Cisco IOS ソフトウェアが稼働する Catalyst 6500/6000 シリーズ スイッチの QoS 分類およびマーキング

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[用語](#)
[入力ポートにおける処理](#)
[スイッチング エンジン（PFC）](#)
[12.1(12c)E 以降の Cisco IOS ソフトウェアでパケットを分類、またはマーキングするためのサービス ポリシーの設定](#)
[12.1(12c)E 以前の Cisco IOS ソフトウェアでパケットを分類、またはマーキングするためのサービス ポリシーの設定](#)
[内部 DSCP に使用される可能性のある 4 つのソース](#)
[内部 DSCP が選択される仕組み](#)
[出力ポートにおける処理](#)
[注意と制限](#)
[デフォルト ACL](#)
[WS-X61xx、WS-X6248-xx、WS-X6224-xx および WS-X6348-xx ラインカードの制限](#)
[Supervisor Engine 1A/PFC の MSFC1 または MSFC2 から送信されるパケット](#)
[分類の要約](#)
[設定の監視と検証](#)
[ポート設定の確認](#)
[定義クラスの確認](#)
[インターフェイスに適用されているポリシー マップの確認](#)
[ケース スタディ](#)
[ケース 1： エッジでのマーキング](#)
[ケース 2： ギガビット イーサネット インターフェイスのみを搭載したコアでの信頼設定](#)
[関連情報](#)

概要

このドキュメントでは、Cisco IOS® ソフトウェアが稼働する Cisco Catalyst 6500/6000 シャーシ内のさまざまな段階でのパケットのマーキングや分類がどのようになるかを調べます。 このドキュメントでは、特殊な状況や制約事項について説明し、簡単な事例を紹介します。

QoS やマーキングに関連する Cisco IOS ソフトウェアのコマンドをすべてまとめたリストは、このドキュメントには掲載されていません。 Cisco IOS ソフトウェア コマンドライン インターフェイス (CLI) の詳細については、『PFC QoS の設定』を参照してください。

前提条件

要件

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

このドキュメントの情報は、次のハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェアが稼働し、次の Supervisor Engine のいずれかを使用している Catalyst 6500/6000 シリーズ スイッチポリシー フィーチャ カード (PFC) とマルチレイヤ スイッチ フィーチャ カード (MSFC) を搭載した Supervisor Engine 1APFC と MSFC2 を搭載した Supervisor Engine 1APFC2 と MSFC2 を搭載した Supervisor Engine 2

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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

用語

次のリストは、このドキュメントで使用する用語をまとめたものです。

- DiffServ Code Poin t （ DSCP ）：IP ヘッダー内のタイプ オブ サービス (ToS) バイトの上位 6 ビット。 DSCP があるのは IP パケットだけです。**注:** このスイッチは、IP か IP 以外かにかかわらず、すべてのパケットに内部 DSCP を割り当てます。 内部 DSCP の割り当てについては、このドキュメントの「内部 DSCP に使用される可能性のある 4 つのソース」セクションで説明しています。
- IP precedence：IP ヘッダー内の ToS バイトの上位 3 ビット。
- Class of Service (CoS) ：レイヤ 2 (L2) でパケットをマーキングするために使用できる唯一のフィールド。 CoS は次のいずれかの 3 ビットで構成されます。dot1q パケット用に用意された IEEE 802.1Q (dot1q) タグ内の 3 つの IEEE 802.1p (dot1p) ビット**注:** デフォルトでは、シスコのスイッチはネイティブ VLAN パケットにタグ付けしません。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。**注:** 非 dot1q パケットまたは ISL パケット内には CoS がありません。
- 分類：マーキングの対象となるトラフィックを選択するためのプロセス。
- マーキング：パケットにレイヤ 3 (L3) DSCP 値を設定するプロセス。 このドキュメントでは、マーキングの定義に L2 CoS 値の設定を含めています。

Catalyst 6500/6000 シリーズ スイッチは、次の 3 つのパラメータをベースにして分類を行います。

- DSCP
- IP precedence
- CoS

Catalyst 6500/6000 シリーズ スイッチは、さまざまなステージで分類とマーキングを実行します。 これは、次のような複数の場所で発生します。

- 入力ポート（入力 ASIC）
- スイッチング エンジン（PFC）
- 出力ポート（出力 ASIC）

入力ポートにおける処理

分類に関連して、ingress ポートで重要とされる設定パラメータは、ポートの trust 状態です。 システムの各ポートには、次の trust 状態のいずれかを指定できます。

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

ポートの trust 状態を設定または変更する場合は、インターフェイス モードでこの Cisco IOS ソフトウェア コマンドを発行します。

```
6k(config-if)#mls qos trust ?
  cos            cos keyword
  dscp           dscp keyword
  ip-precedence  ip-precedence keyword
  <cr>
```

注: QoS を有効にした場合、デフォルトでは、すべてのポートが untrusted 状態になります。 Cisco IOS ソフトウェアを実行する Catalyst 6500 で QoS を有効にするには、メインの設定モードで **mls qos** コマンドを発行します。

入力ポート レベルで、ポートごとにデフォルト CoS を適用することもできます。 次に例を示します。

```
6k(config-if)#mls qos cos cos-value
```

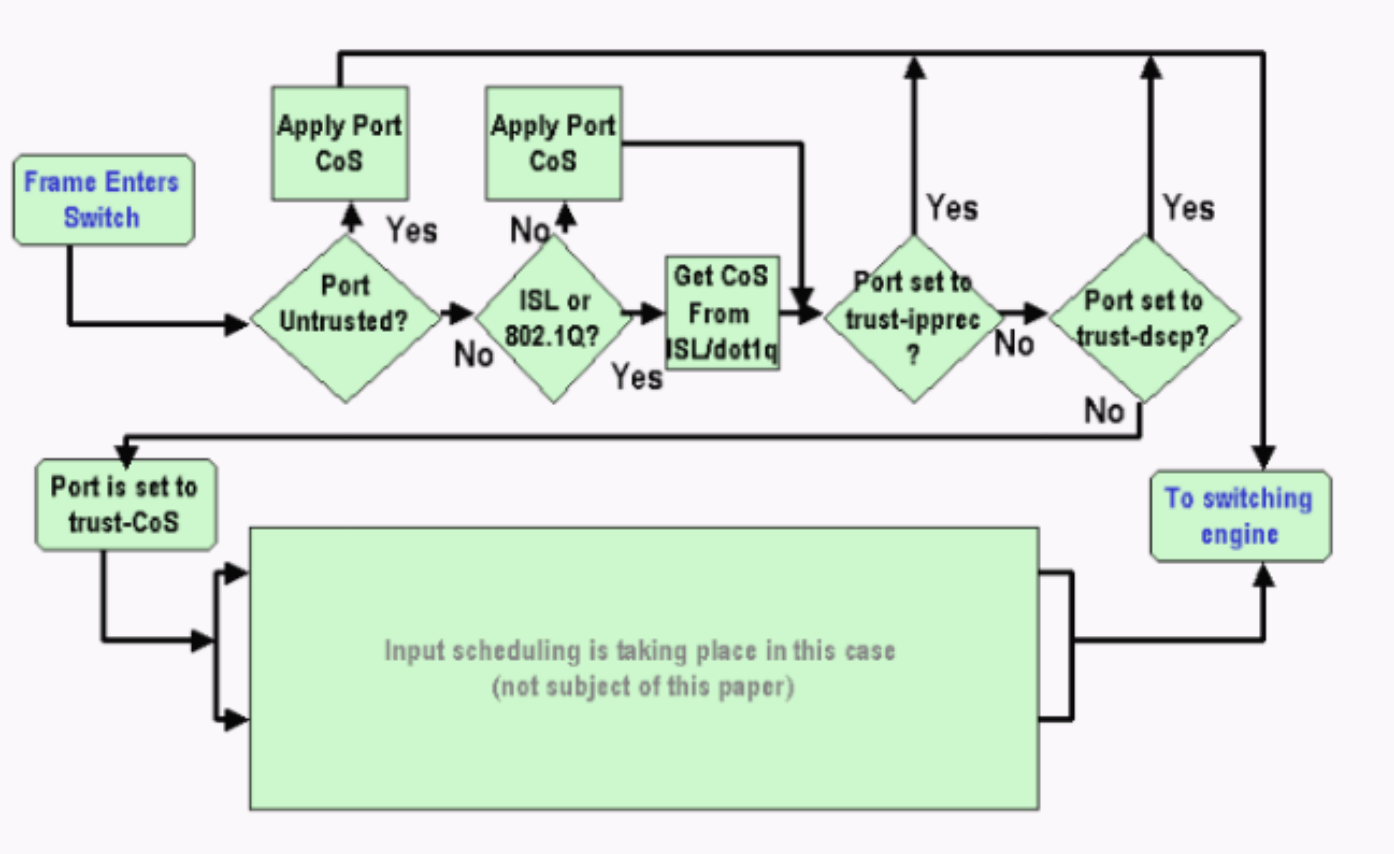
このデフォルト CoS は、IP や Internetwork Packet Exchange（IPX）など、すべてのパケットに適用できます。 デフォルト CoS はどの物理ポートにも適用できます。

ポートが untrusted 状態の場合、ポートのデフォルト CoS でフレームをマーキングし、このヘッダーをスイッチング エンジン（PFC）に渡します。 ポートがいずれかの trust 状態に設定されている場合は、次の 2 つの手順のいずれかを実行します。

- フレームに受信 CoS（dot1q または ISL）がない場合は、デフォルトのポート CoS を適用します。
- dot1q フレームおよび ISL フレームでは、CoS をそのままの状態に維持します。

次に、スイッチング エンジンにフレームを渡します。

次の例は、入力の分類とマーキングを示したものです。 内部 CoS を各フレームに割り当てる仕組みが示されています。



注: この例が示すように、各フレームは内部 CoS に割り当てられます。 割り当ては、受信 CoS またはデフォルトのポート CoS のいずれかに基づいて決定されます。 内部 CoS には、実際の CoS を伝送しないタグなしフレームも含まれます。 内部 CoS は特殊なパケット ヘッダー (データ バス ヘッダーと呼ばれる) に書き込まれ、データ バスを通じてスイッチング エンジンに送信されます。

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、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、フレームがスイッチを通過する際に PFC によって割り当てられる内部優先順位です。 これは、IP version 4 (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、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、IP 以外のフレームも含まれます。

このセクションでは、サービス ポリシーをインターフェイスに割り当ててマーキングを行う方法について説明します。 また、内部 DSCP の最終設定についても説明しますが、これはポートの trust 状態と、適用されているサービス ポリシーによって異なります。

12.1(12c)E 以降の Cisco IOS ソフトウェアでパケットを分類、またはマーキングするためのサービス ポリシーの設定

サービス ポリシーを設定するには、次の手順を実行します。

1. 検討対象のトラフィックを定義できるように、アクセス コントロール リスト (ACL) を設定します。ACL には番号や名前を付けることができます。また、Catalyst 6500/6000 では拡張 ACL もサポートされています。 次の例のように、**access-list xxx** Cisco IOS ソフトウェ

ア コマンドを発行します。(config)#**access-list 101 permit ip any host 10.1.1.1**

2. トラフィック クラス (クラス マップ) を設定し、定義済みの ACL、または受信した DSCP を基にトラフィックを照合します。**class-map** Cisco IOS ソフトウェア コマンドを発行します。 PFC QoS では、1 つのクラス マップに対して複数の match ステートメントを指定できません。 また、PFC QoS では、次の match ステートメントだけをサポートしています。**match ip access-groupmatch ip dscpmatch ip precedencematch protocol注: match protocol** コマンドでは、Network Based Application Recognition (NBAR) を使って、トラフィックを照合できます。**注:** 上記のオプションのうち、**match ip dscp** と **match ip precedence** ステートメントだけがサポート対象であり、機能します。 ただし、これらのステートメントはパケットのマーキングや分類には役立ちません。 これらのステートメントは、特定の DSCP と一致するすべてのパケットでポリシングを行う場合などに使用できます。 ただし、このドキュメントでは、このアクションについて説明しません。(config)#**class-map** *class-name*
(config-cmap)#**match {access-group | input-interface | ip dscp}** **注:** この例では、**match** コマンドの 3 つのオプションだけを示しています。 ただし、このコマンド プロンプトでは、もっと多くのオプションを設定できます。**注:** 着信パケットによっては、この **match** コマンドのオプションのいずれかが照合基準となり、他のオプションは省略されます。次に例を示します。

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. ポリシー マップを設定し、すでに定義してあるクラスにポリシーを適用します。ポリシー マップには次の要素が含まれます。名前class ステートメントのセット各 class ステートメントごとに、そのクラスに対して実行する必要があるアクションPFC1 および PFC2 の QoS でサポートされているアクションは次のとおりです。**trust dscptrust ip precedencetrust cosset ip dscp** (Cisco IOS ソフトウェア リリース 12.1(12c)E1 以降) **set ip precedence** (Cisco IOS ソフトウェア リリース 12.1(12c)E1 以降) **police注:** このドキュメントでは、このアクションについて説明しません。(config)#**policy-map** *policy-name*
(config-pmap)#**class** *class-name*
(config-pmap-c)#**{police | set ip dscp}**
注: この例では 2 つのオプションのみを示していますが、この (config-pmap-c)# コマンド プロンプトでは、もっと多くのオプションを設定できます。次に例を示します。

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   set ip dscp 16
```

4. service-policy input を設定し、すでに定義してあるポリシー マップを 1 つ以上のインターフェイスに適用します。**注:** 物理インターフェイス、スイッチ仮想インターフェイス (SVI)、VLAN インターフェイスのいずれかにサービス ポリシーを割り当てることができます。 VLAN インターフェイスにサービス ポリシーを割り当てた場合、そのサービス ポリシーを使用するのは、該当する VLAN に属し、VLAN ベースの QoS 用に設定されたポートだけです。 ポートが VLAN ベースの QoS 用に設定されていない場合、このポートはデフォルトのポート ベースの QoS を使い続け、物理インターフェイスに割り当てられたサービス ポリシーだけを参照します。次の例では、サービス ポリシー test_policy をポート Gigabit Ethernet 1/1 に適用しています。(config) **interface gigabitethernet 1/1**
(config-if)#**service-policy input test_policy**
次の例では、サービス ポリシー test_policy を QoS 側から見て VLAN ベースの設定を持つ VLAN 10 のすべてのポートに適用しています。(config) **interface gigabitethernet 1/2**

```
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

注: クラスの特定の定義を省略し、ポリシー マップの定義に ACL を直接割り当てる場合は、手順 2 と手順 3 を組み合わせることができます。 この例では、TEST police クラスがポリシー マップの設定前に定義されていなかった場合に、ポリシー マップ内にクラスを定義します。`(config)#policy-map` *policy-name*

```
(config-pmap)#class class_name {access-group acl_index_or_name | dscp dscp_1 [dscp_2
[dscp_N]] | precedence ipp_1 [ipp_2 [ipp_N]]}
!--- Note: This command should be on one line.

policy-map TEST
class TEST police access-group 101
```

12.1(12c)E 以前の Cisco IOS ソフトウェアでパケットを分類、またはマーキングするためのサービス ポリシーの設定

12.1(12c)E 以前の Cisco IOS ソフトウェアでは、**set ip dscp** や **set ip precedence** アクションをポリシー マップで使用できません。 そのため、クラスが定義する特定のトラフィックをマーキングするには、非常に高いレートのポリサーを設定しなければなりません。 このレートは、少なくともポートの回線レートか、すべてのトラフィックがポリサーにヒットできる高いレートにする必要があります。 そして、conform-action として **set-dscp-transmit xx** を使用します。 この設定を実装するには、次の手順に従います。

1. ACL を設定し、検討対象のトラフィックを定義します。ACL には番号や名前を付けることができます。また、Catalyst 6500/6000 では拡張 ACL もサポートされています。 次の例のように、**access-list xxx** Cisco IOS ソフトウェア コマンドを発行します。`(config)#access-list 101 permit ip any host 10.1.1.1`
2. トラフィック クラス (クラス マップ) を設定し、定義済みの ACL、または受信した DSCP を基にトラフィックを照合します。**class-map** Cisco IOS ソフトウェア コマンドを発行します。 PFC QoS では、1 つのクラス マップに対して複数の match ステートメントを指定できません。 また、PFC QoS では、次の match ステートメントだけをサポートしています。 **match ip access-groupmatch ip dscpmatch ip precedencematch protocol注: match protocol** コマンドでは、NBAR を使ってトラフィックを照合できます。**注:** 上記のステートメントのうち、**match ip dscp** と **match ip precedence** ステートメントだけがサポート対象であり、機能します。 ただし、これらのステートメントはパケットのマーキングや分類には役立ちません。 これらのステートメントは、特定の DSCP と一致するすべてのパケットでポリシングを行う場合などに使用できます。 ただし、このドキュメントでは、このアクションについて説明しません。`(config)#class-map` *class-name*

   ```
   (config-cmap)#match {access-group | input-interface | ip dscp}
   ```

   注: この例では、**match** コマンドの 3 つのオプションだけを示しています。 ただし、このコマンド プロンプトでは、もっと多くのオプションを設定できます。次に例を示します。

   ```
   class-map match-any TEST
    match access-group 101

   class-map match-all TEST2
    match ip precedence 6
   ```
3. ポリシー マップを設定し、すでに定義してあるクラスにポリシーを適用します。ポリシー マップには次の要素が含まれます。名前class ステートメントのセット各 class ステートメントごとに、そのクラスに対して実行する必要があるアクションPFC1 あるいは PFC2 の

QoS でサポートされているアクションは次のとおりです。**trust dscptrust ip precedencetrust cospoliceset ip dscp** および **set ip precedence** アクションはサポートされていないため、**police** ステートメントを使用する必要があります。 トラフィックを実際にポリシングするのではなく、ただマーキングするだけなので、すべてのトラフィックを許可するように定義されたポリサーを使用します。 そのため、大きなレート値とバースト値をポリサーに設定します。 たとえば、許容されている最大のレート値とバースト値を設定できます。 次に例を示します。

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   police  4000000000 31250000 conform-action
   set-dscp-transmit 16 exceed-action policed-dscp-transmit
```

4. service-policy input を設定し、すでに定義してあるポリシー マップを 1 つ以上のインターフェイスに適用します。**注:** サービス ポリシーは、物理インターフェイス、SVI、または VLAN インターフェイスのいずれかに割り当てることができます。 VLAN インターフェイスにサービス ポリシーを割り当てた場合、そのサービス ポリシーを使用するのは、該当する VLAN に属し、VLAN ベースの QoS 用に設定されたポートだけです。 ポートが VLAN ベースの QoS 用に設定されていない場合、このポートはデフォルトのポート ベースの QoS を使い続け、物理インターフェイスに割り当てられたサービス ポリシーだけを参照します。 次の例では、サービス ポリシー test_policy をポート Gigabit Ethernet 1/1 に適用しています。

```
(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
```

次の例では、サービス ポリシー test_policy を QoS 側から見て VLAN ベースの設定を持つ VLAN 10 のすべてのポートに適用しています。

```
(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

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、次のいずれかから取得されます。

1. フレームがスイッチに入る前に設定されていた、既存の受信済み DSCP 値たとえば、**trust dscp** です。
2. IPv4 ヘッダーにすでに設定されていた、受信済み IP precedence ビットDSCP 値は 64 種類、IP precedence 値は 8 種類あるため、スイッチが DSCP を取得するためのマッピングを設定します。 管理者がマッピングを設定していない場合は、デフォルトのマッピングが使用されます。 たとえば、**trust ip precedence** です。
3. フレームがスイッチに入る前に設定済みで、データ バス ヘッダーに保存された受信 CoS ビット、または着信ポートのデフォルト CoS からの受信 CoS ビット (着信フレームに CoS がない場合) 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。 このマッピングは管理者が設定できます。また、スイッチでは、すでにあるデフォルトのマップを使うこともできます。
4. サービス ポリシーでは、内部 DSCP を特定の値に設定できます。

このリストの 2 番と 3 番では、スタティックなマッピングがデフォルトです。

- CoS-to-DSCP マッピングでは、取得される DSCP は 8 倍の CoS に相当します。
- IP precedence-to-DSCP マッピングでは、取得される DSCP は 8 倍の IP precedence に相当します。

スタティックなマッピングをオーバーライドして検証するには、次のコマンドを発行します。

- **mls qos map ip-prec-dscp dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8**
- **mls qos map cos-dscp dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8**

CoS（または IP precedence）のマッピングに対応する DSCP の最初の値は 0 です。 CoS（または IP precedence）の 2 番目の値は 1 です。パターンはこのように続きます。 たとえば、次のコマンドによって、CoS 0 が 0 の DSCP にマップされ、1 の CoS が 8 の DSCP にマップされるようにマッピングが変更されます。

```
Cat65(config)#mls qos map cos-dscp 0 8 16 26 32 46 48 54
Cat65#show mls qos maps
CoS-dscp map:
 cos:     0 1  2   3   4   5   6   7
  ---------------------------------
 dscp:    0 8 16  26  32  46  48  54
```

内部 DSCP が選択される仕組み

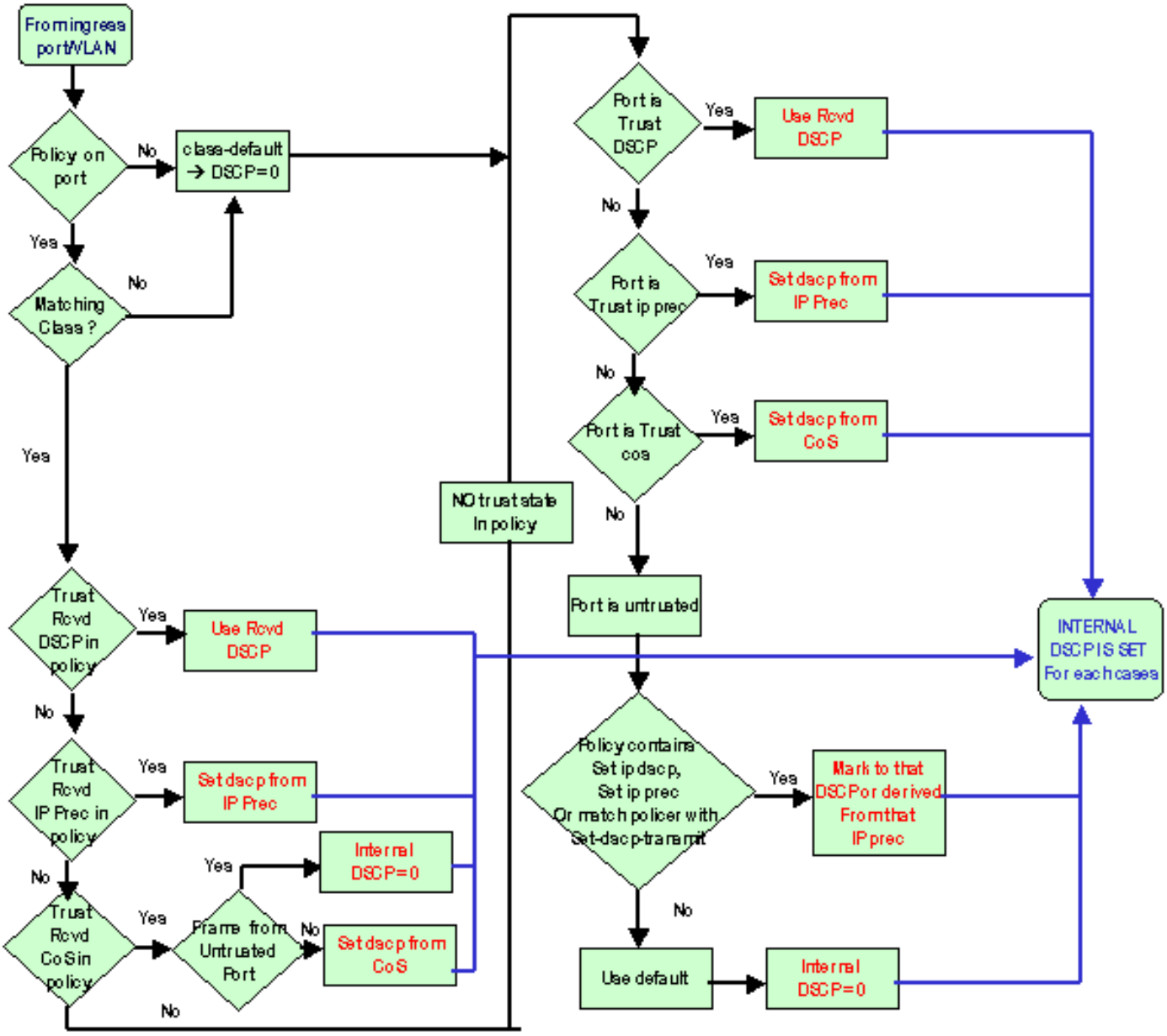
内部 DSCP は、次のパラメータに基づいて選択されます。

- パケットに適用されている QoS ポリシー マップQoS ポリシー マップは、次のルールで決定されます。着信ポートや VLAN にサービス ポリシーが割り当てられていない場合は、デフォルトが使用されます。**注:** このデフォルトのアクションでは、内部 DSCP が 0 に設定されます。着信ポートや VLAN にサービス ポリシーが割り当てられていて、ポリシーが定義するクラスのいずれかにトラフィックが一致する場合は、このエントリが使用されます。着信ポートや VLAN にサービス ポリシーが割り当てられておらず、ポリシーが定義するクラスのいずれかにトラフィックが一致しない場合は、デフォルトが使用されます。
- ポートの trust 状態とポリシー マップのアクションポートが特定の trust 状態で、特定のマーキングを持つポリシーが設定されている場合（同時にアクションを信頼する場合）は、次のルールが適用されます。ポートが untrusted 状態のままの場合、適用されるのは **set ip dscp** コマンドか、ポリシー マップでポリサーごとに定義された DSCP だけです。ポートが trust 状態の場合、その trust 状態を使用して、内部 DSCP が取得されます。 ポートの trust 状態は常に、set ip dscp コマンドよりも優先されます。ポリシー マップの **trust xx** コマンドは、ポートの trust 状態より優先されます。ポートとポリシーが別々の trust 状態を含んでいる場合は、ポリシー マップからの trust 状態が考慮されます。

そのため、内部 DSCP は次の要因に基づいて決定されます。

- ポートの trust 状態
- ポートに割り当てられたサービス ポリシー（ACL を使用）
- デフォルトのポリシー マップ**注:** このデフォルトは DSCP を 0 にリセットします。
- ACL が VLAN ベースか、またはポート ベースであるか

次の図は、設定に基づいて内部 DSCP が選択される方法の概要を示したものです。



PFC はポリシングも行うことができます。 この結果、内部 DSCP がマークダウンされることがあります。 ポリシングの詳細については、『Catalyst 6500/6000 シリーズ スイッチの QoS ポリシング』を参照してください。

出力ポートにおける処理

出力ポート レベルでは、分類を変更できません。 ただし、次のルールに従ってパケットをマーキングできます。

- パケットが IPv4 パケットの場合、スイッチング 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 カプセル化に対応した設定になっている場合、内部 DSCP から取得した CoS を使用します。 ISL または dot1q フレームの CoS をコピーします。

注: スタティックの場合、CoS は内部 DSCP から取得されます。 スタティックを設定するには、次のコマンドを発行します。

```
Router(config)#mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7
[dscp8]]]]]]] to cos_value
!--- Note: This command should be on one line.
```

デフォルトの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。 マッピングを確認するには、次のコマンドを発行します。

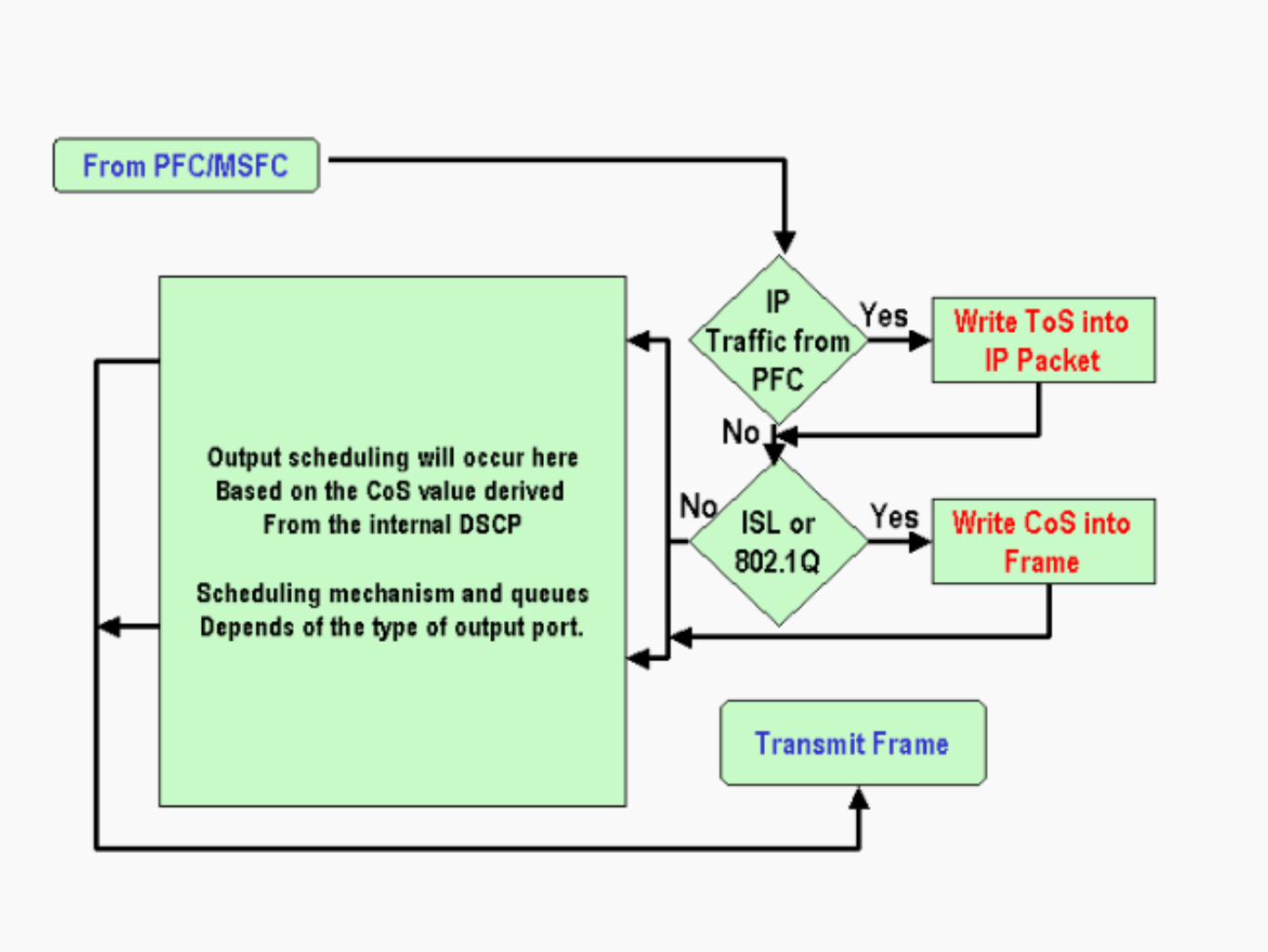
```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ---------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 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
```

このマッピングを変更するには、通常の設定モードでこの設定コマンドを発行します。

```
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 8 9 10 11 12 13 14 15 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
...
```

DSCP が IP ヘッダーに書き込まれ、DSCP から CoS が取得されると、パケットは、CoS を基に決定した出力スケジューリングに合わせて出力キューの 1 つに送信されます。 この動作は、パケットが dot1q や ISL でなくても発生します。 出力キューのスケジューリングの詳細については、『Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 シリーズ スイッチの QoS 出力スケジューリング』を参照してください。

次の図は、出力ポートのマーキングに関するパケットの処理の概要を示したものです。



注意と制限

デフォルト ACL

デフォルト ACL では、分類のキーワードとして「dscp 0」を使用します。 信頼できないポートからスイッチに入り、サービス ポリシーのエントリにヒットしないトラフィックは、すべて DSCP が 0 としてマーキングされます（QoS が有効の場合）。 現時点では、Cisco IOS ソフトウェアでデフォルトの ACL を変更することはできません。

注: Catalyst OS（CatOS）ソフトウェアでは、このデフォルト動作を設定および変更できます。詳細については、『ハイブリッド モードで動作する Catalyst 6500/6000 ファミリ スイッチの QoS の分類とマーキング』の「*デフォルト ACL*」セクションを参照してください。

WS-X61xx、WS-X6248-xx、WS-X6224-xx および WS-X6348-xx ラインカードの制限

このセクションの対象となるのは、次のライン カードだけです。

- 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 100 FX, Enhanced QoS, MT
- WS-X6324-100FX-SM： Catalyst 6000 24-Port 100 FX, Enhanced QoS, MT
- WS-X6348-RJ-45： Catalyst 6000 48-Port 10/100, Enhanced QoS
- WS-X6348-RJ21V： Catalyst 6000 48-Port 10/100, Inline Power
- WS-X6348-RJ45V： Catalyst 6000 48-Port 10/100, Enhanced QoS, Inline Power
- WS-X6148-RJ21V： Catalyst 6500 48-Port 10/100 Inline Power
- WS-X6148-RJ45V： Catalyst 6500 48-Port 10/100 Inline Power

これらのライン カードには制限があり、 ポート レベルでは、次のキーワードを使って trust 状態を設定することはできません。

- `trust-dscp`
- `trust-ipprec`
- `trust-cos`

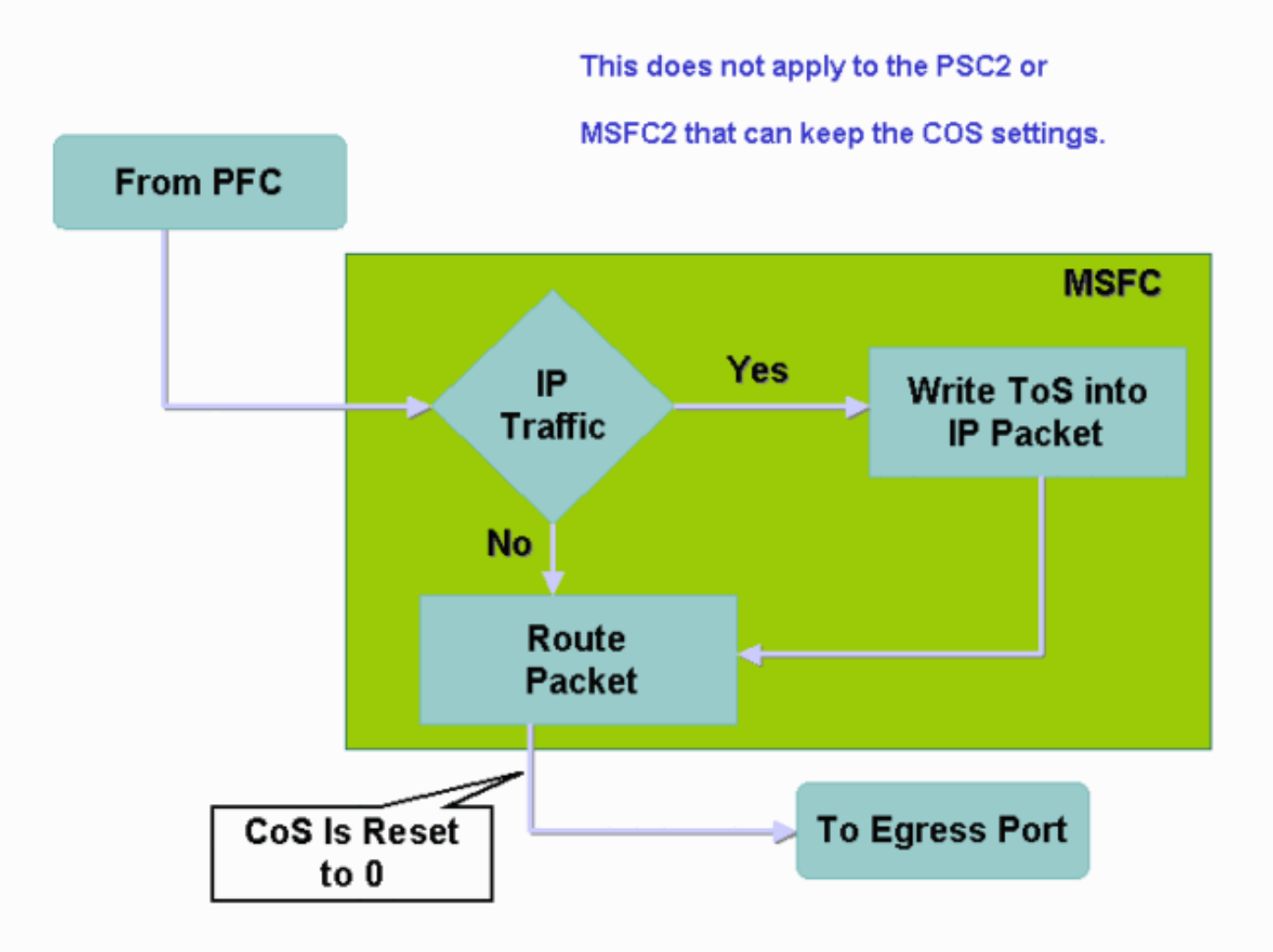
使用できるのは、untrusted 状態だけです。 これらのポートのいずれかに、trust 状態を設定しようとすると、次のいずれかの警告メッセージが表示されます。

```
Tank(config-if)#mls qos trust ?
  extend  extend keyword
Tank(config-if)#mls qos trust
% Incomplete command.
Tank(config-if)#mls qos trust cos
                              ^
% Invalid input detected at '^' marker.
Tank(config-if)#mls qos trust ip-pre
                              ^
% Invalid input detected at '^' marker.
```

このようなライン カードに信頼できるフレームが着信するようにする場合は、ポートか VLAN にサービス ポリシーを割り当てる必要があります。 このドキュメントの「ケース 1： エッジでのマーキング」セクションで説明する方法を使用してください。

Supervisor Engine 1A/PFC の MSFC1 または MSFC2 から送信されるパケット

MSFC1 または MSFC2 から送信されるパケットは、すべて CoS が 0 になります。 このようなパケットは、ソフトウェア ルーティングされたパケット、または MSFC が発行したパケットのいずれかです。 これは PFC の制約で、MSFC から受信したすべてのパケットは CoS がリセットされます。 DSCP と IP precedence は維持されます。 また、PFC2 にはこの制約はありません。 PFC2 の既存の CoS は、パケットの IP precedence と同じものになります。



分類の要約

このセクションでは、次の分類に基づいて取得される DSCP をまとめた表を示します。

- 着信ポートの trust 状態
- 適用される ACL の分類キーワード

次の表は、WS-X62xx および WS-X63xx 以外のすべてのポートに関する一般情報の要約を示したものです。

ポリシー マップ キーワード ポートの信頼状態	set-ip-dscp xx または set-dscp-transmit xx	trust-dscp	trust-ipprec	trust-cos
untrusted	xx1	Rx2 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 から取得
trust-ipprec	Rx ipprec か	Rx	Rx	Rx CoS

	から取得	DSCP	ipprec から取得	またはポート CoS から取得
trust-cos	Rx CoS またはポート CoS から取得	Rx DSCP	Rx ipprec から取得	Rx CoS またはポート CoS から取得

1フレームに新しいマーキングを行う唯一の方法です。

2 Rx = 受信

次の表は、WS-X61xx、WS-X62xx、WS-X63xx の各ポートに関する要約を示したものです。

ポリシー マップ キーワード **ポートの信頼状態**	**set-ip-dscp xx または set-dscp-transmit 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	非サポート	非サポート	非サポート	非サポート

設定の監視と検証

ポート設定の確認

ポートの設定を検証するには、**show queuing interface interface-id** コマンドを発行します。

このコマンドを発行すると、次の分類パラメータを検証できます。

- ポートベースか VLAN ベースか
- ポートの trust タイプ
- ポートに割り当てられた ACL

次にこのコマンド出力例を示します。 分類に関連する重要なフィールドは、太字で示しています。

```
6500#show queuing interface gigabitethernet 3/2
Interface GigabitEthernet3/2 queuing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust COS
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
```

この出力は、特定のポートの設定では、ポート レベルで trust cos が使われていることを示しています。 また、デフォルトのポート CoS 値は 0 です。

定義クラスの確認

定義クラスをチェックするには、**show class-map** コマンドを発行します。 次に例を示します。

```
Boris#show class-map
 Class Map match-all test (id 3)
   Match access-group  112

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all voice (id 4)
```

インターフェイスに適用されているポリシー マップの確認

以前のコマンドによって適用されたり、表示されたりしているポリシー マップをチェックするには、次のコマンドを発行します。

- **show mls qos ip interface interface-id**
- **show policy-map interface interface-id**

これらのコマンドの出力例は次のとおりです。

```
Boris#show mls qos ip gigabitethernet 1/1
   [In] Default.   [Out] Default.
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

 Int  Mod Dir  Class-map  DSCP AgId Trust FlId AgForward-Pk AgPoliced-k
 ---------------------------------------------------------------------
 Gi1/1 1  In   TEST       0    0*   No    0    1242120099            0
```

注: 確認できるのは、分類に関連する次のフィールドです。

- Class-map：このインターフェイスに割り当てられているサービス ポリシーに割り当てられたクラスを示します。
- Trust：そのクラスのポリシー アクションに trust コマンドが含まれているかどうかと、そのクラスで信頼される対象を示します。
- dscp – そのクラスを押すパケットのために送信される DSCP を言います。

```
Tank#show policy-map interface fastethernet 4/4

 FastEthernet4/4

  service-policy input: TEST_aggre2

    class-map: Test_marking (match-all)
      27315332 packets
      5 minute offered rate 25726 pps
      match: access-group 101
      police :
        10000000 bps 10000 limit 10000 extended limit
        aggregate-forwarded 20155529 packets action: transmit
        exceeded 7159803 packets action: drop
        aggregate-forward 19498 pps exceed 6926 pps
```

ケース スタディ

このセクションでは、ネットワークでよく見られる設定の例を紹介します。

ケース 1： エッジでのマーキング

アクセス スイッチとして使用されている Catalyst 6000 を設定すると仮定します。 多くのユーザが、スイッチ スロット 2 に接続しています。このスロットは、WS-X6348 ライン カード（10/100 Mbps）です。 ユーザが送信できるトラフィックは次のとおりです。

- 通常のデータ トラフィック：このトラフィックは常に VLAN 100 に属し、DSCP 値 0 を付与される必要があります。
- IP Phone からの音声トラフィック：このトラフィックは常に音声補助 VLAN 101 に属し、DSCP 値 46 を付与される必要があります。
- ミッションクリティカルなトラフィック：このトラフィックも VLAN 100 に着信し、サーバ 10.10.10.20 に送信されます。 このトラフィックは DSCP 値 32 を付与される必要があります。

このアプリケーションは、どのトラフィックもマーキングしません。 そのため、ポートを untrusted のままにし、トラフィックを分類する特定の ACL を設定します。 ある ACL が VLAN 100 に適用され、別の ACL が VLAN 101 に適用されるようにします。 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。 結果として、次の例のような設定になります。

```
Boris(config)#mls qos
Boris(config)#interface range fastethernet 2/1-48
Boris(config-if)#mls qos vlan-based
Boris(config-if)#exit
Boris(config)#ip access-list extended Mission_critical
Boris(config-ext-nacl)#permit ip any host 10.10.10.20
Boris(config)#ip access-list extended Voice_traffic
Boris(config-ext-nacl)#permit ip any any
Boris(config)#class-map voice

Boris(config-cmap)#match access-group Voice_traffic
Boris(config)#class-map Critical

Boris(config-cmap)#match access-group Mission_critical
Boris(config)#policy-map Voice_vlan
Boris(config-pmap)#class voice
Boris(config-pmap-c)#set ip dscp 46
Boris(config)#policy-map Data_vlan
Boris(config-pmap)#class Critical
Boris(config-pmap-c)#set ip dscp 32
Boris(config)#interface vlan 100
Boris(config-if)#service-policy input Data_vlan
Boris(config)#interface vlan 101
Boris(config-if)#service-policy input Voice_vlan
```

ケース 2： ギガビット イーサネット インターフェイスのみを搭載したコアでの信頼設定

スロット 1 およびスロット 2 にギガビット イーサネット インターフェイスのみが搭載されたコアの Catalyst 6000 を設定すると仮定します。 アクセス スイッチは、これまで正常にトラフィックをマーキングしています。 そのため、マーキングを再度行う必要はありません。 ただし、コアスイッチが着信 DSCP を確実に信頼するようにしなければなりません。 このケースでは、ポートがすべて trust-dscp としてマークされるため、比較的易しいケースです。

```
6k(config)#mls qos
6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-2
```

```
6k(config-if)#mls qos trust dscp
```

関連情報

- Catalyst 6000 ファミリ スイッチでのサービス品質について
- CatOS ソフトウェアが稼働している Catalyst 6500/6000 シリーズ スイッチの QoS 分類およびマーキング
- 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とドキュメント - Cisco Systems