了解 Catalyst 3550 上的 QoS 策略与标记

目录

简介

策略功能可确定流量水平是否符合指定配置文件或合同规定，通过该功能可以丢弃超出配置文件规定的流量或将流量降级标记为另一个差分服务代码点 (DSCP) 值。这样会强制执行某个约定服务级别。

DSCP 是数据包服务质量 (QoS) 级别的一个度量指标。与 DSCP 一起，IP 优先级和业务类别 (CoS) 也用于确定数据包的 QoS 级别。

策略不应与流量整形相混淆，尽管二者都是确保流量不超出配置文件或合同的规定。

策略不会缓存流量，因而策略不会影响传输延迟。策略不缓存超出配置文件规定的数据包，而是丢弃这些数据包，或将其标记为其他 QoS 级别（DSCP 降级）。

流量整形则缓存超出配置文件规定的流量并平滑流量突发，但会影响延时和延时变化。虽然策略可以应用在流入和流出接口，但整形只能应用在流出接口。

Catalyst 3550 同时支持传入和传出两个方向的策略。不支持流量整形。

标记会根据策略更改数据包 QoS 级别。

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。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

硬件与软件版本

所有软件版本都支持 Catalyst 3550 上的策略和标记。下面列出了最新配置指南。有关所有受支持的功能，请参阅此文档。

- 配置 QoS

QoS 策略和标记参数

要设置策略，必须定义 QoS 策略映射并应用于端口。这也称为基于端口的 QoS。

注意： Catalyst 3550 当前不支持基于 VLAN 的 QoS。

监察器是根据以下几方面定义的：速率和突发参数，以及针对超出配置文件规定的流量的操作。

支持以下两类监察器：

- 聚合
- 个人

聚合监察器作用于其所有应用实例的流量。独立监察器分别作用于其每个应用实例的流量。

注意： 在Catalyst 3550上，聚合策略器只能适用于同一策略的不同级别。不支持聚合监察多个接口或策略。

例如，应用聚合监察器，从而将同一策略映射中的 customer1 类别和 customer2 类别的流量限制为 1 Mbps。这样的监察器允许 customer1 类别和 customer2 类别中的流量之和为 1 Mbps。如果应用独立监察器，则监察器将 customer1 类别的流量限制为 1 Mbps，将 customer2 类别的流量限制为 1 Mbps。因而，每个监察器实例都是独立的。

下表总结了在同时应用入口策略和出口策略处理数据包时的 QoS 操作：

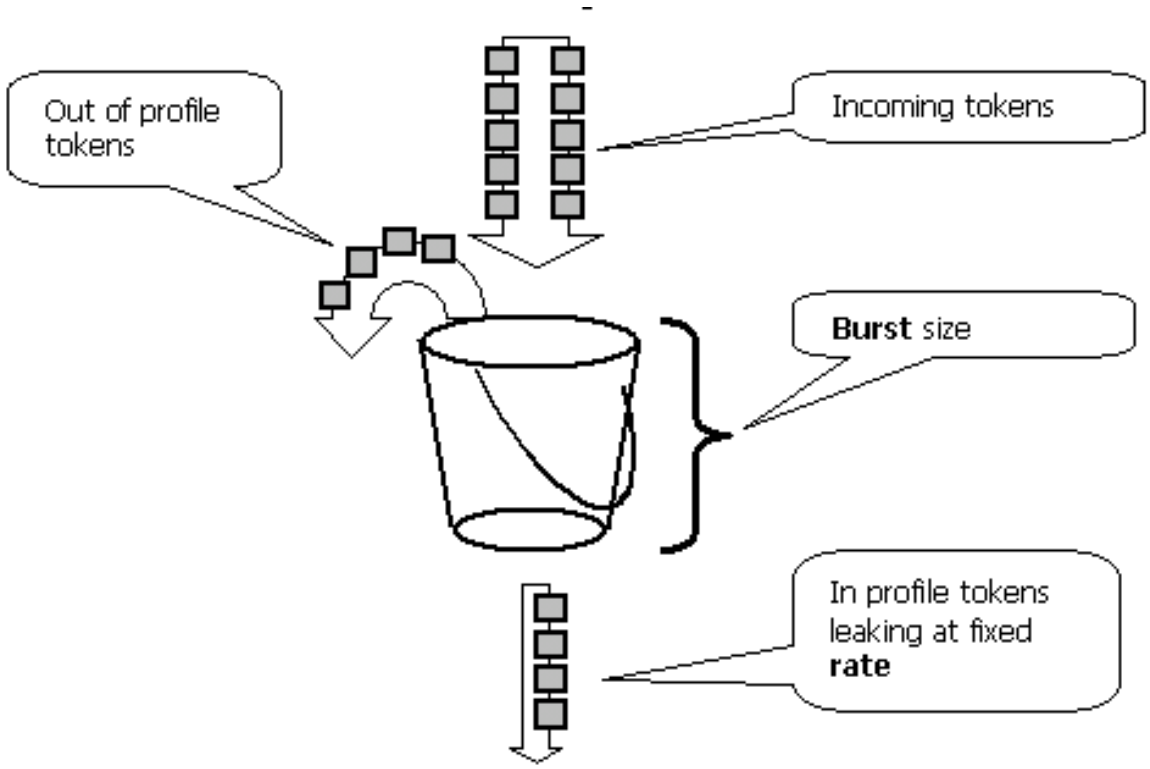
	Ingress policy			
Egress policy	Transmit	Drop	Markdown$_i$	Mark$_i$
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_i$ then Markdown$_e$	Mark$_i$ then Markdown$_e$

注意： 在同一策略的同一流量类别内，可能进行标记和降级。在这种情况下，首先标记特定类别的所有流量。监察和降级发生于标记后的流量。

Catalyst 3550 中的 QoS 策略遵从以下漏桶概念：

在令牌桶中会放入令牌，令牌数目与传入流量数据包大小成正比；令牌的数目等于数据包的大小。派生自所配置速率的规定数量的令牌会定期从桶中删除。如果桶中没有空间容纳某个传入数据包，该数据包就被视为超出配置文件规定的数据包，会根据所配置的策略操作丢弃或降级。

下面的示例说明了这一概念：



注意： 如本例所示，流量不在桶中缓存。实际流量根本不会流经桶；桶仅用于确定数据包是符合还是超出配置文件规定。

注意： 策略的硬件实施可能不尽相同，但在功能方面仍遵循此模型。

以下参数控制策略的运行：

- **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。低于该速率的所有流量都符合配置文件规定。速率支持范围为 8 Kbps - 2 Gbps，增量为 8 Kbps。
- **时间间隔 -** 定义了从桶中删除令牌的频率。时间间隔固定为 0.125 毫秒（即每秒 8000 次）。此时间间隔不可更改。
- **突发** - 定义桶在任何时候可以容纳的最大令牌数。突发支持范围为 8000 - 2000000 字节，增量为 64 字节。

注意： 虽然命令行帮助串显示一个大范围的值，但费率-bps选项不能超过配置端口的速度，并且破裂字节选项不能超出2000000个字节。如果输入更大的值，在您试图将它附加到它接口上时，交换机会拒绝策略映射。

为了保持指定的流量速率，突发不能低于此等式之和：

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

例如，计算最小突发值以保持速率 1 Mbps。速率定义为 1000 Kbps，因此，所需最小突发是此等式之和：

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

支持的最低突发流量大小为8000字节，比计算出的最小突发流量更大。

注意： 由于硬件管制粒度的原因，精确的速率和突发值将舍入为最接近的支持值。

配置突发速率时，必须考虑数据包丢失所引发的某些协议实施机制。例如，每丢失一个数据包，传输控制协议 (TCP) 将窗口缩减一半。当TCP设法加速到线速率，并被策略器扼杀时，会引发TCP数据流中的“锯齿”效应。如果计算锯齿型流量的平均速率，该速率比监察速率低得多。不过，您可以提高突发以实现更高的利用率。首先应将突发设置为往返时间 (TCP RTT) 内以所需速率发送的流量的两倍。如果 RTT 未知，可以将突发参数的值增加一倍。

出于相同原因，建议不要使用面向连接的流量来衡量监察器运行。否则通常会导致性能低于监察器的要求。

无连接流量对于策略也可能有不同反应。例如，网络文件系统 (NFS) 使用块，其中可能包含多个用户数据报协议 (UDP) 数据包。丢弃一个数据包可能导致许多数据包甚至整个块需要重新传输。

下面的示例计算 TCP 会话的突发，策略速率为 64 Kbps、TCP RTT 为 0.05 秒：

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

在此示例中，<burst> 是一个 TCP 会话的。利用这个数字可以计算通过监察器的预期会话数。

注意： 这只是示例，在每一种情况中都需要评估流量和应用程序需求、运行情况和可用资源，以便选择策略参数。

Policing操作可以是丢弃数据包，也可以是更改数据包的DSCP(markdown) 。要使数据包降级，必须修改所监察的 DSCP 映射。默认的所监察 DSCP 映射将数据包重新标记为同一 DSCP。因此不会发生降级。

如果某个超出配置文件规定的数据包降级标记为某个 DSCP，而该 DSCP 映射到不同于原 DSCP 的其他输出队列中，则可以不按顺序发送该数据包。如果数据包的顺序十分重要，请将超出配置文件规定的数据包降级标记至映射到与符合配置文件规定的数据包相同的输出队列。

Catalyst 3550 支持的策略与标记功能

下表按方向划分，总结了 Catalyst 3550 支持的策略和标记的相关功能：

	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

每个类映射支持一个匹配语句。入口策略的有效匹配语句：

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

注意： 在 Catalyst 3550 中，不支持 **match interface** 命令，并且在一个类映射中只能有一个匹配语句。因此，很难为通过某个接口传入的所有流量分类，也很难只用一个监察器来监察所有流量。请参阅本文档的如何只用一个监察器为所有接口流量分类部分。

下面是出口策略的有效匹配语句：

- match ip dscp

下面是入口策略的有效策略操作：

- police
- set ip dscp (标记)
- set ip precedence (标记)
- trust dscp
- trust ip-precedence
- trust cos

下表列出了受支持的入口 QoS 策略矩阵：

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. 此选项也涵盖 match IP precedence。
2. 此选项涵盖信任 CoS、IP 优先级和 DSCP。
3. 此选项也涵盖设置 IP 优先级。

下面是出口策略的有效策略操作：

- police

下表列出了受支持的出口 QoS 策略矩阵：

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

通过标记，数据包的 QoS 级别可以根据分类或策略而更改。分类将流量划分为不同类别，以便根据定义的标准进行 QoS 处理。

QoS 处理以内部 DSCP 为基础；数据包的 QoS 级别度量。内部 DSCP 是根据信任配置派生的。系统支持信任 CoS、DSCP、IP 优先级和不受信任的接口。信任指定相应字段，每个数据包的内部 DSCP 是从该字段派生的，如下所示：

- 信任 CoS 时，QoS 级别派生自交换机间链路协议 (ISL) 或 802.1Q 封装数据包的第 2 层 (L2) 报头。
- 信任 DSCP 或 IP 优先级时，系统从数据包的 DSCP 或 IP 优先级字段相应派生 QoS 级别。

委托CoS只有在中继接口和委托DSCP(或IP优先级)上有意义，只能用于IP信息包。

如果不信任某个接口，则从可配置的默认 CoS 为相应接口派生内部 DSCP。这是启用 QoS 时的默认状态。如果没有配置默认 CoS，则默认值为零。

一旦内部DSCP确定，它可以通过标记、警管进行更改或保留。

数据包经过 QoS 处理之后，其 QoS 级别字段（在 IP 的 IP/DSCP 字段内，在 ISL/802.1Q 报头内（如果有））将从内部 DSCP 进行更新。下面是与策略相关的特殊 QoS 映射：

- **DSCP-被监察的 DSCP** — 用于在数据包降级时派生被监察的 DSCP。
- **DSCP-CoS** — 用于从内部 DSCP 派生 CoS 级别，以更新传出数据包 ISL/802.1Q 报头。
- **CoS-DSCP** — 用于在接口处于信任 CoS 模式时，从传入 CoS（ISL/802.1Q 报头）派生内部 DSCP。

下面是特定于实施的重要注意事项：

- 如果将接口配置为信任任何 QoS 度量指标（如 CoS/DSCP 或 IP 优先级），则入口服务策略不可附加于接口。要匹配 DSCP/IP 优先级和入口策略，则必须在策略内，而不是在接口上为特定类别配置信任。要根据 DSCP/IP 优先级进行标记，则不必配置任何信任。
- 从硬件和 QoS 的角度，只有没有 IP 选项和以太网 II 高级研究项目管理局 (ARPA) 封装的 IPv4 流量才视为 IP 流量。其他所有数据流视为包括非IP和带选项的IP，例如子网访问协议 (SNAP)封装的IP和IPv6。
- 对于非 IP 数据包，“匹配访问组”是唯一的分类方式，因为不能为非 IP 流量匹配 DSCP。媒体访问控制 (MAC) 访问列表 (ACL) 用于该目的；可以根据源 MAC 地址、目的 MAC 地址和以太网类型对数据包进行匹配。因为交换机区分 IP 流量和非 IP 流量，所以无法匹配 IP 流量与 MAC ACL。

配置和监控策略

要在 Cisco IOS 中配置策略，需要执行以下步骤：

1. 定义监察器（对于聚合监察器）
2. 定义标准以选择流量进行监察
3. 定义类映射以使用所定义标准选择流量
4. 通过使用类别并将监察器应用于指定的类别，定义服务策略
5. 将服务策略应用于端口

支持以下两类监察器：

- 命名聚合
- 个人

命名聚合监察器对自己所应用于的策略内所有类别的流量之和进行监察。不支持聚合监察不同接口。

注意： 聚合监察器不能应用于多个策略。否则会显示以下错误消息：

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

请考虑以下示例：

端口 GigabitEthernet0/3 附有流量生成器，发送大约 17 Mbps UDP 流量（目的端口 111）。另外还有来自端口 20 的 TCP 流量。您希望将这两个数据流限制为 1 Mbps，则必须丢弃多余流量。下面介绍如何完成这一过程：

```
!--- 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
!
```

第一个示例使用命名聚合监察器。与命名监察器不同，独立监察器分别监察它所应用于的每个类别。独立监察器是在策略映射配置内定义的。在本示例中，两个流量类别由两个独立监察器监察；cl_udp111 限制于 1 Mbps/8K 突发，而 cl_tcp20 限制于 512 Kbps/32K 突发：

```
!--- 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
```

此命令用于监控监察操作：

```
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
```

注意： 默认情况下，没有每 DSCP 统计信息。Catalyst 3550 支持最多八个不同 DSCP 值的每接口、每方向统计信息收集。当您发出 **mls qos monitor** 命令时会对此进行配置。要监控 DSCP 8、16、24 和 32 的统计信息，您必须发出此 **per-interface** 命令：

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

注意： **mls qos monitor dscp 8 16 24 32** 命令将 **show mls qos int g0/3 statistics** 命令的输出更改为：

```
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
```

下面是本示例中各字段的说明：

- **Incoming** — 显示从每个方向达到多少数据包
- **NO_change** — 显示有多少信任数据包（如未更改的 QoS 级别）
- **Classified** — 显示有多少数据包在分类之后分配得到了此内部 DSCP
- **Policed** — 显示有多少数据包根据策略降级；降级前显示的 DSCP。
- **Dropped** — 显示有多少数据包根据策略被丢弃

请注意以下特定于实施的注意事项：

- 如果发出 **mls qos monitor** 命令时配置了八个 DSCP 值，则在发出 **show mls qos int statistics** 命令时所见到的其他计数器可能显示不适当的信息。
- 没有特定命令用于验证每个监察器的传入或传出流量速率。
- 因为依次从硬件检索计数器，所以计数器计和可能不正确。例如，监察、分类或丢弃的数据包与传入数据包的数量可能略有不同。

配置和监控标记

若要配置标记，需要执行以下步骤：

1. 定义流量分类标准
2. 定义要用以前定义的标准分类的流量类别
3. 创建策略映射，将标记操作和策略操作附加于定义的类别。
4. 将相应接口配置为信任模式
5. 将策略映射应用于接口

在本示例中，您希望将主机 192.168.192.168 的传入 IP 流量标记为 IP 优先级 6，并限制于 1 Mbps；多余流量必须降级标记为 IP 优先级 2：

```
!--- 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
```

发出了同一 **show mls qos interface statistics** 命令以监控标记。有关示例输出和含义，请参阅本文这部分内容。

如何只用一个监察器为所有接口流量分类

在 Catalyst 3550 中，不支持 **match interface** 命令，并且每个类映射只能有一个匹配语句。而且，Catalyst 3550 不允许依据 MAC ACL 匹配 IP 流量。因此，必须借助两个独立的类映射为 IP 流量和非 IP 流量分类。这样，很难为通过某个接口传入的所有流量分类，也很难只用一个监察器来监察所有流量。这里的配置示例可完成这一任务。在此配置中，IP 流量和非 IP 流量与两个不同的类映射匹配。不过，这两种流量共用一个监察器。

```
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.
```

相关信息

- 在 Catalyst 3550 上配置 QoS
- 服务质量支持页
- LAN 交换技术支持页
- LAN 产品支持页
- 技术支持和文档 - Cisco Systems