使用Catalyst 4000/4500基于IOS的Supervisor引擎的QoS策略和标记

目录

简介

策略功能可确定数据流量是否在指定配置文件（合同）的规定范围内。策略功能允许丢弃超出配置文件规定的数据流，或者将其降级为另一个差分服务代码点 (DSCP) 值，以强制执行约定的服务级别。DSCP 是数据包服务质量 (QoS) 级别的一个度量指标。与DSCp一起，IP优先级和服务等级 (CoS) 还可以用来传送信息包QoS级别。

策略不应与流量整形相混淆，尽管二者都是为了确保数据流不超出配置文件（合同）的规定范围而制定的。策略并不对数据流进行缓冲，因而不会影响传输延迟。对于超出配置文件规定的数据包，策略不对其进行缓冲，而是丢弃数据包，或将其标记为另一个 QoS 级别（DSCP 降级）。流量整形则会对超出配置文件规定的流量进行缓冲并使流量突发平缓进行，但这会影响延时和延时变化。整形只能应用于输出流量接口，而策略则可同时应用于输入和输出接口。

配备 Supervisor 引擎 3、4 和 2+（此后称为 SE3、SE4、SE2+）的 Catalyst 4000/4500 同时支持传入和传出方向的策略。流量整形也在支持范围之内，但本文仅涉及策略和标记功能。标记是一个根据策略更改数据包 QoS 级别的过程。

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。

QoS 策略和标记参数

策略通过定义 QoS 策略映射并将它们应用于端口（基于端口的 QoS）或 VLAN（基于 VLAN 的 QoS）的办法来设定。监察器是根据以下几方面定义的：速率和突发参数，以及针对符合和超出配置文件规定的流量的操作。

可支持以下这两类监察器：聚合型和接口型。每个监察器均可应用于多个端口或 VLAN。

聚合监察器会对所有端口/VLAN 的流量进行监察。例如，我们可应用聚合策略器，将基于 VLAN 1 和 3 的简单文件传输协议 (TFTP) 流量限制为 1 Mbps。此监察器将允许 VLAN 1 和 3 总共传输 1 Mbps 的数据流。如果我们应用接口型监察器，它会将基于 VLAN 1 和 3 的 TFTP 流量分别限制为 1 Mbps。

注意： 如果对数据包同时应用了入口和出口策略，则将采取严重级别最高的措施。也就是说，如果入口监察器指定丢弃数据包，但出口监察器指定将数据包降级，数据包将丢弃。表 1 总结了同时应用入口和出口策略处理数据包时的 QoS 操作：

表 1：QoS 操作取决于入口和出口策略

	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$_e$

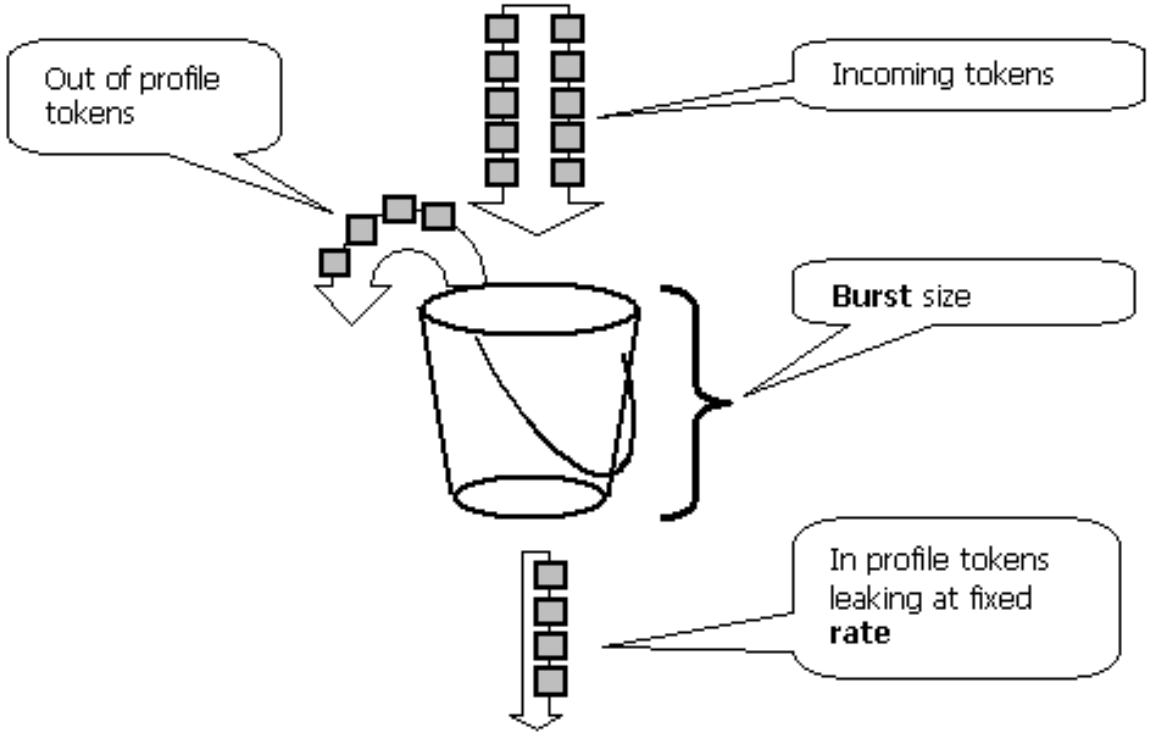
Catalyst 4000 SE3、SE4、SE2+ QoS 硬件会在数据流经出口监察器之后再对数据包真正进行标记。这意味着，即使入口策略重新标记数据包（通过监察器降级或正常标记），出口策略看到的仍将是标记为原始 QoS 级别的数据包。出口策略看到的数据包就像是未经入口策略标记一样。这意味着：

- 出口标记会覆盖入口标记。
- 出口策略与经入口策略更改的新 QoS 级别并不匹配。

其他重要提示如下所示：

- 不能在同一策略的同一数据流级别执行标记和降级。
- 聚合监察器是有方向性的。也就是说，如要将聚合监察器同时应用至入口和出口，则将存在两个聚合监察器，一个用于输入，另一个用于输出。
- 当聚合监察器在其策略内应用至 VLAN 和物理接口时，将会存在两个聚合监察器，一个用于 VLAN 接口，一个用于物理接口。目前，尚无法将 VLAN 接口和物理接口同时添加到聚合监察器的策略中。

Catalyst 4000 SE3、SE4、SE2+ 中的策略符合漏桶的概念，如下方的模型所示。与传入流量数据包对应的令牌被置于一个桶中（令牌数 = 数据包大小）。指定的令牌数量（源自所配置的速率）将定时从桶中删除。如果桶中没有空间容纳传入的数据包，该数据包将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。



值得注意的是，数据流在桶中并不进行缓冲，正如它在上述模型中所出现的情况一样。实际数据流根本不流经桶。桶仅用于确定数据包是否符合或超出配置文件规定。

请注意策略在实际硬件上的实施可以会不一样，但就其功能而言与上述模型一致。

下列参数可以控制策略的执行：

- 速率 定义在每个时间间隔内将有多少令牌取出。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 定义令牌隔多长时间从桶内取出一次。时间间隔固定为 16 纳秒（16 秒乘以 10 的负 9 次方）。时间间隔不能更改。
- 突发 定义了桶在任意时间可容纳的最大令牌数。

请参阅本文档末尾的”比较基于 Catalyst 6000 和 Catalyst 4000/4500 IOS Supervisor 引擎的策略和标记功能“部分，了解 Catalyst 6000 和 Catalyst 4000 SE3、SE4、SE2+ 间的突发差异。

监察器可确保如果您在任意时段（从零到无穷）内进行检查，该时段

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

内的流量都不会超出规定的范围。

Catalyst 4000 SE3、SE4、SE2+ QoS 硬件的策略精细程度都相当高。根据所配置的速率，速率的最大偏差约为 1.5%。

配置突发速率时，您需要考虑到有些协议（如 TCP）会实施用于对数据包丢失做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。当策略规定为某个特定速率时，有效的链路利用率将会低于所配置的速率。您可以增加突发值以实现更高的利用率。对于这样的数据流，首先应将突发值设为往返时间 (RTT) 内以所需速率发送的流量的两倍。出于相同原因，建议不要使用面向连接的流量作为监察器运行的衡量基准，因为它显示的性能一般要低于监察器所允许的性能。

注意： 无连接流量对于策略也可能会有不同的反应。例如，网络文件系统 (NFS) 使用数据块，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会导致多个数据包（整个块）需要重新传输。

例如，以下示例计算了 TCP 会话的突发值，策略速率为 64 Kbps，TCP RTT 为 0.05 秒。

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

注意： <突发>用于一次 TCP 会话，因此应该增大，以均衡通过监察器的预计会话数。这只是一个示例，因此在每一种情况下都需要评估流量需求、应用程序需求、运行情况以及可用资源，以便选择策略参数。

策略操作可以是丢弃数据包（丢弃），也可以是更改数据包的 DSCP（降级）。为了降级标记数据包，policed DSCP 映射必须修改。默认的受监察 DSCP 会将数据包重新标注为相同的 DSCP，即不会发生降级。

注意： 如果对某个超出配置文件规定的数据包降级时，将其降级为与原有 DSCP 位于不同输出列队中的 DSCP，可能会使数据包无序发送。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 映射的队列与符合配置文件规定的数据包所映射的队列相同。

Catalyst 4000/4500 IOS Supervisor 引擎支持的策略与标记功能

Catalyst 4000 SE3、SE4、SE2+ 同时支持入口（传入接口）和出口（传出接口）策略。交换机支持 1024 个入口和 1024 个出口监察器。系统在默认的无策略行为中各使用两个入口和出口监察器。

请注意，当聚合监察器在其策略内同时应用至 VLAN 和物理接口时，会启用一个额外的硬件监察器条目。目前，尚无法将 VLAN 接口和物理接口同时添加到聚合监察器的策略中。这可能会在未来的软件版本中有所改变。

所有的软件版本均包含对策略功能的支持。Catalyst 4000 最多可对每个类支持 8 个有效的匹配语句，而每个策略映射最多支持 8 个类。有效的匹配语句如下所示：

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

注意： 对于非 IP V4 数据包，只要数据包进入的是中继端口所信任的 CoS，**match ip dscp**语句就将是唯一的分类方式。不要被“match ip dscp”命令中的关键字 ip 所误导，因为内部 DSCP 匹配这一特点适用于所有数据包，而不仅仅是 IP。如果将端口配置为信任 CoS，则后者会从 L2（802.1Q 或 ISL 标记）帧解压缩，并使用 CoS 到 DSCP QoS 的映射转换成内部 DSCP。然后，即可在策略中使用 **match ip dscp** 匹配此内部 DSCP 值。

有效的策略操作如下所示：

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

通过标记，数据包的 QoS 级别可以根据分类或策略更改。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。要与 IP 优先级或 DSCP 匹配，应将相应的传入接口设为信任模式。交换机支持信任的 CoS、信任的 DSCP 以及不可信的接口。“信任”用于指定将从中派生数据包 QoS 级

别的字段。

当信任 CoS 时，QoS 级别将从 ISL 或 802.1Q 封装信息包的 L2 报头中派生。当信任 DSCP 时，交换机将从数据包的 DSCP 字段中获得 QoS 级别。信任 CoS 只对中继接口有意义，而信任 DSCP 仅对 IP V4 数据包有意义。

当接口不可信时（这是 QoS 启用时的默认状态），内部 DSCP 将派生自相应接口的可配置默认 CoS 或 DSCP。如果并未配置默认 CoS 或 DSCP，默认值将为零 (0)。数据包的原始 QoS 级别一经确定，则会被映射至内部 DSCP 中。内部 DSCP 可通过标记或策略功能保留或更改。

数据包经过 QoS 处理之后，其 QoS 级别字段（在 IP 的 IP DSCP 字段以及 ISL/802.1Q 报头内，如果有）将从内部 DSCP 更新。

有某些特殊映射可用于将数据包中的可信 QoS 度量指标转换为内部 DSCP，反之亦然。这些映射如下所示：

- “DSCP”到“被监察的 DSCP”；用于在数据包降级时派生被监察的 DSCP。
- “DSCP”到“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”到“DSCP”：用于在接口处于信任 CoS 模式时，从传入 DSCP（ISL/802.1Q 报头）派生内部 DSCP。

请注意，当接口处于信任 CoS 模式时，传出 CoS 总是与传入 CoS 相同。这一点是专门针对 Catalyst 4000 SE3、SE4、SE2+ 中 QoS 实施的特点。

配置和监控策略

在 IOS 中配置策略包括以下步骤：

1. 定义一个监察器。
2. 定义标准以选择要设定策略的流量。
3. 使用类来定义服务策略，并对一个特定的类应用一个监察器。
4. 将服务策略应用于端口或 VLAN。

请考虑以下示例。有数据流生成器附加对发送UDP流量的~17 Mbps与端口111的目的地的端口5/14。我们希望将这个数据流限制为 1 Mbps，同时丢弃超额的流量。

```
! 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
!
```

请注意，当端口位于基于 QoS 模式的 VLAN 中，但相应的 VLAN 尚未应用服务策略时，交换机将遵从物理端口上的服务策略（如果有）。这可以为基于端口和基于 VLAN 的 QoS 间的结合提供额外的灵活性。

可支持以下这两类监察器：指定的聚合型和接口型。指定的聚合监察器将对应用该监察器的所有接口上的流量整体实施策略。以上事例使用了一个指定监察器。与指定的监察器不同，接口型监察器会对应用该监察器的每个接口上的流量分别实施策略。每接口策略器在策略映射配置中定义。请参见下列使用接口型聚合监察器的示例：

```
! 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
```

以下命令用于监控策略操作：

```
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
```

类映射旁的计数器会计算与相应类匹配的数据包数量。

请注意下列特定于实施的注意事项：

- 类数据包计数器不是接口型计数器。也就是说，对于所有在服务策略内应用了此类的所有接口，它会计算与之相匹配的数据包总数。
- 监察器不维护数据包计数器，它只支持字节计数器。
- 没有特定的命令可用于验证每个监察器的传入或传出流量速率。
- 计数器会定时更新。如果快速地重复执行上述指令，计数器仍可能会在某个时段出现。

配置和监控标记

配置标记包括以下步骤：

1. 定义流量、访问列表、DSCP、IP 优先级等内容的分类标准。
2. 定义通过先前所定义的标准分类的流量类别。
3. 创建策略映射，对所定义的类别附加标记操作和/或策略操作。
4. 对相应接口配置信任模式。
5. 将策略映射应用于接口。

请考虑以下示例，我们希望将主机 192.168.196.3 UDP 端口 777 的 IP 优先级为 3 的传入流量映射为 IP 优先级 6。并将其他所有 IP 优先级为 3 的流量通过策略限制在 1 Mbps 以内，超出的流量则应降级为 IP 优先级 2。

```
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
```

sh policy interface 命令用于监控标记。示例输出和提示在上面的策略配置中均有介绍。

比较基于 Catalyst 6000 和 Catalyst 4000/4500 IOS Supervisor 引擎的策略和标记

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.

相关信息

- 了解和配置 QoS
- 技术支持 - Cisco Systems