Catalyst 3550 のQoS ポリシングおよびマーキングの理解

内容

概要

ポリシング機能は、トラフィックレベルが指定されたプロファイルまたは契約内にあるかどうかを判別し、プロファイル外のトラフィックをドロップするか、別のDifferential Services Code Point(DSCP)値にマークダウンできます。これにより契約サービス レベルが施行されます。

DSCP は、パケットの Quality of Service（QoS）レベルの測定値です。パケットの QoS レベルを伝えるためには、DSCP とともに、IP 優先順位や CoS も使用されます。

ポリシングとトラフィック シェーピングはともに、トラフィックをプロファイルまたはコントラクト内にとどめる機能ですが、この 2 つは明確に区別する必要があります。

ポリシングではトラフィックのバッファリングは行われないため、伝搬遅延への影響はありません。プロファイル外のパケットをバッファリングする代わりに、ポリシングではそれらを廃棄するか、異なる QoS レベルにマーキング（DSCP マークダウン）します。

トラフィック シェーピングでは、プロファイル外のトラフィックをバッファリングして、トラフィックのバーストの平滑化を行いますが、遅延や遅延変動に影響を与えます。シェーピングが適用できるのは発信インターフェイスだけですが、ポリシングは着信インターフェイスと発信インターフェイスの両方に適用できます。

Catalyst 3550 では、着信と発信の両方向のポリシングをサポートしています。トラフィック シェーピングはサポートしていません。

マーキングにより、パケットの QoS レベルがポリシーに従って変更されます。

前提条件

要件

このドキュメントに特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内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、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。

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。

ハードウェアとソフトウェアのバージョン

Catalyst 3550 でのポリシングとマーキングはすべてのソフトウェア バージョンでサポートされています。最新の設定ガイドを次に示します。サポートされているすべての機能については、次のドキュメントを参照してください。

- QoS の設定

QoS ポリシングと QoS マーキングのパラメータ

ポリシングを設定するには、QoS ポリシー マップを定義してポートに適用する必要があります。これは、ポートベース QoS とも呼ばれます。

注： Catalyst 3550 では VLAN ベースの QoS は現在サポートされていません。

ポリサーには、プロファイル外のトラフィックに対するアクションとともにレートやバースト パラメータが定義されています。

次の 2 つのタイプのポリサーがサポートされています。

- 集約
- 個別

集約ポリサーは、適用されるすべてのインスタンス間のトラフィックに対応します。個別ポリサーは、適用される各インスタンス間のトラフィックに個別に対応します。

注：Catalyst 3550では、集約ポリサーは同じポリシーの異なるクラスにのみ適用できます。複数のインターフェイスまたはポリシー間の集約ポリシングはサポートしていません。

たとえば、同じポリシーマップの customer1 クラスと customer2 クラスのトラフィックを 1 Mbps に制限するには集約ポリサーを適用します。そのようなポリサーでは、customer1 クラスと customer2 クラスを合せて 1 Mbps のトラフィックが許可されます。個別ポリサーを適用した場合、customer1 クラスのトラフィックが 1 Mbps に、customer2 クラスのトラフィックが 1 Mbps にそれぞれ制限されます。つまり、ポリサーの各インスタンスは個別に扱われます。

着信ポリシーと発信ポリシーの両方でパケットを処理した際の QoS の対応を次の表に要約します。

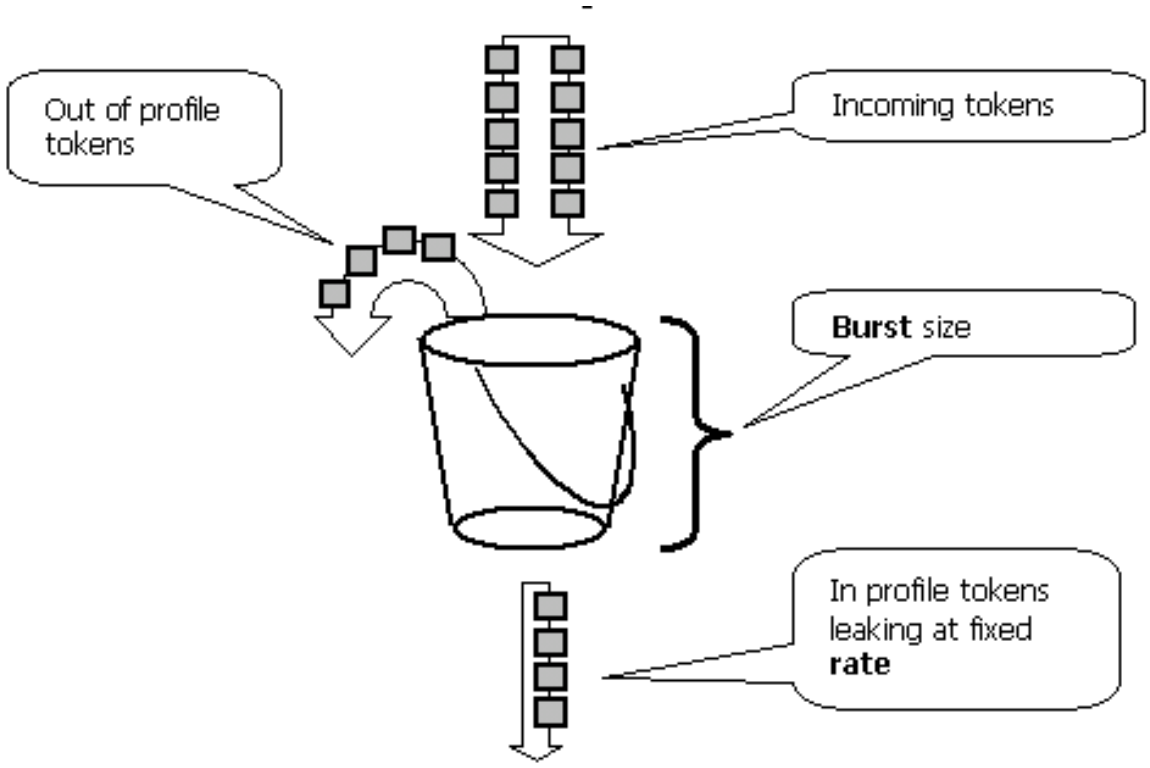
	Ingress policy			
Egress policy	Transmit	Drop	Markdown$_i$	Mark$_i$
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_i$ then Markdown$_e$	Mark$_i$ then Markdown$_e$

注：同じポリシーの同じトラフィッククラス内でマークとマークダウンを行うことができます。そのような場合、特定のクラスに対するすべてのトラフィックが最初にマークされます。ポリシングとマークダウンは、マーキング済みのトラフィックに対して行われます。

Catalyst 3550 の QoS のポリシングは、次のような漏出バケットの概念に従っています。

着信トラフィックパケットサイズに比例するトークンの数がトークンバケットに配置されます。トークンの数は、パケットのサイズと同じです。一定の間隔で、定義された (設定レートから求めた) 数のトークンがバケットから取り出されます。着信パケットに対応できる余裕がバケットにない場合は、そのパケットはプロファイル外とみなされ、設定されたポリシング アクションに従って廃棄されるか、マークダウンされます。

この概念を次の例で示します。



注：この例に示すように、トラフィックはバケットにバッファリングされません。実際のトラフィックはバケットを通過しません。バケットは、パケットがプロファイル内にあるかプロファイ

ル外にあるかを判断するためにのみ使用されます。

注：ポリシングのハードウェア実装は異なる場合がありますが、機能的には、このモデルに準拠しています。

ポリシングの動作を制御するパラメータには、次のものがあります。

- **レート**：各インターバルで取り出すトークンの数を定義します。ポリシング レートを効果的に設定します。このレートより低いトラフィックはすべて、プロファイル内とみなされます。サポートされるレートの範囲は 8 Kbps ~ 2 Gbps で、8 Kbps 単位で指定できます。
- **インターバル**：バケットからトークンを取り出す頻度を定義します。インターバルは、0.125 ミリ秒 (つまり、1 秒当り 8000 回) に固定されています。 このインターバルは変更できません。
- **バースト**：一時点でバケットが保持できるトークンの最大容量を定義します。サポートされるバーストの範囲は、8000 バイト ~ 2000000 バイトで、64 バイト単位で指定できます。

注：コマンドラインヘルプ文字列には大きな範囲の値が表示されますが、rate-bpsオプションは設定されたポート速度を超えることはできません。また、burst-byteオプションは2000000バイトを超えることはできません。それよりも大きい値を入力した場合、ポリシーマップをインターフェイスに適用する際にスイッチに拒否されます。

指定したトラフィック レートを維持するには、次の等式で求める値以上のバースト値を指定する必要があります。

```
Burstmin (bits) = Rate (bps) / 8000 (1/sec)
```

例として、1 Mbps のレートを維持するための最小バースト値を計算してみます。レートは 1000 Kbps に定義されているので、必要とされる最小バースト値は次の式で求められます。

```
1000 (Kbps) / 8000 (1/sec) =125 (bits)
```

サポートされる最小バーストサイズは 8000 バイトなので、計算した最小バースト値を超えています。

注：ハードウェアポリシングの粒度により、正確なレートとバーストはサポートされる最も近い値に丸められます。

バースト レートを設定する際には、一部のプロトコルにはパケットの損失に対応するメカニズムが実装されていることを考慮する必要があります。たとえば、Transmission Control Protocol (TCP; 伝送制御プロトコル) では、損失したパケットごとにウィンドウが半分に縮小されます。そのため、TCP がライン レートを上げようとするときにポリサーが抑制すると、「鋸歯」状の影響が TCP のトラフィックに現れます。鋸歯状のトラフィックの平均レートを計算すると、ポリシングされたレートよりずっと低くなります。ただし、この場合、使用率を上げるためにバースト値を増やすことができます。手始めに、ラウンドトリップ時間 (TCP RTT) の間に希望レートで送信されるトラフィック量の 2 倍をバースト値に指定してみます。 RTT がわからない場合は、バースト パラメータの値を 2 倍にしてみることができます。

同じ理由から、コネクション型トラフィックによるポリサー動作のベンチマークを行うことはお勧めしません。このシナリオでは、一般にポリサーによって許可されたパフォーマンスよりも低いパフォーマンスが示されます。

コネクションレス型トラフィックもポリシングに対して異なる反応を示す可能性があります。たとえば、Network File System (NFS; ネットワーク ファイル システム) では、複数の User

Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットが含まれる可能性のあるブロックが使用されます。1 つのパケットの破棄が原因で、多数のパケット（場合によってはブロック全体）が再送信される場合があります。

次の例では、ポリシング レートが 64 Kbps で TCP RTT が 0.05 秒の場合の TCP セッションのバースト値を計算しています。

```
<burst> = 2*  *  = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800    [bytes]
```

この例では、<burst>は1つのTCPセッション用です。ポリサーを通過する予想されるセッション数を平均するように、この図を拡張します。

注：これは例にすぎません。各ケースでは、ポリシングパラメータを選択するために、トラフィックとアプリケーションの要件と動作を、使用可能なリソースと比較して評価する必要があります。

ポリシング アクションには、パケットの廃棄とパケットの DSCP の変更（マークダウン）のいずれかを指定できます。 パケットをマークダウンするには、ポリシングされた DSCP マップを修正する必要があります。デフォルトのポリシングされたDSCPマップは、パケットを同じDSCPに再マーキングします。したがって、マークダウンは発生しません。

プロファイル外のパケットが元の DSCP とは異なる出力キューにマップされる DSCP にマークダウンされると、パケットは誤った順序で送信される可能性があります。パケットの順序が重要な場合は、プロファイル内のパケットと同じ出力キューにマップされる DSCP に、プロファイル外のパケットがマークダウンされるように指定します。

Catalyst 3550 がサポートするポリシングとマーキングの機能

次の表には、Catalyst 3550 でサポートされるポリシングとマーキングに関連する機能が通信方向に従って要約されています。

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

クラスマップごとに 1 つの match ステートメントを指定できます。入力ポリシーには次の match 文が有効です。

- match access-group
- match ip dscp
- match ip precedence

注：Catalyst 3550では、match interfaceコマンドはサポートされず、クラスマップで許可されるmatchコマンドは1つだけです。したがって、インターフェイスを通じて入ってくるすべてのトラフィックを分類し、単一のポリサーを使用してすべてのトラフィックをポリシングするのは複雑になります。このドキュメントの「単一のポリサーですべてのインターフェイス トラフィックを分類する方法」を参照してください。

出力ポリシーには次の match 文が有効です。

- match ip dscp

入力ポリシーには次のポリシーアクションが有効です。

- police
- set ip dscp（マーキング）
- set ip precedence（マーキング）
- trust dscp
- trust ip-precedence
- trust cos

サポートされている入力 QoS ポリシー マトリックスを次の表に示します。

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. このオプションには、IP 優先順位のマッチングも含まれます。
2. このオプションには、CoS、IP 優先順位、DSCP の信頼も含まれます。
3. このオプションには、IP 優先順位の設定も含まれます。

出力ポリシーには次のポリシーアクションが有効です。

- police

サポートされている出力 QoS ポリシー マトリックスを次の表に示します。

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

マーキングにより、分類またはポリシングに基づいたパケットの QoS レベルの変更が可能になります。分類により、定義した基準に従って、トラフィックを異なるクラスの QoS 処理に分割することができます。

QoS処理は内部DSCPに基づいています。パケットのQoSレベルの測定値。内部 DSCP は信頼設定に基づいて取得されます。このシステムでは、CoS、DSCP、IP 優先順位を信頼する設定、およびインターフェイスを信頼しない設定がサポートされています。フィールドを信頼する設定をすると、内部 DSCP がそれぞれのパケットから次のように取得されます。

- CoS を信頼する場合、QoS レベルは、Inter-Switch Link (ISL; スイッチ間リンク) プロトコルまたは 802.1Q カプセル化パケットのレイヤ 2 (L2) ヘッダーから取得されます。
- DSCP または IP 優先順位を信頼する場合、システムは QoS レベルを DSCP または IP 優先順位フィールドからそれぞれ取得します。

CoS の信頼は、トランキング インターフェイスだけで有効であり、DSCP (または IP 優先順位) の信頼は、IP パケットに対してだけ有効です。

インターフェイスを信頼しない場合、内部 DSCP はそのインターフェイスの設定可能なデフォルト CoS から取得されます。QoS が有効である場合、これはデフォルトの状態です。デフォルト CoS が設定されていない場合、デフォルト値はゼロになります。

内部 DSCP が決定されると、マーキングやポリシングで変更することも、そのまま維持することもできます。

パケットに QoS の処理が実行された後、その QoS レベル フィールド (IP の場合は IP/DSCP フィールド内、および存在する場合は ISL/802.1Q ヘッダー内) は内部 DSCP より更新されます。ポリシングに関連した次の特別な QoS マップがあります。

- **DSCP-to-Policed DSCP**：パケットのマークダウン時に、ポリシングされた DSCP を取得するために使用。
- **DSCP-to-CoS**：発信パケットの ISL/802.1Q ヘッダーを更新するために、内部 DSCP から CoS レベルを取得するのに使用。
- **CoS-to-DSCP**：インターフェイスが trust CoS モードの場合に、着信 CoS (ISL/802.1Q ヘッダー) から内部 DSCP を取得するために使用。

特定の実装方法で考慮する必要のある重要な点を次に説明します。

- インターフェイスが任意の QoS メトリック (CoS/DSCP または IP 優先順位など) を信頼するように設定されている場合は、入力サービス ポリシーをインターフェイスに適用できません。DSCP/IP 優先順位を照合して入力をポリシングするには、インターフェイスに対してではなく、ポリシー内の特定のクラスに対して信頼設定を行う必要があります。DSCP/IP 優先順位に基づいてマーキングするには、特に信頼設定を行う必要はありません。
- ハードウェアと QoS の観点からは、IP オプションのない、Ethernet II Advanced Research Projects Agency (ARPA) カプセル化による IPv4 トラフィックのみが IP トラフィックとみ

なされます。SubNetwork Access Protocol (SNAP) カプセル化 IP や IPv6 などのオプション付き IP も含めて、他のすべてのトラフィックは非 IP とみなされます。
- 非 IP トラフィックには DSCP の照合ができないので、非 IP パケットに関しては、「match access group」が分類する唯一の方法です。その目的には、メディアアクセスコントロール(MAC)アクセスリスト(ACL)が使用されます。パケットは、送信元MACアドレス、宛先MACアドレス、およびEtherTypeに基づいて照合できます。スイッチでは IP と非 IP のトラフィックが区別されるので、IP トラフィックを MAC ACL に照合することはできません。

ポリシングの設定と監視

Cisco IOS でポリシングを設定する方法は次のとおりです。

1. ポリサーを定義する（集約ポリサーの場合）。
2. ポリシングするトラフィックの選択基準を定義する。
3. 定義した基準を使用してトラフィックを選択するクラスマップを定義する。
4. クラスを使用したサービスポリシーを定義し、指定したクラスにポリサーを適用する。
5. サービスポリシーをポートに適用する。

次の 2 つのタイプのポリサーがサポートされています。

- 名前付き集約
- 個別

名前付き集約ポリサーは、それが適用されている同一のポリシー内にあるすべてのクラスから結合されたトラフィックに対してポリシングを行います。異なるインターフェイス間での集約ポリシングはサポートしていません。

注：集約ポリサーは複数のポリシーに適用できません。適用した場合には、次のエラー メッセージが表示されます。

```
QoS: Cannot allocate policer for policy map <policy name>
```

次の例を検討します。

GigabitEthernet0/3 ポートに接続されたトラフィック ジェネレータがあり、宛先ポートが 111 の UDP トラフィックを約 17 Mbps で送信しています。ポート 20 からの TCP トラフィックもあり、これら 2 つのトラフィック ストリームを 1 Mbps にポリシング ダウンし、超過したトラフィックは廃棄すると仮定します。次の例は、どのようにそれを行えるかを示しています。

```
!--- Globally enables QoS. mls qos !--- Defines the QoS policer, sets the burst !--- to 16000
for better TCP performance. mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop
!--- Defines the ACLs to select traffic. access-list 123 permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111 match access-group
123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. policy-map
po_test
  class cl_udp111
    police aggregate pol_1mbps
  class cl_tcp20
    police aggregate pol_1mbps
```

```
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test
!
```

最初の例では、名前付き集約ポリサーを使用しています。個別ポリサーは、名前付きポリサーとは異なり、適用されるクラスごとに個別にトラフィックのポリシングを行います。個別ポリサーは、ポリシー マップ設定で定義されます。この例では、2つのトラフィッククラスが2つの個別ポリサーによってポリシングされます。cl_udp111は8Kバーストごとに1 Mbpsにポリシングされ、cl_tcp20は32Kバーストごとに512 Kbpsにポリシングされます。

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123
permit udp any any eq 111
access-list 145 permit tcp any eq 20 any
!--- Defines the traffic classes to be policed. class-map match-all cl_udp111
  match access-group 123
class-map match-all cl_tcp20
  match access-group 145
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test2
  class cl_udp111
    police 1000000 8000 exceed-action drop
  class cl_tcp20
    police 512000 32000 exceed-action drop
!--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport
access vlan 2 service-policy input po_test2
```

ポリシング処理を監視するには、次のコマンドを使用します。

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 267718     0          267717     0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
Others: 590877        n/a        n/a      266303     0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         8
   4 : 0          0         1024
```

注：デフォルトでは、DSCPごとの統計情報はありません。Catalyst 3550 では、最大 8 個の DSCP 値のインターフェイスごと、方向ごとの統計収集をサポートしています。これは、**mls qos monitor** コマンドを発行することで設定されます。DSCP 8、16、24、32 の統計情報を監視するには、次のコマンドを**インターフェイスごとに**発行する必要があります。

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

注：mls qos monitor dscp **8 16 24 32コマンドは、show mls qos int g0/3 statisticsコマンドの出力を次のように**変更します。

```
cat3550#show mls qos interface g0/3 statistics
GigabitEthernet0/3
Ingress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 0          0          675053785  0          0
    16: 1811748    0          0          0          0         ? per DSCP statistics
    24: 1227820404 15241073   0          0          0
    32: 0          0          539337294  0          0
Others: 1658208    0          1658208    0          0
Egress
  dscp: incoming   no_change  classified policed    dropped (in pkts)
    8 : 675425886     n/a        n/a      0          0
    16: 0             n/a        n/a      0          0         ? per DSCP statistics
    24: 15239542      n/a        n/a      0          0
    32: 539289117     n/a        n/a      536486430  0
Others: 1983055       n/a        n/a      1649446    0

WRED drop counts:
  qid  thresh1    thresh2   FreeQ
   1 : 0          0         1024
   2 : 0          0         1024
   3 : 0          0         6
   4 : 0          0         1024
```

次に上の例のフィールドについて説明します。

- **Incoming**：各方向から到達したパケット数を表示。
- **NO_change**：信頼された (QoS レベルを変更しなかったなど) パケットの数を表示。
- **Classified**：分類後にこの内部 DSCP を割り当てられたパケットの数を表示。
- **Policed**：ポリシングによってマークダウンされたパケットの数を表示します。マークダウンの前に表示されるDSCP。
- **Dropped**：ポリシングにより廃棄されたパケットの数を表示。

実装時に固有な次の考慮事項に注意してください。

- **mls qos monitor** コマンドを発行した際に 8 個の DSCP 値が設定されていると、**show mls qos int statistics** コマンドを発行して表示される others カウンタに不適切な情報が表示される場合があります。
- ポリサーごとの提供トラフィック レートや発信トラフィック レートを確認するコマンドはありません。
- カウンタはハードウェアから順次取得されるため、カウンタが正しく加算されていない可能性があります。たとえば、ポリシング、分類、または破棄されたパケットの合計が、着信パケット数とわずかに異なる場合があります。

マーキングの設定と監視

マーキングを設定する方法は次のとおりです。

1. トラフィックを分類する基準を定義します。
2. 事前に定義された基準で分類するトラフィック クラスを定義します。
3. 定義したクラスにマーキング アクションとポリシング アクションを適用するポリシーマップを作成します。
4. 関連するインターフェイスを信頼できるモードに設定します。
5. ポリシー マップをインターフェイスに適用します。

この例では、着信IPトラフィックをホスト192.168.192.168に対してIP precedence 6とマークし、1 Mbpsまでポリシングします。超過トラフィックはIP precedence 2にマークダウンする必要が

あります。

```
!--- Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167
permit ip any host 192.168.192.168
!--- Defines the traffic class. class-map match-all cl_2host
  match access-group 167
!--- Defines QoS policy, and creates and attaches !--- the policers to the traffic classes.
policy-map po_test3
  class cl_2host
!--- Marks all the class traffic with the IP precedence 6. set ip precedence 6
!--- Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed-
action policed-dscp-transmit
!--- Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
switchport access vlan 2 service-policy input po_test3
```

同じ **show mls qos interface statistics** コマンドを、マーキングを監視するためにも発行します。サンプル出力とその意味は、このドキュメントのセクションで説明されています。

単一のポリサーですべてのインターフェイス トラフィックを分類する方法

Catalyst 3550 では、**match interface** コマンドがサポートされておらず、1 つのクラスマップで使用できる match コマンドは 1 つだけです。さらに、Catalyst 3550 では、MAC ACL で IP トラフィックを照合できません。そのため、IP トラフィックと非 IP トラフィックは、2 つの独立したクラスマップを使用して分類する必要があります。したがって、インターフェイスを通じて入ってくるすべてのトラフィックを分類し、単一のポリサーを使用してすべてのトラフィックをポリシングするのは複雑になります。ここに示す設定例を使用すれば、これが可能です。この設定では、IP トラフィックと非 IP トラフィックが 2 つの独立したクラスマップで照合されます。ただし、それぞれのクラスマップでは、両方のトラフィックに対して共通のポリサーが使用されます。

```
access-list 100 permit ip any any

class-map ip
match access-group 100
!--- This class-map classifies all IP traffic. mac access-list extended non-ip-acl
permit any any

class-map non-ip
match access-group name non-ip-acl
!--- Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000
8000 exceed-action drop
!--- This command configures a common policer that is applied for both IP and non-IP traffic.
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
!--- This command applies the policy map to the physical interface.
```

関連情報

- Catalyst 3550 での QoS の設定
- Quality of Service（QOS）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
- LAN 製品に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems