Catalyst 6500/6000 系列交换机上的 QoS 策略

目录

简介

网络上的 QoS 管制可确定网络数据流是否在指定配置文件（合同）的规定范围内。 这可能会导致将超出配置文件规定的数据流丢弃或降级到另一差分服务代码点 (DSCP) 值，以强制执行约定服务级别。（DSCP 是衡量帧的 Qos 级别的一种指标。）

请勿将流量管制与流量整形相混淆。流量管制和流量整形均可确保数据流处在配置文件（合同）规定范围内。 管制数据流时，不对超出配置文件规定的数据包进行缓冲。因此，不会影响传输延迟。可将数据流丢弃或使用较低的 QoS 级别对其进行标记（DSCP 降级）。 相比之下，在流量整形时，将对超出配置文件规定的数据流进行缓冲，并使突发数据流更为平缓。这会影响延迟和延迟变化。仅可在出站接口上应用流量整形。在入站和出站接口上均可应用流量管制。

Catalyst 6500/6000策略功能卡(PFC)和PFC2仅支持入口策略。PFC3 同时支持入口和出口管制。流量整形仅在Catalyst 6500/7600系列的某些WAN模块(如光纤服务模块(OSM)和FlexWAN模块)上受支持。有关详细信息，请参阅 Cisco 7600 系列路由器模块配置说明

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

QoS 策略参数

要设置管制，请定义监察器，并将其应用到端口（基于端口的 QoS）或 VLAN（基于 VLAN 的 QoS）。 每个策略器都为要求内和要求外的流量定义名称、类型、速率、突发速率以及采取的操作等。Supervisor 引擎 II 上的策略还支持超额速率参数。有两种类型的策略器：微流 (microflow) 和集合 (aggregate)：微流和聚合。

- **微流监察器 - 基于每个数据流单独管制应用监察器的每个端口/VLAN 上的数据流。**
- **聚合监察器 - 横跨应用监察器的所有端口/VLAN 对数据流进行管制。**

每个监察器均可应用于多个端口或 VLAN。可使用以下参数定义流：

- 源 IP 地址
- 目的 IP 地址
- 第 4 层协议（如用户数据报协议 [UDP]）
- 源端口号
- 目的端口号

可以这样说，与同一组已定义参数相匹配的数据包将被视为属于相同的流。（此处的流概念与 NetFlow 交换所采用的流概念本质上相同。）

例如，如果配置微流监察器，让其将 VLAN 1 和 VLAN 3 上的 TFTP 数据流的速率限制为 1 Mbps，则会允许 VLAN 1 上的每个流的速率为 1 Mbps，也允许 VLAN 3 上的每个流的速率为 1 Mbps。换言之，如果在 VLAN 1 上存在三个流，在 VLAN3 上存在四个流，则微流监察器将允许这些流中每个流的速率都为 1 Mbps。如果配置聚合监察器，它会将 VLAN 1 和 VLAN3 上所有流加起来的总 TFTP 数据流限制为 1 Mbps。

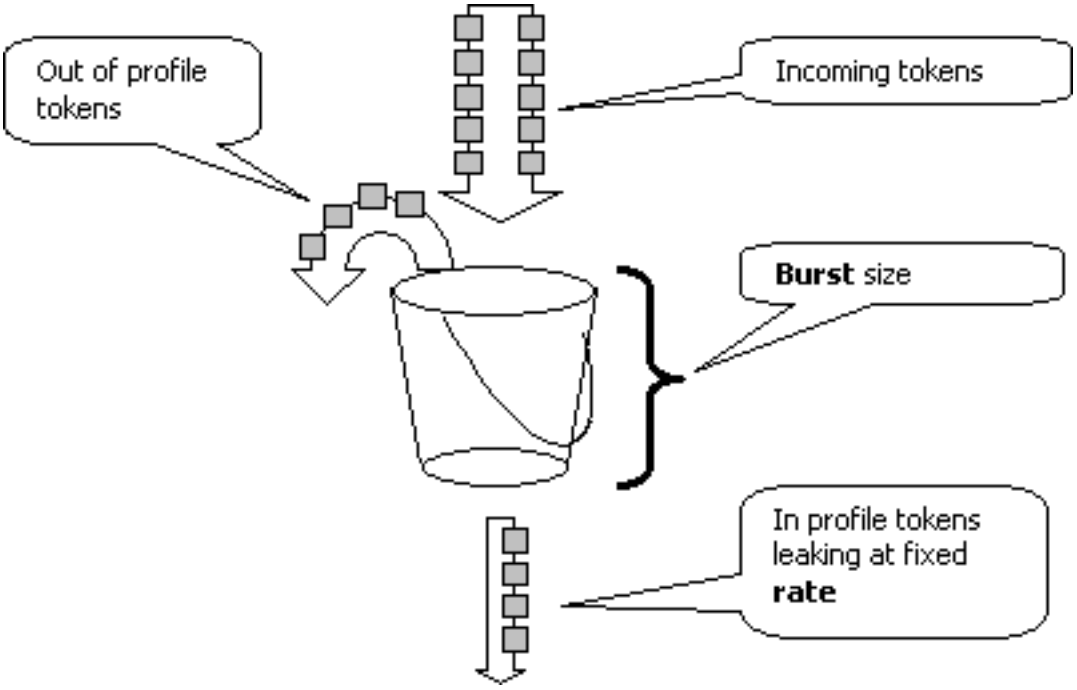
如果同时应用聚合监察器和微流监察器，则 QoS 将始终执行监察器所指定的最严格的措施。例如，如果一个监察器指定丢弃数据包，但另一个监察器指定将数据包降级，则数据包将会被丢弃。

默认情况下，微流监察器仅对路由的（第 3 层 [L3]）数据流起作用。要对桥接的（第 2 层 [L2]）数据流也进行管制，需要启用桥接微流管制。在 Supervisor 引擎 II 上，您甚至需要为 L3 微流管制启用桥接微流管制。

管制是感知协议的。所有数据流分为三种类型：

- IP
- 互联网分组交换 (IPX)
- Other（其他）

在 Catalyst 6500/6000 上，管制是根据“漏桶”概念实施的。与入站数据包对应的令牌被置于桶中。（每个令牌表示一个位，因此，与小数据包相比，大数据包由更多的令牌表示。）在定期的时间间隔内，一定数量的令牌数将从桶中取出并被发送。如果桶中没有容纳入站数据包的地方，则认为这些数据包超出配置文件范围。根据配置的管制操作，这些数据包将被丢弃或者降级。



注意：流量不会缓冲在桶中，因为它可能出现在上图中。实际数据流根本不会通过桶；桶仅用于确定数据包是否符合或超出配置文件规定。

计算参数

有多个参数可用来控制令牌桶的运行，如以下所示：

- **速率 - 定义了在每个时间间隔中删除的令牌数。**这样就能够有效地设置策略速率。低于速率的所有流量都被视为是符合配置要求的。
- **时间间隔 - 定义了从桶中删除令牌的频率。**时间间隔固定为 0.00025 秒，因此每秒从桶中删除令牌 4,000 次。时间间隔不能更改。
- **突发 - 定义了任何时候桶中可以容纳的最大令牌数。**要维持指定的数据流速率，突发不应小于速率与时间间隔的乘积。另外一种考虑就是最大尺寸的数据包也必须能够置入桶内。

要确定突发参数，请使用以下等式：

- 突发 =（速率 [bps] * 0.00025 [秒/时间间隔]）*或（最大数据包大小 [位]），取二者中较大的值*。

例如，如果希望计算维持以太网上 1 Mbps 的速率所需的最小突发值，则速率定义为 1 Mbps，最大以太网数据包大小为 1518 字节。等式为：

- 突发速率 =（1,000,000bps*0.00025）或（1518字节* 8位/字节）= 250 或 12144

两者中较大的结果为 12144，可将其舍入为 13 kbps。

注意：在Cisco IOS®软件中，管制速率以比特/秒(bps)定义，而在Catalyst OS(CatOS)中则以kbps定义。 此外，在 Cisco IOS 软件中以字节为单位定义突发速率，而在 CatOS 中则以千比特为单位定义。

注意：由于硬件策略粒度，精确速率和突发量会四舍五入到最接近的支持值。请确保突发值不小于最大大小的数据包。否则，大于突发值的所有数据包都将被丢弃。

例如，如果您尝试在 Cisco IOS 软件中将突发值设置为 1518，则该值将舍入为 1000。这将导致大于 1000 字节的所有帧都被丢弃。解决方案是将突发速率配置为 2000。

配置突发速率时，请考虑有些协议（如 TCP）会实施对数据包丢失作出反应的流控制机制。例如，TCP 会为每个丢失的数据包将窗口大小减小一半。因此，通过限制到特定速率进行管制时，有效的链路利用率将低于配置的速率。您可以增加突发值以实现更佳的利用率。对于这样的数据流，将突发值加倍是一个不错的开端。（在本示例中，突发大小将从 13 kbps 增加到 26 kbps）。 然后，监控性能并根据需要进行进一步的调整。

出于同样的原因，不建议使用面向连接的数据流来衡量监察器操作。通常这样显示的性能会比监察器所允许的性能要更低。

管制操作

正如我们在简介中所提到的，策略器可以对超出配置规定的数据包采取两种措施中的一种：

- 丢弃数据包（配置中的 `drop`
- 将数据包降级为更低的 DSCP（配置中的 `policed-dscp`

要将数据包降级，必须修改管制 DSCP 映射。默认情况下，策略DSCP设置为将数据包重新标记到同一DSCP。（不发生降级。）

注意：如果“超出配置”数据包被降级到映射到与原始DSCP不同的输出队列的DSCP，则某些数据包可能会无序发送。因此，如果数据包的顺序十分重要，则建议将“超出配置文件规定”的数据包降级到这样一个 DSCP，该 DSCP 映射到与“符合配置文件规定”的数据包映射到的相同输出队列中。

在Supervisor 引擎 II 上可以支持超额速率，有两种触发器可用：

- 当流量超出正常速率
- 当流量超过超额速率

有关超额速率应用的一个示例是将超过正常速率的数据包降级，而将超过超额速率的数据包丢弃。

Catalyst 6500/6000 支持的管制功能

如简介中所述，Supervisor 引擎 1a 上的 PFC1 和 Supervisor 引擎 2 上的 PFC2 仅支持入口（入站接口）管制。Supervisor 引擎 720 上的 PFC3 同时支持入口和出口（出站接口）管制。

Catalyst 6500/6000 最多支持 63 个微流监察器和 1023 个聚合监察器。

从 CatOS 版本 5.3(1) 和 Cisco IOS 软件版本 12.0(7)XE 开始，Supervisor 引擎 1a 支持入口管制。

注意：使用Supervisor引擎1a进行策略管制需要PFC或PFC2子卡。

从 CatOS 版本 6.1(1) 和 Cisco IOS 软件版本 12.1(5c)EX 开始，Supervisor 引擎 2 支持入口管制。Supervisor 引擎 II 支持超额速率管制参数。

使用分布式转发卡(DFC)的配置仅支持基于端口的策略。此外，聚合监察器仅基于每个转发引擎而不是基于每个系统对数据流进行计数。DFC 和 PFC 都是转发引擎；如果模块（板卡）没有 DFC，则使用 PFC 作为转发引擎。

Supervisor 引擎 720 的管制功能更新

注意：如果您不熟悉Catalyst 6500/6000 QoS策略，请务必阅读本文档的QoS策略参数和Catalyst 6500/6000支持的策略功能部分。

Supervisor 引擎 720 引入了以下新的 QoS 管制功能：

- **出口管制**。Supervisor 720 支持端口或 VLAN 接口上的入口管制。它也支持端口或 L3 路由接口上的出口管制（使用 Cisco IOS 系统软件的情况下）。 无论端口为何种 Qos 模式（是基于端口的 Qos 还是基于 VLAN 的 Qos），VLAN 中的所有端口均在出口受管制。 出口上不支持微流管制。本文档的配置和监控 CatOS 软件中的管制部分及配置和监控 Cisco IOS 软件中的管制部分提供了配置示例。
- **每用户微流管制**。Supervisor 720 支持称为每用户微流管制的微流管制增强功能。此功能仅在 Cisco IOS 系统软件上受支持。它允许您为给定接口后的每个用户（每个IP地址）提供特定带宽。这是通过在服务策略内指定流掩码来实现的。流掩码定义了使用哪些信息来区分不同的流。例如，如果指定了“仅源地址”流掩码，则会认为来自一个 IP 地址的所有数据流属于一个流。使用此技术可在某些接口（在这些接口上配置了相应的服务策略）上基于每个用户管制数据流；在其他接口上继续使用默认的流掩码。在指定时间，系统中最多可以存在两个处于活动状态的不同 Qos 流掩码。仅可将一个类与一个流掩码相关联。一个策略最多可具有两个不同的流掩码。

Supervisor 引擎 720 上的管制功能的另一个重要变化是，它可以按帧的 L2 长度对数据流计数。这与按 IP 帧和 IPX 帧的 L3 长度对其进行计数的 Supervisor 引擎 1 和 Supervisor 引擎 2 不同。在某些应用中，L2 和 L3 的长度可能不一致。例如，较大的 L2 帧中可能存在较小的 L3 数据包。在这种情况下，与 Supervisor 引擎 1 和 Supervisor 引擎 2 相比，Supervisor 引擎 720 显示的管制数据流速率可能会稍有不同。

配置和监控 CatOS 软件中的管制

CatOS 的管制配置包括三个主要步骤：

1. 定义监察器 - 正常流量速率、超额速率（如果适用）、突发和管制操作。
2. 创建 Qos ACL 以选择要管制的数据流，并将监察器附加到此 ACL。
3. 将 Qos ACL 应用到必需的端口或 VLAN。

以下示例显示了如何管制流向端口 2/8 上的 UDP 端口 111 的所有数据流。

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.`

以下为相同的示例；但是，在本示例中，将监察器附加到了 VLAN 上。端口 2/8 属于 VLAN 20。

注意：您需要将端口QoS更改为VLAN模式。使用 **set port qos 命令执行此操作。**

此监察器将评估来自为基于 VLAN 的 QoS 配置的 VLAN 中的所有端口的数据流。

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.
```

下一步不是使用 DSCP 32 丢弃超出配置文件规定的数据包，而是将这些数据包降级到 DSCP 0（尽力）。

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.
```

以下示例仅显示 Supervisor 引擎 720 的出口管制的配置。它显示了进行管制时，如何将 VLAN 3 上的所有传出 IP 数据流的总速率限制为 10 Mbps。

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** 可查看当前的管制 DSCP 映射。

使用 **show qos policer runtime {*policer_name* | all}**以验证监察器的参数。还可查看监察器附加到的 Qos ACL。

注意：使用Supervisor引擎1和1a时，无法为单个聚合策略器提供策略统计信息。要查看每个系统的管制统计信息，请使用以下命令：

```
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
```

要查看微流管制统计信息，请使用以下命令：

```
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)
```

对于 Supervisor 引擎 II，可使用 **show qos statistics aggregate-policer 命令查看基于每个监察器的聚合管制统计信息。**

在本例中，流量生成器连接到端口2/8。它发送17 Mbps的UDP流量，目标端口111。预计监察器会丢弃16/17的流量，因此1 Mbps应该通过：

```
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：请注意，允许的数据包增加了65个，超额数据包增加了1090个。这意味着监察器丢弃了 1090 个数据包，而允许了 65 个数据包通过。您可以计算65 /(1090 + 65)= 0.056，或大约1/17。因此，策略器工作正常。

配置和监控 Cisco IOS 软件中的管制

Cisco IOS 软件中的管制配置涉及以下步骤：

1. 定义监察器。
2. 创建 ACL 以选择要管制的数据流。
3. 定义类映射，以通过 ACL 和/或 DSCP/IP 优先级选择数据流。
4. 定义使用类的服务策略，并将监察器应用于指定的类。
5. 将服务策略应用于端口或 VLAN。

请考虑与配置和监控 CatOS 软件中的管制部分所提供的示例相同的示例，但此时使用 Cisco IOS 软件。在本例中，您有一个流量生成器连接到端口2/8。它发送17 Mbps的UDP流量，目的端口为 111:

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.
```

在 Cisco IOS 软件中存在两种类型的聚合监察器：**named 和 per-interface.**named 聚合监察器管制应用该监察器的所有接口上的总数据流。上面的例子就是使用这个类型。per-interface 监察器在应用该监察器的每个入站接口上单独对数据流进行管制。每接口策略器在策略映射配置中定义。参见以下示例，该示例中存在一个 per-interface 聚合监察器：

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.
```

与 per-interface 聚合监察器一样，微流监察器也在策略映射配置中进行定义。在以下示例中，管制从主机 192.168.2.2 进入 VLAN 2 的流时，每个流的速率限制为 100 kbps。在管制来自 192.168.2.2 的所有数据流时，总的数据流速率限制为 500 kbps。VLAN 2 包括接口 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.
```

以下示例显示Supervisor引擎720的出口管制配置。它建立了对接口千兆以太网8/6到100 kbps上所有出站流量的管制：

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.
```

以下示例显示Supervisor引擎720的每用户策略配置。从端口1/1后的用户传入Internet的流量被策略为每用户1 Mbps。该示例也对从 Internet 传向用户的数据流进行管制并将速率限制为每用户 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
```

要监控管制，可使用以下命令：

```
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
```

注意：允许的数据包增加了304个，超额数据包增加了5068个。这意味着监察器丢弃了 5068 个数据包，并允许了 304 个数据包通过。鉴于输入速率为 17 Mbps，监察器应传递流量的 1/17。如果将丢弃和转发的数据包进行比较，您将发现情况确实如此：304 /(304 + 5068)= 0.057，或大约1/17。由于硬件策略粒度，可能会出现一些细微的变化。

对于微流管制统计信息，请使用 **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`段显示每个流的管制数据包数。

相关信息

- 配置 QoS
- 了解 Catalyst 6000 系列交换机的服务质量
- LAN 产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems