CatOS ソフトウェアが稼働する Catalyst 6500/6000 シリーズ スイッチの QoS の分類とマーキング

目次

概要

この文書では、パケットが Catalyst 6000 シャーシ内のさまざまな場所を移動する際に、パケットのマーキングや分類にどのような変化が生じるかを詳細に説明します。 特別なケースや制限についても説明し、簡単なケース スタディも紹介します。

この資料は Quality of Service（QoS）またはマーキングに関するすべての Catalyst OS（CatOS）コマンドの網羅的なリストであるように意図されていません。 CatOS Command Line

Interface（CLI）に関する詳細については、次に挙げるドキュメントを参照して下さい:

- QoS の設定

注: この文書では、IP トラフィックのみを考慮しています。

はじめに

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

前提条件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この資料は CatOS ソフトウェアが稼働している、および次のスーパバイザ エンジンの 1 つを使用する Catalyst 6000 ファミリ スイッチのために有効です:

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2 + PFC2
- SUP2 + PFC2 + MSFC2

ただし、すべてのサンプル コマンドは、sup1A/PFC を搭載した、ソフトウェア バージョン 6.3 を実行する Catalyst 6506 で動作確認しています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

用語

この文書で使用される用語は次のとおりです。

- Differentiated Services Code Point（DSCP）： IP ヘッダー内の Type of Service（ToS; サービス タイプ）バイトの最初の 6 ビット。 DSCP があるのは IP パケットだけです。**注:** すべてのパケット（IP または非 IP）には内部 DSCP も割り当てられます。この内部 DSCP の割り当てについては、この文書で後ほど詳細に説明します。
- IP 優先順位： IP ヘッダー内の ToS バイトの最初の 3 ビット。
- Class of Service (CoS; サービス クラス)： レイヤ 2（L2）でパケットをマークするために使用できる唯一のフィールド。 次の 3 ビットのいずれかを含んでいます。IEEE dot1q パケットの dot1q タグの 3 つの dot1p ビット。ISL カプセル化パケットの Inter-Switch Link（ISL）ヘッダー内の「ユーザ フィールド」と呼ばれる 3 ビット。非 dot1q パケットまたは ISL パケット内には CoS がない。
- 分類： マークするトラフィックの選択に使用するプロセス。

- マーキング： レイヤ 3 (L3) DSCP 値をパケット内に設定するプロセス。 この文書では、マーキングの定義を拡張して L2 の CoS 値の設定もマーキングに含めています。

Catalyst 6000 ファミリ スイッチでは、次の 3 つのパラメータに基づいた分類を行うことができます。

- DSCP
- IP precedence
- CoS

Catalyst 6000 ファミリ スイッチでは、さまざまな場所で分類とマーキングを行っています。 次の 3 つの異なる場所でどのように行われているかを説明します。

- 入力ポート（ 入力 Application-Specific Integrated Circuit（ ASIC; 特定用途向け集積回路 ））
- スイッチング エンジン（ Policy Feature Card（ PFC; ポリシー フィーチャ カード ））
- 出力ポート（ 出力 ASIC ）

QoS の有効化

デフォルトで、QoS は Catalyst 6000 スイッチでディセーブルにされます。 QoS は CatOS コマンド **set qos enable** の発行によって有効に することができます。

QoS がディセーブルにされるとき分類がありませんまたはそしてそれ自体スイッチによってされるマーキングは持っていた DSCP/IP 優位を各パケット スイッチに残しますスイッチに入るとき。

入力ポートにおける処理

入力ポートにおける分類に関する主な設定パラメータは、ポートの信頼状態です。 システムの各ポートには、次の信頼状態のうちの 1 つを設定できます。

- trust-ip-precedence
- trust-dscp
- trust-cos
- untrusted

この項の残りの部分では、ポートの信頼状態がパケットの最終分類にどのように影響するかを説明します。 ポートの信頼状態は、次の CatOS コマンドで設定または変更できます。

set port qos mod/port trust {信頼できない | trust-cos | trust-ipprec | trust-dscp}

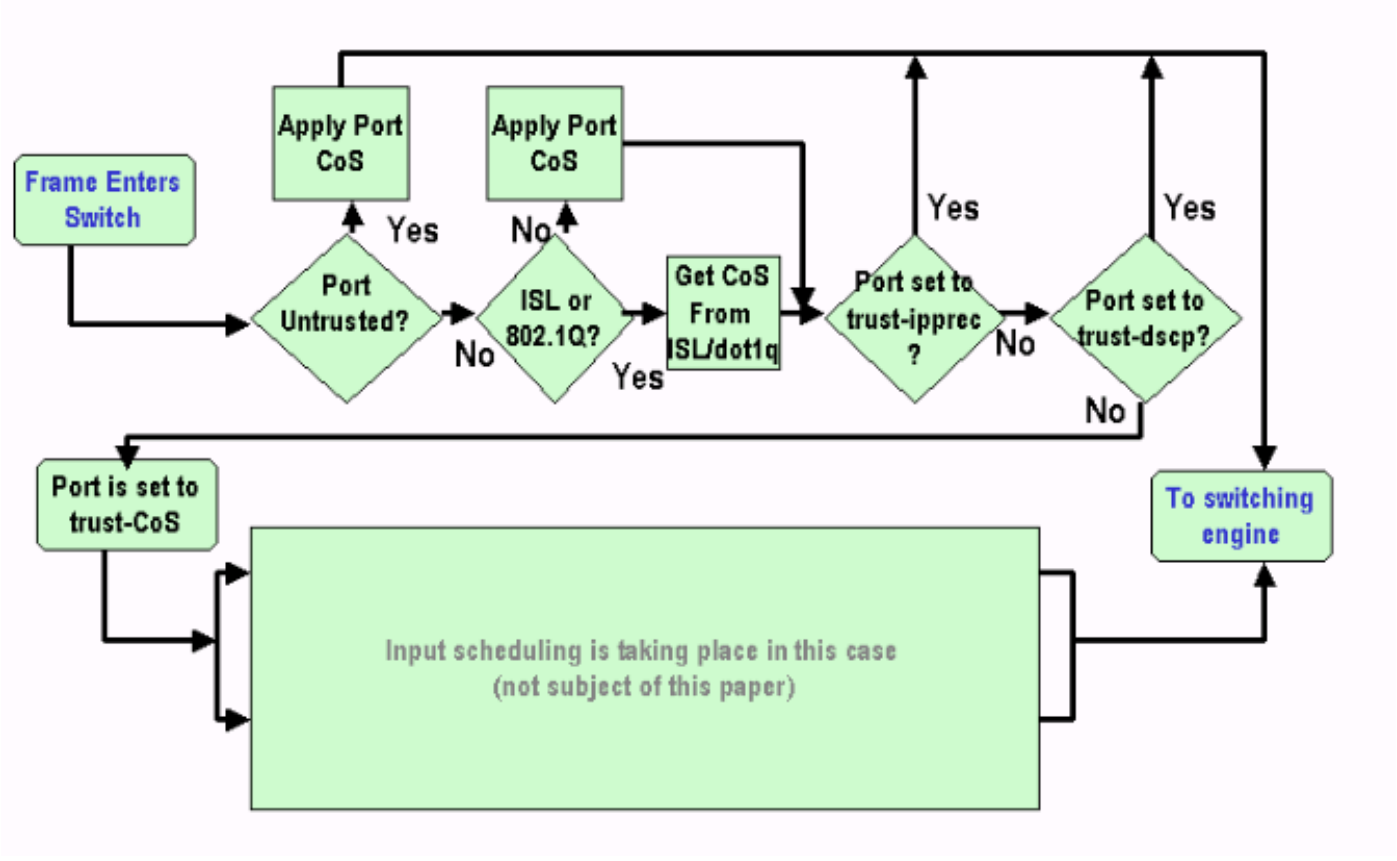
注: デフォルトでは、QoS が有効になった時点では、すべてのポートが untrusted 状態になっています。

次の例に示すように、入力ポートレベルで、ポートごとにデフォルトの CoS を適用することもできます。

set port qos mod/port cos cos-value

ポートが untrusted 状態に設定されている場合は、フレームは単にポートのデフォルト CoS でマークされ、そのヘッダーがスイッチング エンジン（ PFC ）に渡されます。 ポートが trust 状態のいずれかでマークされている場合、（ フレームが受信した CoS（ dot1q または ISL ）を保持して

いない場合は）ポートのデフォルト CoS でマークするか、、あるようにまたは CoS を（dot1q および ISL 帯のために）保存して下さいおよびスイッチング エンジンにフレームを渡して下さい。 入力分類を図示すると次のフローチャートのようになります。



注: 上のフローチャートに示されているとおり、意味のある CoS を持たないタグなしフレームを含めた各フレームには、内部 CoS（受信した CoS または デフォルトのポート CoS のいずれか）が割り当てられます。 この内部 CoS と受信した DSCP が（データ バス ヘッダーと呼ばれる）特別なパケット ヘッダーに書き込まれ、データ バスを通ってスイッチング エンジンに送信されます。 これは入力 ラインカードで起こり、この内部 CoS が egresss ASIC に運ばれ、発信 フレームで挿入されるかどうかこの時点でまだ知られていません。 このすべては PFC が次の セクションにし、更に説明があることをによって決まります。

スイッチング エンジン（PFC）

ヘッダーがスイッチング エンジンに到達すると、そのスイッチング エンジンの Encoded Address Recognition Logic (EARL) によって各フレームに内部 DSCP が割り当てられます。 この内部 DSCP は、PFC がスイッチを通過する際にフレームに割り当てる内部優先順位になります。 これは、IPv4 ヘッダーの DSCP ではありません。 この内部 DSCP は、既存の CoS または ToS の設定から取得され、フレームがスイッチを出る際に CoS または ToS をリセットするために使われます。 この内部 DSCP は、IP 以外のフレームも含む、PFC によってスイッチング（またはルーティング）されるすべてのフレームに割り当てられます。

内部 DSCP に使用される可能性のある 4 つのソース

内部 DSCP は次の 1 つから取得されます。

1. フレームがスイッチに入る前に設定された既存の DSCP 値。
2. IPv4 ヘッダーにすでに設定されている、受信した IP 優先順位ビット。 64 の DSCP 値にし

て、IP 優先順位の値は 8 個しかないので、スイッチが DSCP を取得するためのマッピングは管理者が設定します。 管理者がマップを設定しない場合は、デフォルト マッピングが使用されます。
3. フレームがスイッチに入る前にすでに設定されている受信 CoS ビットか、着信フレームに CoS がない場合は、着信ポートのデフォルト CoS から取得します。 IP precedence の場合と同様に、最大 8 種類の CoS 値があるので、それぞれを 64 種類の DSCP 値のいずれかにマッピングする必要があります。 このマップは設定可能ですが、スイッチは、設定済みのデフォルト マップも使用できます。
4. DSCP は、通常 Access Control List (ACL; アクセス コントロール リスト) エントリで設定される DSCP のデフォルト値を使用してフレームに設定できます。

上のリストの NOS 2 と NOS 3 については、次の静的マッピングの使用がデフォルトとなっています。

- CoS から DSCP へのマッピングの場合、取得した DSCP は CoS の 8 倍と等価。
- IP 優先順位から DSCP へのマッピングの場合、取得した DSCP は IP 優先順位の 8 倍と等価。

ユーザは次のコマンドを発行してこの静的マッピングを上書きできます。

QoS ipprec-dscp-map <dscp1> <dscp2>...<dscp8> **を設定 して下さい**

QoS cos-dscp-map <dscp1> <dscp2>...<dscp8> **を設定 して下さい**

CoS (または IP 優先順位) へのマッピングに対応する DSCP の最初の値は「0」です。2 番目の値は「1」で、そのパターンに従って順次、値が設定されます。

内部 DSCP に 4 つの可能なソースのどれが使用されるか

この項では、各パケットに上記の 4 つの発信元のうちどれを使用するかを決定する規則について説明します。 決定は次のパラメータに基づいて行われます。

1. どの QoS ACL がパケットに適用されるのか。 これは次の規則で決定されます。**注:** 各パケットは ACL エントリを通過します。着信ポートまたは VLAN に ACL が接続されていない場合は、デフォルト ACL を適用します。着信ポートまたは VLAN に ACL が接続されており、トラフィックが ACL 内のエントリの 1 つに合致する場合は、そのエントリを使用します。着信ポートまたは VLAN に ACL が接続されているが、トラフィックが ACL 内のエントリに合致しない場合は、デフォルト エントリを使用します。
2. 各エントリには分類キーワードが含まれています。 指定可能なキーワードのリストとその説明は次のとおりです。trust-ipprec： 内部 DSCP は、ポートの信頼状態に関わりなく、受信した IP 優先順位から静的マッピングに従って取得される。trust-dscp： 内部 DSCP は、ポートの信頼状態に関わりなく、受信した DSCP から取得される。trust-cos： 内部 DSCP は、ポートの信頼状態が trusted (trust-cos、trust-dscp、trust-ipprec) の場合に、受信した CoS から静的マッピングに従って取得される。 ポートの信頼状態が trust-xx の場合、DSCP はポートのデフォルト CoS から同じ静的マッピングに従って取得されます。dscp xx： 内部 DSCP は次に示す着信ポートの信頼状態によって決定されます。ポートが untrusted の場合、内部 DSCP は xx に設定されます。ポートが trust-dscp の場合、内部 DSCP は着信パケットで受信した DSCP となります。ポートが trust-CoS の場合、内部 DSCP は着信パケットの CoS から取得されます。ポートが trust-ipprec の場合、内部 DSCP は着信パケットの IP 優先順位から取得されます。
3. 各 QoS ACL はポートまたは VLAN に適用することができますが考慮に入れるべき追加コン

フィギュレーションパラメータがあります; ポートは、VLAN ベースまたはポート ベースのいずれかに設定できます。 それら 2 つの設定タイプについて次に説明します。VLAN ベースに設定されたポートは、ポートが属する VLAN に適用された ACL のみを参照します。 ポートに接続された ACL がある場合、その ACL はそのポートに着信するパケットに対しては無視されます。VLAN に属するポートがポート ベースに設定されている場合、その VLAN に接続された ACL がある場合でも、そのポートから着信するトラフィックに対しては影響しません。

IP トラフィックをマークするために、QoS ACL を作成するための構文を次に示します。

set qos acl ip acl_name [DSCP XX | trust-cos | trust-dscp | trust-ipprec] *ACL項目ルール*

次の ACL は、ホスト 1.1.1.1 宛てのすべての IP トラフィックを DSCP「40」でマークし、他のすべての IP トラフィックを trust-dscp にします。

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

ACL を作成したら、それをポートまたは VLAN にマップする必要があります。その作業は次のコマンドで行えます。

set qos acl map acl_name [モジュール/ポート | VLAN]

デフォルトでは、ACL に対する各ポートの設定はポート ベースになっています。そのため、VLAN に ACL を接続するには、この VLAN のポートを vlan-based に設定する必要があります この作業は次のコマンドを発行することにより行えます。

set port qos module/port vlan-based

次のコマンドを実行して、port-based モードに戻すこともできます。

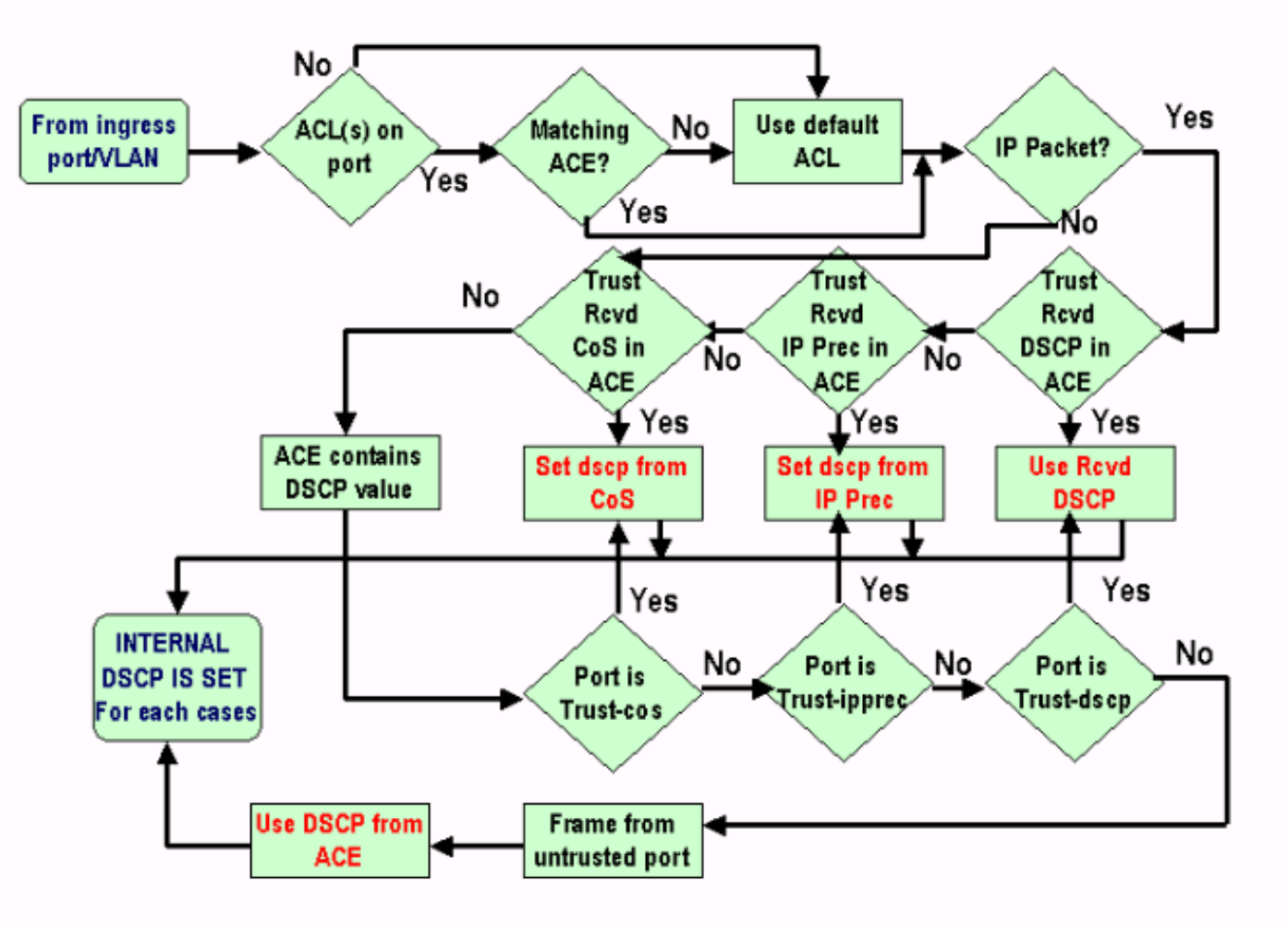
set port qos module/port port-based

要約： 内部 DSCP の選択方法

内部 DSCP の選択は次の要因によって決定されます。

- ポートの信頼状態
- ポートに接続された ACL
- デフォルト ACL
- ACL が VLAN-based か port-based か

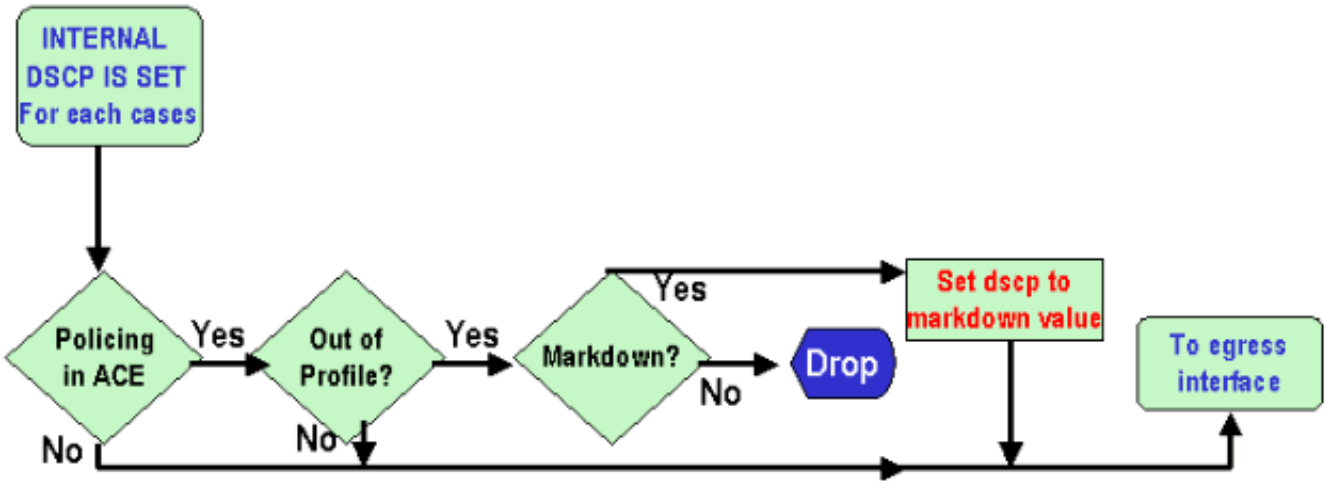
次のフローチャートで内部 DSCP の選択が、設定によってどのように選択されるかを要約します。



PFC はポリシングも行うことができます。 このことが結果的に内部 DSCP のマークダウンにつながる場合もあります。 ポリシングの詳細は、次の資料を参照してください。

- Catalyst 6000 での QoS ポリシング

次のフローチャートにポリシングがどのように適用されるかを示します。



出力ポートにおける処理

出力ポート レベルでは、分類を変更するために行えることはありません。しかし、この項では次のルールに従ってパケットをマークします。

- パケットが IPv4 パケットの場合、スイッチ エンジンが割り当てた内部 DSCP を IPv4 ヘッダーの ToS バイトにコピーします。
- 出力ポートが ISL または dot1q カプセル化用に設定されている場合、内部 DSCP から取得した CoS を使用して、ISL または dot1q フレームにコピーします。

注: CoS は内部 DSCP からユーザが次のコマンドを発行して設定した静的マッピングに従って取得されます。

注: **set qos dscp-cos-map dscp_list:** *cos_value*

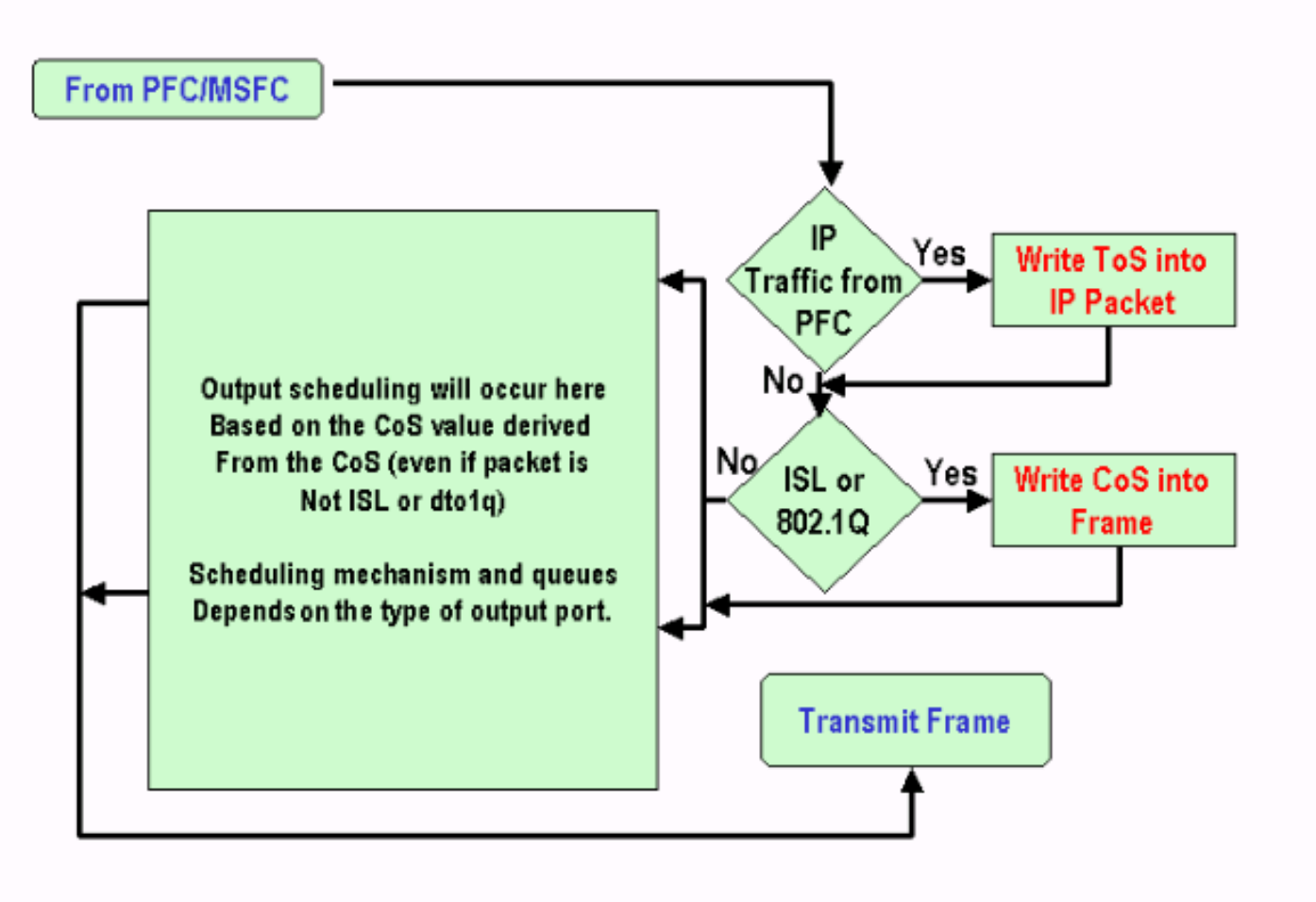
注: デフォルト設定は次のとおりです。 デフォルトでは、CoS は DSCP を 8 で割った整数部分となります。

```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

DSCP が IP ヘッダーに書き込まれ、CoS が DSCP から取得されると、パケットはいずれかの出力キューに送信され、（そのパケットが dot1q または ISL パケットでない場合も）CoS に基づいて出力スケジューリングが行われます。 出力キューのスケジューリングの詳細は、次の文書を参照してください。

- Catalyst 6000 シリーズ スイッチの QoS: CatOS ソフトウェアを使用して PFC または PFC 2 の Catalyst 6000 の出力スケジューリング

次のフローチャートでは、出力ポートでのマーキングに関するパケットの処理の概要を示します。



注意と制限

デフォルト ACL

デフォルトでは、デフォルト ACL は「dscp 0」を分類キーワードとして使用します。 そのため、untrusted のポートからスイッチに入ってくるトラフィックはすべて、QoS が有効になっている場合、「0」の DSCP でマークされます。 次のコマンドを発行すれば、IP のデフォルト ACL を確認できます。

```
Boris-1> (enable) show qos acl info default-action ip set qos acl default-action ----------
---------- ip dscp 0
```

次のコマンドを発行すれば、デフォルト ACL を変更することもできます。

set qos acl default-action ip [DSCP XX | trust-cos | trust-dscp | trust-ipprec]

ACL エントリ内の trust-cos の制限

エントリ内で trust-CoS キーワードを使用する際には、追加の制限があります。 エントリ内の CoS を信頼できるのは、受信の信頼状態が untrusted でない場合だけです。 エントリを trust-CoS で設定しようとすると、次の警告が表示されます。

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any Warning: ACL trust-CoS should only be
used with ports that are also configured with port trust=trust-CoS test_2 editbuffer modified.
Use 'commit' command to apply changes.
```

この制限は、前述の入力ポートにおける処理の項で説明したことの結果として生じます。 その項のフローチャートで示したように、ポートが untrusted の場合、フレームにはただちにポートの

デフォルト CoS が割り当てられます。 そのため、着信 CoS は維持されず、スイッチング エンジンに送信されることもありません。その結果、特定の ACL があっても CoS を信頼できなくなるのです。

WS-X6248-xx、WS-X6224-xx、WS-X6348-xx ラインカードの制限

この項では次のラインカードのみを対象としています。

- WS-X6224-100FX-MT： CATALYST 6000 24 PORT 100 FX MULTIMODE
- WS-X6248-RJ-45： CATALYST 6000 48-PORT 10/100 RJ-45 MODULE
- WS-X6248-TEL： CATALYST 6000 48-PORT 10/100 TELCO MODULE
- WS-X6248A-RJ-45： CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6248A-TEL： CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6324-100FX-MM： CATALYST 6000 24-PORT 100FX, ENH QOS, MT
- WS-X6324-100FX-SM： CATALYST 6000 24-PORT 100FX, ENH QOS, MT
- WS-X6348-RJ-45： CATALYST 6000 48-PORT 10/100, ENHANCED QO
- WS-X6348-RJ21V： CATALYST 6000 48-PORT 10/100, INLINE POWER
- WS-X6348-RJ45V： CATALYST 6000 48-PORT 10/100, ENH QOS, INLI NE POWER

ただし、これらのラインカードには追加の制限事項があります。

- ポート レベルで、trust-dscp または trust-ipprec を指定できない。
- ポート レベルで、ポートの信頼状態が trust-CoS の場合、次の条件が適用される。入力スケジューリングの受信しきい値が有効になる。 さらに、受信パケットの CoS が、バスにアクセスするパケットの優先順位決定に使用されます。そのトラフィックの ACL も trust-cos に設定しないと、CoS は内部 DSCP を取得する際に信頼されず使用されない。 さらに、ラインカードがポートを trust-cos にするだけでは不十分で、トラフィックの ACL も trust-cos になっている必要があります。
- ポートの信頼状態が untrusted の場合、（標準ケースと同様に）通常のマーキングが行われる。 これは、トラフィックに適用される ACL に依存しています。

これらのポートのいずれかで信頼状態を設定しようとすると、次の警告メッセージが表示されます。

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

分類の要約

次の表に、次の要因によって分類された後の DSCP の状態を示します。

- 着信ポートの信頼状態。
- 適用される ACL 内の分類キーワード。

WS-X62xx および WS-X63xx以外のすべてのポートに関する要約表

ACL キーワード ポートの信頼状態	dscp xx	trust-dscp	trust-ipprec	trust-cos
Untrusted	xx (1)	Rx dscp	Rx ipprec から取得	0
trust-dscp	Rx-dscp	Rx dscp	Rx ipprec から取得	Rx CoS またはポート CoS を基に決定
trust-ipprec	Rx ipprec から取得	Rx dscp	Rx ipprec から取得	Rx CoS またはポート CoS を基に決定
trust-cos	Rx cos かポート CoS から得られる	Rx dscp	Rx ipprec から取得	Rx CoS またはポート CoS を基に決定

(1) これがフレームに新しくマーキングする唯一の方法です。

WS-X62xx または WS-X63xx の要約表

ACL キーワード ポートの信頼状態	dscp xx	trust-dscp	trust-ipprec	trust-cos
Untrusted	xx	Rx dscp	Rx ipprec から取得	0
trust-dscp	非サポート	非サポート	非サポート	非サポート
trust-ipprec	非サポート	非サポート	非サポート	非サポート
trust-cos	xx	Rx dscp	Rx ipprec から取得	Rx CoS かポート CoS（2）から得られる

(2) これが、62xx または 63xx ラインカードからのトラフィックの着信 CoS を維持する唯一の方法です。

設定の監視と確認

ポート設定のチェック

次のコマンドを発行して、ポートの設定と構成を確認できます。

show port qos *モジュール/ポート*

このコマンドを使用すると、他のパラメータとともに次の分類パラメータの確認ができます。

- ポートベースもしくは VLAN ベース
- 信頼ポートのタイプ
- ポートに接続された ACL

次に分類に関連する重要なフィールドを強調した、このコマンドの出力例を示します。

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------ -------------
 1/1    port-based     port-based COPS local Port TxPort Type RxPort Type Trust Type Trust Type
Def CoS Def CoS config runtime config runtime ----- ------------ ------------ ------------ -----
-------- ------- ------- 1/1 1p2q2t 1p1q4t untrusted untrusted 0 0 (*)Runtime trust type set to
untrusted. Config: Port ACL name Type ----- ------------------------------ ---- 1/1 test_2 IP
Runtime: Port ACL name Type ----- ------------------------------ ---- 1/1 test_2 IP
```

注: 各フィールドには、設定されたパラメータとランタイム パラメータがあります。 パケットに適用されるのはランタイム パラメータです。

ACL のチェック

次のコマンドを発行することにより、前述のコマンドで適用され、表示された ACL をチェックできます。

show qos ACL ヒント ランタイム *acl_name*

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
---------------------------------------------
1. dscp 32 ip any host 1.1.1.1 2. trust-dscp any
```

ケース スタディ

ネットワークで一般的に使用される設定例を次に示します。

ケース 1： エッジでのマーキング

Catalyst 6000 を、WS-X6348 ラインカード（10/100M）のスロット 2 に多数のユーザが接続しているアクセス スイッチとして使用するように設定すると仮定します。 ユーザは次のトラフィックを送信できます。

- 通常のデータ トラフィック： これは常に VLAN 100 を使用しており、「0」の DSCP を獲得する必要がある。
- IP 電話からの音声トラフィック： これは常に音声補助 VLAN 101 を使用しており、「40」の DSCP を獲得する必要がある。

- ミッション クリティカルなアプリケーション トラフィック： これも VLAN 100 を使用しており、宛て先はサーバ 10.10.10.20 になっている。 このトラフィックは「32」の DSCP を獲得する必要がある。

トラフィックはいずれもアプリケーションでマークされることはありません。そのため、ポートは untrusted のままにしておき、トラフィックを分類するために特定の ACL を設定します。 1 ACL は VLAN 100 に適用され、1 ACL は VLAN 101 に適用されます。 また、すべてのポートを VLAN ベースに設定する必要があります。 次に、そのように設定した例を示します。

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

ケース 2： ギガビット インターフェイスだけのコアを信頼する

スロット 1 とスロット 2 にギガビット インターフェイスのみを持つ（62xx または 63xxラインカードがシャーシ内にない）コア Catalyst 6000 を設定しようとしていると仮定します。 トラフィックはアクセス スイッチにより、事前に正しくマーキングされています。そのため、再度マーキングする必要はありませんが、必ず着信 DSCP を信頼する設定にする必要があります。 これは、すべてのポートを trust-dscp にマークするだけで十分なので、最も簡単なケースです。

```
set qos enable
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

ケース 3： シャーシ内に 62xx または 63xx ポートを持つコアを信頼する

WS-X6416-GBIC ラインカード（スロット 2）にギガビット リンクを持ち、WS-X6348 ラインカード（スロット 3）に 10/100 リンクを持つ、コア/ディストリビューション デバイスを設定しようとしていると仮定します。 すべての着信トラフィックは、アクセス スイッチ レベルですでにマークされているので信頼する必要があります。 6348 ラインカードには trust-dscp を設定できないので、この場合の最も簡単な方法は、すべてのポートを untrusted のままにしておき、次の例のようにデフォルト ACL を trust-dscp に変更することです。

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
set qos acl default-action ip trust-dscp
```

関連情報

- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカルサポート - Cisco Systems