

Catalyst 6500/6000 シリーズ スイッチでの QoS ポリシング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[QoS ポリシング パラメータ](#)

[パラメータの計算](#)

[ポリシング アクション](#)

[Catalyst 6500/6000 でサポートされているポリシング機能](#)

[スーパーバイザ エンジン 720 を対象としたポリシング機能の更新](#)

[CatOS ソフトウェアでのポリシングの設定と監視](#)

[Cisco IOS ソフトウェアでのポリシングの設定と監視](#)

[関連情報](#)

概要

ネットワーク上で QoS ポリシングを実行することで、ネットワークトラフィックが所定のプロファイル (契約) の範囲内にあるかどうか判断されます。これにより、プロファイルの範囲外のトラフィックを廃棄したり、別の DiffServ コード ポイント (DSCP) 値まで下げて、契約したサービス レベルを適用したりすることができます。(DSCP はフレームの QoS レベルの基準となります)。

トラフィック ポリシングとトラフィックシェーピングを混同しないようにしてください。どちらもトラフィックがプロファイル (契約) の範囲内に留まることを保証します。トラフィックのポリシングを行っている場合には、プロファイル外のパケットはバッファリングされません。そのため、伝送の遅延への影響はありません。トラフィックは、廃棄されるか、またはより低い QoS レベルでマーキングされます (DSCP マークダウン)。これに対し、トラフィックシェーピングによる契約の場合は、プロファイル外トラフィックはバッファリングされて、トラフィックのバーストが平滑化されます。これにより、遅延と遅延変動への影響があります。トラフィックシェーピングを適用できるのは、発信インターフェイスだけです。ポリシングは、着信と発信の両方のインターフェイスに適用できます。

Catalyst 6500/6000 Policy Feature Card (PFC; ポリシー フィーチャ カード) および PFC2 でサポートされるのは、入力方向ポリシングだけです。PFC3 では、入力方向と出力方向の両方のポリシングがサポートされます。トラフィックシェーピングがサポートされているのは、Catalyst 6500/7600 シリーズの Optical Services Module (OSM; オプティカル サービス モジュール) や FlexWAN モジュールなどの特定の WAN モジュールのみです。詳細は、『[Cisco 7600 シリーズ ルータ モジュール コンフィギュレーション ノート](#)』を参照してください。

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。

表記法

ドキュメント表記の詳細については、『[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。

QoS ポリシング パラメータ

ポリシングをセットアップするには、ポリサーを定義した後、それをポート（ポートベースの QoS）または VLAN（VLAN ベースの QoS）に適用します。それぞれのポリサーは名前、タイプ、レート、バースト、およびプロファイル内外のトラフィックに対する動作を定義します。Supervisor Engine II のポリシング機能は超過レートパラメータもサポートします。ポリサーには 2 つのタイプがあります: microflow と aggregate です。

- **microflow** : 適用されたポート/VLAN においてフローごとにトラフィックをポリシングします。
- **aggregate** : 適用されたポート/VLAN のすべてのトラフィックをポリシングします。

各ポリサーは、複数のポートまたは VLAN に適用できます。フローは、次のパラメータを使用して定義します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- レイヤ 4 プロトコル (User Datagram Protocol (UDP; ユーザ データグラム プロトコル) など)
- 送信元ポート番号
- 宛先ポート番号

定義されている特定の一連のパラメータと一致するパケットは同じフローに属すると見なすことができます。これは、NetFlow スイッチングで使用されるのと基本的に同じフロー概念です。

一例として、VLAN 1 および VLAN 3 で TFTP トラフィックを 1 Mbps に制限するようにマイクロフロー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、マイクロフローポリサーはこの各フローにそれぞれ 1 Mbps を許可します。一方、集約ポリサーを設定すると、VLAN 1 と VLAN 3 をまとめた全フローの TFTP トラフィックが 1 Mbps に制限されます。

集約ポリサーとマイクロフローポリサーを両方とも適用すると、QoS では常に、両方のポリサーで指定されている最も厳しいアクションが使用されます。たとえば、あるポリサーではパケット

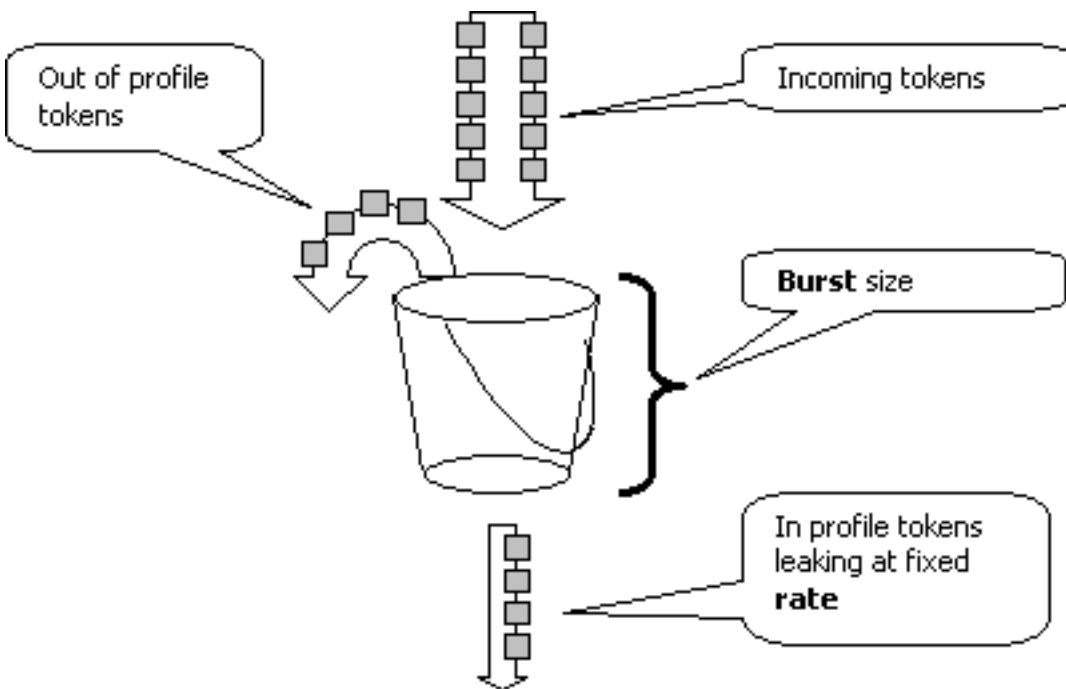
の廃棄が指定されていて、別のポリサーではパケットのマークダウンが指定されている場合、パケットは廃棄されます。

デフォルトでは、マイクロフロー ポリサーはルーティングされる (レイヤ 3 (L3)) トラフィックに対してのみ有効です。ブリッジされる (レイヤ 2 (L2)) トラフィックにもポリシングを行うには、ブリッジ マイクロフロー ポリシングを有効にする必要があります。スーパーバイザ エンジン II では、L3 マイクロフロー ポリシングに対してもブリッジ マイクロフロー ポリシングを有効にする必要があります。

ポリシングはプロトコルが認識されます。すべてのトラフィックは次の 3 つのタイプに分類されます。

- IP
- Internetwork Packet Exchange (IPX)
- その他

Catalyst 6500/6000 では、ポリシングが「リーキー バケツ」の概念に従って実装されています。着信トラフィック パケットに対応するトークンが、バケツに格納されます。各トークンはビットを表すので、パケットが大きいほど、それを表すために使用されるトークンが多くなります。通常のインターバルでは定義されたトークンの多くはバケツから取り除かれその宛先に送られます。着信パケットを収納する場所がバケツにない場合、そのパケットはプロファイル外と見なされます。プロファイル外と見なされたパケットは、設定されているポリシング アクションに従って廃棄またはマークダウンされます。



注：上の図に示すように、トラフィックはバケツにバッファリングされません。実際のトラフィックがバケツを経由することはありません。バケツは、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際に使用されるだけです。

パラメータの計算

トークン バケツの動作は、次に示す複数のパラメータによって制御されています。

- 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、プロファイル内と見なされます

- 。
- **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。間隔は 0.00025 秒に固定されているので、トークンはバケットから毎秒 4,000 回削除されます。この間隔を変更することはできません。
- **Burst**：バケットが一度に保持できるトークンの最大数を定義します。指定されたトラフィックレートを維持するためには、レートと間隔の積以上の値をバーストに指定する必要があります。また、最大サイズの packets がバケットに収まらなければならないことに注意しなければなりません。

バーストパラメータを決定するには、次の式を使用します。

- $Burst = (Rate [bps]) * 0.00025 [sec/interval])$ または (最大パケットサイズ (ビット)) のどちらか大きい方。

たとえば、イーサネットネットワークで 1 Mbps のレートを維持するために必要な最小バースト値を計算する場合は、レートを 1 Mbps、イーサネットの最大パケットサイズを 1518 バイトに指定します。式は次のようになります。

- $Burst = (1,000,000 \text{ bps} * 0.00025)$ または $(1518 \text{ bytes} * 8 \text{ bits/byte}) = 250$ または 12144 。値が大きい方の結果は 12144 なので、切り上げて 13 kbps にします。

注：Cisco IOS®ソフトウェアでは、ポリシングレートはCatalyst OS(CatOS)のkbpsではなくbps (ビット/秒) で定義されます。また、Cisco IOS ソフトウェアではバーストレートがバイト単位で指定されていますが、CatOS ではキロビット単位で指定されています。

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。バースト値が最大パケットサイズ未満の値にならないように注意してください。そうしないと、バーストサイズより大きなパケットがすべて廃棄されます。

たとえば、Cisco IOS ソフトウェアでバーストを 1518 に設定しようとするすると、切り下げられて 1000 になります。そのため、1000 バイトより大きなすべてのフレームが廃棄されることになります。これを解決するためには、バーストを 2000 に設定します。

バーストレートを設定する際には、一部のプロトコル (TCP など) には、パケットの損失に反応するフロー制御メカニズムが実装されていることを考慮に入れる必要があります。たとえば、TCP では、パケットの損失があるたびにウィンドウが半分にされます。その結果、特定のレートにポリシングしている場合は、リンクの実効使用率が設定した値よりも低くなります。バーストを増やせば、使用率を向上させることができます。そのようなトラフィックの場合は、バーストサイズを 2 倍にすることから始めます。(この例では、バーストサイズが 13 kbps から 26 kbps に増やされています)。次に、パフォーマンスを監視して、必要に応じてさらに調整します。

同じ理由により、コネクション型のトラフィックを使用して動作するポリサーのベンチマークを行うことは推奨されません。通常、そのようなベンチマークでは、ポリサーが許可するよりも低いパフォーマンスが表示されます。

ポリシングアクション

「概要」で述べたように、ポリサーはアウトオブプロファイルパケットに対して、以下の 2 つのうち 1 つのを行うことができます。

- パケットを廃棄する (設定の `drop`)
- パケットをより低い DSCP にマーキングする (設定の `policed-dscp`)

パケットをマークダウンするには、ポリシングされる DSCP マップを変更する必要があります。ポリシングされたDSCPは、パケットを同じDSCPに再マーキングするようにデフォルトで設定されます (マークダウンは行われません)。

注 : 「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ピングされたDSCPにマークダウンされる場合、一部のパケットが順序を誤って送信されることがあります。このため、パケットの順序が重要な場合は、プロファイル内パケットと同じ出力キューにマップされる DSCP にプロファイル外パケットをマークダウンすることが推奨されます。

超過レートをサポートする Supervisor Engine II では、2 個のトリガーが考えられます。

- トラフィックが標準のレートを超える場合
- トラフィックが余分なレートを超える場合

超過レートには、通常レートを超えたパケットはマークダウンし、超過レートを超えたパケットは廃棄するといった使用方法があります。

Catalyst 6500/6000 でサポートされているポリシング機能

「[概要](#)」で説明したように、スーパーバイザ エンジン 1a の PFC1 とスーパーバイザ エンジン 2 の PFC2 でサポートされるのは、入力方向 (着信インターフェイス) のポリシングだけです。スーパーバイザ エンジン 720 の PFC3 は、入力方向と出力方向 (発信インターフェイス) の両方のポリシングがサポートされます。

Catalyst 6500/6000 では、最大 63 個のマイクロフロー ポリサーと最大 1023 個の集約ポリサーがサポートされています。

スーパーバイザ エンジン 1a では、CatOS バージョン 5.3(1) 以降および Cisco IOS ソフトウェア リリース 12.0(7)XE 以降で、入力ポリシングがサポートされます。

注 : Supervisor Engine 1aでのポリシングには、PFCまたはPFC2ドーターカードが必要です。

スーパーバイザ エンジン 2 では、CatOS バージョン 6.1(1) 以降および Cisco IOS ソフトウェア リリース 12.1(5c)EX 以降で、入力ポリシングがサポートされます。スーパーバイザ エンジン II では、超過レート ポリシング パラメータがサポートされています。

Distributed Forwarding Card (DFC) の設定でサポートされるのは、ポートベースのポリシングだけです。また、集約ポリサーでは、システム単位ではなく、フォワーディング エンジン単位でのみトラフィックがカウントされます。DFC と PFC はどちらもフォワーディング エンジンです。モジュール (ライン カード) に DFC がいない場合、そのモジュールはフォワーディング エンジンとして PFC を使用します。

スーパーバイザ エンジン 720 を対象としたポリシング機能の更新

注 : Catalyst 6500/6000 QoSポリシングに慣れていない場合は、このドキュメントの「[QoSポリシングパラメータとCatalyst 6500/6000でサポートされるポリシング機能](#)」を参照してください。

スーパーバイザ エンジン 720 には、次の新しい QoS ポリシング機能が導入されています。

- 出力ポリシング。スーパーバイザ 720 では、ポートまたは VLAN インターフェイスでの入力

ポリシングがサポートされています。出力ポリシングは、ポートまたは L3 ルーテッド インターフェイス (Cisco IOS システム ソフトウェアの場合) でサポートされます。VLAN のすべてのポートでは、ポートの QoS モード (ポートベースの QoS または VLAN ベースの QoS) に関係なく、出力にポリシングが適用されます。出力では、マイクロフロー ポリシングはサポートされません。設定例は、このドキュメントの「[CatOS ソフトウェアでのポリシングの設定と監視](#)」セクションおよび「[Cisco IOS ソフトウェアでのポリシングの設定と監視](#)」セクションを参照してください。

- **ユーザ別マイクロフロー ポリシング。** スーパーバイザ 720 では、ユーザ別マイクロフロー ポリシングと呼ばれるマイクロフロー ポリシングの拡張機能がサポートされています。この機能がサポートされているのは Cisco IOS システム ソフトウェアだけです。これにより、特定のインターフェイスの背後にある各ユーザ (IP アドレスごと) に特定の帯域幅を提供できます。これは、サービスポリシー内でフローマスクを指定することによって実現されます。フロー マスクにより、フローの区別に使用する情報が定義されます。たとえば、送信元専用のフロー マスクを指定すると、1 つの IP アドレスから送信されるすべてのトラフィックが、1 つのフローと見なされます。この方法を使用して、(対応するサービス ポリシーを設定済みの) インターフェイス上でユーザごとにトラフィックをポリシングできます。他のインターフェイスでは、引き続きデフォルトのフロー マスクを使用します。1 つのシステムで同時に 2 つの異なる QoS フロー マスクまでアクティブにできます。1 つのフロー マスクと関連付けることができるのは、1 つのクラスだけです。1 つのポリシーには、最高で 2 つの異なるフロー マスクを指定できます。

スーパーバイザ エンジン 720 でのポリシングのもう 1 つの重要な変更点は、フレームの L2 の長さでトラフィックをカウントできるようになったことです。これは、IP フレームと IPX フレームを L3 の長さでカウントするスーパーバイザ エンジン 2 およびスーパーバイザ エンジン 1 とは異なります。一部のアプリケーションでは、L2 と L3 で長さが異なる場合があります。一例として、大きな L2 フレームの中に小さな L3 パケットがある場合があります。この場合、スーパーバイザ エンジン 720 では、ポリシングされたトラフィック レートが、スーパーバイザ エンジン 1 およびスーパーバイザ エンジン 2 の場合とはわずかに異なって表示される場合があります。

[CatOS ソフトウェアでのポリシングの設定と監視](#)

CatOS に対するポリシングの設定は、次の 3 つの主要手順で構成されます。

1. ポリサー (通常のトラフィック レート、超過レート (該当する場合)、バースト、およびポリシング アクション) を定義します。
2. ポリシング対象のトラフィックを選択する QoS ACL を作成して、ポリサーをこの ACL と関連付けます。
3. この QoS ACL を、必要なポートや VLAN に適用します。

次の例では、ポート 2/8 上の UDP ポート 111 に対して、すべてのトラフィックにポリシングを適用する方法を示しています。

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
```

```
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

次の例も同じです。ただし、この例では、ポリサーを VLAN に関連付けます。ポート 2/8 は VLAN 20 に属しています。

注：ポートのQoSをVLANベースのモードに変更します。そのためには、set port qos コマンドを使用します。

このポリサーにより、VLAN ベースの QoS に設定されているその VLAN でのすべてのポートからのトラフィックが評価されます。

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_lmbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_lmbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

次では、DSCP 32 のプロファイル外パケットを廃棄するのではなく、DSCP 0 (ベスト エフォート) にマークダウンしています。

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_lmbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_lmbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

次の例では、スーパーバイザ エンジン 720 のみに対する出力ポリシングの設定が示されています。VLAN 3 のすべての発信 IP トラフィックを全体で 10 Mbps にポリシングする方法が示されています。

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
egress_10mbps rate 10000 burst 20 drop !--- This defines
a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
trust-ipprec aggregate egress_10mbps ip any any !---
This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
This compiles the QoS ACL. set qos acl map egress_pol 3
output !--- This maps the QoS ACL to VLAN 3 in the
output direction.
```

現在のポリシング対象の DSCP マップを表示するには、**show qos maps runtime policed-dscp-map** を使用します。

show qos policer runtime {policer_name | all} をクリックして、ポリサーのパラメータを確認します。ポリサーが関連付けられている QoS ACL を確認することもできます。

注 : Supervisor Engine 1 および 1a では、個々の集約ポリサーに対するポリシングの統計情報を持つことはできません。システムごとのポリシングの統計情報を表示するには、次のコマンドを使用します。

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

マイクロフローのポリシングの統計情報を確認するには、次のコマンドを使用します。

```
Cat6k> (enable) show mls entry qos short
Destination-IP Source-IP Port DstPrt SrcPrt Uptime Age
-----
IP bridged entries:
239.77.77.77 192.168.10.200UDP 63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP 888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628
```

Only out of the profile MLS entries are displayed

```
Cat6k> (enable)
```

スーパーバイザ エンジン II では、ポリサーごとの集約ポリシングの統計情報を **show qos statistics aggregate-policer** コマンドで表示できます。

この例では、トラフィックジェネレータがポート 2/8 に接続されています。宛先ポート 111 で 17 Mbps の UDP トラフィックを送信します。ポリサーがトラフィックの 16/17 をドロップすると、1 Mbps が通過します。

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
```



```

Aggregate policerAllowed packet Packets exceed Packets exceed
                count          normal rate          excess rate
-----
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count          normal rate          excess rate
-----
udp_1mbps58250497331989733198

```

注：許可されるパケットは65増加し、超過パケットは1090増加していることに注意してください。これは 1090 パケットがポリサーによってドロップされたことと、65 パケットが許可されて通過したことを意味します。65 / (1090 + 65) = 0.056、または約1/17を計算できます。したがって、ポリサーは正しく動作します。

Cisco IOS ソフトウェアでのポリシングの設定と監視

Cisco IOS ソフトウェアでのポリシングの設定は、次の手順で行います。

1. ポリサーを定義します。
2. ポリシング対象のトラフィックを選択するための ACL を作成します。
3. ACL と DSCP/IP 優先順位的一方または両方でトラフィックを選択するためのクラス マップを定義します。
4. クラスを使用するサービス ポリシーを定義し、ポリサーを指定したクラスに適用します。
5. ポートまたは VLAN にサービス ポリシーを適用します。

「[CatOS ソフトウェアでのポリシングの設定と監視](#)」セクションと同じ例について検討しますが、ここでは Cisco IOS ソフトウェアを使用します。この例では、トラフィックジェネレータがポート2/8に接続されています。宛先ポート111で17 MbpsのUDPトラフィックを送信します。

Catalyst 6500/6000

```

mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.

```

Cisco IOS ソフトウェアには次の2つのタイプの集約ポリサーがあります。名前付き集約ポリサーとインターフェイス単位の集約ポリサーです。名前付き集約ポリサーでは、適用されるすべてのインターフェイスから結合されたトラフィックに対してポリシングが実行されます。上記の例ではこのタイプが使われています。インターフェイス単位のポリサーでは、適用される各着信イ

インターフェイス上のトラフィックに対して個別にポリシングが実行されます。per-interface ポリサーは、ポリシー マップの設定において定義されます。次に示す例では、インターフェイス単位の集約ポリサーが使用されています。

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit udp any
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
interface.
```

マイクロフロー ポリサーは、インターフェイス単位の集約ポリサーと同様に、ポリシー マップの設定で定義されます。次に示す例では、ホスト 192.168.2.2 から VLAN 2 に送信されるすべてのフローが 100 kbps にポリシングされています。192.168.2.2 からのすべてのトラフィックは、全部で 500 kbps にポリシングされます。VLAN 2 には、インターフェイス fa4/11 と fa4/12 があります。

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 1 permit 192.168.2.2
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
This applies the QoS policy to VLAN 2.
```

次の例は、Supervisor Engine 720の出力ポリシングの設定を示しています。インターフェイス Gigabit Ethernet 8/6のすべての発信トラフィックのポリシングを100 kbpsに設定します。

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
```

```
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
pol_out !--- This attaches the policy to an interface.
```

次の例は、Supervisor Engine 720のユーザごとのポリシングの設定を示しています。ポート1/1の背後にあるユーザからインターネットに向かうトラフィックは、ユーザごとに1 Mbpsにポリシングされます。インターネットからユーザに向けて送信されてくるトラフィックは、ユーザごとに5 Mbpsにポリシングされています。

Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in
```

ポリシングを監視するには、次のコマンドを使用できます。

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0
```

```
bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)
```

```
Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
-----
Gi2/8 1   In  udp_qos    0    1*   No0 127451 2129602
```

```
bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)
```

```
Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
```

Gi2/8 1 In udp_qos 0 1* No0 127755 2134670

注：許可されるパケットは304増加し、超過パケットは5068増加しています。これは 5068 パケットがポリサーによってドロップされたことと、304 パケットが許可されて通過したことを意味します。入力レートが 17 Mbps であるとする、ポリサーはトラフィックの 1/17 を通したことになります。ドロップされたパケットと転送されたパケットを比較すると、次の計算が当てはまることがわかります。 $304 / (304 + 5068) = 0.057$ 、または約1/17。ハードウェアポリシングの精度により、若干の変動が発生する可能性があります。

マイクロフロー ポリシングの統計情報を表示するには、`show mls ip detail` コマンドを使用します。

Orion# `show mls ip detail`

IP Destination	IP Source	Protocol	L4 Ports	Vlan	Xtag	L3-protocol
192.168.3.33	192.168.2.2	udp	555 / 5550			lip
192.168.3.31	192.168.2.2	udp	63 / 630			lip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes

Ports	Encapsulation	RW-Vlan	RW-MACSource	RW-MACDestination	Bytes
Fa4/11 -	----ARPA3	0030.7137.1000	0000.3333.3333	314548	
Fa4/11 -	----ARPA3	0030.7137.1000	0000.2222.2222	314824	

Packets Age Last SeenQoS Police Count ThresholdLeak

Packets	Age	Last Seen	QoS	Police Count	Threshold	Leak
6838	36	18:50:09	0x80	34619762*2^5	3*2^0	
6844	36	18:50:09	0x80	34669562*2^5	3*2^0	

Drop Bucket Use-Tbl Use-Enable

Drop	Bucket	Use-Tbl	Use-Enable
YES	1968	NONO	
YES	1937	NONO	

注：[Police Count]フィールドフローごとのポリシングされたパケットの数を示します。

[関連情報](#)

- [QoS の設定](#)
- [Catalyst 6000 ファミリ スイッチの Quality of Service \(QoS \) について](#)
- [LAN 製品に関するサポート ページ](#)
- [LAN スイッチング テクノロジーに関するサポート ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)