Catalyst 6500/6000系列交換器上的QoS管制

目錄

簡介

網路上的QoS策略確定網路流量是否在指定的配置檔案（合約）內。 這可能會導致超出設定檔的流量捨棄或降級到另一個區別服務代碼點(DSCP)值，以強制實施約定服務等級。（DSCP是衡量幀的QoS級別的指標。）

請勿將流量管制與流量整形混淆。兩者都確保流量保持在設定檔（合約）內。 管制流量時，不會緩衝超出設定檔的資料包。因此，您不影響傳輸延遲。您可以丟棄流量或將其標籤為較低QoS級別（DSCP降級）。 相反，在流量整形中，您可以緩衝超出配置檔案的流量，並對突發流量進行平滑。這會影響延遲和延遲的變化。您只能對出站介面應用流量調節。您可以在入站和出站介面上應用管制。

Catalyst 6500/6000原則功能卡(PFC)和PFC2僅支援輸入管制。PFC3同時支援入口和出口策略。Catalyst 6500/7600系列的某些WAN模組(例如光纖服務模組(OSM)和FlexWAN模組)僅支援流量調節。有關詳細資訊，請參閱Cisco 7600系列路由器模組配置說明

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

QoS管制引數

要設定管制，您可以定義管制器並將其應用於埠（基於埠的QoS）或VLAN（基於VLAN的QoS）。每個策略器都定義配置內和配置外流量的名稱、型別、速率、突發和操作。Supervisor引擎II上的策略器還支援超額速率引數。有兩種策略器：微流和聚集。

- Microflow — 按流量分別管制每個應用的埠/VLAN的流量。
- Aggregate — 管制所有應用的埠/VLAN的流量。

每個監察器可應用於多個埠或VLAN。使用以下引數定義流：

- 源IP地址
- 目的IP地址
- 第4層通訊協定（例如使用者資料包通訊協定[UDP]）
- 源埠號
- 目的地連線埠號碼

可以說，與特定一組已定義引數匹配的資料包屬於同一流。（這基本上與NetFlow交換使用的流量概念相同。）

例如，如果您配置微流監察器，將VLAN 1和VLAN 3上的TFTP流量限製為1 Mbps，則對於VLAN 1中的每個流允許1 Mbps，對於VLAN 3中的每個流允許1 Mbps。換句話說，如果VLAN 1中有三個流，而VLAN 3中有四個流，則微流監察器允許這些流中的每一個都為1 Mbps。如果設定聚合管制器，則會將VLAN 1和VLAN 3上合併的所有流量的TFTP流量限製為1 Mbps。

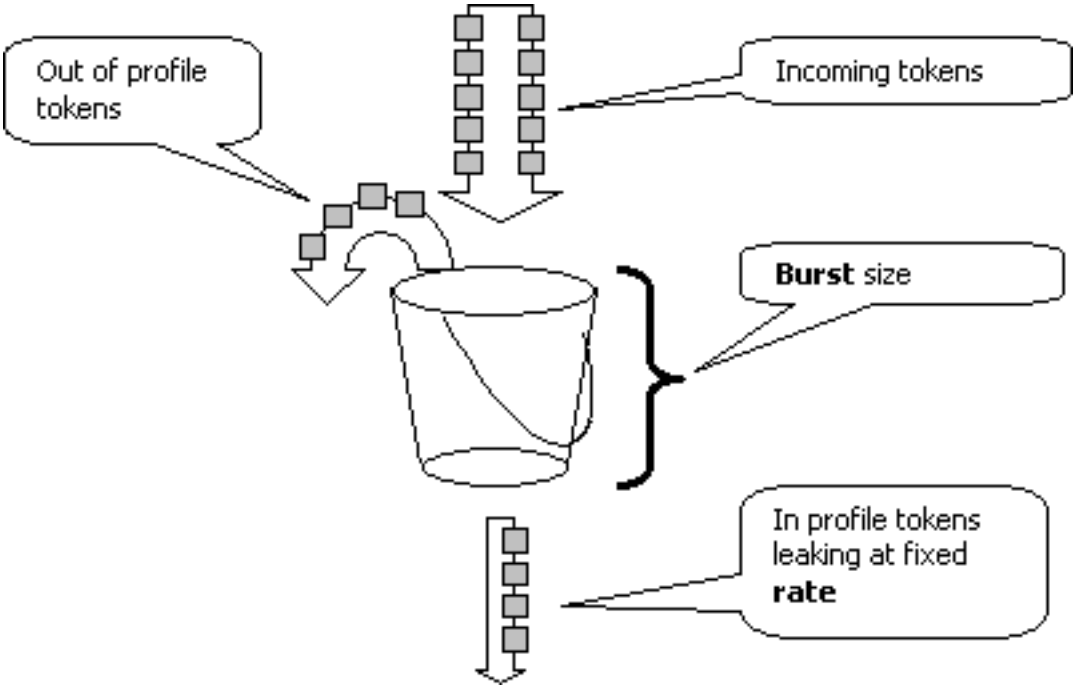
如果同時應用聚合和微流管制器，則QoS始終採取管制器指定的最嚴厲的操作。例如，如果一個管制器指定丟棄資料包，而另一個管制器指定標籤該資料包，則丟棄該資料包。

預設情況下，微流管制器僅對路由（第3層[L3]）流量起作用。要管制橋接（第2層[L2]）流量，您需要啟用橋接微流量管制。在Supervisor引擎II上，即使是L3微流管制，也需要啟用橋接微流管制。

策略感知協定。所有流量分為三種型別：

- IP
- 網際網路封包交換(IPX)
- 其他

根據「漏桶」概念，在Catalyst 6500/6000上實施管制。與入站流量資料包對應的令牌被放入桶中。（每個令牌代表一個位，因此一個大資料包所代表的令牌比一個小資料包更多。）每隔一定時間，會從儲存桶中取出指定數量的令牌並在傳送過程中傳送。如果儲存桶中沒有位置容納入站資料包，則認為這些資料包超出配置檔案。系統會根據配置的策略操作刪除或標籤它們。



注意：流量不會快取在桶中，因為流量可能出現在上圖中。實際流量根本不會通過儲存桶；bucket僅用於決定資料包是位於配置檔案中還是位於配置外。

計算引數

以下幾個引數用於控制令牌桶的操作：

- **Rate** — 定義在每個間隔移除的令牌數。這有效地設定了管制速率。低於該速率的所有流量都視為配置內。
- **Interval** — 定義令牌從桶中刪除的頻率。間隔固定為0.00025秒，因此令牌每秒從桶中移除4,000次。不能更改間隔。
- **突發**(Burst) — 定義儲存段在任一時間可以容納的最大令牌數。要維持指定的流量速率，突發速率應不小於速率與時間間隔的乘積。另一個考慮事項是，最大大小的資料包必須適合儲存桶。

要確定突發引數，請使用以下等式：

- 突發量=（速率[bps]）* 0.00025 [sec/interval])或*（最大資料包大小[位]），取兩者中較大者。*

例如，如果要計算在乙太網絡上保持1 Mbps的速率所需的最小突發值，則速率定義為1 Mbps，而最大乙太網資料包大小為1518位元組。等式為：

- 突發量=(1,000,000 bps * 0.00025)或（1518位元組* 8位/位元組）= 250或12144。

較大的結果為12144，您將舍入為13 kbps。

注意：在Cisco IOS®軟體中，原則速率以位每秒(bps)定義，而Catalyst OS(CatOS)中則為kbps。此外，在Cisco IOS軟體中，猝發速率以位元組定義，而不是CatOS中的千位元。

註：由於硬體策略粒度，準確的速率和突發量將舍入到最接近的支援值。確保突發值不小於最大大小資料包。否則，大於突發大小的所有資料包都會被丟棄。

例如，如果您嘗試在Cisco IOS軟體中將突發量設定為1518，它將被舍入為1000。這會導致丟棄所有大於1000位元組的幀。解決方案是將突發配置為2000。

設定突發速率時，請考慮某些通訊協定（例如TCP）實作對封包遺失作出反應的流量控制機制。例

如，TCP將每個丟失資料包的視窗減少一半。因此，當管制到一定速率時，有效鏈路利用率低於配置的速率。您可以增加突發量，以實現更好的利用率。此類流量的一個良好開端是突發大小的兩倍。（在本示例中，突發大小從13 kbps增加到26 kbps）。 然後，監控績效，並在必要時做出進一步調整。

出於同樣的原因，建議不要使用面向連線的流量來設定監察器操作的基準。這通常顯示比監察器所允許的效能更差。

警察行動

如簡介所述，策略器可以對超出配置檔案的資料包執行以下兩種操作之一：

- 捨棄封包(組態中的`drop`引數)
- 將資料包標籤為較低的DSCP(配置中的`policed-dscp`引數)

要標籤資料包，必須修改策略的DSCP對映。預設情況下，策略化的DSCP設定為將資料包重新標籤到同一個DSCP。（不發生降級。）

注意：如果將「超出配置檔案」的資料包降級為對映到與原始DSCP不同的輸出隊列的DSCP，則某些資料包可能會按順序傳送。因此，如果資料包的順序非常重要，建議將超出配置檔案的資料包標籤為對映到與內配置檔案的資料包對映到同一輸出隊列的DSCP。

在支援超額速率的Supervisor引擎II上，可能有兩個觸發器：

- 當流量超過正常速率時
- 當流量超過超額速率時

應用超額速率的一個示例是標籤超出正常速率的資料包，並丟棄超出超額速率的資料包。

Catalyst 6500/6000支援的管制功能

如簡介所述，Supervisor引擎1a上的PFC1和Supervisor引擎2上的PFC2僅支援輸入（入站介面）管制。Supervisor Engine 720上的PFC3同時支援輸入和輸出（傳出介面）管制。

Catalyst 6500/6000最多支援63個微流監察器和最多1023個聚合監察器。

Supervisor Engine 1a支援輸入管制，從CatOS版本5.3(1)和Cisco IOS軟體版本12.0(7)XE開始。

注意：使用Supervisor引擎1a進行策略管制時需要PFC或PFC2子卡。

Supervisor Engine 2支援輸入管制，從CatOS版本6.1(1)和Cisco IOS軟體版本12.1(5c)EX開始。Supervisor引擎II支援超額速率管制引數。

使用分散式轉發卡(DFC)的配置僅支援基於埠的管制。此外，聚合監察器僅按轉發引擎而不是按系統計算流量。DFC和PFC都是轉發引擎；如果模組（線卡）沒有DFC，則使用PFC作為轉發引擎。

Supervisor Engine 720的管制功能更新

註：如果您不熟悉Catalyst 6500/6000 QoS管制，請務必閱讀本檔案的QoS管制引數和Catalyst 6500/6000支援的管制功能。

Supervisor Engine 720引入了以下新的QoS管制功能：

- **出口管制**。Supervisor 720支援埠或VLAN介面上的入口管制。它支援埠或L3路由介面上的出口管制（對於Cisco IOS系統軟體）。 VLAN中的所有埠都會在出口上受到管制，而不考慮埠QoS模式（無論是基於埠的QoS還是基於VLAN的QoS）。 輸出上不支援微流管制。本文檔的在CatOS軟體中配置和監控策略部分和在Cisco IOS軟體中配置和監控策略部分提供了示例配置。
- **每使用者微流量管制**。Supervisor 720支援增強微流策略，稱為每使用者微流策略。只有Cisco IOS系統軟體支援此功能。它允許您為給定介面後的每個使用者（每個IP地址）提供一定的頻寬。這可以通過在服務策略中指定流掩碼來實現。流掩碼定義用於區分流的資訊。例如，如果指定僅源流掩碼，則來自一個IP地址的所有流量都視為一個流。使用此技術，可以管制某些介面（其中配置了相應的服務策略）上的每使用者流量；在其他介面上，您繼續使用預設流掩碼。在給定時間系統中最多可以有兩個不同的QoS流掩碼處於活動狀態。只能將一個類與一個流掩碼相關聯。一個策略最多可以有兩個不同的流掩碼。

Supervisor引擎720上的另一個重要的策略更改是，它可以按幀的L2長度計算流量。這與Supervisor Engine 2和Supervisor Engine 1不同，後者按L3長度計算IP和IPX幀。在某些應用中，L2和L3的長度可能不一致。一個示例是大L2幀內的小L3資料包。在這種情況下，與Supervisor引擎1和Supervisor引擎2相比，Supervisor引擎720顯示的管制流量速率可能略有不同。

在CatOS軟體中設定和監控管制

CatOS的管制設定包括三個主要步驟：

1. 定義監察器 — 正常流量速率、超額速率（如果適用）、突發和管制操作。
2. 建立QoS ACL以選擇要管制的資料流，並將管制器附加到此ACL。
3. 將QoS ACL應用於必要的埠或VLAN。

此範例顯示如何管制連線埠2/8上前往UDP連線埠111的所有流量。

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.*

下一個例子是相同的；但是在本範例中，您將監察器連線到VLAN。連接埠 2/8 屬於 VLAN 20.

注意：您需要將埠QoS更改為VLAN模式。使用**set port qos**命令執行此操作。

此管制器評估來自為基於VLAN的QoS配置的VLAN中所有埠的流量：

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_vlan dscp 0 aggregate udp_1mbps 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.
```

接下來，不要使用DSCP 32丟棄超出配置檔案的資料包，而是將其標籤為DSCP 0（盡力而為）。

Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps 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_1mbps 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.
```

此範例僅顯示監督器引擎720的出口管制組態。它顯示如何將VLAN 3上的所有傳出IP流量管製為10 Mbps的聚合。

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.
```

使用**show qos maps runtime policed-dscp-map**檢視當前管制的DSCP對映。

使用**show qos policer runtime {*policer_name* | all}**驗證監察器的引數。您還可以看到管制器所連線的QoS ACL。

注意：使用Supervisor Engine 1和1a時，無法擁有單個聚合監察器的策略統計資訊。要檢視每個系統的策略統計資訊，請使用以下命令：

```
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
```

要檢查微流策略統計資訊，請使用以下命令：

```
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)
```

使用Supervisor引擎II，可以使用**show qos statistics aggregate-policer**命令檢視每個監察器的聚合策略統計資訊。

在本例中，流量產生器連線到連線埠2/8。其傳送的UDP流量為17 Mbps，目的地連線埠為111。您預期管制器會捨棄流量的16/17，因此1 Mbps應通過：

```
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
```

注意：請注意，允許的資料包增加了65，而多餘的資料包增加了1090。這表示管制器已丟棄1090個封包並允許65個封包通過。您可以計算65 /(1090 + 65)= 0.056，或大約1/17。因此，監察器工作正常。

在Cisco IOS軟體中設定和監控管制

Cisco IOS軟體中的原則制定設定包括下列步驟：

1. 定義監察器。
2. 建立一個ACL以選擇要強制控制的流量。
3. 定義類對映以選擇具有ACL和/或DSCP/IP優先順序的流量。
4. 定義使用類的服務策略，並將策略器應用於指定的類。

5. 將服務策略應用於埠或VLAN。

請考慮與在CatOS軟體中設定和監控管制一節中提供的範例相同的範例，但目前的範例是Cisco IOS軟體。在本範例中，連線埠2/8的流量產生器。它透過目的地連線埠111傳送17 Mbps的UDP流量：

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軟體中有兩種型別的聚合管制器：**命名**和**每個介面**。命名的聚合管制器會管制從應用該策略的所有介面合併的流量。以上示例中使用的型別是。每個介面監察器會在其應用到的每個入站介面上分別管制流量。在策略對映配置中定義每個介面的策略器。請考慮以下示例，該示例具有每個介面的聚合管制器：

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.
```

Microflow策略器是在策略對映配置中定義的，每個介面的聚合策略器也是如此。在下面的示例中，來自主機192.168.2.2且進入VLAN 2的每個流都管製為100 kbps。所有來自192.168.2.2的流量都被管製為500 kbps的聚合流量。VLAN 2包括介面fa4/11和fa4/12:

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.
```

以下範例顯示Supervisor Engine 720的出口管制組態。該組態會建立介面千兆位乙太網路8/6到100 kbps上所有傳出流量的管制：

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.
```

以下範例顯示Supervisor Engine 720的每使用者原則管制組態。從連線埠1/1背後的使用者傳入Internet的流量會原則控制為每使用者1 Mbps。從Internet流向使用者的流量被控制為每使用者5 Mbps:

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
```

要監控管制，可以使用以下命令：

```
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
```

註：允許的資料包增加了304，多餘的資料包增加了5068。這表示管制器已丟棄5068個封包並允許304個封包通過。假定輸入速率為17 Mbps，監察器應該會通過1/17的流量。如果比較丟棄和轉發的資料包，您會發現情況確實如此：304 /(304 + 5068)= 0.057，或大約1/17。由於硬體策略粒度不同，可能存在一些細微差異。

對於微流策略統計資訊，請使用**show mls ip detail**命令：

```
Orion# show mls ip detail
IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
--------------+---------------+--------+-------------+----+----+-----------+
192.168.3.33192.168.2.2udp555 / 5550   1ip
192.168.3.3192.168.2.2udp63 / 630   1ip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
--------------+-------------+-------+--------------+-----------------+------------+
Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

Packets     Age   Last SeenQoS      Police Count ThresholdLeak
------------+-----+---------+-----------+------------+---------+-----------+
6838     36   18:50:090x80  34619762*2^5 3*2^0
6844     36   18:50:090x80  34669562*2^5 3*2^0

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

注意：Police Count顯示每個流的受管制資料包數。

相關資訊

- 配置QoS
- 瞭解Catalyst 6000系列交換器上的服務品質
- LAN 產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems