設定する場合、次の点に注意してください。

- IP アドレスが設定されている VLAN インターフェイス上で、プロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックがブリッジされる場合、またはレイヤ 3 がハードウェアで PFC3BXL によってスイッチングされる場合は、microflow ポリシングにプロトコル独立型 MAC ACL フィルタリングを設定しないでください。
- 許可トラフィックが MSFC3 によってソフトウェアでルーティングされる場合は、プロトコル独立型 MAC ACL フィルタリングは microflow ポリシングをサポートします。

次に、VLAN インターフェイス 4018 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface vlan 4018
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface vlan 4018 | begin 4018
interface Vlan4018
mtu 9216
ipv6 enable
mac packet-classify
end
```

次に、インターフェイス GigabitEthernet 6/1 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface gigabitethernet 6/1
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface gigabitethernet 6/1 | begin 6/1
interface GigabitEthernet6/1
mtu 9216
no ip address
mac packet-classify
mpls l2transport route 4.4.4.4 4094
end
```

次に、インターフェイス GigabitEthernet 3/24 およびサブインターフェイス 4000 をプロトコル独立型 MAC ACL フィルタリングに設定し、設定を確認する例を示します。

```
Router(config)# interface gigabitethernet 3/24.4000
Router(config-if)# mac packet-classify
Router(config-if)# end
Router# show running-config interface gigabitethernet 3/24.4000 | begin 3/24.4000
interface GigabitEthernet3/24.4000
encapsulation dot1Q 4000
mac packet-classify
mpls l2transport route 4.4.4.4 4000
end
```

VLAN ベースの MAC QoS フィルタリングのイネーブル化

Release 12.2(18)SXD 以降のリリースでは、MAC ACL の VLAN ベースの QoS フィルタリングを、PFC3BXL または PFC3B モードでグローバルにイネーブルまたはディセーブルにできます。MAC ACL の VLAN ベースの QoS フィルタリングは、デフォルトではディセーブルに設定されています。

MAC ACL の VLAN ベースの QoS フィルタリングをイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# mac packet-classify use vlan`	MAC ACL の VLAN ベースの QoS フィルタリングをイネーブルにします。

MAC ACL の VLAN ベースの QoS フィルタリングをディセーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# no mac packet-classify use vlan`	MAC ACL の VLAN ベースの QoS フィルタリングをディセーブルにします。

MAC ACL の設定

MAC アドレスに基づいて IPX（PFC3 でのみサポートされている MAC ACL による IPX フィルタリング）、DECnet、AppleTalk、VINES、または XNS トラフィックをフィルタリングする名前付き ACL を設定できます。

Release 12.2(17b)SXA 以降のリリースの PFC3BXL または PFC3B モードでは、VLAN ベースのフィルタリング、CoS ベースのフィルタリング、または両方のフィルタリングを行うように MAC ACL を設定できます。

Release 12.2(18)SXD 以降のリリースでは、MAC ACL の VLAN ベースの QoS フィルタリングを、グローバルにイネーブルまたはディセーブルにできます（デフォルトではディセーブル）。

MAC ACL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mac access-list extended` *list_name*	MAC ACL を設定します。
	`Router(config)# no mac access-list extended` *list_name*	MAC ACL を削除します。
ステップ 2	`Router(config-ext-macl)#` {**permit** | **deny**} {*src_mac_mask* | **any**} {*dest_mac_mask* | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]	MAC ACL に Access Control Entry（ACE; アクセス制御エントリ）を設定します。
	`Router(config-ext-macl)# no` {**permit** | **deny**} {*src_mac_mask* | **any**} {*dest_mac_mask* | **any**} [{*protocol_keyword* | {*ethertype_number ethertype_mask*}} [**vlan** *vlan_ID*] [**cos** *cos_value*]]	MAC ACL から ACE を削除します。

MAC レイヤ ACL のエントリを設定する場合、次の点に注意してください。

- PFC3 は、**ipx-arpa** および **ipx-non-arpa** キーワードをサポートしています。
- PFC2 は、**ipx-arpa** および **ipx-non-arpa** キーワードをサポートしていません。
- **vlan** および **cos** キーワードは、Release 12.2(17b)SXA 以降のリリースの PFC3BXL または PFC3B モードでサポートされます。
- **vlan** および **cos** キーワードは、VACL フィルタリングに使用する MAC ACL ではサポートされません。
- Release 12.2(18)SXD 以降のリリースでは、MAC ACL の VLAN ベースの QoS フィルタリングに対する **vlan** キーワードは、グローバルにイネーブルまたはディセーブルにできます。デフォルトではディセーブルに設定されています。
- MAC アドレスは、ドット付き 16 進表記の 3 つの 4 バイト値で入力できます。たとえば、0030.9629.9f84 を入力できます。
- MAC アドレス マスクは、ドット付き 16 進表記の 3 つの 4 バイト値で入力できます。1 のビットをワイルドカードとして使用します。たとえば、アドレスを完全に一致させるには、0000.0000.0000 を使用します（0.0.0 と入力してもかまいません）。
- EtherType および EtherType マスクを 16 進値で入力できます。
- プロトコル パラメータを指定しないエントリは、どのプロトコルとも一致します。

- ACL　エントリは、入力順に従ってスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを向上させるには、最もよく使用されるエントリを ACL の先頭に置きます。
- ACL の末尾に **permit any any** エントリを明示的に指定する場合を除いて、ACL の末尾には暗黙的な **deny any any** エントリが存在します。
- 既存のリストに新しいエントリを追加すると、新しいエントリはすべてリストの末尾に置かれます。リストの途中にエントリを追加することはできません。
- 次に、EtherType の値と対応するプロトコル キーワードを示します。
  - 0x0600 — xns-idp — Xerox XNS IDP
  - 0x0BAD — vines-ip — Banyan VINES IP
  - 0x0baf — vines-echo — Banyan VINES Echo
  - 0x6000 — etype-6000 — DEC 未割り当て、実験的
  - 0x6001 — mop-dump — DEC Maintenance Operation Protocol（MOP）ダンプ / ロード補助
  - 0x6002 — mop-console — DEC MOP リモート コンソール
  - 0x6003 — decnet-iv — DEC DECnet Phase IV Route
  - 0x6004 — lat — DEC Local Area Transport（LAT）
  - 0x6005 — diagnostic — DEC DECnet Diagnostics
  - 0x6007 — lavc-sca — DEC Local-Area VAX Cluster（LAVC）、SCA
  - 0x6008 — amber — DEC AMBER
  - 0x6009 — mumps — DEC MUMPS
  - 0x0800 — ip — Malformed、invalid、または deliberately corrupt IP フレーム
  - 0x8038 — dec-spanning — DEC LANBridge Management
  - 0x8039 — dsm — DEC DSM/DDP
  - 0x8040 — netbios — DEC PATHWORKS DECnet NETBIOS Emulation
  - 0x8041 — msdos — DEC Local Area System Transport
  - 0x8042 — etype-8042 — DEC 未割り当て
  - 0x809B — appletalk — Kinetics EtherTalk（AppleTalk over Ethernet）
  - 0x80F3 — aarp — Kinetics AppleTalk Address Resolution Protocol（AARP）

次に、mac_layer という名前の MAC レイヤ ACL を作成する例を示します。この ACL は、送信元アドレスが 0000.4700.0001、宛先アドレスが 0000.4700.0009 である dec-phase-iv トラフィックを拒否しますが、それ以外のトラフィックをすべて許可します。

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# permit any any
```

QoS フィルタリングに対する ARP ACL の設定

（注）
- PFC2 では、IP ACL を ARP トラフィックに適用します。
- PFC3 では、IP ACL を ARP トラフィックに適用しません。
- PFC3 では、microflow ポリシングを ARP トラフィックに適用できません。

PFC3 および Release 12.2(18)SXD 以降のリリースを使用する場合、ARP トラフィック（EtherType 0x0806）を QoS にフィルタリングする名前付き ACL を設定できます。

QoS フィルタリング用に ARP ACL を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# arp access-list list_name`	QoS フィルタリングに ARP ACL を設定します。
	`Router(config)# no arp access-list list_name`	ARP ACL を削除します。
ステップ 2	`Router(config-arp-nacl)# {permit | deny} {ip {any | host sender_ip | sender_ip sender_ip_wildcardmask} mac any`	QoS フィルタリングに対する ARP ACL の ACE を設定します。
	`Router(config-arp-nacl)# no {permit | deny} {ip {any | host sender_ip | sender_ip sender_ip_wildcardmask} mac any`	ARP ACL から ACE を削除します。

ARP ACL のエントリを QoS フィルタリングに設定する場合、次の点に注意してください。

- このマニュアルでは、PFC3 によってハードウェアでサポートされる ARP ACL 構文について説明します。疑問符（?）を入力した場合に CLI（コマンドライン インターフェイス）ヘルプで表示されるその他の ARP ACL 構文はサポートされず、QoS の ARP トラフィックのフィルタリング処理にも使用できません。
- ACL　エントリは、入力順に従ってスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを向上させるには、最もよく使用されるエントリを ACL の先頭に置きます。
- ACL の末尾に **permit ip any mac any** エントリを明示的に指定する場合を除いて、ACL の末尾には暗黙的な **deny ip any mac any** エントリが存在します。
- 既存のリストに新しいエントリを追加すると、新しいエントリはすべてリストの末尾に置かれます。リストの途中にエントリを追加することはできません。

次に、arp_filtering という名前の ARP ACL を作成する例を示します。この ACL は、IP アドレスが 1.1.1.1 から始まるトラフィックのみを許可します。

```
Router(config)# arp access-list arp_filtering
Router(config-arp-nacl)# permit ip host 1.1.1.1 mac any
```

クラス マップの設定

ここでは、クラス マップの設定手順について説明します。

- クラス マップの作成（p.42-70）
- クラス マップ フィルタリングの注意事項および制約事項（p.42-70）
- クラス マップでのフィルタリングの設定（p.42-71）

クラス マップの作成

クラス マップを作成するには、次の作業を行います。

コマンド	目的
`Router(config)# class-map class_name`	クラス マップを作成します。
`Router(config)# no class-map class_name`	クラス マップを削除します。

クラス マップ フィルタリングの注意事項および制約事項

クラス マップ フィルタリングを設定する場合は、次の注意事項および制約事項に従ってください。

- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は、**match-any** キーワードを使用して設定した複数の一致基準をクラス マップ内でサポートします。

- Release 12.2(18)SXE より前のリリースでは、PFC QoS は 1 つの **match** コマンドを保持するクラス マップをサポートします。
- Release 12.2(18)SXE 以降のリリースでは、PFC3 は **match protocol ipv6** コマンドをサポートします。
- TCAM 検索のフロー キー ビット要件が競合するため、IPv6 DSCP ベースのフィルタリングと IPv6 レイヤ 4 範囲ベースのフィルタリングを同一インターフェイス上に設定することはできません。次に、例を示します。
  - 1 つの IPv6 ACE 内に DSCP 値と、レイヤ 4 の「greater than（gt）」または「less than（lt）」演算子の両方を設定した場合は、この ACL は PFC QoS フィルタリングには使用できません。
  - 1 つの IPv6 ACL 内に DSCP 値を設定し、別の IPv6 ACL 内にレイヤ 4 の greater than（gt）または less than（lt）演算子を設定した場合は、同一インターフェイス上の異なるクラス マップで両方の ACL を使用して、PFC QoS フィルタリングを行うことはできません。
- Release 12.2(18)SXE 以降のリリースでは、IPv4 トラフィックに対して **match protocol ip** コマンドがサポートされます。
- PFC QoS は、**match cos**、**match any**、**match classmap**、**match destination-address**、**match input-interface**、**match qos-group**、および **match source-address** クラス マップ コマンドをサポートしません。
- Catalyst 6500 シリーズ スイッチは、インターフェイスにポリシー マップが付加されないかぎり、サポート対象外のコマンドが使用されているかどうかを検出しません。
- PFC2 は **match protocol** クラス マップ コマンドをサポートしています。これにより、NBAR を設定して、レイヤ 3 インターフェイスの入力と出力の両方のトラフィックをすべて MSFC2 ソフトウェアで処理できます。NBAR を設定するには、次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm
- 出力 QoS の IP precedence または DSCP に基づいたフィルタリングでは、受信した IP precedence または DSCP を使用します。出力 QoS フィルタリングは、入力 QoS による IP precedence または DSCP の変更には基づいていません。

（注）　ここでは、次の ACL に関する内容を説明します。

- MAC ACL の設定（p.42-66）
- QoS フィルタリングに対する ARP ACL の設定（p.42-69）

このマニュアルでは、その他の ACL については説明しません。「PFC QoS ポリシー設定作業の概要」（p.42-65）に記載されている **access-list** の説明を参照してください。

クラス マップでのフィルタリングの設定

クラス マップにフィルタリングを設定するには、次のいずれかの作業を行います。

コマンド	目的
`Router(config-cmap)# match access-group name acl_index_or_name`	（任意）ACL を使用してフィルタリングするように、クラス マップを設定します。
`Router(config-cmap)# no match access-group name acl_index_or_name`	クラス マップから ACL 設定を消去します。
`Router (config-cmap)# match protocol ipv6`	（任意 — IPv6 トラフィック用）IPv6 トラフィックをフィルタリングするように、クラス マップを設定します。
`Router (config-cmap)# no match protocol ipv6`	IPv6 フィルタリングを消去します。

コマンド	目的
`Router (config-cmap)# match precedence ipp_value1 [ipp_value2 [ipp_valueN]]`	（任意 — IPv4 または IPv6 トラフィック用）最大 8 つの IP precedence 値に基づいてフィルタリングするように、クラス マップを設定します。 （注）　送信元ベース、または宛先ベースの microflow ポリシングをサポートしません。
`Router (config-cmap)# no match precedence ipp_value1 [ipp_value2 [ipp_valueN]]`	設定された IP precedence 値をクラス マップから消去します。
`Router (config-cmap)# match dscp dscp_value1 [dscp_value2 [dscp_valueN]]`	（任意 — IPv4 または IPv6 トラフィックのみ）最大 8 つの DSCP 値に基づいてフィルタリングするように、クラス マップを設定します。 （注）　送信元ベース、または宛先ベースの microflow ポリシングをサポートしません。
`Router (config-cmap)# no match dscp dscp_value1 [dscp_value2 [dscp_valueN]]`	設定された DSCP 値をクラス マップから消去します。
`Router (config-cmap)# match ip precedence ipp_value1 [ipp_value2 [ipp_valueN]]`	（任意 — IPv4 トラフィック用）最大 8 つの IP precedence 値に基づいてフィルタリングするように、クラス マップを設定します。 （注）　送信元ベース、または宛先ベースの microflow ポリシングをサポートしません。
`Router (config-cmap)# no match ip precedence ipp_value1 [ipp_value2 [ipp_valueN]]`	設定された IP precedence 値をクラス マップから消去します。
`Router (config-cmap)# match ip dscp dscp_value1 [dscp_value2 [dscp_valueN]]`	（任意 — IPv4 トラフィック用）最大 8 つの DSCP 値に基づいてフィルタリングするように、クラス マップを設定します。 （注）　送信元ベース、または宛先ベースの microflow ポリシングをサポートしません。
`Router (config-cmap)# no match ip dscp dscp_value1 [dscp_value2 [dscp_valueN]]`	設定された DSCP 値をクラス マップから消去します。

クラス マップの設定の確認

クラス マップの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router (config-cmap)# end`	コンフィギュレーション モードを終了します。
ステップ 2	`Router# show class-map class_name`	設定を確認します。

次に、**ipp5** という名前のクラス マップを作成し、IP precedence 5 のトラフィックと一致するようにフィルタリングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# end
```

次に、設定を確認する例を示します。

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

ポリシー マップの設定

1 つのインターフェイスに付加できるポリシー マップは、1 つに限られます。ポリシー マップには、ポリシー マップ コマンドがそれぞれ異なる 1 つまたは複数のポリシー マップ クラスを含めることができます。

インターフェイスで受信するトラフィック タイプごとに、個別のポリシー マップ クラスをポリシー マップ内に設定します。各トラフィック タイプ用の全コマンドを、同一のポリシー マップ クラスに入れます。PFC QoS は、一致したトラフィックに複数のポリシー マップ クラスのコマンドを適用することはありません。

ここでは、ポリシー マップの設定手順について説明します。

- ポリシー マップの作成（p.42-73）
- ポリシー マップ クラスの設定に関する注意事項および制約事項（p.42-73）
- ポリシー マップ クラスの作成およびフィルタリングの設定（p.42-74）
- ポリシー マップ クラス アクションの設定（p.42-74）

ポリシー マップの作成

ポリシー マップを作成するには、次の作業を行います。

コマンド	目的
`Router(config)# policy-map` *policy_name*	ポリシー マップを作成します。
`Router(config)# no policy-map` *policy_name*	ポリシー マップを削除します。

ポリシー マップ クラスの設定に関する注意事項および制約事項

ポリシー マップ クラスを設定する場合は、次の注意事項および制約事項に従ってください。

- PFC2 は **class** *class_name* **protocol** ポリシー マップ コマンドをサポートしています。これにより、NBAR を設定して、レイヤ 3 インターフェイスの入力と出力の両方のトラフィックをすべて MSFC2 ソフトウェアで処理できます。NBAR を設定するには、次のマニュアルを参照してください。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

- PFC QoS は、**class** *class_name* **destination-address**、**class** *class_name* **input-interface**、**class** *class_name* **qos-group**、および **class** *class_name* **source-address** ポリシー マップ コマンドをサポートしていません。
- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は **class default** ポリシー マップ コマンドをサポートします。

- PFC QoS は、インターフェイスにポリシー マップが付加されないかぎり、サポート対象外のコマンドが使用されているかどうかを検出しません。

ポリシー マップ クラスの作成およびフィルタリングの設定

ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリングするように設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap)# class class_name`	ポリシー マップ クラスを作成し、クラス マップを使用してフィルタリングするように設定します。 （注）　PFC QoS は、**match** コマンドが 1 つだけ指定されているクラス マップをサポートします。
`Router(config-pmap)# no class class_name`	クラス マップの使用を解除します。

ポリシー マップ クラス アクションの設定

ポリシー マップ クラスのアクションを設定する場合、次の点に注意してください。

- ポリシー マップには、1 つまたは複数のポリシー マップ クラスを含めることができます。
- トラフィック タイプごとに、すべての信頼状態およびポリシング コマンドを、同一のポリシー マップ クラスに入れてください。
- PFC QoS は、1 つのポリシー マップ クラスのコマンドのみをトラフィックに適用します。1 つのポリシー マップ クラスのフィルタリングに一致したトラフィックには、他のポリシー マップ クラスで設定したフィルタリングが適用されます。
- ハードウェアでスイッチングされるトラフィックの場合、PFC QoS は **bandwidth**、**priority**、**queue-limit**、または **random-detect** ポリシー マップ クラス コマンドをサポートしません。これらのコマンドはソフトウェアでスイッチングされるトラフィックに使用できるので、設定が可能です。
- PFC QoS では、**set qos-group** ポリシー マップ クラス コマンドはサポートされません。
- PFC QoS では、IPv4 トラフィック用の **set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドがサポートされます。
  - Release 12.2(18)SXD 以降のリリースおよび Release 12.2(17d)SXB 以降のリリースでは、非 IP トラフィック上の **set ip dscp** および **set ip precedence** コマンドを使用して、出力レイヤ 2 CoS 値の基準である内部 DSCP 値をマーキングできます。
  - Release 12.2(18)SXE 以降のリリースでは、**set ip dscp** および **set ip precedence** コマンドは **set dscp** および **set precedence** コマンドとしてコンフィギュレーション ファイルに保存されます。
- Release 12.2(18)SXE 以降のリリースでは、PFC QoS は IPv4 および IPv6 トラフィックに対して **set dscp** および **set precedence** ポリシー マップ クラス コマンドをサポートします。
- ポリシー マップ クラスで、次の 3 つすべてを実行することはできません。
  - **set** コマンドによるトラフィックのマーキング
  - 信頼状態の設定
  - ポリシングの設定

  ポリシー マップ クラスでは、トラフィックを **set** コマンドによってマーキングするか、次のいずれか、あるいは両方を実行できます。
  - 信頼状態の設定
  - ポリシングの設定

（注）　ポリシングを設定する場合は、ポリシング　キーワードでトラフィックをマーキングできます。

ここでは、ポリシー マップ クラスのアクションを設定する手順について説明します。

- ポリシー マップ クラス マーキングの設定（p.42-75）
- ポリシー マップ クラスの信頼状態の設定（p.42-75）
- ポリシー マップ クラスのポリシングの設定（p.42-76）

ポリシー マップ クラス マーキングの設定

Release 12.2(18)SXF5 以降のリリースでは、ignore port trust 機能をイネーブルにしている場合、PFC QoS はすべてのトラフィックに対し、**set** ポリシー マップ クラス コマンドを使用したポリシー マップ クラス マーキングをサポートします。

すべてのリリースにおいて PFC QoS は、信頼できないトラフィックに対し、**set** ポリシー マップ クラス コマンドを使用したポリシー マップ クラス マーキングをサポートします。

ポリシー マップ クラス マーキングを設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# set {dscp dscp_value | precedence ip_precedence_value}`	ポリシー マップ クラスを設定して、設定されている DSCP 値または IP precedence 値と一致する信頼できないトラフィックをマーキングするようにします。
`Router(config-pmap-c)# no set {dscp dscp_value | precedence ip_precedence_value}`	マーキングの設定を消去します。

（注）　Release 12.2(18)SXE より前のリリースでは、**set ip dscp** および **set ip precedence** ポリシー マップ クラス コマンドがサポートされます。

ポリシー マップ クラスの信頼状態の設定

（注）　**service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを付加することはできません。

ポリシー マップ クラスの信頼状態を設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# trust {cos | dscp | ip-precedence}`	ポリシー マップ クラスの信頼状態を設定します。この設定によって、PFC QoS が初期内部 DSCP 値の作成元として使用する値が選択されます。
`Router(config-pmap-c)# no trust`	デフォルトのポリシー マップ クラスの信頼状態（untrusted）に戻します。

ポリシー マップ クラスの信頼状態を設定する場合、次の点に注意してください。

- 入力ポート上に設定されている信頼状態を使用するには、**no trust** コマンド（これがデフォルトです）を使用します。
- **cos** キーワードを使用すると、PFC QoS は受信した CoS または入力ポートの CoS に基づいて、内部 DSCP 値を設定します。
- **dscp** キーワードを使用すると、PFC QoS は受信した DSCP を使用します。
- **ip-precedence** キーワードを使用すると、PFC QoS は受信した IP precedence に基づいて DSCP を設定します。

ポリシー マップ クラスのポリシングの設定

ポリシー マップ クラスのポリシングを設定する場合、次の点に注意してください。

- PFC QoS は **set-qos-transmit** ポリサー キーワードをサポートしません。
- PFC QoS は、**exceed-action** キーワードの引数として **set-dscp-transmit** キーワードまたは **set-prec-transmit** キーワードをサポートしません。
- PFC QoS は、インターフェイスにポリシー マップが付加されないかぎり、サポート対象外のキーワードが使用されているかどうかを検出しません。

ここではポリシー マップ クラスによるポリシングを設定する手順について説明します。

- 名前付き aggregate ポリサーの使用（p.42-76）
- インターフェイス別ポリサーの設定（p.42-76）

（注）　**conform-action transmit** キーワードによるポリシングでは、一致するトラフィックのポート信頼状態が、trust dscp またはポリシー マップ クラスの **trust** コマンドで設定される信頼状態に設定されます。

名前付き aggregate ポリサーの使用

名前付き aggregate ポリサーを使用するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# police aggregate aggregate_name`	定義済みの名前付き aggregate ポリサーを使用するように、ポリシー マップ クラスを設定します。
`Router(config-pmap-c)# no police aggregate aggregate_name`	名前付き aggregate ポリサーの使用を解除します。

インターフェイス別ポリサーの設定

インターフェイス別のポリサーを設定するには、次の作業を行います。

コマンド	目的
`Router(config-pmap-c)# police [flow [mask {src-only | dest-only | full-flow}]] bits_per_second normal_burst_bytes [maximum_burst_bytes] [pir peak_rate_bps] [[[conform-action {drop | set-dscp-transmit dscp_value | set-prec-transmit ip_precedence_value | transmit}] exceed-action {drop | policed-dscp | transmit}] violate-action {drop | policed-dscp | transmit}]`	インターフェイス別のポリサーを作成して、それを使用するようにポリシー マップ クラスを設定します。
`Router(config-pmap-c)# no police [flow [mask {src-only | dest-only | full-flow}]] bits_per_second normal_burst_bytes [maximum_burst_bytes] [pir peak_rate_bps] [[[conform-action {drop | set-dscp-transmit dscp_value | set-prec-transmit ip_precedence_value | transmit}] exceed-action {drop | policed-dscp | transmit}] violate-action {drop | policed-dscp | transmit}]`	ポリシー マップ クラスからインターフェイス別のポリサーを削除します。

インターフェイス別ポリサーを設定する場合、次の点に注意してください。

- aggregate ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。aggregate ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。aggregate ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチングされた仮想インターフェイスに適用されたポリサー
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。
- PFC3 の場合、入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。
- Release 12.2(18)SXE 以降のリリースでは、IPv6 トラフィックに aggregate ポリサーおよび microflow ポリサーを適用できます。
- PFC3 のポリシングでは、レイヤ 2 のフレーム サイズを使用します。
- PFC2 のポリシングでは、レイヤ 3 のパケット サイズを使用します。
- レートおよびバースト サイズの粒度については、「PFC QoS 設定時の注意事項および制約事項」（p.42-50）を参照してください。
- microflow ポリサーを定義するには、**flow** キーワードを入力します（microflow ポリシングは ARP トラフィックには適用できません）。microflow ポリサーを設定する場合、次の点に注意してください。
  - PFC3 の場合、送信元アドレスのみに基づいてフローの識別を行うには、**mask src-only** キーワードを入力します。これにより microflow ポリサーが、各送信元アドレスからのすべてのトラフィックに適用されます。Release 12.2(17d)SXB 以降のリリースでは、IP トラフィックと MAC トラフィックの両方で **mask src-only** キーワードをサポートしています。Release 12.2(17d)SXB より以前のリリースでは、IP トラフィックのみで **mask src-only** キーワードをサポートしています。
  - PFC3 の場合、宛先アドレスのみに基づいてフローの識別を行うには、**mask dest-only** キーワードを入力します。これにより microflow ポリサーが、各送信元アドレスのすべてのトラフィックに適用されます。Release 12.2(17d)SXB 以降のリリースでは、IP トラフィックと MAC トラフィックの両方で **mask dest-only** キーワードをサポートしています。Release 12.2(17d)SXB より以前のリリースでは、IP トラフィックのみで **mask dest-only** キーワードをサポートしています。
  - デフォルトおよび **mask full-flow** キーワードを使用する場合は、PFC QoS は送信元 IP アドレス、宛先 IP アドレス、レイヤ 3 プロトコル、レイヤ 4 ポート番号に基づいて IP フローの識別を行います。
  - PFC2 の場合、PFC QoS は、送信元ノードまたは送信元ソケットが異なるトラフィックを含め、同じ送信元ネットワーク、宛先ネットワーク、および宛先ノードを持つ IPX トラフィックを同じフローの一部であるとみなします。
  - PFC QoS は、プロトコルおよび送信元と宛先 MAC レイヤ アドレスが同じである MAC レイヤ トラフィックについては、EtherType が違っていても、同じフローの一部であるとみなします。

　－ microflow ポリサーでは、*maximum_burst_bytes* パラメータ、**pir** *bits_per_second* キーワードおよびパラメータ、または **violate-action** キーワードはサポートされません。

（注） microflow ポリシング、NetFlow、および NetFlow Data Export（NDE; NetFlow データ エクスポート）のフローマスク要件は、競合する可能性があります。

- 有効な CIR *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 ― 32 Kbps（32000 と入力）
  - Release 12.2(18)SXE 以降のリリースでの最大：10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE 以前のリリースでの最大：4 Gbps（4000000000 と入力）
- *normal_burst_bytes* パラメータでは、CIR トークン バケット サイズを設定します。
- *maximum_burst_bytes* パラメータでは、PIR トークン バケット サイズを設定します（**flow** キーワードではサポートされません）。
- トークン バケット サイズを設定する場合、次の点に注意してください。
  - 最小トークン バケット サイズは 1 KB（1000 と入力）（*maximum_burst_bytes* パラメータは、*normal_burst_bytes* パラメータより大きい値に設定する必要があります）。
  - 最大トークン バケット サイズは 32 MB（32000000 と入力）。
  - 特定のレートを維持するには、トークン バケット サイズがレート値を 4000 で割った値よりも大きくなるように設定します。トークンは 1 秒の 4000 分の 1（0.25 ミリ秒）ごとにバケットから削除されるからです。
  - トークン バケットは 1 つ以上のフレームを格納できる容量が必要なので、パラメータには、ポリシングするトラフィックの最大サイズより大きい値を設定してください。
  - TCP トラフィックの場合は、トークン バケット サイズを TCP ウィンドウ サイズの倍数になるように設定します。最小値はポリシングするトラフィックの最大サイズの 2 倍以上にする必要があります。
- （**flow** キーワードではサポートされません。）有効な **pir** *bits_per_second* パラメータ値の範囲は、次のとおりです。
  - 最小 ― 32 Kbps（32000 と入力、CIR *bits_per_second* パラメータより小さい値は使用できません）
  - Release 12.2(18)SXE 以降のリリースでの最大：10 Gbps（10000000000 と入力）
  - Release 12.2(18)SXE 以前のリリースでの最大：4 Gbps（4000000000 と入力）
- （任意）一致する適合トラフィックに対応する conform アクションを、次のように指定できます。
  - デフォルトの conform アクションは、**transmit** です。このアクションでは、ポリシー マップ クラスに **trust** コマンドが含まれている場合を除いて、ポリシー マップ クラスの信頼状態が *trust dscp* に設定されます。
  - 信頼できないトラフィックで PFC QoS ラベルを設定するには、**set-dscp-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい DSCP 値をマークするか、または **set-prec-transmit** キーワードを入力し、一致する信頼できないトラフィックに新しい IP precedence 値をマークします。**set-dscp-transmit** キーワードおよび **set-prec-transmit** キーワードは IP トラフィックに対してのみサポートされます。PFC QoS は、設定された値に基づいて出力 ToS および CoS を設定します。
  - 一致するトラフィックをすべて廃棄するには、**drop** キーワードを入力します。
  - 同じトラフィックに適用する aggregate ポリサーおよび microflow ポリサーで、それぞれ同じ conform アクションの動作が指定されていることを確認してください。

- （任意）CIR を超過するトラフィックに対しては、exceed アクションを次のように指定できます。
  - ポリシングを行わずにマーキングするには、**transmit** キーワードを入力して、一致したすべての不適合トラフィックを送信します。
  - デフォルトの exceed アクションは、*maximum_burst_bytes* パラメータを使用しない場合は **drop** です（*maximum_burst_bytes* パラメータでは、**drop** はサポートされません）。

（注） exceed アクションが **drop** の場合、PFC QoS は設定された violate アクションを無視します。

  - 一致した不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

（注） **pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- （任意 **— flow** キーワードではサポートされません。）PIR を超過するトラフィックに対して、violate アクションを次のように指定できます。
  - ポリシングを行わずにマーキングするには、**transmit** キーワードを入力して、一致したすべての不適合トラフィックを送信します。
  - デフォルトの violate アクションは、exceed アクションと同じものです。
  - 一致したすべての不適合トラフィックを、マークダウン マップの指定に従ってマークダウンするには、**policed-dscp-transmit** キーワードを入力します。

次に、**max-pol-ipp5** という名前のポリシー マップを作成する例を示します。このポリシー マップは、クラス マップ **ipp5** を使用し、受信した IP precedence 値に基づいて信頼状態を設定し、最大容量に関する aggregate ポリサーおよび microflow ポリサーを設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
```

ポリシー マップの設定の確認

ポリシー マップの設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了します。 （注）　ポリシー マップにクラスを追加するには、追加の **class** コマンドを入力します。
ステップ 2	`Router# show policy-map policy_name`	設定を確認します。

次に、設定を確認する例を示します。

```
Router# show policy-map max-pol-ipp5
 Policy Map max-pol-ipp5
  class  ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit
    trust precedence
    police 2000000000 2000000 2000000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit

Router#
```

インターフェイスへのポリシー マップの付加

ポリシー マップをインターフェイスに付加するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type[1] slot/port[.subinterface]} | {port-channel number[.subinterface]}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# service-policy [input | output] policy_map_name` `Router(config-if)# no service-policy [input | output] policy_map_name`	ポリシー マップをインターフェイスに付加します。 インターフェイスからポリシー マップを削除します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show policy-map interface {{vlan vlan_ID} | {type[1] slot/port} | {port-channel number}}`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

ポリシー マップをインターフェイスに付加するには、次の点に注意してください。

- EtherChannel のメンバーであるポートに、サービス ポリシーを付加しないでください。
- DFC が搭載されている場合は、PFC2 は VLAN ベースの QoS をサポートしません。**mls qos vlan-based** コマンドを入力することも、VLAN インターフェイスにサービス ポリシーを付加することもできなくなります。

- PFC QoS は、PFC3 を搭載している場合にのみ、レイヤ 3 インターフェイス（レイヤ 3 インターフェイスまたは VLAN インターフェイスとして設定された LAN ポート）で **output** キーワードをサポートします。PFC3 の場合、入力ポリシー マップと出力ポリシー マップの両方をレイヤ 3 インターフェイスに付加できます。
- レイヤ 2 ポート上の VLAN ベースまたはポートベースの PFC QoS は、**output** キーワードを使用してレイヤ 3 インターフェイスに付加されたポリシーとは関係ありません。
- **output** キーワードが付いたポリシーでは、microflow ポリシングはサポートされません。
- **service-policy output** コマンドを使用して、信頼状態を設定するポリシー マップを付加することはできません。
- **output** キーワードを使用して付加されたポリシーの IP precedence または DSCP に基づいたフィルタリングでは、受信した IP precedence 値または DSCP 値が使用されます。**output** キーワードを使用して付加されたポリシーの IP precedence または DSCP に基づいたフィルタリングは、入力 QoS による IP precedence または DSCP の変更には基づいていません。
- aggregate ポリシングは、DFC を装備した各スイッチング モジュール上、および PFC（DFC を装備していないスイッチング モジュールをサポート）上で独立して動作します。aggregate ポリシングでは、DFC を装備した異なるスイッチング モジュールからのフロー統計情報は合算されません。aggregate ポリシングの統計情報は、DFC を装備した各スイッチング モジュール、PFC、および PFC がサポートする DFC を装備していないスイッチング モジュールについて、表示できます。
- 個々の PFC または DFC ポリシングは独立して実行されます。これにより、PFC およびすべての DFC 間で分散されているトラフィックに適用される QoS 機能が影響を受けることがあります。このような QoS 機能には、次のようなものがあります。
  - ポート チャネル インターフェイスに適用されたポリサー
  - スイッチングされた仮想インターフェイスに適用されたポリサー
  - レイヤ 3 インターフェイスまたは SVI のいずれかに適用された出力ポリサー。PFC QoS は、PFC または入力 DFC 上の入力インターフェイスにおいて、出力ポリシングの決定を行います。

  この制限の影響を受けるポリサーは、集約レートを提供します。これは、独立したすべてのポリシング レートの合計です。
- PFC3　の場合、入力および出力ポリシング両方を同じトラフィックに適用した場合、入力および出力ポリシーの両方がトラフィックのマークダウンまたはトラフィックの廃棄のいずれかを実行する必要があります。PFC QoS では、出力廃棄を使用した入力マークダウン、または出力マークダウンを使用した入力廃棄をサポートしません。

次に、ポリシー マップ **pmap1** をポート FastEthernet 5/36 に付加する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# service-policy input pmap1
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show policy-map interface fastethernet 5/36
 FastEthernet5/36
  service-policy input: pmap1
    class-map: cmap1 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class cmap1
    police 8000 8000 conform-action transmit exceed-action drop
    class-map: cmap2 (match-any)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 2
        0 packets, 0 bytes
        5 minute rate 0 bps
  class cmap2
    police 8000 10000 conform-action transmit exceed-action drop
Router#
```

PFC3 による出力 DSCP 変換の設定

（注）　PFC2 は出力 DSCP 変換をサポートしません。

ここでは、PFC3 で出力 DSCP 変換を設定する手順について説明します。

- 名前付き DSCP 変換マップの設定（p.42-82）
- インターフェイスへの出力 DSCP 変換マップの付加（p.42-83）

名前付き DSCP 変換マップの設定

名前付き DSCP 変換マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map dscp-mutation** *map_name dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *mutated_dscp*	名前付き DSCP 変換マップを設定します。
	Router(config)# **no mls qos map dscp-mutation** *map_name*	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

名前付き DSCP 変換マップを設定する場合、次の点に注意してください。

- 変換された DSCP 値にマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値を変換された DSCP 値にマッピングできます。
- 変換された DSCP 値ごとに個別のコマンドを入力できます。

次に、DSCP 30 を変換された DSCP 値 8 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map dscp-mutation mutmap1 30 to 8
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos map | begin DSCP mutation
DSCP mutation map mutmap1:                    (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    08 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
(テキスト出力は省略)
Router#
```

（注） DSCP 変換マップの出力で、マトリクスの本体に表示されるのがマークダウンされた DSCP 値です。元の DSCP 値の最初の桁の数字は d1 のカラムに、2 番めの桁の数字は一番上の行に表示されます。上記の例では、DSCP 30 は DSCP 08 にマッピングされています。

インターフェイスへの出力 DSCP 変換マップの付加

出力 DSCP 変換マップをインターフェイスに付加するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*[.*subinterface*]} | {**port-channel** *number*[.*subinterface*]}}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **mls qos dscp-mutation** *mutation_map_name* Router(config-if)# **no mls qos dscp-mutation** *mutation_map_name*	出力 DSCP 変換マップをインターフェイスに付加します。 インターフェイスから出力 DSCP 変換マップを削除します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show running-config interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*} | {**port-channel** *number*}}	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、mutmap1 という名前の出力 DSCP 変換マップをポート FastEthernet 5/36 に付加する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# mls qos dscp-mutation mutmap1
Router(config-if)# end
```

IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定

（注）　Supervisor Engine 2 は、入力 CoS 変換に対応したスイッチング モジュールをサポートしていません。

Release 12.2(17b)SXA 以降のリリースでは、受信した CoS を信頼するように設定された、IEEE 802.1Q トンネル ポートの入力 CoS 変換をサポートします（サポート対象モジュールについては、「IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用」[p.42-86] を参照）。

受信した CoS を信頼するように設定された IEEE 802.1Q トンネル ポート上で入力 CoS 変換を設定する場合、PFC QoS は、入力廃棄スレッシュホールド内および任意の trust-CoS マーキングおよびポリシング用の受信した CoS 値ではなく、変換された CoS 値を使用します。

ここでは、入力 CoS 変換の設定手順について説明します。

- 入力 CoS 変換の設定に関する注意事項および制約事項（p.42-84）
- 入力 CoS 変換マップの設定（p.42-85）
- IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用（p.42-86）

入力 CoS 変換の設定に関する注意事項および制約事項

入力 CoS 変換を設定する場合は、次の注意事項および制約事項に従ってください。

- IEEE 802.1Q トンネル ポートとして設定されていないポートは、入力 CoS 変換をサポートしません。
- 受信した CoS を信頼するよう設定されていないポートは、入力 CoS 変換をサポートしません。
- 入力 CoS 変換では、カスタマー フレームにより伝送された CoS 値を変更しません。カスタマー トラフィックが 802.1Q トンネルから送出される場合、元の CoS がそのまま残ります。
- Release 12.2(17b)SXA 以降のリリースでは、WS-X6704-10GE、WS-X6748-SFP、WS-X6724-SFP、および WS-X6748-GE-TX スイッチング モジュールで入力 CoS 変換がサポートされます。
- 入力 CoS 変換の設定は、ポート グループ内のすべてのポートに適用されます。ポート グループは次のとおりです。
  - WS-X6704-10GE — 4 ポート、4 ポート グループ、各グループに 1 ポート
  - WS-X6748-SFP — 48 ポート、4 ポート グループ：ポート 1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48
  - WS-X6724-SFP — 24 ポート、2 ポート グループ：ポート 1 ～ 12、13 ～ 24
  - WS-X6748-GE-TX — 48 ポート、4 ポート グループ：ポート 1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48
- 入力 CoS 変換の設定エラーを回避するために、メンバー ポートのすべてが入力 CoS 変換をサポートしている、またはメンバー ポートのすべてが入力 CoS 変換をサポートしていない EtherChannel だけを作成してください。入力 CoS 変換に対するサポートが混在する EtherChannel を作成しないでください。
- EtherChannel のメンバーであるポート上で 入力 CoS 変換を設定する場合、入力 CoS 変換はポートチャネル インターフェイスに適用されます。
- ポートチャネル インターフェイス上で、入力 CoS 変換を設定できます。
- ポートチャネル インターフェイス上で入力 CoS 変換が設定されている場合、次の動作が発生します。
  - 入力 CoS 変換の設定は、EtherChannel のすべてのメンバー ポートのポート グループに適用されます。任意のメンバー ポートが、入力 CoS 変換をサポートできない場合、設定はエラーになります。

- ポート グループ内のあるポートが、2 番めの EtherChannel のメンバーである場合、入力 CoS 変換の設定は、2 番めのポートチャネル インターフェイスおよび 2 番めの EtherChannel のすべてのメンバー ポートのポート グループに適用されます。2 番めの EtherChannel の任意のメンバー ポートが入力 CoS 変換をサポートできない場合、1 番めの EtherChannel 上の設定がエラーになります。1 番めの EtherChannel のメンバー ポートがあるポート グループ内の非メンバー ポートで、設定が行われた場合、この設定は非メンバー ポート上でエラーになります。
- ポートが CoS を信用するように設定されているかどうか、または IEEE 802.1Q トンネル ポートとして設定されているかどうかにかかわらず、入力 CoS 変換の設定はポート グループ、メンバー ポート、ポートチャネル インターフェイスを通して、制限なく伝播します。

- 入力 CoS 変換を設定する予定の EtherChannel では、入力 CoS 変換をサポートしていないメンバー ポートがある他の EtherChannel のメンバー ポートを含むポート グループ内のポートをメンバーとすることができません（この制約は、ポートグループにリンクされるすべてのメンバー ポートおよびポートチャネルインターフェイスにリンクされるすべてのポートに、制限なく適用されます）。
- 入力 CoS 変換を設定する予定のポートは、入力 CoS 変換をサポートしていないメンバーがある EtherChannel のメンバー ポートを含むポート グループ内に組み込むことはできません（この制約は、ポートグループにリンクされるすべてのメンバー ポートおよびポートチャネルインターフェイスにリンクされるすべてのポートに、制限なく適用されます）。
- ポートグループにリンクされるメンバー　ポートおよびポートチャネルインターフェイスにリンクされるポートすべてに適用される入力 CoS 変換の設定は、1 つだけです。

入力 CoS 変換マップの設定

入力 CoS 変換マップを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map cos-mutation** *mutation_map_name mutated_cos1 mutated_cos2 mutated_cos3 mutated_cos4 mutated_cos5 mutated_cos6 mutated_cos7 mutated_cos8*	入力 CoS 変換マップを設定します。PFC QoS が入力 CoS 値 0 ～ 7 をマッピングする、8 つの変換 CoS 値を入力する必要があります。
	Router(config)# **no mls qos map cos-mutation** *map_name*	名前付きマップを削除します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps cos-mutation**	設定を確認します。

次に、testmap という名前の CoS 変換マップを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map cos-mutation testmap 4 5 6 7 0 1 2 3
Router(config)# end
Router#
```

次に、マップの設定を確認する例を示します。

```
Router(config)# show mls qos maps cos-mutation
COS mutation map testmap
cos-in  :   0  1  2  3  4  5  6  7
------------------------------------
cos-out :   4  5  6  7  0  1  2  3
Router#
```

IEEE 802.1Q トンネル ポートへの入力 CoS 変換マップの適用

IEEE 802.1Q トンネル ポートに入力 CoS 変換マップを付加するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port} | {port-channel number}}`	設定するインターフェイスを選択します。

ステップ 2	`Router(config-if)# mls qos cos-mutation mutation_map_name`
	
	`Router(config-if)# no mls qos cos-mutation mutation_map_name`
		入力 CoS 変換マップをインターフェイスに付加します。
		インターフェイスから入力 CoS 変換マップを削除します。

ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show running-config interface {{type[1] slot/port} | {port-channel number}}` `Router# show mls qos maps cos-mutation`	設定を確認します。

1. *type* = **gigabitethernet** または **tengigabitethernet**

次に、testmap という名前の入力 CoS 変換マップを、ポート GigabitEthernet 1/1 に付加する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# mls qos cos-mutation testmap
Router(config-if)# end
Router# show mls qos maps cos-mutation
COS mutation map testmap
cos-in  :   0  1  2  3  4  5  6  7
------------------------------------
cos-out :   4  5  6  7  0  1  2  3

testmap is attached on the following interfaces
Gi1/1
Router#
```

DSCP 値マッピングの設定

ここでは、DSCP 値を他の値にマッピングする方法について説明します。

- 受信 CoS 値から内部 DSCP 値へのマッピング（p.42-86）
- 受信 IP precedence 値から内部 DSCP 値へのマッピング（p.42-87）
- DSCP マークダウン値の設定（p.42-88）
- 内部 DSCP 値から出力 CoS 値へのマッピング（p.42-89）

受信 CoS 値から内部 DSCP 値へのマッピング

受信した CoS 値から、PFC QoS が PFC 上で内部的に使用する DSCP 値へのマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map cos-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	受信した CoS 値から内部 DSCP 値へのマッピングを設定します。PFC QoS が CoS 値 0 ～ 7 をマッピングする、8 つの DSCP 値を入力する必要があります。
	Router(config)# **no mls qos map cos-dscp**	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

次に、受信した CoS 値から内部 DSCP 値へのマッピングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map cos-dscp 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos maps | begin Cos-dscp map
   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
      ---------------------------------
        dscp:   0  1  2  3  4  5  6  7
(テキスト出力は省略)
Router#
```

受信 IP precedence 値から内部 DSCP 値へのマッピング

受信した IP precedence 値から、PFC QoS が PFC 上で内部的に使用する DSCP 値へのマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map ip-prec-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	受信した IP precedence 値から内部 DSCP 値へのマッピングを設定します。PFC QoS が受信した IP precedence 値 0 ～ 7 をマッピングする、8 つの内部 DSCP 値を入力する必要があります。
	Router(config)# **no mls qos map ip-prec-dscp**	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

次に、受信した IP precedence 値から内部 DSCP 値へのマッピングを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map ip-prec-dscp 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos maps | begin IpPrecedence-dscp map
   IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     ---------------------------------
       dscp:   0  1  2  3  4  5  6  7
(テキスト出力は省略)
Router#
```

DSCP マークダウン値の設定

ポリサーが使用する DSCP マークダウン値のマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **mls qos map policed-dscp** {**normal-burst** | **max-burst**} *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *markdown_dscp*	DSCP マークダウン値のマッピングを設定します。
	Router(config)# **no mls qos map policed-dscp** {**normal-burst** | **max-burst**}	デフォルトのマッピングに戻します。
ステップ 2	Router(config)# **end**	コンフィギュレーション モードを終了します。
ステップ 3	Router# **show mls qos maps**	設定を確認します。

DSCP マークダウン値のマッピングを設定する場合、次の点に注意してください。

- **exceed-action policed-dscp-transmit** キーワードによって使用されるマークダウン値のマッピングを設定するには、**normal-burst** キーワードを使用します。
- **violate-action policed-dscp-transmit** キーワードによって使用されるマークダウン値のマッピングを設定するには、**max-burst** キーワードを使用します。

（注）　**pir** キーワードを使用せずにポリサーを作成し、かつ *maximum_burst_bytes* パラメータが *normal_burst_bytes* パラメータに等しい場合（*maximum_burst_bytes* パラメータを入力しない場合）、**exceed-action policed-dscp-transmit** キーワードを使用すると、PFC QoS は **policed-dscp max-burst** マークダウン マップの定義に従ってトラフィックをマークダウンします。

- パケットの順序誤りを防ぐため、適合するトラフィックおよび適合しないトラフィックが同じキューを使用するように、マークダウン値のマッピングを設定してください。
- マークダウンされた DSCP 値にマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をマークダウンされた DSCP 値にマッピングできます。
- マークダウンされた DSCP 値ごとに個別のコマンドを入力できます。

（注）　マークダウンされた DSCP 値は、マークダウン ペナルティと矛盾しない CoS 値にマッピングするように設定してください。

次に、DSCP 1 をマークダウンされた DSCP 値 0 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map policed-dscp normal-burst 1 to 0
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos map
   Normal Burst Policed-dscp map:                                    (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

   Maximum Burst Policed-dscp map:                                   (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
(テキスト出力は省略)
Router#
```

（注） Policed-dscp の出力で、マトリクスの本体に表示されるのがマークダウンされた DSCP 値です。元の DSCP 値の最初の桁の数字は d1 のカラムに、2 番めの桁の数字は一番上の行に表示されます。上記の例では、DSCP 41 は DSCP 41 にマッピングされています。

内部 DSCP 値から出力 CoS 値へのマッピング

PFC QoS が PFC 上で内部的に使用する DSCP 値から、出力 LAN ポートのスケジューリングおよび輻輳回避に使用される CoS 値へのマッピングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls qos map dscp-cos` *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] `to` *cos_value*	内部 DSCP 値から出力 CoS 値へのマッピングを設定します。
	`Router(config)# no mls qos map dscp-cos`	デフォルトのマッピングに戻します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls qos maps`	設定を確認します。

内部 DSCP 値から出力 CoS 値へのマッピングを設定する場合、次の点に注意してください。

- PFC QoS が CoS 値にマッピングする DSCP 値は、8 つまで入力できます。
- 複数のコマンドを入力して、追加の DSCP 値を CoS 値にマッピングできます。
- CoS 値ごとに個別のコマンドを入力できます。

次に、内部 DSCP 値 0、8、16、24、32、40、48、および 54 を、出力 CoS 値 0 にマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 54 to 0
Router(config)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show mls qos map | begin Dscp-cos map
   Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 00 01
      1 :    01 01 01 01 01 01 00 02 02 02
      2 :    02 02 02 02 00 03 03 03 03 03
      3 :    03 03 00 04 04 04 04 04 04 04
      4 :    00 05 05 05 05 05 05 05 00 06
      5 :    06 06 06 06 00 06 07 07 07 07
      6 :    07 07 07 07
(テキスト出力は省略)
Router#
```

（注） Dscp-cos map の出力で、マトリクスの本体に表示されるのが CoS 値です。DSCP 値の最初の桁の数字は d1 のカラムに、2 番めの桁の数字は一番上の行に表示されます。上記の例では、DSCP 値 41 ～ 47 は、いずれも CoS 05 にマッピングしています。

イーサネット LAN ポートおよび OSM ポートの信頼状態の設定

デフォルトでは、すべてのポートは信頼できない（untrusted）状態です。すべてのイーサネット LAN ポートおよび OSM ポートに対し、ポートの信頼状態を設定できます。

（注） 非ギガビット イーサネット **1q4t/2q2t** ポートの場合は、信頼状態をクラス マップ内でも繰り返し設定する必要があります。

ポートの信頼状態を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {{*type*[1] *slot/port*} | {**port-channel** *number*}}	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **mls qos trust** [**dscp** | **ip-precedence** | **cos**[2]]	ポートの信頼状態を設定します。
	Router(config-if)# **no mls qos trust**	デフォルトの信頼状態（untrusted）に戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port* | **include Trust state**	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、**tengigabitethernet**、**ge-wan**、**pos**、または **atm**
2. **serial**、**pos**、または **atm** インターフェイス タイプではサポートされません。

ポートの信頼状態を設定する場合、次の点に注意してください。

- 他のキーワードを指定しない場合、**mls qos trust** コマンドは **mls qos trust dscp** コマンドと同じです。
- Release 12.2(18)SXF5 以降のリリースでは、WS-X6708-10GE ポートで **mls qos trust dscp** コマンドを使用して、DSCP ベースの受信キュー廃棄スレッシュホールドをイネーブルにできます（「DSCP ベースのキュー マッピングの設定」[p.42-99] を参照）。DSCP ベースのキュー マッピングがイネーブルにされている場合に、DSCP 値の矛盾によるトラフィック廃棄を防ぐには、受信するトラフィックが明らかにネットワーク ポリシーと矛盾しない DSCP 値である場合に限り、**mls qos trust cos** コマンドを使用してポートを設定します。
- **mls qos trust cos** コマンドを使用すると、CoS ベースの受信キュー廃棄スレッシュホールドがイネーブルになります。CoS 値の矛盾によるトラフィック廃棄を防ぐには、受信するトラフィックが明らかにネットワーク ポリシーと矛盾しない CoS 値を伝送する ISL または 802.1Q フレームである場合に限り、**mls qos trust cos** コマンドを使用してポートを設定します。
- Release 12.2(17b)SXA 以降のリリースでは、**mls qos trust cos** コマンドで設定される IEEE 802.1Q トンネル ポートに、受信された CoS 値ではなく変換された CoS 値を使用するよう設定できます（「IEEE 802.1Q トンネル ポートの入力 CoS 変換の設定」[p.42-84] を参照）。
- ポート状態を untrusted に戻すには、**no mls qos trust** コマンドを使用します。

次に、**trust cos** キーワードを使用してポート GigabitEthernet 1/1 を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# mls qos trust cos
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | include trust
  Trust state: trust COS
Router#
```

入力 LAN ポート CoS 値の設定

（注）　PFC QoS が **mls qos cos** コマンドによって適用された CoS 値を使用するかどうかは、ポートの信頼状態とそのポート経由で受信したトラフィックの信頼状態によって決まります。**mls qos cos** コマンドを入力しても、ポートの信頼状態またはポート経由で受信したトラフィックの信頼状態は設定されません。

mls qos cos コマンドを使用して適用された CoS 値を内部 DSCP の基準として使用するには、次の設定を行います。

- タグなし入力トラフィックのみを受信するポートでは、入力ポートを信頼できるポートとして設定するか、または入力トラフィックと一致する trust CoS ポリシー マップを設定します。
- タグ付き入力トラフィックを受信するポートでは、入力トラフィックと一致する trust CoS ポリシー マップを設定します。

trusted として設定されている入力 LAN ポートからのタグなしフレーム、および untrusted として設定されている入力 LAN ポートからの全フレームに PFC QoS が割り当てる CoS 値を設定できます。

入力 LAN ポートの CoS 値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{type[1] slot/port} | {port-channel number}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos cos port_cos` `Router(config-if)# no mls qos cos port_cos`	入力 LAN ポートの CoS 値を設定します。 デフォルトのポート CoS 値に戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queuing interface {ethernet | fastethernet | gigabitethernet} slot/port`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート FastEthernet 5/24 に CoS 値 5 を設定し、設定を確認する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/24
Router(config-if)# mls qos cos 5
Router(config-if)# end
Router# show queueing interface fastethernet 5/24 | include Default COS
  Default COS is 5
Router#
```

標準キューの廃棄スレッシュホールドの割合設定

ここでは、標準キューの廃棄スレッシュホールドの割合を設定する手順を説明します。

- テール廃棄受信キューの設定（p.42-93）
- WRED 廃棄送信キューの設定（p.42-94）
- WRED 廃棄およびテール廃棄受信キューの設定（p.42-94）
- WRED 廃棄およびテール廃棄送信キューの設定（p.42-95）
- 1q4t/2q2t テール廃棄スレッシュホールドの割合設定（p.42-96）

（注）

- ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。
- **1p1q0t** ポートに、設定変更可能なスレッシュホールドはありません。
- **1p3q1t**（送信）、**1p2q1t**（送信）、および **1p1q8t**（受信）ポートにも、設定変更できないテール廃棄スレッシュホールドがあります。

スレッシュホールドを設定する場合、次の点に注意してください。

- キュー番号 1 は、プライオリティが一番低い標準キューです。
- キュー番号が大きくなると、標準キューのプライオリティが高くなります。

複数のスレッシュホールド標準キューを設定する場合、次の点に注意してください。

- 最初に入力したパーセント値は、プライオリティが一番低いスレッシュホールドを設定します。
- 2 番めに入力したパーセント値は、2 番めにプライオリティが高いスレッシュホールドを設定します。

- 最後に入力したパーセント値は、プライオリティが一番高いスレッシュホールドを設定します。
- 1 ～ 100 の範囲のパーセント値を使用します。10 という値は、バッファが 10% 満たされている場合のスレッシュホールドを意味します。
- プライオリティが一番高いスレッシュホールドは、常に 100% に設定してください。

WRED 廃棄スレッシュホールドを設定する場合、次の点に注意してください。

- WRED 廃棄 スレッシュホールドには、それぞれロー WRED 値およびハイ WRED 値があります。
- ローおよびハイ WRED 値は、キュー容量のパーセント値で表されます（範囲は 1 ～ 100）。
- ロー WRED 値は、トラフィック レベルがその値より下がるとトラフィックがまったく廃棄されなくなる限界を表します。ロー WRED 値には、ハイ WRED 値より小さい値を指定する必要があります。
- ハイ WRED 値は、トラフィック レベルがその値を超過するとすべてのトラフィックが廃棄される限界を表します。
- ロー WRED 値とハイ WRED 値の中間にあるキュー内のトラフィックは、キューが満たされるにつれて、廃棄される可能性が高くなります。

テール廃棄受信キューの設定

次のポート タイプには、受信キューにテール廃棄スレッシュホールドのみがあります。

- **1q2t**
- **1p1q4t**
- **2q8t**
- **1q8t**

廃棄スレッシュホールドを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {fastethernet | gigabitethernet} slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# rcv-queue threshold queue_id thr1% thr2% thr3% thr4% {thr5% thr6% thr7% thr8%}`	受信キューのテール廃棄スレッシュホールドの割合を設定します。
	`Router(config-if)# no rcv-queue threshold [queue_id]`	受信キューのテール廃棄スレッシュホールドをデフォルトの割合に戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queueing interface {fastethernet | gigabitethernet} slot/port`	設定を確認します。

次に、ポート GigabitEthernet 1/1 について、受信キュー廃棄スレッシュホールドを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# rcv-queue threshold 1 60 75 85 100
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | begin Receive queues
Receive queues [type = 1p1q4t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         Standard            4
       2         Priority            1

  Trust state: trust COS

    queue tail-drop-thresholds
    --------------------------
    1     60[1] 75[2] 85[3] 100[4]
(テキスト出力は省略)
Router#
```

WRED 廃棄送信キューの設定

次のポート タイプには、送信キューに WRED 廃棄スレッシュホールドのみがあります。

- **1p2q2t**（送信）
- **1p2q1t**（送信）

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# wrr-queue random-detect min-threshold queue_id thr1% [thr2%]`	ロー WRED 廃棄スレッシュホールドを設定します。
	`Router(config-if)# no wrr-queue random-detect min-threshold [queue_id]`	デフォルトのロー WRED 廃棄スレッシュホールドに戻します。
ステップ 3	`Router(config-if)# wrr-queue random-detect max-threshold queue_id thr1% [thr2%]`	ハイ WRED 廃棄スレッシュホールドを設定します。
	`Router(config-if)# no wrr-queue random-detect max-threshold [queue_id]`	デフォルトのハイ WRED 廃棄スレッシュホールドに戻します。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show queueing interface type[1] slot/port`	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

WRED 廃棄およびテール廃棄受信キューの設定

次のポート タイプは、受信キューに WRED 廃棄およびテール廃棄スレッシュホールドの両方があります。

- **8q4t**（受信）
- **8q8t**（受信）
- **1p1q8t**（受信）

廃棄スレッシュホールドを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue threshold** *queue_id thr1% thr2% thr3% thr4% thr5% thr6% thr7% thr8%*	テール廃棄スレッシュホールドを設定します。
	Router(config-if)# **no rcv-queue threshold** [*queue_id*]	デフォルトのテール廃棄スレッシュホールドに戻します。
ステップ 3	Router(config-if)# **rcv-queue random-detect min-threshold** *queue_id thr1% thr2% thr3% thr4% thr5% thr6% thr7% thr8%*	ロー WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no rcv-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED 廃棄スレッシュホールドに戻します。
ステップ 4	Router(config-if)# **rcv-queue random-detect max-threshold** *queue_id thr1% thr2% thr3% thr4% thr5% thr6% thr7% thr8%*	ハイ WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no rcv-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED 廃棄スレッシュホールドに戻します。
ステップ 5	Router(config-if)# **rcv-queue random-detect** *queue_id*	WRED 廃棄スレッシュホールドをイネーブルにします。
	Router(config-if)# **no rcv-queue random-detect** [*queue_id*]	テール廃棄スレッシュホールドをイネーブルにします。
ステップ 6	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 7	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

WRED 廃棄およびテール廃棄送信キューの設定

次のポート タイプは、送信キューに WRED 廃棄およびテール廃棄スレッシュホールドの両方があります。

- **1p3q1t**（送信）
- **1p3q8t**（送信）
- **1p7q8t**（送信）

廃棄スレッシュホールドを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue threshold** *queue_id thr1% [thr2% thr3% thr4% thr5% thr6% thr7% thr8%]*	テール廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue threshold** [*queue_id*]	デフォルトのテール廃棄スレッシュホールドに戻します。
ステップ 3	Router(config-if)# **wrr-queue random-detect min-threshold** *queue_id thr1% [thr2% thr3% thr4% thr5% thr6% thr7% thr8%]*	ロー WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue random-detect min-threshold** [*queue_id*]	デフォルトのロー WRED 廃棄スレッシュホールドに戻します。

	コマンド	目的
ステップ 4	Router(config-if)# **wrr-queue random-detect max-threshold** *queue_id thr1% [thr2% thr3% thr4% thr5% thr6% thr7% thr8%]*	ハイ WRED 廃棄スレッシュホールドを設定します。
	Router(config-if)# **no wrr-queue random-detect max-threshold** [*queue_id*]	デフォルトのハイ WRED 廃棄スレッシュホールドに戻します。
ステップ 5	Router(config-if)# **wrr-queue random-detect** *queue_id*	WRED 廃棄スレッシュホールドをイネーブルにします。
	Router(config-if)# **no wrr-queue random-detect** [*queue_id*]	テール廃棄スレッシュホールドをイネーブルにします。
ステップ 6	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 7	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート GigabitEthernet 1/1 について、ロー プライオリティ送信キューのハイ WRED 廃棄スレッシュホールドを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# wrr-queue random-detect max-threshold 1 70 70
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1 | begin Transmit queues
  Transmit queues [type = 1p2q2t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         WRR low             2
       2         WRR high            2
       3         Priority            1

    queue random-detect-max-thresholds
    ----------------------------------
      1    40[1] 70[2]
      2    40[1] 70[2]
(テキスト出力は省略)
Router#
```

1q4t/2q2t テール廃棄スレッシュホールドの割合設定

次に、**1q4t/2q2t** ポートでの受信キューおよび送信キューの廃棄スレッシュホールドの関係を示します。

- 受信キュー 1（標準）スレッシュホールド 1 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 2 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 2
- 受信キュー 1（標準）スレッシュホールド 3 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 4 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 2

1q4t/2q2t LAN ポートに標準受信キューおよび送信キューのテール廃棄スレッシュホールドの割合を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {**ethernet** | **fastethernet** | **gigabitethernet**} *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue threshold** *queue_id thr1% thr2%* Router(config-if)# **no wrr-queue threshold** [*queue_id*]	受信キューおよび送信キューのテール廃棄スレッシュホールドを設定します。 受信キューおよび送信キューのデフォルトのテール廃棄スレッシュホールドに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# show queueing interface {**ethernet** | **fastethernet** | **gigabitethernet**} *slot/port*	設定を確認します。

受信キューおよび送信キューのテール廃棄スレッシュホールドを設定する場合、次の点に注意してください。

- 送信キュー番号およびスレッシュホールド番号を使用する必要があります。
- *queue_id* は、標準ロー プライオリティ キューについては 1、標準ハイ プライオリティ キューについては 2 です。
- 1 ～ 100 の範囲のパーセント値を使用します。10 という値は、バッファが 10% 満たされている場合のスレッシュホールドを意味します。
- スレッシュホールドは常に 2 ～ 100% の範囲で設定してください。
- イーサネットおよびファスト イーサネット **1q4t** ポートは、受信キュー テール廃棄スレッシュホールドをサポートしません。

次に、ポート GigabitEthernet 2/1 について、受信キュー 1/ スレッシュホールド 1、および送信キュー 1/ スレッシュホールド 1 を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 2/1
Router(config-if)# wrr-queue threshold 1 60 100
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 2/1
  Transmit queues [type = 2q2t]:

(テキスト出力は省略)

queue tail-drop-thresholds
    -------------------------
    1     60[1] 100[2]
    2     40[1] 100[2]

(テキスト出力は省略)

Receive queues [type = 1q4t]:

(テキスト出力は省略)

queue tail-drop-thresholds
    -------------------------
    1     60[1] 100[2] 40[3] 100[4]
(テキスト出力は省略)
Router#
```

QoS ラベルのキューおよび廃棄スレッシュホールドへのマッピング

ここでは、QoS ラベルをキューおよび廃棄スレッシュホールドにマッピングする方法について説明します。

（注）　ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。

ここでは、QoS ラベルをキューおよび廃棄スレッシュホールドにマッピングする方法について説明します。

- キューおよび廃棄スレッシュホールドへのマッピングに関する注意事項および制約事項（p.42-98）
- DSCP ベースのキュー マッピングの設定（p.42-99）
- CoS ベースのキュー マッピングの設定（p.42-104）

キューおよび廃棄スレッシュホールドへのマッピングに関する注意事項および制約事項

QoS ラベルをキューおよびスレッシュホールドにマッピングする場合、次の点に注意してください。

- SRR がイネーブルにされている場合は、CoS 値 または DSCP 値を完全優先キューにマッピングできません。
- キュー番号 1 は、プライオリティが一番低い標準キューです。
- キュー番号が大きくなると、標準キューのプライオリティが高くなります。
- 最大 8 つの CoS 値をスレッシュホールドにマッピングできます。
- 最大 64 個の DSCP 値をスレッシュホールドにマッピングできます。
- スレッシュホールド 0 は、次のポート タイプの場合、設定変更できない 100% テール廃棄スレッシュホールドを意味します。
  - **1p1q0t**（受信）
  - **1p1q8t**（受信）
  - **1p3q1t**（送信）
  - **1p2q1t**（送信）
- 標準キュー スレッシュホールドは、次のポート タイプでテール廃棄または WRED 廃棄スレッシュホールドとして設定できます。
  - **1p1q8t**（受信）
  - **1p3q1t**（送信）
  - **1p3q8t**（送信）
  - **1p7q1t**（送信）

DSCP ベースのキュー マッピングの設定

ここでは、DSCP ベースのキュー マッピングを設定する手順について説明します。

- 入力 DSCP ベースのキュー マッピングの設定（p.42-99）
- 標準送信キュー スレッショルドへの DSCP 値のマッピング（p.42-102）
- 送信完全優先キューへの DSCP 値のマッピング（p.42-103）

（注）　DSCP ベースのキュー マッピングは、WS-X6708-10GE ポートでサポートされます。

DSCP ベースのキュー マッピングのイネーブル化

DSCP ベースのキュー マッピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface tengigabitethernet` *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos queue-mode mode-dscp`	DSCP ベースのキュー マッピングをイネーブルにします。
	`Router(config-if)# no mls qos queue-mode mode-dscp`	CoS ベースのキュー マッピングに戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queueing interface tengigabitethernet` *slot/port* `| include Queueing Mode`	設定を確認します。

次に、10 ギガビット イーサネット ポート 6/1 上で DSCP ベースのキュー マッピングをイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# mls qos queue-mode mode-dscp
Router(config-if)# end
```

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | include Queueing Mode
    Queueing Mode In Tx direction: mode-dscp
    Queueing Mode In Rx direction: mode-dscp
```

入力 DSCP ベースのキュー マッピングの設定

入力 DSCP とキューとのマッピングは、DSCP を信頼するように設定されたポートのみでサポートされます。

ここでは、入力 DSCP ベースのキュー マッピングを設定する手順について説明します。

- DSCP ベースのキュー マッピングのイネーブル化（p.42-99）
- 標準受信キュー スレッショルドへの DSCP 値のマッピング（p.42-100）

信頼 DSCP ポートの設定

DSCP を信頼するようにポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface tengigabitethernet slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# mls qos trust dscp`	受信した DSCP 値を信頼するようにポートを設定します。
	`Router(config-if)# no mls qos trust`	デフォルトの信頼状態（untrusted）に戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queueing interface tengigabitethernet slot/port | include Trust state`	設定を確認します。

次に、10 ギガビット イーサネット ポート 6/1 を、受信した DSCP 値を信頼するように設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 6/1
Router(config-if)# mls qos trust dscp
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 6/1 | include Trust state
  Trust state: trust DSCP
```

標準受信キュー スレッシュホールドへの DSCP 値のマッピング

DSCP 値を標準受信キュー スレッシュホールドにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface tengigabitethernet slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# rcv-queue dscp-map queue_# threshold_# dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]]`	標準受信キューのスレッシュホールドに DSCP 値をマッピングします。
	`Router(config-if)# no rcv-queue dscp-map`	デフォルトのマッピングに戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queueing interface tengigabitethernet slot/port`	設定を確認します。

DSCP 値をマッピングする場合、次の点に注意してください。

- キューおよびスレッシュホールドにマッピングする DSCP 値は、8 つまで入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューおよびスレッシュホールドにマッピングできます。
- キューおよびスレッシュホールドごとに個別のコマンドを入力する必要があります。

次に、10 ギガビット イーサネット ポート 1/6 に対して、標準受信キューのスレッシュホールド 1 に DSCP 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# rcv-queue dscp-map 1 1 0 1
Router(config-if)# end
Router#
```

（注）　受信キュー マッピングは、**show queueing interface** コマンドによって表示される、2 回めの「queue thresh dscp-map」に表示されます。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 1/1 | begin queue thresh dscp-map
(テキスト出力は省略)
queue thresh dscp-map
---------------------------------------
1     1      0 1 2 3 4 5 6 7 8 9 11 13 15 16 17 19 21 23 25 27 29 31 33 39 41 42 43 44 45
47
1     2
1     3
1     4
2     1      14
2     2      12
2     3      10
2     4
3     1      22
3     2      20
3     3      18
3     4
4     1      24 30
4     2      28
4     3      26
4     4
5     1      32 34 35 36 37 38
5     2
5     3
5     4
6     1      48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
6     2
6     3
6     4
7     1
7     2
7     3
7     4
8     1      40 46
8     2
8     3
8     4
(テキスト出力は省略)
Router#
```

標準送信キュー スレッシュホールドへの DSCP 値のマッピング

標準送信キュー スレッシュホールドに DSCP 値をマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface tengigabitethernet** *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue dscp-map** *transmit_queue_# threshold_# dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]]	標準送信キューのスレッシュホールドに DSCP 値をマッピングします。
	Router(config-if)# **no wrr-queue dscp-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface tengigabitethernet** *slot/port*	設定を確認します。

DSCP 値をマッピングする場合、次の点に注意してください。

- キューおよびスレッシュホールドにマッピングする DSCP 値は、8 つまで入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューおよびスレッシュホールドにマッピングできます。
- キューおよびスレッシュホールドごとに個別のコマンドを入力する必要があります。

次に、10 ギガビット イーサネット ポート 6/1 に対して、標準送信キュー 1、およびスレッシュホールド 1 に、DSCP 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# wrr-queue dscp-map 1 1 0 1
Router(config-if)# end
Router#
```

（注）　**show queueing interface** コマンドの出力では、8 番めのキューは完全優先キューです。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | begin queue thresh dscp-map
queue thresh dscp-map
---------------------------------------
1     1      0 1 2 3 4 5 6 7 8 9 11 13 15 16 17 19 21 23 25 27 29 31 33 39 41 42 43 44 45
47
1     2
1     3
1     4
2     1      14
2     2      12
2     3      10
2     4
3     1      22
3     2      20
3     3      18
3     4
4     1      24 30
4     2      28
4     3      26
4     4
5     1      32 34 35 36 37 38
5     2
5     3
5     4
6     1      48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
6     2
6     3
6     4
7     1
7     2
7     3
7     4
8     1      40 46
(テキスト出力は省略)
Router#
```

送信完全優先キューへの DSCP 値のマッピング

DSCP 値を送信完全優先キューにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface tengigabitethernet** *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **priority-queue dscp-map** *queue_# dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]]	送信完全優先キューに DSCP 値をマッピングします。複数の **priority-queue dscp-map** コマンドを入力することで、8 つ以上の DSCP 値を完全優先キューにマッピングできます。
	Router(config-if)# **no priority-queue dscp-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface tengigabitethernet** *slot/port*	設定を確認します。

完全優先キューに DSCP 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に 1 です。
- キューにマッピングする、最大 8 つの DSCP 値を入力できます。
- 複数のコマンドを入力して、追加の DSCP 値をキューにマッピングできます。

次に、10 ギガビット イーサネット ポート 6/1 の完全優先キューに、DSCP 値 7 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tengigabitethernet 6/1
Router(config-if)# priority-queue dscp-map 1 7
Router(config-if)# end
Router#
```

（注）　**show queueing interface** コマンドの出力では、完全優先キューは 8 番めのキューです。

次に、設定を確認する例を示します。

```
Router# show queueing interface tengigabitethernet 6/1 | begin queue thresh dscp-map
   queue thresh dscp-map
   ---------------------------------------
(テキスト出力は省略)
   8     1       7 40 46
(テキスト出力は省略)
Router#
```

CoS ベースのキュー マッピングの設定

ここでは、CoS ベースのキュー マッピングを設定する手順について説明します。

- 標準受信キュー スレッショルドへの CoS 値のマッピング（p.42-104）
- 標準送信キュー スレッショルドへの CoS 値のマッピング（p.42-105）
- 完全優先キューへの CoS 値のマッピング（p.42-106）
- 1q4t/2q2t LAN ポートのテール廃棄スレッショルドへの CoS 値のマッピング（p.42-107）

標準受信キュー スレッショルドへの CoS 値のマッピング

CoS 値を標準受信キュー スレッショルドにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue cos-map** *queue_# threshold_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	標準受信キューのスレッショルドに CoS 値をマッピングします。
	Router(config-if)# **no rcv-queue cos-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート GigabitEthernet 1/1 に対して、標準受信キューのスレッシュホールド 1 に CoS 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# rcv-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1
(テキスト出力は省略)
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    1     3      4 5
    1     4      6 7
(テキスト出力は省略)
Router#
```

標準送信キュー スレッシュホールドへの CoS 値のマッピング

標準送信キュー スレッシュホールドに CoS 値をマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **wrr-queue cos-map** *transmit_queue_# threshold_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	標準送信キューのスレッシュホールドに CoS 値をマッピングします。
	Router(config-if)# **no wrr-queue cos-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート FastEthernet 5/36 に対して、標準送信キュー 1/ スレッシュホールド 1 に、CoS 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4 5
    2     2      6 7
(テキスト出力は省略)
Router#
```

完全優先キューへの CoS 値のマッピング

CoS 値を送受信完全優先キューにマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **priority-queue cos-map** *queue_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	受信および送信完全優先キューに CoS 値をマッピングします。
	Router(config-if)# **no priority-queue cos-map**	デフォルトのマッピングに戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** *type*[1] *slot/port*	設定を確認します。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

完全優先キューに CoS 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に 1 です。
- キューにマッピングする、最大 8 つの CoS 値を入力できます。

次に、ポート GigabitEthernet 1/1 の完全優先キューに、CoS 値 7 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/1
(テキスト出力は省略)
Transmit queues [type = 1p2q2t]:
(テキスト出力は省略)
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4
    2     2      6
    3     1      5 7

  Receive queues [type = 1p1q4t]:
(テキスト出力は省略)
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    1     3      4
    1     4      6
    2     1      5 7
(テキスト出力は省略)
Router#
```

1q4t/2q2t LAN ポートのテール廃棄スレッシュホールドへの CoS 値のマッピング

（注）　ポートのキュー構造を表示するには、**show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** コマンドを使用します。

次に、**1q4t/2q2t** LAN ポートでの受信キューおよび送信キューのテール廃棄スレッシュホールドの関係を示します。

- 受信キュー 1（標準）スレッシュホールド 1 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 2 = 送信キュー 1（標準ロー プライオリティ）スレッシュホールド 2
- 受信キュー 1（標準）スレッシュホールド 3 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 1
- 受信キュー 1（標準）スレッシュホールド 4 = 送信キュー 2（標準ハイ プライオリティ）スレッシュホールド 2

テール廃棄スレッシュホールドに CoS 値をマッピングするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface` *type*[1] *slot/port*	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# wrr-queue cos-map transmit_queue_# threshold_# cos1` [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	テール廃棄スレッシュホールドに CoS 値をマッピングします。
ステップ 3	`Router(config-if)# no wrr-queue cos-map`	デフォルトのマッピングに戻します。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show queueing interface` *type*[1] *slot/port*	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

テール廃棄スレッシュホールドに CoS 値をマッピングする場合、次の点に注意してください。

- 送信キュー番号およびスレッシュホールド番号を使用する必要があります。
- キュー 1 は、ロー プライオリティ標準送信キューです。
- キュー 2 は、ハイ プライオリティ標準送信キューです。
- キューごとに 2 つのスレッシュホールドがあります。
- スレッシュホールドにマッピングする、最大 8 つの CoS 値を入力します。

次に、ポート FastEthernet 5/36 に対して、標準送信キュー 1/ スレッシュホールド 1 に、CoS 値 0 および 1 をマッピングする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
    queue thresh cos-map
    ---------------------------------------
    1     1       0 1
    1     2       2 3
    2     1       4 5
    2     2       6 7
(テキスト出力は省略)
Router#
```

標準送信キュー間での帯域幅の割り当て

スイッチはいずれかのデキューイング アルゴリズムを使用して、一度に 1 つの標準キューからフレームを送信します。デキューイング アルゴリズムはパーセント値または重み値を使用して、ラウンドロビン方式で処理された各キューに、相対的な帯域幅を割り当てます。

- Shaped Round Robin（SRR; シェイプド ラウンド ロビン）— SRR を使用すると、1 つのキューは、割り当てられた帯域幅のみの使用が許可されます。Supervisor Engine 32 SFP の **1p3q8t** ポートおよび **1p7q4t** ポートのオプションとしてサポートされます。
- Deficit Weighted Round Robin（DWRR）— より高いプライオリティのキュー内のトラフィックによってプライオリティを低く設定されている、転送中のすべてのキューを追跡し、次回のラウンドでこの差分を補います。DWRR は、**1p3q1t**、**1p2q1t**、**1p3q8t**、**1p7q4t**、および **1p7q8t** ポートでのデキューイング アルゴリズムです。

（注）　DWRR ポートの設定には、WRR ポートで使用するものと同じコマンドを使用します。

- Weighted Round-Robin（WRR; 重み付きラウンドロビン）— WRR では、他のキューが帯域幅を使用していない場合、キューは割り当てられた帯域幅を超えて、ポートの最大帯域幅まで使用できます。WRR は、他のすべてのポートで有効なデキューイング アルゴリズムです。

Release 12.2(18)SXF 以降のリリースでは、帯域幅の割り当てにパーセント値または重み値を入力できます。Release 12.2(18)SXF より前のリリースでは、重み値を入力して帯域幅を割り当てます。

割り当てられたパーセント値または重み値の比率が大きいキューほど、多くの送信帯域幅が割り当てられます。重み値を入力した場合は、重み値間の比率によってキューの合計帯域幅の分割比率が決定します。たとえば、ギガビット イーサネット ポート上の 3 つのキューの場合、重み値は 25:25:50 になり、次のように割り当てられます。

- キュー 1 — 250 Mbps
- キュー 2 — 250 Mbps
- キュー 3 — 500 Mbps

（注）　実際の帯域幅の割り当ては、設定済みのパーセント値または重み値に対してポート ハードウェアが適用する粒度によって異なります。

標準送信キュー間で帯域幅を割り当てるには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。

ステップ 2	`Router(config-if)# wrr-queue [bandwidth | shape] percent low_priority_queue_percentage [intermediate_priority_queue_percentages] high_priority_queue_percentage`
	
	または
	
	`Router(config-if)# wrr-queue [bandwidth | shape] low_priority_queue_weight [intermediate_priority_queue_weights] high_priority_queue_weight`
		標準送信キュー間で帯域幅を割り当てます。
		• **bandwidth** キーワードを入力して、DWRR または WRR を設定します。
		• **shape** キーワードを入力して、SRR を設定します。SRR を使用する場合は、完全優先キューを使用できません。SRR を設定する場合は、完全優先キューにマッピングされたすべての CoS 値または DSCP 値を、標準キューに再マッピングする必要があります（「QoS ラベルのキューおよび廃棄スレッシュホールドへのマッピング」[p.42-98] を参照）。
		• 各パーセント値は、必ず合計で 100 となるようにします。また、ポートのすべての標準送信キューに対してパーセント値を入力する必要があります（Release 12.2(18)SXF 以降のリリースでサポートされます）。
		• 重み値の有効範囲は 1 ～ 255 です。ポートのすべての標準送信キューに対して重み値を入力する必要があります。

	`Router(config-if)# no wrr-queue [bandwidth | shape]`	デフォルトの帯域幅の割り当てに戻します。
ステップ 3	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show queueing interface type[1] slot/port`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、ポート GigabitEthernet 1/2 に対して、帯域幅の比率を 3 対 1 に割り当てる例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue bandwidth 3 1
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/2 | include bandwidth
WRR bandwidth ratios:    3[queue 1]   1[queue 2]
Router#
```

受信キューのサイズ比の設定

2q8t、**8q4t**、および **8q8t** ポートの標準受信キュー間で、さらに **1p1q0t** または **1p1q8t** ポートの完全優先受信キューと標準受信キューとの間で、サイズ比を設定できます。

受信キュー間のサイズ比を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router(config)# **interface** {**fastethernet** | **tengigabitethernet**} *slot/port*	設定するインターフェイスを選択します。
ステップ 2	Router(config-if)# **rcv-queue queue-limit** *low_priority_queue_weight* [*intermediate_priority_queue_weights*] *high_priority_queue_weight* または Router(config-if)# **rcv-queue queue-limit** *standard_queue_weight strict_priority_queue_weight* Router(config-if)# **no rcv-queue queue-limit**	受信キュー間のサイズ比を設定します。 デフォルトのサイズ比に戻します。
ステップ 3	Router(config-if)# **end**	コンフィギュレーション モードを終了します。
ステップ 4	Router# **show queueing interface** {**fastethernet** | **tengigabitethernet**} *slot/port*	設定を確認します。

受信キュー サイズ比を設定する場合、次の点に注意してください。

- **rcv-queue queue-limit** コマンドは、ASIC 単位でポートを設定します。
- ネットワークにおける、プライオリティの異なるトラフィックの比率を概算してください（例：標準トラフィック 80%、完全優先トラフィック 20% など）。
- 概算したパーセント値を、各キューの重みとして使用します。
- 有効値は 1 ～ 100% です。ただし、**1p1q8t** ポートの場合、完全優先キューの有効値は 3 ～ 100% です。

次に、ポート FastEthernet 2/2 について、受信キュー サイズ比を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 2/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface fastethernet 2/2 | include queue-limit
    queue-limit ratios:     75[queue 1]  15[queue 2]
Router#
```

送信キューのサイズ比の設定

送信キューのサイズ比を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# wrr-queue queue-limit low_priority_queue_weight [intermediate_priority_queue_weights] high_priority_queue_weight`	送信キュー間のキュー サイズ比を設定します。
ステップ 3	`Router(config-if)# priority-queue queue-limit strict_priority_queue_weight`	完全優先キューのサイズを設定します。 （注）　この機能は、すべてのスイッチング モジュールでサポートされているわけではありません。
ステップ 4	`Router(config-if)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show queueing interface type[1] slot/port`	設定を確認します。

1. *type* = **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet**

送信キュー間の送信キュー サイズ比を設定する場合、次の点に注意してください。

- **wrr-queue queue-limit** コマンドは、**2q2t** および **1p3q1t** ポートではサポートされません。
- 出力完全優先キューを持つポートの場合：
  - Release 12.2(18)SXF2 以降のリリースでは、**priority-queue queue-limit** インターフェイス コマンドを入力することで、次のスイッチング モジュールに対して出力完全優先キューのサイズを設定できます。
    - WS-X6502-10GE（**1p2q1t**）
    - WS-X6148A-GE-TX（**1p3q8t**）
    - WS-X6148-RJ-45（**1p3q8t**）
    - WS-X6148-FE-SFP（**1p3q8t**）
    - WS-X6748-SFP（**1p3q8t**）
    - WS-X6724-SFP（**1p7q8t**）
    - WS-X6704-10GE（**1p7q4t**）
    - WS-SUP32-10GE-3B（**1p3q8t**）
    - WS-SUP32-GE-3B（**1p3q8t**）
    - WS-X6708-10GE（**1p7q4t**）
  - Release 12.2(18)SXF2 より前のリリース、および他のモジュールでは、PFC QoS は出力完全優先キューのサイズを、ハイ プライオリティ キューと同じサイズに設定します。
- ネットワークにおけるロー プライオリティ トラフィックとハイ プライオリティ トラフィックの比率を概算してください（例：ロー プライオリティ トラフィック 80%、ハイ プライオリティ トラフィック 20% など）。
- 概算したパーセント値を、各キューの重みとして使用します。
- インターフェイス上の標準送信キューすべてに重み（2、3、または 7 の重み）を入力する必要があります。
- 有効値は 1 ～ 100% です。ただし、**1p2q1t** 出力 LAN ポートの場合、ハイ プライオリティ キューの有効値は 5 ～ 100% です。

次に、ポート GigabitEthernet 1/2 に対して、送信キュー サイズ比を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue queue-limit 75 15
Router(config-if)# end
Router#
```

次に、設定を確認する例を示します。

```
Router# show queueing interface gigabitethernet 1/2 | include queue-limit
    queue-limit ratios:     75[queue 1]  25[queue 2]
Router#
```

一般的な QoS のシナリオ

ここでは、いくつかの一般的な QoS シナリオでの設定例を示します。使用するネットワークでの PFC QoS の設定方法をすでに理解している場合、または特定の設定情報を確認する場合は、この章内の他のセクションを参照してください。

このセクションで示す各シナリオは、「サンプル ネットワークの設計の概要」（p.42-113）で説明したサンプル ネットワークに基づいています。ここでは、このサンプル ネットワークを使用して、一般的に使用されるいくつかの QoS 設定について説明します。

ここで説明する一般的な QoS シナリオは、次のとおりです。

- サンプル ネットワークの設計の概要（p.42-113）
- アクセス レイヤにおける PC および IP Phone からのトラフィックの分類（p.42-114）
- スイッチ間リンクでのトラフィック プライオリティ値の受け入れ（p.42-117）
- スイッチ間リンクでのトラフィックの優先付け（p.42-118）
- ポリサーによる PC からのトラフィック量の制限（p.42-122）

サンプル ネットワークの設計の概要

このサンプル ネットワークは、アクセス レイヤ、ディストリビューション レイヤ、およびコア レイヤに Catalyst 6500 シリーズ スイッチを使用した、従来的なキャンパス ネットワーク アーキテクチャに基づきます。アクセス レイヤは、デスクトップ ユーザに 10/100 イーサネット サービスを提供します。このネットワークでは、アクセス レイヤとディストリビューション レイヤはギガビット イーサネット リンクで接続され、ディストリビューション レイヤとコア レイヤはギガビットまたは 10 ギガビット イーサネット リンクで接続されます。

基本的なポート設定は次のとおりです。

アクセス レイヤ

```
switchport mode access
switchport access vlan 10
switchport voice vlan 110
```

ディストリビューションおよびコア レイヤのスイッチ間リンク

```
switchport mode trunk
```

このサンプル ネットワークには、次の 3 つのトラフィック クラスがあります。

- 音声
- ハイ プライオリティ アプリケーション トラフィック
- ベストエフォート トラフィック

ここで説明する QoS 設定では、上記の各トラフィック クラスが識別され、優先付けられます。

（注）　これより多くのサービス レベルを必要とするネットワークの場合も、PFC QoS は最大 64 のトラフィック クラスをサポートできます。

各 QoS シナリオでは、次の 3 つの基本的な QoS 設定について説明します。これらは、多くの場合に QoS 構成の基本部分となります。

- アクセス レイヤにおいて、PC および IP Phone からのトラフィックを分類
- レイヤ間のスイッチ間リンクで、トラフィック プライオリティ値を受け入れ
- レイヤ間のスイッチ間リンクで、各トラフィックを優先付け

各 QoS シナリオでは、ネットワーク上では IP トラフィックのみが伝送され、トラフィック プライオリティの割り当てには IP DSCP 値が使用されることを前提とします。IP Type of Service（ToS; サービス タイプ）または Ethernet 802.1p CoS は直接使用しません。

IP パケットはプライオリティ値を伝送できますが、この値は、ネットワーク トポロジー内のさまざまな地点で設定できます。設計に関して推奨されるベスト プラクティスは、トラフィックの送信元にできるだけ近い位置でトラフィックを分類およびマーキングすることです。ネットワーク エッジでトラフィックのプライオリティが正しく設定されていれば、中間ホップではトラフィックを詳しく識別する必要がなくなります。代わりに、すでに設定済みのプライオリティ値に基づき、QoS ポリシーを管理できます。この方法だと、ポリシー管理が容易です。

（注）

- 特定のネットワーク トラフィック タイプとアプリケーションにパケット プライオリティを割り当てるための、適切な QoS 構成戦略を作成する必要があります。QoS に関する注意事項については、RFC 2597、RFC 2598、および米国シスコシステムズ社の発行するさまざまな QoS 設計ガイドを参照してください。
- PFC QoS をグローバルにイネーブルにし、他のすべての PFC QoS 設定をデフォルト値のままにすることはしないでください。PFC QoS をグローバルにイネーブル化すると、デフォルト値が使用されます。PFC QoS のデフォルト設定の使用には、次のような 2 つの問題があります。
  - PFC QoS をグローバルにイネーブル化すると、システム内のイーサネット ポートのデフォルトの信頼状態が untrusted となります。ポートの信頼状態が untrusted の場合は、スイッチ経由で送信されるすべてのトラフィックの QoS プライオリティが、ポートの CoS 値（デフォルトでは 0）に設定されます。つまり、すべてのトラフィックがプライオリティ 0 となります。
  - PFC QoS をグローバルにイネーブル化すると、ポートのバッファが CoS ベースのキューに割り当てられるので、プライオリティ 0 のトラフィックはバッファの一部しか使用できなくなります。つまり、プライオリティ 0 のトラフィックが使用できるバッファの量が、PFC QoS がディセーブルにされている場合よりも少なくなります。

  PFC QoS のデフォルト設定を使用することで生じるこのような問題は、ネットワーク パフォーマンスに悪影響を及ぼす可能性があります。

アクセス レイヤにおける PC および IP Phone からのトラフィックの分類

アクセス レイヤのスイッチには、100 Mbps リンクによって、IP Phone と PC がデイジーチェーン接続されています。ここでは、IP Phone からの音声トラフィックと PC からのデータ トラフィックを分類し、それぞれ異なるプライオリティを設定する方法について説明します。

アクセス レイヤ ポートで受信したトラフィックに対する QoS 分類スキームは、次のとおりです。

- 音声トラフィック：DSCP 46（最大プライオリティ）
- 音声シグナリング トラフィック：DSCP 24（ミディアム プライオリティ）
- PC SAP トラフィック：DSCP 25（ミディアム プライオリティ）
- 他のすべての PC トラフィック：DSCP 0（ベスト エフォート）

この分類戦略によって、ネットワーク上の次の 3 種類のサービス クラスをサポートできるようになります。

- ハイ プライオリティの音声トラフィック
- ミディアム プライオリティの音声シグナリング トラフィックおよび重要なアプリケーション トラフィック
- ロー プライオリティの残りのトラフィック

このモデルは、他のネットワーク環境に合わせて適宜変更できます。

PFC QoS は受信したプライオリティを信頼することも、QoS ポリシーをトラフィックに適用して、新たなプライオリティを割り当てることもできます。QoS ポリシーを設定するには、Modular QoS CLI（MQC; モジュラ QoS コマンドライン インターフェイス）を使用します。アクセス スイッチでは、トラフィックは ACL によって識別されます。ACL は、ポートに送られるさまざまなトラフィック タイプを区別します。識別されたトラフィックは、QoS ポリシーによって、適切な DSCP 値がマーキングされます。このように割り当てられた DSCP 値は、トラフィックがディストリビューション スイッチおよびコア スイッチに送られたときに信頼されます。

IP Phone と PC が接続されているアクセス スイッチのポートは、音声 VLAN（VLAN 110）用に設定されています。これは、IP Phone のトラフィック（サブネット 10.1.110.0/24）を PC トラフィック（サブネット 10.1.110.0/24）から区別する働きをします。音声 VLAN サブネットは、音声トラフィックを一意に識別します。UDP および TCP ポート番号は、異なるアプリケーションの識別に使用されます。

次に、アクセス ポートの ACL 設定を示します。

IP Phone からの音声トラフィック（VVLAN）を識別

```
ip access-list extended CLASSIFY-VOICE
    permit udp 10.1.110.0 0.0.0.255 any range 16384 32767
```

IP Phone からの音声シグナリング トラフィック（VVLAN）を識別

```
ip access-list extended CLASSIFY-VOICE-SIGNAL

    permit udp 10.1.110.0 0.0.0.255 any range 2000 2002
```

PC からの SAP トラフィック（DVLAN）を識別

```
ip access-list extended CLASSIFY-PC-SAP
    permit tcp 10.1.10.0 0.0.0.255 any range 3200 3203
    permit tcp 10.1.10.0 0.0.0.255 any eq 3600 any

ip access-list extended CLASSIFY-OTHER
    permit ip any any
```

QoS ポリシー設定の次の手順は、クラス マップを定義することです。クラス マップは、識別に使用する ACL を、実行させたい QoS アクション（この場合はマーキング）に関連付けます。クラス マップの構文は次のとおりです。

```
class-map match-all CLASSIFY-VOICE
    match access-group name CLASSIFY-VOICE
class-map match-all CLASSIFY-VOICE-SIGNAL
    match access-group name CLASSIFY-VOICE-SIGNAL
class-map match-all CLASSIFY-PC-SAP
    match access-group name CLASSIFY-PC-SAP
class-map match-all CLASSIFY-OTHER
    match access-group name CLASSIFY-OTHER
```

クラス マップを作成したら、次はポリシー マップを作成します。ポリシー マップは、各トラフィック タイプまたは各トラフィック クラスに特定の DSCP 値を設定できるように、QoS ポリシーのアクションを定義します。この例では 1 つのポリシー マップ（IPPHONE-PC）を作成します。すべてのクラス マップはこの単一ポリシー マップに含まれ、クラス マップごとに 1 つのアクションが定義されます。ポリシー マップとクラス マップの構文は次のとおりです。

```
policy-map IPPHONE-PC
   class CLASSIFY-VOICE
    set dscp ef
   class CLASSIFY-VOICE-SIGNAL
    set dscp cs3
   class CLASSIFY-PC-SAP
    set dscp 25
   class CLASSIFY-OTHER
    set dscp 0
```

この時点では、ポリシー マップ内で定義された QoS ポリシーは、まだ有効ではありません。設定の済んだポリシー マップは、トラフィックが影響を受けるように、インターフェイスに適用する必要があります。ポリシー マップを適用するには、**service-policy** コマンドを使用します。入力サービス ポリシーはポートにも VLAN インターフェイスにも適用できますが、出力サービス ポリシーは VLAN インターフェイスにしか適用できないことに注意してください（PFC3 のみが出力ポリシーをサポート）。この例では、PC と IP Phone がそれぞれ接続された各インターフェイスに、ポリシーを入力サービス ポリシーとして適用します。ここではポートベースの QoS を使用しますが、これはイーサネット ポートのデフォルトです。

```
interface FastEthernet5/1
 service-policy input IPPHONE-PC
```

これで、QoS ポリシーは正しく設定され、IP Phone と PC 両方から送信されるトラフィックを分類できるようになりました。

ポリシー マップが正しく設定されたことを確認するには、次のコマンドを入力します。

```
Router# show policy-map interface fastethernet 5/1
 FastEthernet5/1

  Service-policy input:IPPHONE-PC

    class-map:CLASSIFY-VOICE (match-all)
      Match:access-group name CLASSIFY-VOICE
      set dscp 46:

    class-map:CLASSIFY-PC-SAP (match-all)
      Match:access-group name CLASSIFY-PC-SAP
      set dscp 25:

    class-map:CLASSIFY-OTHER (match-all)
      Match:access-group name CLASSIFY-OTHER
      set dscp 0:

    class-map:CLASSIFY-VOICE-SIGNAL (match-all)
      Match:access-group name CLASSIFY-VOICE-SIGNAL
      set dscp 24:
```

ポートに正しい QoS モードが使用されているかどうかを確認するには、次のコマンドを入力します。

```
Router# show queueing interface gigabitethernet 5/1 | include Port QoS
Port QoS is enabled
```

クラス マップの設定が正しいかどうかを確認するには、次のコマンドを入力します。

```
Router# show class-map
 Class Map match-all CLASSIFY-OTHER (id 1)
   Match access-group name CLASSIFY-OTHER

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all CLASSIFY-PC-SAP (id 2)
   Match access-group name CLASSIFY-PC-SAP

 Class Map match-all CLASSIFY-VOICE-SIGNAL (id 4)
   Match access-group name CLASSIFY-VOICE-SIGNAL

 Class Map match-all CLASSIFY-VOICE (id 5)
   Match access-group name CLASSIFY-VOICE
```

各トラフィック クラスのバイト統計をモニタするには、次のコマンドを入力します。

```
Router# show mls qos ip gig 5/1
   [In] Policy map is IPPHONE-PC   [Out] Default.
 QoS Summary [IP]:     (* - shared aggregates, Mod - switch module)

           Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                        Id         Id

-------------------------------------------------------------------------------
          Gi5/1  5  In CLASSIFY-V   46    1     No  0              0  0
          Gi5/1  5  In CLASSIFY-V   24    2     No  0              0  0
          Gi5/1  5  In CLASSIFY-O    0    3     No  0              0  0
          Gi5/1  5  In CLASSIFY-P   25    4     No  0              0  0
Router#
```

スイッチ間リンクでのトラフィック プライオリティ値の受け入れ

前のセクションでは、マーキング処理の設定方法について説明しました。ここでは、アップストリーム装置がこのパケット マーキングを使用する仕組みについて説明します。

着信トラフィックのプライオリティが受け入れられるかどうかを決定する必要があります。この決定を反映させるには、ポートの信頼状態を設定します。着信トラフィックのプライオリティ設定を信頼しないように設定されたポートにトラフィックが着信すると、この着信トラフィックのプライオリティ設定は、最小プライオリティ（0）に書き換えられます。着信トラフィックのプライオリティ設定を信頼するように設定されたインターフェイスにトラフィックが着信した場合は、このトラフィックのプライオリティ設定は維持されます。

着信するプライオリティ設定を信頼するポートの例は、IP Phone や他の IP 音声装置、ビデオ装置、または、定義済みの有効なプライオリティが設定されたフレームの送信が信頼されるさまざまな装置に接続されているポートです。トラフィックが最初にネットワークに送信された時点で、適切なマーキングが完了していることがわかっている場合は、着信したプライオリティ設定を信頼するようにアップリンク インターフェイスを設定することもできます。

定義済みの有効なプライオリティを持つどのトラフィックも伝送しないワークステーションまたは他の装置に接続されたポートは、untrusted（デフォルト）として設定します。

前の例では、アクセス レイヤにおいて、音声、SAP、および他のベスト エフォート トラフィックを適切にマーキングするように QoS を設定しました。次の例では、トラフィックが他のネットワーク装置を通過するときに、これらのプライオリティ値が受け入れられるように QoS を設定します。これには、パケットの DSCP 値を信頼するようにスイッチ間リンクを設定します。

前の例では、いくつかの種類のトラフィック クラスがポートに入力されると仮定して、個々のトラフィック タイプにそれぞれ異なる QoS ポリシーを選択して適用しました。この設定は、MQC QoS ポリシー構文によって行いました。これにより、1 つのポートに着信するさまざまな種類のトラフィック クラスに対し、異なるマーキングまたは信頼アクションを個別に適用できます。

すべてのトラフィックが、信頼可能な 1 つの特定ポートに着信することがわかっている場合は（アクセス レイヤとディストリビューション レイヤ間、またはディストリビューション レイヤとコア レイヤ間のアップリンク ポートがこれに該当）、ポートを trust 状態に設定できます。ポートの trust 設定を使用すると、このポートで受信するさまざまなトラフィック タイプは区別されませんが、設定作業は大幅に単純化されます。ポートの trust 設定のコマンド構文は次のとおりです。

```
interface gigabitethernet 5/1
 mls qos trust dscp
```

受信した DSCP を信頼するようにポートを設定した場合は、スイッチから送信されるトラフィックの DSCP 値は、信頼されたポートに送られるトラフィックの DSCP 値と同じです。信頼状態を設定したあとは、次のコマンドを使用して、設定が有効になっているかどうかを確認できます。

```
Router# show queueing interface gigabitethernet 5/1 | include Trust
Trust state:trust DSCP
```

スイッチ間リンクでのトラフィックの優先付け

ここでは、スイッチが信頼値を使用してどのように動作するかを説明します。

QoS の基本原則の 1 つは、オーバーサブスクリプションが発生した場合に、プライオリティの高いトラフィックを保護することです。「アクセス レイヤにおける PC および IP Phone からのトラフィックの分類」（p.42-114）および「スイッチ間リンクでのトラフィック プライオリティ値の受け入れ」（p.42-117）で説明したマーキングおよび信頼アクションでは、オーバーサブスクリプションに対処できるようにトラフィックを準備しますが、さまざまなレベルのサービスを提供することはできません。さまざまなレベルのサービスを実現するには、ネットワーク装置が、特定のインターフェイスからトラフィックを送信するときに各トラフィックを優先付ける、高度なスケジューリング アルゴリズムを備えている必要があります。このようなスケジューリング機能は、プライオリティの高いトラフィックが、プライオリティの低いトラフィックよりも高頻度に送信されることを保証します。最終的に得られる効果は、さまざまなトラフィック クラスに対して差別化したサービスを提供できることです。

さまざまなトラフィック クラスに対して差別化したサービスを提供する上で、次の 2 つの基本概念があります。

- トラフィックを特定のキューに割り当て
- キューのスケジューリング アルゴリズムを設定

QoS をイネーブルにすると、これらの各機能にデフォルト値が適用されます。多くのネットワークでは、ネットワーク トラフィックを区別するのに、デフォルト値で十分対応できます。それ以外のネットワークでは、必要とする結果が得られるように、デフォルト値を調整しなければならない場合もあります。これらの機能に対するデフォルト設定を大幅に変更しなければならないのは、ごくまれなケースのみです。

Catalyst 6500 シリーズ スイッチのイーサネット モジュールは、単一キュー アーキテクチャから、最大 8 つのキューからなるアーキテクチャまで、さまざまなキュー構造をサポートします。キュー構造は、トラフィック タイプごとに異なるサービスを提供する複数の車線をグループ化したようなもの、と考えることができます。たとえば警官は高速道路において、事故現場や犯罪現場に迅速に到着できるように、優先的に走行できる権限を持ちます。同様に、IP ネットワーク上の音声トラフィックも、このように優先的に扱われる必要があります。スイッチはキュー構造を使用して、差別化された各サービスに対して個別のレーンを用意しています。

具体的なキュー タイプは、使用するイーサネット モジュールによって異なります。この例では、4 つの送信キューを持つモジュールを使用します。このキューは 1p3q8t と表され、次の内容を意味します。

- 1 つの完全優先キュー（1p）
- WRR スケジューリングをサポートする、3 つの標準キュー（3q）。各キューはそれぞれ 8 つの WRED スレッシュホールドを保持します（8t、ここでは説明しません）。

Catalyst 6500 シリーズ スイッチのイーサネット モジュールは入力キュー構造も備えていますが、これはあまり使用されません。また、スイッチ ファブリック内ではあまり輻輳が発生しないと考えられるため、この例では入力キュー構造を扱いません。

これらのキューにトラフィックを割り当てるには、プライオリティ値をキューにマッピングする必要があります。QoS では DSCP と CoS のマッピングを使用して、発信される 64 の DSCP 値を 8 つの 802.1p 値に対応付けてから、CoS とキューのマッピングを使用して、CoS 値をキューに対応付けます。

パケットがスイッチに入力されると、QoS は設定に応じて、設定済み DSCP 値に基づきパケットを分類およびマーキングするか（「アクセス レイヤにおける PC および IP Phone からのトラフィックの分類」[p.42-114] を参照）、またはパケットの着信 DSCP 値を信頼します（「スイッチ間リンクでのトラフィック プライオリティ値の受け入れ」[p.42-117] を参照）。これらのオプションに応じて、スイッチから出力される際のパケットのプライオリティが決まります。

次に、DSCP と CoS のマッピングを表示する例を示します。

```
Router# show mls qos maps dscp-cos
   Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
Router#
```

この例では、音声トラフィックに DSCP 値 64 をマーキングします。コマンドの出力結果を使用して、DSCP 46 を CoS 5 に変換できます。また、コマンドの出力結果を使用して、マーキングされた他の DSCP 値を CoS 値に変換することもできます。

特定のネットワーク要件に応じて、このマッピング テーブルを変更してください。通常は、少量の変更が必要になるだけです。この例では変更を加えません。

キューイングを行う目的のため、この設定では発信される DSCP 値に基づいて CoS 値を導出しています。この CoS 値は、発信ポートがトランク ポートではなくアクセス ポートであっても、キューの割り当てに使用されます。ただし、発信ポートがアクセス ポートである場合は、ネットワーク上に 802.1q VLAN タグは送信されません。

導出された各 CoS 値を、キュー構造にマッピングします。次に、CoS とキューとのデフォルト マッピングを表示する例を示します。これにより、8 つの CoS 値それぞれがマッピングされているキューを確認できます。

```
Router# show queueing interface gigabitethernet 5/1 | begin cos-map
    queue thresh cos-map
    ---------------------------------------
    1     1      0
    1     2      1
    1     3
    1     4
    1     5
    1     6
    1     7
    1     8
    2     1      2
    2     2      3 4
    2     3
    2     4
    2     5
    2     6
    2     7
    2     8
    3     1      6 7
    3     2
    3     3
    3     4
    3     5
    3     6
    3     7
    3     8
    4     1      5
```

（テキスト出力は省略）

音声トラフィックは完全優先キューにマッピングします。これは、1p3q8t ポートにおけるキュー 4 です。この例では、DSCP 46 音声トラフィックを CoS 5 にマッピングします。つまり、CoS 5 トラフィックを完全優先キューにマッピングする必要があります。**show queueing interface** コマンドの出力結果を使用すると、CoS 5 トラフィックが完全優先キューにマッピングされていることを確認できます。

次に、この例のすべてのトラフィック タイプに対するキュー マッピングの一覧を示します。

トラフィック タイプ	DSCP	CoS（DSCP から CoS へのマッピング）	出力キュー
音声	46	5	完全優先
音声シグナリング	24	3	キュー 2、スレッシュホールド 2
PC SAP	25	3	キュー 2、スレッシュホールド 2
その他のトラフィック	0	0	キュー 1、スレッシュホールド 1

スイッチ経由で送信されるトラフィックは、プライオリティに基づき、各種のキュー（つまり「車線」）に転送されます。出力キュー（この例ではインターフェイスごとに 3 つ）より CoS 値（0 ～ 7）の数が多いため、各標準キュー（完全優先ではないキュー）にはそれぞれ廃棄スレッシュホールドが設定されています。1 つのキューに複数の CoS 値が割り当てられている場合は、各 CoS 値に数種類の廃棄スレッシュホールドを割り当て、異なるプライオリティを区別することができます。スレッシュホールドは、特定の CoS 値を持つトラフィックが、この CoS 値を持つトラフィックの

廃棄が開始される前に使用可能なキューの最大割合を指定します。この例で使用している QoS 値は 3 つだけなので（ハイ、ミディアム、ロー）、各 CoS 値を個別のキューに割り当て、デフォルトの 100% のスレッショルドを使用できます。

特定のネットワーク要件に応じて、DCSP と CoS とのマッピング、および CoS とキューとのマッピングを変更してください。通常は、少量の変更が必要になるだけです。この例では変更を加えていません。異なるマッピングが必要なネットワークの場合は、「標準送信キュー スレッショルドへの CoS 値のマッピング」（p.42-105）を参照してください。

スイッチの出力ポートでの有効なキューに、トラフィックが割り当てられる仕組みについての説明は以上です。次に学習する概念は、キューの重み値が機能する仕組みであり、これをキューのスケジューリング アルゴリズムと呼びます。

Catalyst 6500 シリーズ スイッチでは、LAN スイッチング モジュールに使用されるスケジューリング アルゴリズムは、完全優先（SP）キューイング、および WRR キューイングです。これらのアルゴリズムは、ポート上のさまざまなキューが処理される順序（優先度）を定義します。

完全優先キューイング アルゴリズムは単純です。1 つのキューが、他のすべてのキューより優先される絶対的なプライオリティを付与されます。完全優先キューにパケットが格納されている場合は常に、スケジューラはこのキューを処理します。このため、輻輳が生じた場合であっても、このキュー内のパケットが転送される可能性は最大となり、遅延の可能性が最低限に抑えられます。完全優先キューは、音声トラフィックに対して理想的です。音声トラフィックは、ネットワーク上で最高のプライオリティを必要とし、遅延を最低限に抑える必要があるためです。また、使用する帯域幅が比較的少ないトラフィック タイプでもあるので、通常は、音声トラフィックによってポート上の有効帯域幅がすべて消費されることもありません。FTP などの広帯域幅のアプリケーションは、完全優先キューに割り当てないようにしてください。FTP トラフィックはポートで有効な帯域幅をすべて消費してしまう可能性があり、その場合、他のトラフィック クラスがリソース不足となります。

WRR アルゴリズムでは、各 WRR キューに相対的な重み値を割り当てます。3 つのキューがあり、それぞれの重み値が 22:33:45（デフォルト設定）である場合は、キュー 1 は有効帯域幅の 22% のみを使用でき、キュー 2 は 33%、キュー 3 は 45% の帯域幅を使用できます。WRR では、どのキューもこれらの配分には限定されません。キュー 2 とキュー 3 にトラフィックがまったく存在しない場合は、キュー 1 は有効帯域幅をすべて使用できます。

この例では、キュー 1 よりキュー 2 のプライオリティのほうが高く、キュー 2 よりキュー 3 のプライオリティのほうが高く設定されています。したがって、ロー プライオリティ トラフィック（IP Phone その他、PC その他）はキュー 1 に、ミディアム プライオリティ トラフィック（音声シグナリング、PC SAP）はキュー 2 にマッピングされます。

完全優先キューは、トラフィックをマッピングしたあとは設定は不要です。WRR キューにはデフォルトの帯域幅が割り当てられており、通常のネットワークではこれで十分対応できます。デフォルト値で不十分な場合は、トラフィック タイプに合わせて相対的な重み値を変更できます（「標準送信キュー間での帯域幅の割り当て」[p.42-108] を参照）。

スイッチがオーバーサブスクリプションを適切に処理しているかどうかを確認する最も良い方法は、パケット廃棄が最小限で行われているのを確認することです。パケット損失の発生を確認するには、**show queueing interface** コマンドを使用します。このコマンドでは、各キューで廃棄されたパケット数が表示されます。

ポリサーによる PC からのトラフィック量の制限

特定の装置やトラフィック クラスが予想外の量の帯域幅を消費しないようにするには、レート制限を使用すると便利です。Catalyst 6500 シリーズ スイッチのイーサネット ポートでサポートされるレート制限方法を、ポリシングと呼びます。ポリシングは PFC ハードウェアに実装され、これによるパフォーマンスへの影響はありません。ポリサーは、トラフィック レートが所定のレートを超えないかぎり、トラフィック フローに何の制限も加えません。設定したバースト サイズ内であれば、トラフィック バーストも許可されます。設定したレートまたはバースト サイズを超えたすべてのトラフィックは、廃棄するか、またはより低いプライオリティにマークダウンできます。ポリシングの利点は、特定のアプリケーションが消費する帯域幅の量を制御できることです。これにより、特にウイルスやワーム攻撃などの異常事態がネットワーク上で発生した場合に、ネットワーク上でのサービス品質を保証しやすくなります。

この例では、基本的なインターフェイス別の aggregate ポリサーを、入力方向の単一のインターフェイスに適用します。これ以外のポリシング オプションを使用しても、同じ結果を得ることができます。

ポリサーの設定は、「アクセス レイヤにおける PC および IP Phone からのトラフィックの分類」（p.42-114）で説明したマーキングの例と似ています。これは、ポリシングでも同一の ACL および MQC 構文を使用するためです。この例で使用した構文では、トラフィックを識別するクラス マップを作成してから、トラフィックのマーキング方法を指定するポリシー マップを作成しました。

ポリシングの構文もこれとよく似ているので、マーキングの例に使用した ACL をそのまま使用します。また、マーキングの例に使用したクラス マップは、**set dscp** コマンドを **police** コマンドに置き換えて修正します。この例では、CLASSIFY-OTHER クラス マップを再利用して、修正した IPPHONE-PC ポリシー マップに基づきトラフィックを識別し、一致トラフィックを最大 50 Mbps にポリシングします。同時に、このレートに従うトラフィックを引き続きマーキングします。

参考までに、「その他」のトラフィックを識別するためのクラス マップ、ACL、および **class-map** コマンドを次に示します。変更は加えません。

- ACL コマンド：

```
ip access-list extended CLASSIFY-OTHER
permit ip any any
```

- class-map コマンド：

```
class-map match-all CLASSIFY-OTHER
match access-group name CLASSIFY-OTHER
```

このポリサー設定とマーキング設定との違いは、ポリシー マップ アクションの定義です。マーキングの例では、**set dscp** コマンドを使用して、特定の DSCP 値によってトラフィックをマーキングしました。このポリシング例では、CLASSIFY-OTHER トラフィックの DSCP 値を 0 にマーキングし、このトラフィックを 50 Mbps にポリシングします。これには、**set dscp** コマンドを **police** コマンドに置き換えます。**police** コマンドでは、マーキング アクションの実行を設定できます。50 Mbps の制限を下回るすべてのトラフィックは DSCP が 0 にマーキングされ、50 Mbps スレッシュホールドを超えるすべてのトラフィックは廃棄されます。

次に、**police** コマンドを加えて修正した IPPHONE-PC ポリシー マップを示します。

```
policy-map IPPHONE-PC
class CLASSIFY-OTHER
police 50000000 1562500 conform-action set-dscp-transmit default exceed-action drop
```

police コマンドの各パラメータの機能は次のとおりです。

- 50000000 パラメータは、このトラフィック クラスで許可されたトラフィックに対し、CIR 値を定義します。この例では、CIR を 50 Mbps に設定しています。

- 1562500 パラメータは、このトラフィック クラスのトラフィックの CIR バースト サイズを定義します。この例では、デフォルトの最大バースト サイズを使用します。CIR バースト サイズは、ネットワークで使用される最大の TCP ウィンドウ サイズに設定します。
- **conform action** キーワードは、トラフィック レベルが 50 Mbps レートを下回った場合に、送信された CLASSIFY-OTHER パケットに対してポリサーが実行する動作を定義します。この例では、**set-dscp-transmit default** により、このようなパケットの DSCP が 0 に設定されます。
- **exceed action** は、トラフィック レベルが 50 Mbps CIR を超過した場合に、送信された CLASSIFY-OTHER パケットに対してポリサーが実行する動作を定義します。この例では、**exceed action drop** により、このようなパケットが廃棄されます。

これは、基本的な、単一レートのインターフェイス別 aggregate ポリサーです。Supervisor Engine 2 および Supervisor Engine 720 転送エンジンでは、デュアル レート ポリサーもサポートされるため、CIR および PIR 粒度の両方を使用できます。

service-policy input コマンドを使用して、ポリシー マップを適切なインターフェイスに付加します。

```
interface FastEthernet5/1
service-policy input IPPHONE-PC
```

ポリシングの動作をモニタするには、次のコマンドを使用します。

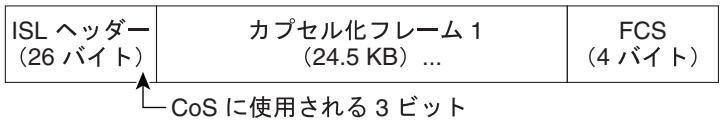
```
show policy-map interface fastethernet 5/1
show class-map
show mls qos ip fastethernet 5/1
```

PFC QoS の用語

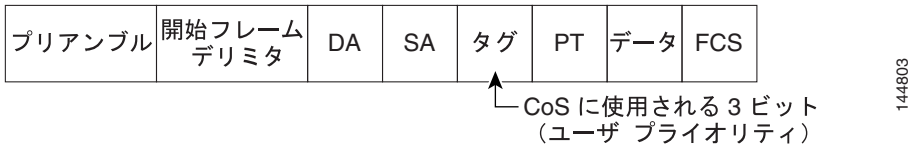
ここでは、この章で使用したいくつかの QoS 用語を定義します。

- *バッファ* — 送信中のデータを処理するための保管領域です。バッファはインターネットワーキングにおいて、ネットワーク装置間の処理速度の違いを補うために使用されます。バーストデータは、より低速な処理装置によって処理されるまで、バッファに保管されることがあります。バッファは、パケット バッファと呼ばれることもあります。
- *Class of Service（CoS; サービス クラス）* は、ISL、802.1Q、または 802.1p ヘッダーの 3 ビットによって伝送される、レイヤ 2 QoS ラベルです。CoS 値は 0 ～ 7 の範囲の値です。

レイヤ 2 ISL フレーム

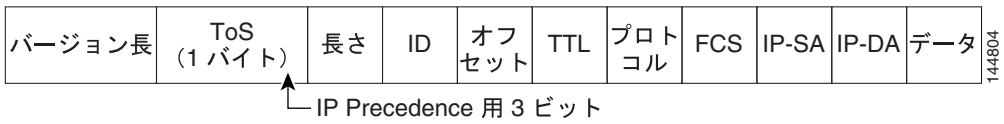


レイヤ 2 802.1Q および 802.1p フレーム



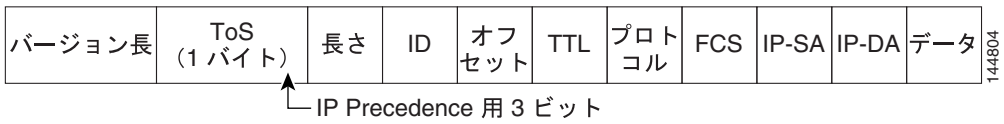
- *分類*は、QoS のマーキングを行うトラフィックを選択する処理です。
- *輻輳回避*は、プライオリティの高いレイヤ 2 CoS 値を持つレイヤ 2 フレームのために、入力 LAN ポートおよび出力 LAN ポートの容量を PFC QoS で確保しておく処理です。PFC QoS では、レイヤ 2 CoS 値ベースの廃棄スレッシュホールドによって輻輳回避を実行します。廃棄スレッシュホールドは、キュー バッファ使用率であり、この割合に達すると、特定のレイヤ 2 CoS 値を持つフレームが廃棄され、よりプライオリティの高いレイヤ 2 CoS 値を持つフレーム用に利用可能なバッファが残されます。
- *Differentiated Services Code Point*（DSCP）は、IP ヘッダー内の ToS バイトの最上位 6 ビットによって伝送される、レイヤ 3 の QoS ラベルです。DSCP 値は 0 ～ 63 の範囲の値です。

レイヤ 3 IPv4 パケット



- *フレーム* — レイヤ 2 でトラフィックを伝送します。レイヤ 2 フレームは、レイヤ 3 パケットを伝送します。
- *IP Precedence* は、IP ヘッダー内の ToS バイトの最上位 3 ビットによって伝送される、レイヤ 3 の QoS ラベルです。IP precedence 値は 0 ～ 7 の範囲の値です。

レイヤ 3 IPv4 パケット



- *ラベル* — QoS ラベルを参照してください。
- *マーキング*は、レイヤ 3 の DSCP 値をパケットに設定する処理です。このマニュアルでは、マーキングの定義を拡大して、レイヤ 2 CoS 値の設定までを含めています。マーキングは、ラベルの値を変更します。
- *パケット* — レイヤ 3 でトラフィックを伝送します。
- *ポリシング* — トラフィック フローが使用する帯域幅を制限する処理です。ポリシングは、PFC および Distributed Forwarding Card（DFC）上で実行されます。ポリシングによって、トラフィックのマーキングまたは廃棄が可能になります。
- *キュー* — データを一時的にポート上に保管しておくための、バッファ領域の割り当てです。
- *QoS ラベル* — PFC QoS では、CoS、DSCP、および IP Precedence が QoS ラベルとして使用されます。QoS ラベルは、レイヤ 3 パケットおよびレイヤ 2 フレームで伝送されるプライオリティ値です。
- *スケジューリング* — レイヤ 2 フレームをキューに割り当てることです。PFC QoS は、レイヤ 2 CoS 値に基づいて、フレームをキューに割り当てます。
- *Shaped Round Robin（SRR; シェイプド ラウンド ロビン）*は、デキューイング アルゴリズムです。
- *スレッショルド* — トラフィックを廃棄する上限となる、キュー容量の割合です。
- *Type of Service（ToS; サービス タイプ）*は、IPv4 ヘッダーに含まれる 1 バイトのフィールドであり、パケットに適用されるプライオリティ値の指定に使用されます。ToS フィールドは 8 ビットで構成されます。最初の 3 ビットは IP precedence 値を指定します。これは 0 ～ 7 の値であり、0 は最小のプライオリティ、7 は最大のプライオリティを示します。ToS フィールドは、DSCP 値の指定にも使用されます。DSCP は、ToS の最上位 6 ビットによって定義されます。DSCP 値は 0 ～ 63 の範囲で指定できます。
- *重み値* — キューに割り当てられる帯域幅の割合です。