Catalyst 4000 スーパーバイザ エンジン 3 での QoS ポリシングと QoS マーキング

内容

概要
前提条件
要件
使用するコンポーネント
QoS ポリシングと QoS マーキングのパラメータ
Catalyst 4000/4500 IOSベースのスーパーバイザエンジンでサポートされるポリシングおよびマーキング機能
ポリシングの設定と監視
マーキングの設定と監視
Catalyst 6000およびCatalyst 4000/4500 IOSベースのスーパーバイザエンジンでのポリシングとマーキングの比較
関連情報

概要

ポリシング機能では、トラフィック レベルが指定されたプロファイル（コントラクト）内にあるかどうかが判別されます。 ポリシング機能を使用すると、プロファイル外トラフィックを破棄したり、トラフィックを別の Differential Services Code Point（DSCP）値にマークダウンしたりして、強制的に契約したサービス レベルを満たすようにすることができます。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 Class of Service（CoS）も使用します。

ポリシングとトラフィック シェーピングにはともに、トラフィックをプロファイル（コントラクト）内にとどめる機能が、この 2 つは明確に区別する必要があります。 ポリシングはトラフィックをバッファリングしないため、伝搬遅延には影響しません。プロファイル外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、これらのパケットは破棄されるか、または別の QoS レベルでマーキングされます（DSCP マークダウン）。 トラフィック シェーピングは、プロファイル外トラフィックをバッファリングし、トラフィック バーストを平滑化しますが、遅延および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上だけですが、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で適用できます。

Supervisor Engine 3、4、および2+（このドキュメントで以降のSE3、SE4、SE2+）を搭載したCatalyst 4000/4500では、着信方向と発信方向でのポリシングがサポートされています。トラフィック シェーピングもサポートされますが、この文書ではポリシングとマーキングのみを扱います。マーキングとは、パケットの QoS レベルをポリシーに従って変更する処理のことです。

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。

QoS ポリシングと QoS マーキングのパラメータ

ポリシングは、QoS ポリシー マップを定義してこれらをポート（ポートベース QoS）または VLAN（VLAN ベース QoS）に適用することで設定されます。 ポリサーは、レート パラメータとバースト パラメータの他に、インプロファイルとプロファイル外のトラフィックに対するアクションによって定義されます。

サポートされているポリサーには 2 つのタイプがあります。集約とインターフェイス別です。各ポリサーは、複数のポートまたは VLAN に適用できます。

集約ポリサーは、適用されるすべてのポートや VLAN を経由するトラフィックで機能します。たとえば、VLAN 1 および VLAN 3 で Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）トラフィックを 1 Mbps に制限する場合に集約ポリサーを適用します。このようなポリサーの場合、VLAN 1 および VLAN 3 を一緒に使用することによって 1 Mbps の TFTP トラフィックを実現できます。インターフェイス別ポリサーを適用した場合は、VLAN 1 および VLAN 3 の TFTP トラフィックはそれぞれ 1 Mbps に制限されます。

注：入力ポリシングと出力ポリシングの両方がパケットに適用される場合、最も重大な決定が行われます。つまり、入力ポリサーによってパケットの破棄が指定され、出力ポリサーによってパケットのマークダウンが指定された場合は、パケットは破棄されます。表 1 には、パケットが入力ポリサーと出力ポリサーの両方で扱われる場合の、パケットに対する QoS アクションがまとめられています。

表 1：入力ポリシーと出力ポリシーに基づく QoS アクション

	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$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

Catalyst 4000 SE3、SE4、SE2+ QoSハードウェアは、出力ポリサーの後にパケットの実際のマーキングが行われるよう実装されています。これは、入力ポリシーによってパケットが（ポリサーによるマークダウンまたは通常のマーキングによって）再度マーキングされた場合でも、出力ポリシーでは、元の QoS レベルでマーキングされたパケットを参照します。出力ポリシーには、パケットが入力ポリシーによってマーキングされていないように見えます。これは、次のことを意味します。

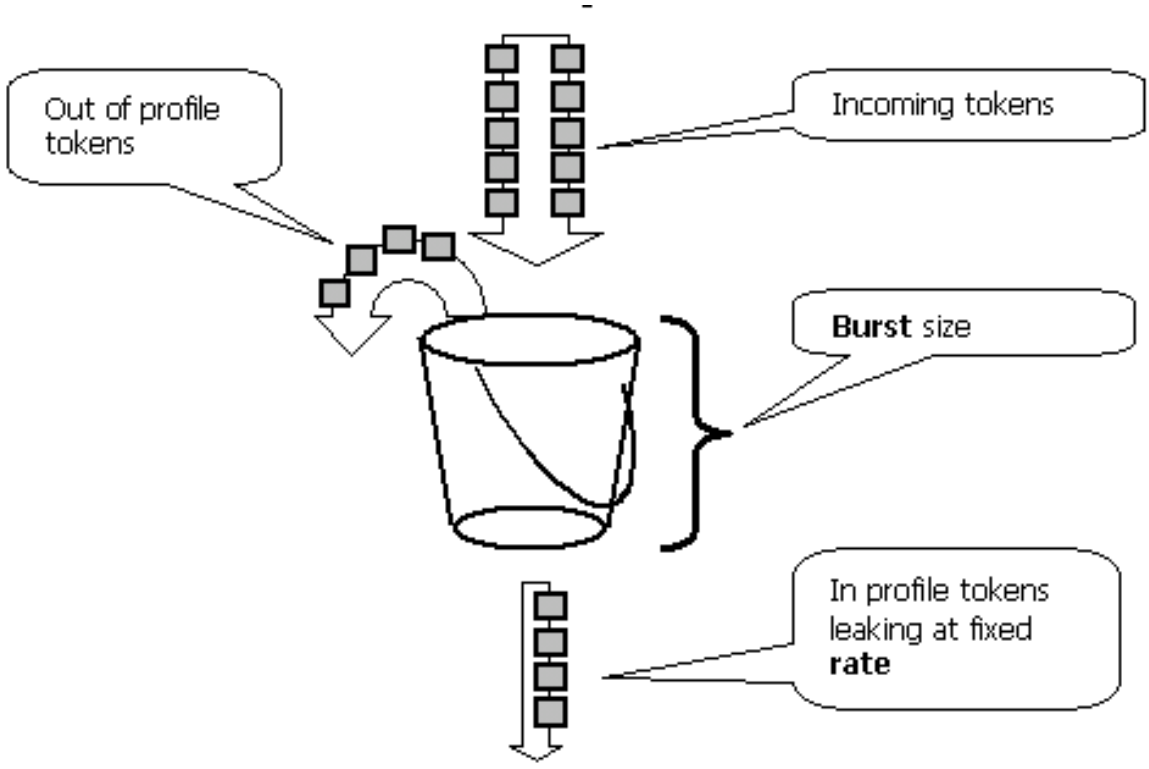
- 出力マーキングによって入力マーキングが上書きされる。

- 出力ポリシーでは、入力マーキングによって変更された新しい QoS レベルを照合できない。

他に次の重要な考慮事項があります。

- 同じポリシー内の同じトラフィック クラス内ではマーキングおよびマークダウンできない。
- 集約ポリサーは、方向別である。つまり、集約ポリサーが入力と出力の両方に適用される場合は、入力と出力の 2 つの集約ポリサーが存在します。
- 集約ポリサーがポリシー内で VLAN および物理インターフェイスに適用される場合は、事実上、VLAN インターフェイス用と物理インターフェイス用の 2 つの集約ポリサーが存在します。現在、集約ポリサーでは VLAN インターフェイスと物理インターフェイスをともにポリシングすることはできません。

Catalyst 4000 SE3、SE4、SE2+のポリシングは、次のモデルが示すように、漏出バケットの概念に準拠しています。着信トラフィックのパケットに対応するトークンは、バケットに配置されます（トークン数 = パケットのサイズ）。 定期的な間隔で、定義されたトークン数（設定されたレートから取得）が、バケットから削除されます。バケットに着信パケットを収容する余裕がない場合は、パケットはプロファイル外と見なされ、設定されたポリシング アクションに基づいて破棄またはマークダウンされます。



トラフィックは、上のモデルで示すように、バケット内でバッファリングされないことに注意が必要です。実際のトラフィックが、バケットを経由して流れることはありません。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際に使用されるだけです。

ポリシングの厳密なハードウェア実装は異なる場合もありますが、機能的には上のモデルに準拠します。

次のパラメータがポリシングの動作を制御しています。

- Rate は、各インターバルでの除去される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。

- Interval では、バケットからトークンが削除される頻度が定義されます。インターバルは、16 ナノ秒 (16 秒 *10-9) に固定されます。 インターバルは変更できません。
- バースト：バケットが一度に保持できるトークンの最大容量が定義されます。

Catalyst 6000とCatalyst 4000 SE3、SE4、SE2+のバーストの違いについては、このドキュメントの最後にある「Catalyst 6000およびCatalyst 4000/4500 IOSベースのスーパーバイザエンジンでのポリシングとマーキングの比較」セクションを参照してください。

ポリサーでは、どの期間 (ゼロから無限) を調査しても、その期間内にポリサーを経由するトラフィックが、

```
<rate> * <period> + <burst-bytes> + <1 packet> bytes
```

を決して超えないことが保証されます。

Catalyst 4000 SE3、SE4、SE2+ QoSハードウェアは、ポリシングに一定の粒度を持ちます。設定されているレートに基づいて、レートからのずれの最大値は、レートの 1.5% になります。

バーストレートを設定する際には、パケット損失に対応するフロー制御メカニズムを実装するプロトコル (TCPなど) を考慮する必要があります。たとえば、TCPは、損失パケットごとにウィンドウを半分に減らします。特定のレートにポリシングされると、有効なリンク使用率は設定されたレートよりも低くなります。バーストを増やすことで、使用率を向上させることができます。このようなトラフィックの適切な開始は、ラウンドトリップ時間(RTT)の間に必要なレートで送信されるトラフィック量の2倍にバーストを設定することです。 同様の理由から、コネクション型トラフィックによってポリサーの動作をベンチマークすることは推奨されません。ポリサーによって許可されたパフォーマンスよりも一般に低いパフォーマンスが示されるためです。

注：コネクショントラフィックは、ポリシングに対しても異なる反応を示す場合があります。たとえば、Network File System (NFS) で使用されるブロックが、複数の User Datagram Protocol (UDP; ユーザ データグラム プロトコル) パケットから構成されることがあります。1 つのパケットの破棄が原因で、多数のパケット (ブロック全体) が再送信される場合があります。

例として、ポリシング レートを 64 Kbps、TCP RTT を 0.05 秒とした TCP セッションのバーストの計算を次に示します。

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

注： <burst>は1つのTCPセッション用であるため、ポリサーを経由する予想セッション数を平均するように拡張する必要があります。これは 1 つの例であり、個々のケースにおいてポリシング パラメータを選択するには、トラフィックとアプリケーションの要件、および使用可能なリソースに対する動作が評価される必要があります。

ポリシング アクションは、パケットの破棄 (drop) またはパケットの DSCP の変更 (マークダウン) のどちらかです。 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 では、パケットが同じ DSCP に再度マーキングされます。つまり、マークダウンは発生しません。

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ークダウンされると、パケットが順序どおりに送信されることがあります。このため、パケットの順序付けが重要な場合は、プロファイル外パケット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た DSCP にマークダウンすることをお勧めします。

Catalyst 4000/4500 IOSベースのスーパーバイザエンジンでサポートされるポリシングおよびマーキング機能

Catalyst 4000 SE3、SE4、SE2+では、入力（着信インターフェイス）と出力（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ています。このスイッチは、1024 入力ポリサーと 1024 出力ポリサーをサポートします。デフォルトの非ポリシング動作では、2 つの入力ポリサーと 2 つの出力ポリサーがシステムで使用されます。

集約ポリサーがポリシー内で VLAN と物理インターフェイスに適用される場合は、追加のハードウェア ポリサー エントリが使用されます。現在、集約ポリサーでは VLAN インターフェイスと物理インターフェイスをともにポリシングすることはできません。これは、将来のソフトウェア リリースで変更される可能性があります。

すべてのソフトウェア バージョンには、ポリシングのサポートが含まれます。Catalyst 4000 は、クラスごとに最大 8 つの有効な match 文をサポートし、ポリシー マップごとに最大 8 つのクラスがサポートされます。有効な match 文を次に示します。

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

注：非IP V4パケットの場合、CoSを信頼するトランキングポートにパケットが着信する場合は、match ip dscp文が唯一の分類方法です。コマンド match ip dscp 内のキーワード ip に惑わされないでください。内部 DSCP が一致しているため、これは IP だけでなくすべてのパケットに適用されます。CoS を信頼するようにポートが設定されている場合、CoS は L2（802.1Q または ISL タグ付き）フレームから取得され、CoS から DSCP QoS へのマップを使用して内部 DSCP に変換されます。その後、この内部 DSCP 値は、match ip dscp を使用してポリシー内で照合されます。

有効なポリシー アクションを次に示します。

- police
- set ip dscp
- set ip precedence
- trust dscp
- trust cos

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。分類では、トラフィックは定義された基準に基づいて QoS 処理のために個々のクラスに分けられます。IP 優先順位または DSCP を照合するため、対応する着信インターフェイスは、trusted モードに設定される必要があります。このスイッチは、CoS の信頼、DSCP の信頼、および信頼されないインターフェイスをサポートします。信頼によって、パケットの QoS レベルの取得元となるフィールドが指定されます。

CoS を信頼する場合、QoS レベルは ISL の L2 ヘッダーまたは 802.1Q のカプセル化されたパケットから取得されます。DSCP を信頼する場合、このスイッチはパケットの DSCP フィールドから QoS レベルを取得します。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 の信頼は、IP V4 パケットに対してだけ有効です。

インターフェイスが信頼されない場合は（これは、QoS が有効化される際のデフォルト）、内部 DSCP は対応するインターフェイスの設定可能なデフォルトの CoS または DSCP から取得され

ます。デフォルトの CoS または DSCP が設定されていない場合は、デフォルト値はゼロ（0）になります。 パケットの元の QoS レベルが決定されると、これは内部 DSCP にマップされます。内部 DSCP は、マーキングまたはポリシングによって保持または変更されます。

パケットによって QoS 処理が実行された後に、QoS レベルのフィールド（IP 用の IP DSCP フィールド内部、および ISL/802.1Q ヘッダーが存在する場合はその内部）は、内部 DSCP から更新されます。

パケットの信頼された QoS メトリックを内部 DSCP に変換（またはその逆に変換）するために使用される特別なマップがあります。これらのマップを次に示します。

- ポリシングされたDSCPへの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されます。
- DSCP から CoS：内部 DSCP から CoS レベルを取得して、発信パケットの ISL/802.1Q ヘッダーを更新するために使用されます。
- CoS から DSCP：インターフェイスが trust CoS モードの場合は、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されます。

インターフェイスが trust CoS モードの場合は、発信 CoS は常に着信 CoS と同じです。これは、Catalyst 4000 SE3、SE4、SE2+でのQoS実装に固有です。

ポリシングの設定と監視

IOS でのポリシングの設定には、次のステップが必要です。

1. ポリサーを定義します。
2. ポリシングするトラフィックの選択基準を定義します。
3. クラスを使用し、ポリサーを特定のクラスに適用して、サービスポリシーを定義します。
4. ポートまたは VLAN にサービスポリシーを適用します。

次の例について考えます。宛先ポート111で17 MbpsのUDPトラフィックを送信するポート5/14にトラフィックジェネレータが接続されています。このトラフィックを1 Mbpsまでポリシングし、過剰なトラフィックを廃棄する必要があります。

```
! enable qos
qos
! define policer, for rate and burst values, see 'policing parameters
qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
exceed-action
drop
! define ACL to select traffic
access-list 111 permit udp any any eq 111
! define traffic class to be policed
class-map match-all cl_test
match access-group 111
! define QoS policy, attach policer to traffic class
policy-map po_test
class cl_test
police aggregate pol_1mbps
! apply QoS policy to an interface
interface FastEthernet5/14
switchport access vlan 2
! switch qos to vlan-based mode on this port
qos vlan-based
! apply QoS policy to an interface
```

```
interface Vlan 2
service-policy output po_test
!
```

ポートが VLAN ベース の QoS モードであり、対応する VLAN に適用されるサービスポリシーがない場合、スイッチは、物理ポートに適用されるサービスポリシーがあればそれに従います。これにより、ポートベースと VLAN ベースの QoS を結合するための柔軟性が追加されます。

サポートされているポリサーには 2 つのタイプがあります。名前付き集約とインターフェイス別です。名前付き集約ポリサーでは、これが適用されるすべてのインターフェイスからのトラフィックを合わせてポリシングします。上の例では、名前付きポリサーが使用されています。インターフェイス別ポリサーでは、名前付きポリサーとは異なり、これが適用される各インターフェイス上で個別にトラフィックがポリシングされます。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。インターフェイス別集約ポリサーを使用した次の例について考えます。

```
! enable qos
qos
! define traffic class to be policed
class-map match-all cl_test2
match ip precedence 3 4
! define QoS policy, attach policer to traffic class
policy-map po_test2
class cl_test2
! per-interface policer is defined inside the policy map
police 512k 1000 conform-action transmit exceed-action drop
interface FastEthernet5/14
switchport
! set port to trust DSCP - need this to be able to match to incoming IP precedence
qos trust dscp
! switch to port-based qos mode
no qos vlan-based
! apply QoS policy to an interface
service-policy input po_test2
```

次のコマンドは、ポリシング動作を監視するために使用されます。

```
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400026 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166067574 bytes Exceed: 5268602114 bytes
class-map: class-default (match-any)
13312 packets
match: any
13312 packets
Yoda#show policy-map interface FastEthernet5/14
FastEthernet5/14
service-policy input: po_test2
class-map: cl_test2 (match-all)
7400138 packets
match: ip precedence 3 4
police: Per-interface
Conform: 1166088574 bytes Exceed: 5268693114 bytes
class-map: class-default (match-any)
13312 packets
```

```
match: any
13312 packets
```

class-map の近くにあるカウンタでは、対応するクラスに一致しているパケット数がカウントされます。

次の実装に固有の考慮事項に注意してください。

- クラス別パケット カウンタは、インターフェイス別ではない。つまり、このクラスがサービスポリシー内で適用されるすべてのインターフェイス間で、クラスが一致するすべてのパケットがカウントされます。
- ポリサーではパケットカウンタは維持されず、バイト カウンタだけがサポートされます。
- 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。
- カウンタは定期的に更新される。上記のコマンドを高速で継続的に繰り返し実行すると、カウンタが表示されることがあるかもしれません。

マーキングの設定と監視

マーキングの設定は次の手順で行います。

1. アクセスリスト、DSCP、IP 優先順位などのトラフィックを分類するための基準を定義します。
2. 先に定義した基準を使用して分類されるトラフィック クラスを定義します。
3. 定義したクラスに対するマーキング アクションやポリシング アクションを含むポリシー マップを作成します。
4. 対応するインターフェイス上で trust モードを設定します。
5. ポリシー マップをインターフェイスに適用します。

次の例では、IP precedence 3の着信トラフィックを、IP precedence 6にマッピングされたホスト192.168.196.3 UDPポート777に送ります。他のすべてのIP precedence 3トラフィックは1 Mbpsにポリシングされ、超過トラフィックはIP precedence 2にマークダウンされます。

```
! enable QoS globally
qos
! define ACL to select UDP traffic to 192.168.196.3 port 777
ip access-list extended acl_test4
permit udp any host 192.168.196.3 eq 777
! define class of traffic using ACL and ip precedence matching
class-map match-all cl_test10
match ip precedence 3
match access-group name acl_test4
! all the remaining ip precedence 3 traffic will match this class
class-map match-all cl_test11
match ip precedence 3
! define policy with above classes
policy-map po_test10
class cl_test10
! mark traffic belonging to class with ip precedence 6
set ip precedence 6
class cl_test11
! police and mark down all other ip precedence 3 traffic
police 1 mbps 1000 exceed-action policed-dscp-transmit
!
```

```
! adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16
qos map dscp policed 24 to dscp 16
!
interface FastEthernet5/14
! set interface to trust IP DSCP
qos trust dscp
! apply policy to interface
service-policy input po_test10
!
```

sh policy interfaceコマンドは、マーキングを監視するために使用します。出力と実装の例は、上記のポリシング設定で説明しています。

Catalyst 6000およびCatalyst 4000/4500 IOSベースのスーパーバイザエンジンでのポリシングとマーキングの比較

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

関連情報

- QoS の概要と設定
- テクニカルサポート - Cisco Systems