

目 录

第 1 章 QoS配置	1-1
1.1 QoS介绍	1-1
1.1.1 QoS术语.....	1-1
1.1.2 QoS实现.....	1-2
1.1.3 QoS基本模型.....	1-2
1.2 QoS配置	1-6
1.3 QoS举例	1-10
1.4 QoS排错帮助	1-13
第 2 章 PBR配置	2-1
2.1 PBR介绍	2-1
2.2 PBR配置	2-1
2.3 PBR举例	2-2
第 3 章 IPv6 PBR配置	3-1
3.1 PBR（基于策略的路由）功能介绍	3-1
3.2 PBR配置任务序列	3-1
3.3 PBR举例	3-2
3.4 PBR排错帮助	3-3
第 4 章 基于流的重定向	4-1
4.1 基于流的重定向介绍	4-1
4.2 基于流的重定向配置任务序列	4-1
4.3 基于流的重定向举例	4-1
4.4 基于流的重定向排错帮助	4-2

第1章 QoS配置

说明：

本章所指的 L3 交换机和路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

1.1 QoS介绍

QoS（Quality of Service，服务品质保证）是指一个网络能够利用各种各样的技术向选定的网络通信提供更好的服务的能力。QoS 是服务品质保证，提供稳定、可预测的数据传送服务，来满足使用程序的要求，QoS 不能产生新的带宽，而是根据应用的需求以及网络管理的设置来有效的管理网络带宽。

1.1.1 QoS术语

QoS: Quality of Service 服务品质保证，提供稳定、可预测的数据传送服务，来满足使用程序的要求，QoS 不能产生新的带宽，而是根据使用程序的需求以及网络管理的设置来有效的管理网络带宽。

QoS 功能域: QoS Domain 支持 QoS 的设备组成的一个能够提供服务品质保证的网络拓扑，定义为 QoS 功能域。

CoS: Class of Service 服务级别，L2 802.1Q 帧携带的分类信息，在帧头的 Tag 字段中占 3bits，称为用户优先级，范围为 0~7。

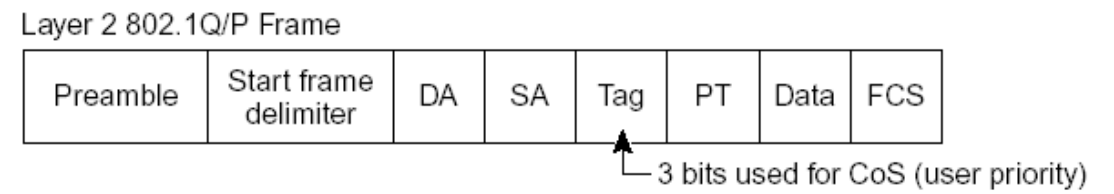


图 1-1 CoS 优先级

ToS: Type of Service 服务类型，L3 IPv4 包头携带的一个字节的字段，标记 IP 包的服务类型，ToS 字段内可以是 IP Precedence 值，也可以是 DSCP 值。

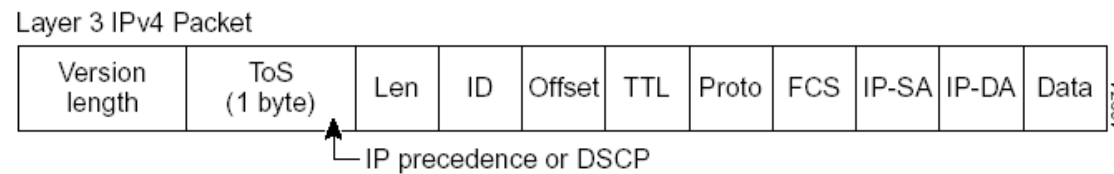


图 1-2 ToS 优先级

IP Precedence: IP 优先级，L3 IP 包头携带的分类信息，共占 3bits，范围为 0~7。

DSCP: Differentiated Services Code Point 差别化业务编码点，L3 IP 包头携带的分类信息，共占 6bits，范围为 0~63，向下兼容 IP Precedence。

MPLS TC(EXP):



MPLS 报文中的一个字段，用来表明 MPLS 报文的服务等级，一共三个 bit，范围为 0~7。

Internal Priority: 交换芯片内部优先级设置，支持范围和芯片相关，后续文档中简写为 Int-Prio 或者 IntP。

Drop Precedence: 丢弃优先级，在交换芯片处理报文的时候，丢弃优先级大的报文将会被优先丢弃，三色算法取值范围为 0-2，双色算法取值范围 0-1，后续文档中简写为 Drop-Prec 或者 DP。

分类: QoS 的入口动作，根据数据包携带的分类信息和 ACLs，将数据包流量进行分类。

监管: QoS 的入口动作，制定监管策略，对分类后的数据包进行监管。

重写: QoS 的入口动作，根据制定的监管策略，对数据包进行通过、降级、丢包等操作。

排程: QoS 的出口动作，配置八条出口队列的 WRR (Weighted Round Robin) 权重。

In-Profile: 对于在 QoS 监管策略规定范围(带宽或突发值)内的流量，我们称它是 In-Profile 的。

Out-of-Profile: 对于超出 QoS 监管策略规定范围(带宽或突发值)的流量，我们称它是 Out-of-Profile 的。

1.1.2 QoS实现

对于 L3 交换机软件 QoS 的实现，首先应该给出一个参考模型，而这个模型要求是通用的，成熟的。QoS 并不能产生新的带宽，但是它可以将现有的带宽资源做一个最佳的调整和配置，完整的应用 QoS，可以对网络的数据传输做到完全的控管。下面将对 QoS 做一个尽量严格的描述：

IP 协议的数据传送规范，只针对发送端和接收端的地址和服务等作出规定，并且利用 OSI 四层以上的，如 TCP 协议等来确认数据包的传送正确无误，但是，IP 协议没有提供和保护传输数据包的带宽，而是以尽力而为 (Best Effort) 的方式来提供带宽服务。此种方式对于 Mail 以及 FTP 等服务尚可以接受，但是对于越来越多的多媒体业务数据和电子商务数据的传输，则无法满足这些应用需要的带宽和低延迟要求。

基于差别化服务的 QoS 在网络的入口指定每个数据包的优先级别，这些分类信息被携带在 L3 的 IP 包头或者 L2 的 802.1Q 帧头中。QoS 对于相同优先级别的数据包提供相同服务，而对不同级别的数据包则提供不同的操作。支持 QoS 的交换机或路由器可以根据数据包的分类信息，为其提供不同的带宽资源，并且可以根据配置的监管策略来重写这些数据包携带的分类信息甚至在带宽紧张的时候丢弃某些低级别的数据包。

如果在一个网络中，每一跳的设备都支持基于差别化服务的 QoS，那么就可以构建一个端到端的 QoS 解决方案。QoS 的配置是很灵活的，可以很复杂，也可以很简单，这一切都依赖于实际的网络拓扑和网络设备，以及对网络出入流量的分析。

1.1.3 QoS基本模型

QoS 的基本模型分为四个部分：Classification (分类)、Policing (监管)、Mark (重写)

和 Scheduling（排程），其中分类、监管和重写是顺序执行的 QoS 的入口行为，整形和排程是 QoS 的出口行为。

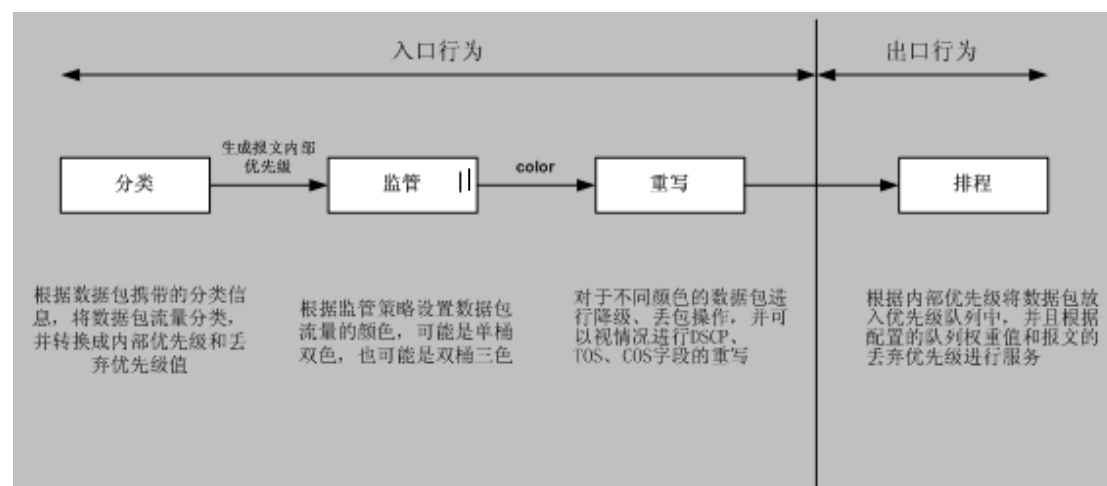


图 1-3 QoS 基本模型

分类：通过检查数据包的分类信息，来区别不同的流量，并且根据数据包的分类信息生成内部优先级和丢弃优先级。对于不同类型的数据包和不同的交换机配置，分类有不同的处理方式，由下面的流程图详细说明：

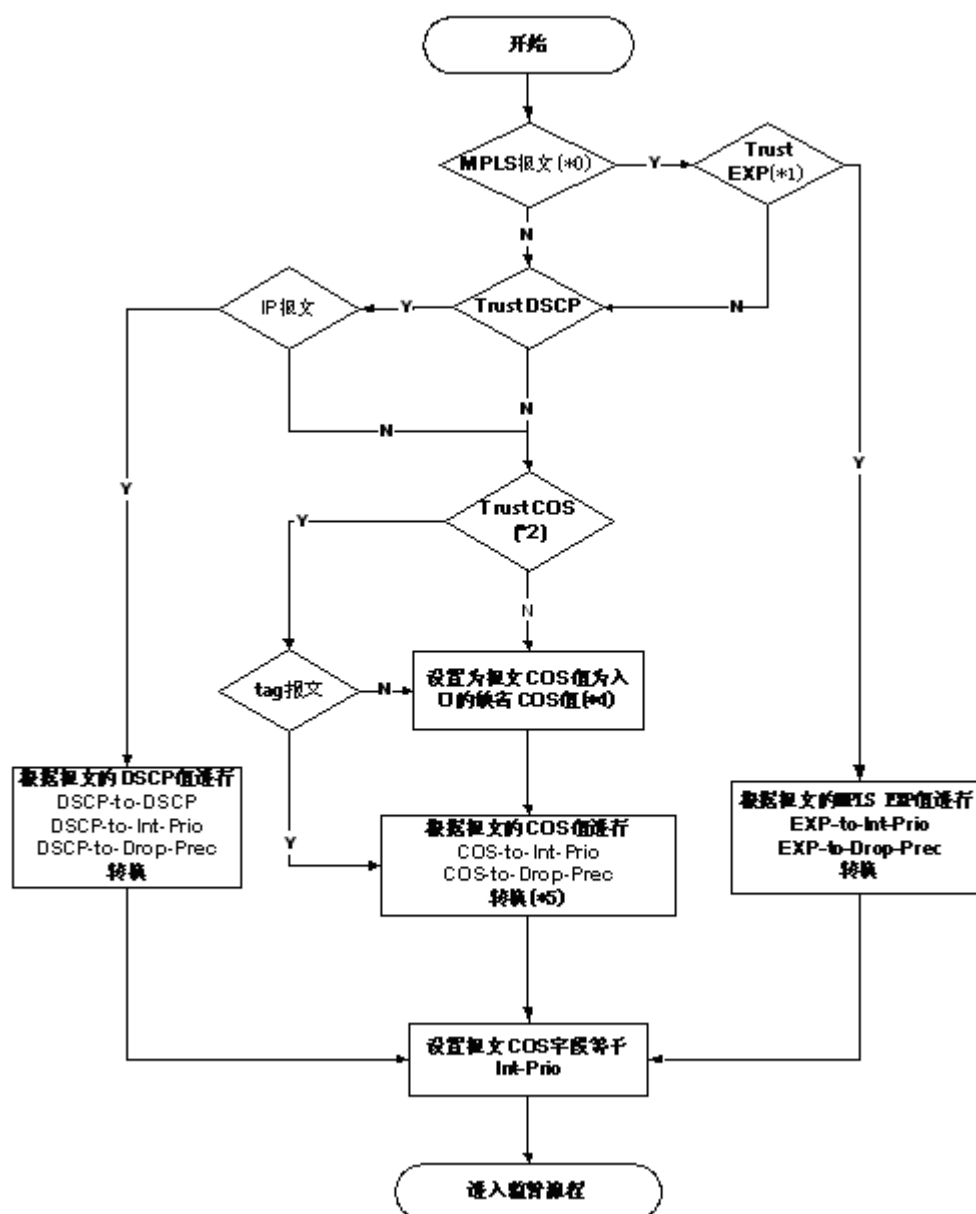


图 1-4 分类流程

监管和重写：在入口的流量经过分类，并且每个数据包都被分配了一个内部优先级和丢弃优先级值以后，就可以进行监管和重写。

监管行为可以基于流配置不同的监管策略，为分类后的流量分配带宽，带宽的分配策略可以是双桶双色，也可以是双桶三色。流量会被分配不同的颜色（color），对不同颜色的流量可以选择丢包、通过两种处理方式；对于通过处理方式的数据包，可以附加重写动作。重写行为即用一个新的优先级较低的 DSCP 值来代替数据包原有的级别较高的 DSCP 值。监管和重写的具体行为，由下面的流程图详细说明：

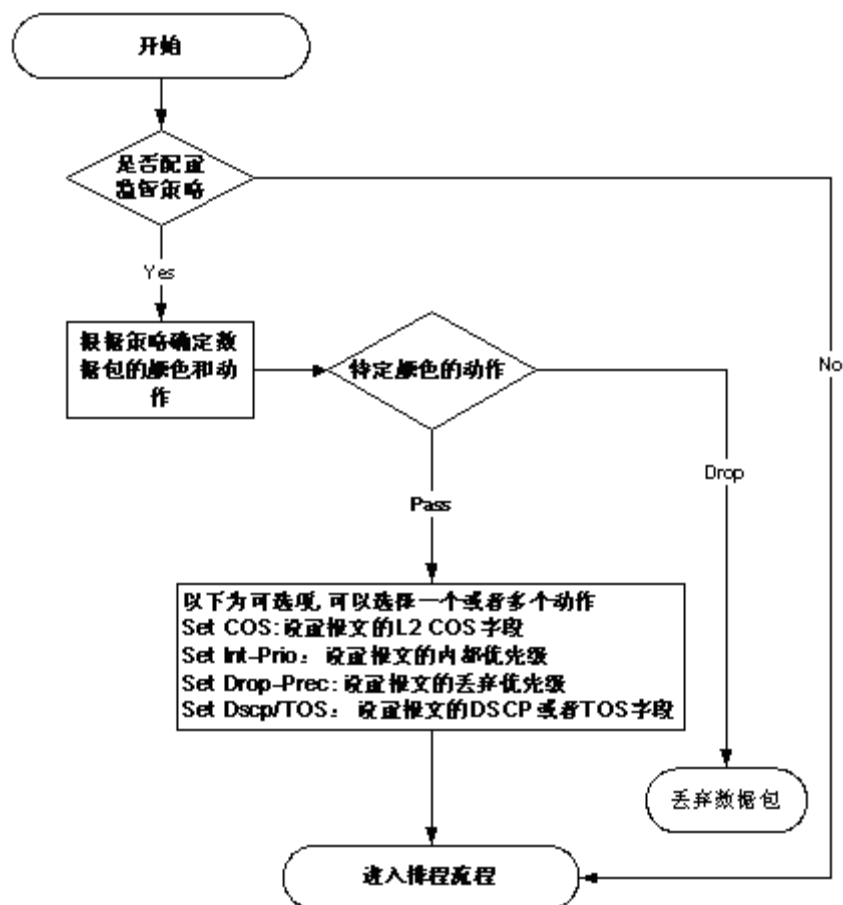


图 1-5 监管和重写流程

整形和排程：出口的数据包会都具有内部优先级值和丢弃优先级。整形行为根据数据包的内部优先级值将其分配到不同的优先级队列中，而排程行为根据配置的优先级队列权重和丢弃优先级来进行数据包转发服务。整形和排程的具体行为，由下面的流程图详细说明：

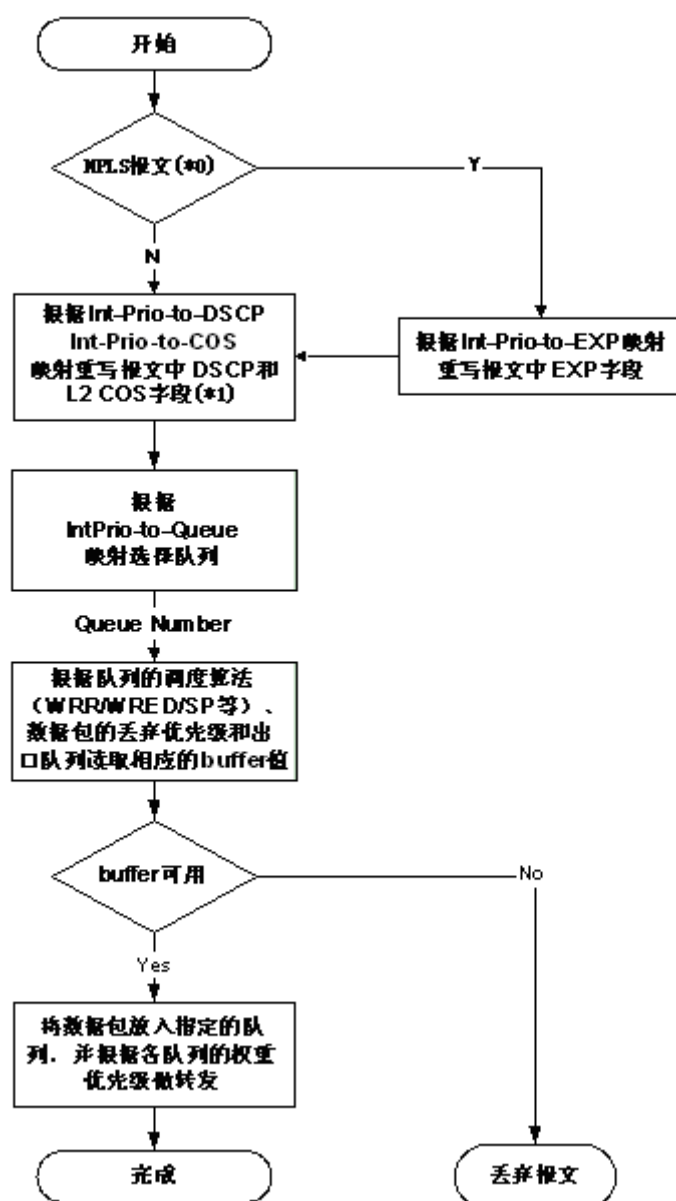


图 1-6 整形和排程流程

1.2 QoS配置

QoS 配置任务序列如下：

配置分类表（classmap）

建立一个分类规则，可以按照 ACL、CoS、VLAN ID、IPV4 Precedent、DSCP、IPV6 FL 来分类。之后，对于不同类别的数据流采取不同的策略。

配置策略表（policymap）

对数据流进行分类之后，就可以建立一个策略表，之后就可以将其对应一个先前建立的 class-map，进入策略分类表模式，然后就可以对于不同的数据流采取不同的策略，如带宽限制、优先级降低、分配新的 DSCP 值等等。也可以定义一个集合策略，这个策略可以在

同一个策略表内部被多个策略分类表使用。

将 QoS 应用到端口或 VLAN

配置端口的信任模式，或者绑定策略。策略只有绑定到具体的端口，才在此端口生效。

策略也可以绑定到具体的 VLAN 上。

建议不要在 VLAN 和属于该 VLAN 的端口上同时使用 policy map。

配置端口队列调度算法

设定端口队列调度算法，如 sp, wrr, wdrr 等。

配置 QoS 映射关系

配置 cos 到 dp, dscp 到 dscp 或 intp 或 dp, intp 到 dscp 的映射关系。

1. 配置分类表 (classmap)

命令	解释
全局配置模式	
class-map <class-map-name> no class-map <class-map-name>	建立一个 class-map (分类表)，并进入 class-map 模式；本命令的 no 操作为删除指定的 class-map。
match {access-group <acl-index-or-name> ip dscp <dscp-list> ip precedence <ip-precedence-list> ipv6 access-group <acl-index-or-name> ipv6 dscp <dscp-list> ipv6 flowlabel <flowlabel-list> vlan <vlan-list> cos <cos-list> exp <exp-list>} no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp ipv6 flowlabel vlan cos exp}	设置分类表中的匹配标准，可以根据 ACL、CoS、VLAN ID、IPV4 Precedent、DSCP、IPV6 FL 优先级等对数据流进行分类；本命令的 no 操作为删除指定的匹配标准。

2. 配置策略表 (policymap)

命令	解释
全局配置模式	
policy-map <policy-map-name> no policy-map <policy-map-name>	建立一个 policy-map (策略表)，并进入 policy-map (策略表) 模式；本命令的 no 操作为删除指定的 policy-map。
class <class-map-name> [insert-before <class-map-name>] no class <class-map-name>	建立一个 policy-map (策略表) 之后，可以将其对应于一个 class (策略分类表)，并进入策略分类表模式，之后就可以对不同的数据流采取不同的策略或者分配一个新的 DSCP 值；本命令的 no 操作为删除指定策略分类表。
set {ip dscp <new-dscp> ip precedence <new-precedence> internal priority <new-inp> drop precedence <new-dp> cos	为分类后的流量分配一个新的 DSCP、CoS 和 IP Precedence 值等；本命令的 no 操作为取消分配新的值。

<pre><new-cos> no set {ip dscp ip precedence internal priority drop precedence cos }</pre>	
单桶模式: <pre>policy <bits_per_second> <normal_burst_bytes> ({conform-action ACTION exceed-action ACTION})</pre> 双桶模式: <pre>policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] <maximum_burst_bytes> [{conform-action ACTION exceed-action ACTION violate-action ACTION }]</pre> ACTION 定义: <pre>drop transmit set-dscp-transmit <dscp_value> set-prec-transmit <ip_precedence_value> set-cos-transmit <cos_value> set-internal-priority <inp_value> set-Drop-Precedence <dp_value> no policy</pre>	为分类后的流量配置一个策略,支持三色color的非聚合Policy命令,根据配置参数解析出令牌桶的工作模式,是单速单桶、单速双桶还是双速双桶,并且给不同颜色报文设置相应动作。no命令删除模式配置。单桶模式只有特定的交换机支持。
<pre>policy aggregate <aggregate-policy-name> no policy aggregate <aggregate-policy-name></pre>	为分类后的流量应用一个聚合策略;本命令的 no 为删除指定的聚合策略。
<pre>accounting no accounting</pre>	为分类后的流量设置统计功能。 在策略分类表配置模式下将功能开启后,会对策略分类表中的流量增加统计功能,单桶模式,报文经过 policy 时仅会有绿色和红色两种颜色,打印统计信息时 in-profile 表示绿色, out-profile 表示红色;双桶模式下,会有三种颜色的报文,in-profile 表示绿色, out-profile 表示红色和黄色。
策略分类表配置模式	
<pre>drop no drop transmit no transmit</pre>	对分类后的流量可以选择丢弃、通过动作;本命令的 no 操作为取消分配的动作。

3. 将 QoS 应用到端口或 VLAN 接口

命令	解释
接口配置模式	
mls qos trust dscp no mls qos trust dscp	配置交换机端口信任状态；本命令的 no 操作为禁止交换机端口的当前信任状态。
mls qos cos {<default-cos> } no mls qos cos	配置交换机端口的缺省 CoS 值；本命令的 no 操作为恢复缺省情况。
service-policy input <policy-map-name> no service-policy input {<policy-map-name>}	在端口上应用一个策略表；本命令的 no 操作为删除应用到交换机端口的某个指定策略表或删除该端口入方向应用的所有策略表。目前在出口不支持出口策略表。
全局配置模式	
service-policy input <policy-map-name> vlan <vlan-list> no service-policy input {<policy-map-name>} vlan <vlan-list>	在交换机 VLAN 接口上应用一个策略表；本命令的 no 操作为删除应用到交换机 VLAN 接口的某个指定策略表或删除该 vlan 接口入方向应用的所有策略表。

4. 配置端口队列调度算法和权重

命令	解释
端口配置模式	
mls qos queue algorithm {sp wrr wdr} no mls qos queue algorithm	端口配置队列调度算法。端口缺省队列调度算法为 wrr 。
mls qos queue wrr weight <weight0..weight7> no mls qos queue wrr weight	基于端口配置队列权重。缺省队列权重为 1 2 3 4 5 6 7 8。
mls qos queue wdr weight <weight0..weight7> no mls qos queue wdr weight	基于端口配置队列权重。缺省队列权重为 10 20 40 80 160 320 640 1280。
mls qos queue <queue-id> bandwidth <minimum-bandwidth> <maximum-bandwidth> no mls qos queue <queue-id> bandwidth	基于端口配置带宽保证值。

5. 配置 QoS 映射关系

命令	解释
全局配置模式	
mls qos map (cos-dp <dp1...dp8> dscp-dscp <in-dscp list> to <out-dscp> 	设置 QoS 的优先级映射， no 命令恢复缺省映射值。

<pre>dscp-intp <in-dscp list> to <intp> dscp-dp <in-dscp list> to <dp>) no mls qos map (cos-dp dscp-dscp dscp-intp dscp-dp) mls qos map intp-dscp <dscp1..dscp8> no mls qos map intp-dscp</pre>	
---	--

6. 清除特定端口或者 VLAN 的 Accounting 数据

命令	解释
特权配置模式	
clear mls qos statistics [interface <interface-name> vlan <vlan-id>]	清除特定端口或者 vlan Policy Map 的 Accounting 数据，如果不带参数，清除所有的 Policy Map 的 Accounting 数据。

7. 显示 QoS 的配置信息

命令	解释
特权配置模式	
show mls qos maps [cos-dp dscp-dscp dscp-intp dscp-dp intp-dscp]	显示 QoS 全局映射相关配置内容。
show class-map [<class-map-name>]	显示 QoS 的分类表信息。
show policy-map [<policy-map-name>]	显示 QoS 的策略表信息。
show mls qos {interface [<interface-id>] [policy queuing] vlan <vlan-id>}	显示 QoS 在交换机端口上的配置信息。

1.3 QoS 举例

案例 1:

启动 QoS 功能，将端口 ethernet 1/0/1 出口队列的权重改为 1:1:2:2:4:4:8:8，配置成信任 cos 模式，但是不改变报文里的 DSCP 值，并且将此端口的默认 cos 值设为 5。

配置步骤如下：

```
Switch#config
```

```
Switch(config)#interface ethernet 1/0/1
```

```
Switch(Config-If-Ethernet1/0/1)# mls qos queue wrr weight 1 1 2 2 4 4 8 8
```

```
Switch(Config-If-Ethernet1/0/1)#mls qos cos 5
```

配置结果：

全局启动了 QoS 功能，端口 ethernet 1/0/1 出口带宽的比例依次为 1:1:2:2:4:4:8:8。当从

ethernet 1/0/1 进来的报文带 cos 值时，根据 cos 值到出口队列的映射关系，cos 值 0—7 分别对应出口队列 1, 2, 3, 4, 5, 6, 7, 8，放到不同的优先队列，如果进来的报文不带 cos 值，则将其 cos 值设为 5，根据对应关系，放入优先级队列 6。所有经过的报文不改变其携带的 DSCP 值。

案例 2:

在端口 ethernet1/0/2 上，将属于网段 192.168.1.0 内的报文带宽限制为 10M 比特/秒，突发值设为 4M 字节，超过带宽的该网段内的报文一律丢弃。

配置步骤如下：

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy 10000 4000 exceed-action drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#service-policy input p1
```

配置结果：

先设置一个 ACL：1，匹配网段 192.168.1.0。全局启动 QoS 功能，创建一个 class-map：c1，在 class-map 中匹配 ACL1，再创建一个 policy-map：p1，在 P1 中引用 c1，设置对应的 policy 来限制带宽和峰值。然后在端口 ethernet 1/0/2 应用此 policy-map。设置后，网段 192.168.1.0 内的报文带宽在端口 ethernet 1/0/2 上被限制为 10M 比特/秒，突发值为 4M 字节，超过带宽的该网段内的报文一律丢弃。

案例 3:

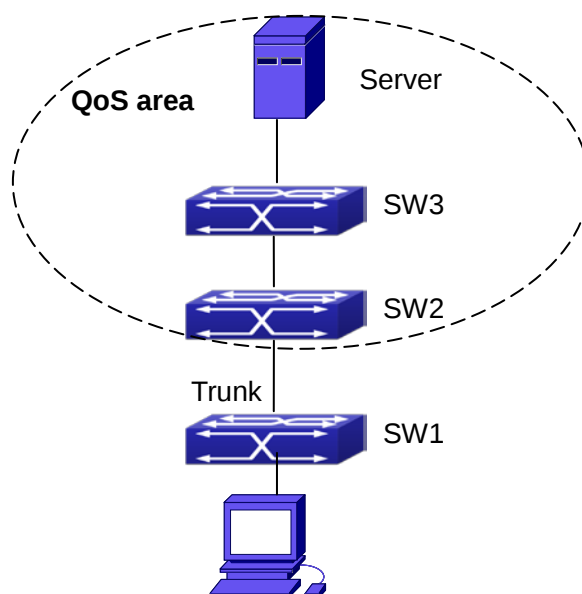


图 1-7 QoS 典型拓扑

如图，虚线框内组成一个 QoS 域，SW1 将不同的流量分类，分配不同的 IP 优先级，如在端口 ethernet 1/0/1 上将属于网段 192.168.1.0 内的报文的 IP 优先级设为 5，与 SW2 相连的端口为 trunk 口。在 SW2 上，将与 SW1 相连的端口 ethernet 1/0/1，设置信任 cos。这样在 QoS 域的内部，不同优先级的报文就走不同的队列，分配不同的带宽。

配置步骤如下：

交换机 1 上的 QoS 配置：

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 5
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#service-policy input p1
```

交换机 2 上的 QoS 配置：

```
Switch#config
Switch(config)#interface ethernet 1/0/1
```

1.4 QoS排错帮助

☞ trust COS 和 exp 配置可以和其他的 trust 一起生效，也可以和 Policy Map 一起使用。

☞ trust dscp 配置可以和其他的 trust 一起生效，也可以和 Policy Map 一起使用。本配置对 IPv4 和 IPv6 报文都生效。

☞ Trust EXP、Trust DSCP 和 Trust COS 可以同时配置，他们之间的优先级如下：
EXP>DSCP>COS

☞ 如果配置了动态 vlan（mac vlan/voice vlan/ip subnet vlan/protocol vlan），报文的 COS 值等于动态 vlan 的 COS 值。

☞ 目前策略表只支持绑定到入口，对出口不支持。

☞ 目前建议不要在 vlan 和属于该 vlan 的端口上同时使用 policy map。

第2章 PBR配置

2.1 PBR介绍

PBR（Policy-Based Routing，策略路由）是根据 IP 包的源地址、目的地址、IP 优先级、TOS 值、IP 协议、源端口号、目的端口号等信息来策略性的指定数据包转发的下一跳的一种方法。

2.2 PBR配置

1. 配置一个 class-map（分类表）
2. 设置分类表中的匹配标准
3. 配置一个 policy-map（策略表）
4. 配置一个策略表对应一个 class（分类表）
5. 配置下一跳 IPv4 地址
6. 配置端口捆绑策略表
7. 配置 VLAN 捆绑策略表

1. 配置一个 class-map（分类表）

命令	解释
全局配置模式	
class-map <class-map-name> no class-map <class-map-name>	建立或删除一个 class-map（分类表）。

2. 设置分类表中的匹配标准

命令	解释
class-map（分类表）配置模式	
match ip {access-group <acl-index-or-name>} no match ip {access-group }	设置分类表中的匹配标准。

3. 配置一个 policy-map（策略表）

命令	解释
全局配置模式	
policy-map <policy-map-name> no policy-map <policy-map-name>	建立或删除一个 policy-map（策略表）。

4. 配置一个策略表对应一个 class（分类表）

命令	解释
策略表配置模式	

class <class-map-name> no class <class-map-name>	对应一个 class（分类表），并进入策略分类表模式。
---	-----------------------------

5. 配置下一跳 IPv4 地址

命令	解释
策略分类表配置模式	
set ipv4 [default] nexthop [vrf <vrf>] <nexthop-ip> no set ipv4 nexthop	为分类后的流量设置下一跳 IP；本命令的 no 操作为取消分配新的值。

6. 配置端口捆绑策略表

命令	解释
端口配置模式	
service-policy {input output} <policy-map-name> <policy-map-name>} no service-policy {input output} <policy-map-name> <policy-map-name>}	在具体端口上应用策略表；每个端口在每个方向上只能应用一个策略表。目前在出口不支持出口策略表。

7. 配置 VLAN 捆绑策略表

命令	解释
全局配置模式	
service-policy input <policy-map-name> vlan <vlan-list> no service-policy input <policy-map-name> vlan <vlan-list>	在具体 VLAN 上绑定策略表。本命令的 no 操作为删除应用到交换机 VLAN 接口的某个指定策略表。

2.3 PBR 举例

案例：

在端口 ethernet 1/0/1 上，设置源 IP 为 192.168.1.0/24 网段内的报文进行策略路由，其下一跳为 218.31.1.119。同时，该网络的内网 IP 是在 192.168.0.0/16 范围。为了保证内网正常通信，对于源 IP 为 192.168.1.0/24，目的 IP 为内网 IP 192.168.0.0/16 范围内的报文不进行策略路由，本设备 192.168.1.0/24 段的接口地址为 192.168.1.1。

配置步骤如下：

```
Switch#config
```

```
Switch(config)#ip access-list extended a1
```

```
Switch(Config-IP-Ext-Nacl-a1)# permit ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255
```

```
Switch(Config-IP-Ext-Nacl-a1)#exit
```

```
Switch(config)#ip access-list extended a2
```

```
Switch(Config-IP-Ext-Nacl-a1)# permit ip 192.168.1.0 0.0.0.255 any-destination
Switch(Config-IP-Ext-Nacl-a1)#exit
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group a1
Switch(Config-ClassMap-c1)# exit
Switch(config)#class-map c2
Switch(Config-ClassMap-c2)#match access-group a2
Switch(Config-ClassMap-c2)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip nexthop 192.168.1.1
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#class c2
Switch(Config-PolicyMap-p1-Class-c2)#set ip nexthop 218.31.1.119
Switch(Config-PolicyMap-p1-Class-c2)#exit
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#service-policy input p1
```

配置结果：

先设置两个包含两个项的 ACL a1、a2，a1 匹配源 IP 网段 192.168.1.0/24 和目的地 IP 网段 192.168.0.0/16，a2 匹配源 IP 网段 192.168.1.0/24。全局启动 QoS 功能，创建两个 class-map：c1 和 c2，在 class-map c1 中匹配 ACL a1，class-map c2 中匹配 ACL a2。再创建一个 policy-map：p1，在 P1 中引用 c1，设置本设备 192.168.1.0/24 段的接口地址为 192.168.1.1，设置下一跳 IP 为 218.31.1.119。然后在端口 ethernet 1/0/1 应用此 policy-map。设置后，端口 ethernet 1/0/1 上对于源 IP 为网段 192.168.1.0/24 的报文，除目的 IP 为网段 192.168.0.0/16 的报文进行正常的 L3 转发之外，其余的报文经 218.31.1.119 转发。

第3章 IPv6 PBR配置

说明：

本章所指的路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

3.1 PBR（基于策略的路由）功能介绍

基于策略的路由为网络管理者提供了比传统路由协议对报文的转发和存储更强的控制能力，传统上，路由器用从路由协议派生出来的路由表，根据目的地址进行报文的转发，基于策略的路由比传统路由强，使用更灵活，它使网络管理者不仅能够根据目的地址而且能够根据报文的大小，应用或 IP 源地址来选择转发路径。策略可以定义为通过多路由器的负载均衡或根据总流量在各线上进行转发的服务质量（QoS）。

PBR（Policy-Based Routing，策略路由）是根据 IP 包的源地址、目的地址、IP 优先级、TOS 值、IP 协议、源端口号、目的端口号等信息来策略性的指定数据包转发的下一跳的一种方法。

3.2 PBR配置任务序列

1. 配置一个 class-map（分类表）
2. 设置分类表中的匹配标准
3. 配置一个 policy-map（策略表）
4. 配置一个策略表对应一个 class（分类表）
5. 配置下一跳 IPv6 地址
6. 配置端口捆绑策略表
7. 配置 VLAN 捆绑策略表

1. 配置一个 class-map（分类表）

命令	解释
全局配置模式	
class-map <class-map-name> no class-map <class-map-name>	建立或删除一个 class-map（分类表）。

2. 设置分类表中的匹配标准

命令	解释
class-map（分类表）配置模式	
match ipv6 {access-group <acl-index-or-name>} no match ipv6 {access-group }	设置分类表中的匹配标准。

3. 配置一个 policy-map（策略表）

命令	解释
----	----

全局配置模式	
policy-map <policy-map-name> no policy-map <policy-map-name>	建立或删除一个 policy-map（策略表）。

4. 配置一个策略表对应一个 class（分类表）

命令	解释
策略表配置模式	
class <class-map-name> no class <class-map-name>	对应一个 class（分类表），并进入策略分类表模式。

5. 配置下一跳 IPv6 地址

命令	解释
策略分类表配置模式	
set ipv6 [default] nexthop [vrf <vrf>] <nexthop-ip> no set ipv6 nexthop	为分类后的流量设置下一跳 IP；本命令的 no 操作为取消分配新的值。

6. 配置端口捆绑策略表

命令	解释
端口配置模式	
service-policy {input <policy-map-name> output <policy-map-name>} no service-policy {input <policy-map-name> output <policy-map-name>}	在具体端口上应用策略表；每个端口在每个方向上只能应用一个策略表。目前在出口不支持出口策略表。

7. 配置 VLAN 捆绑策略表

命令	解释
全局配置模式	
service-policy input <policy-map-name> vlan <vlan-list> no service-policy input <policy-map-name> vlan <vlan-list>	在具体 VLAN 上绑定策略表。本命令的 no 操作为删除应用到交换机 VLAN 接口的某个指定策略表。

3.3 PBR 举例

案例：

在端口 ethernet1/0/1 上，本设备默认网关地址为 3000::1，设置源 IP 为 2000::/64 网段内的报文进行策略路由，其下一跳地址为 3100::2。

配置步骤如下：

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2000::1/64
Switch(Config-if-Vlan1)#ipv6 neighbor 2000::2 00-00-00-00-00-01 interface Ethernet 1/0/1
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 address 3000::1/64
Switch(Config-if-Vlan2)#ipv6 neighbor 3000::2 00-00-00-00-00-02 interface Ethernet 1/0/2
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ipv6 address 3100::1/64
Switch(Config-if-Vlan3)#ipv6 neighbor 3100::2 00-00-00-00-00-03 interface Ethernet 1/0/5
Switch(config)# ipv6 access-list extended b1
Switch(Config-IPv6-Ext-Nacl-b1)# permit 2000::/64 any-destination
Switch(Config-IPv6-Ext-Nacl-b1)#exit
Switch(config)#class-map c1
Switch(config-ClassMap)#match ipv6 access-group b1
Switch(config-ClassMap)#exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config-Policy-Class)#set ipv6 nexthop 3100::2
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)#service-policy input p1
```

配置结果：

先设置一个包含一个项的 ACL b1，匹配源 IP 网段 2000::/64（允许）。全局启动 QoS 功能，创建一个 class-map: c1，在 class-map 中匹配 ACL b1，再创建一个 policy-map: p1，在 p1 中引用 c1，设置下一跳 IP 为 3100::2。然后在端口 ethernet1/0/1 应用此 policy-map。设置后，端口 ethernet1/0/1 上对于源 IP 为网段 2000::/64 的报文经 3100::2 转发。

3.4 PBR排错帮助

- ☞ 目前策略表只支持绑定到入口，对出口不支持。
- ☞ 受硬件资源限制，如果策略过于复杂，配置不上，会提示用户相关信息。

第4章 基于流的重定向

4.1 基于流的重定向介绍

基于流的重定向功能是指交换机把端口接收到的、符合特定条件（ACL 指定）的数据帧转发到另一个指定的端口；其中符合同一个特定的条件称为一类流，数据帧的入端口称为重定向源端口，指定的出端口称为重定向目的端口。通常基于流的重定向应用在两个方面：1.在重定向目的端口处连接一个协议分析仪（如 Sniffer）或者 RMON 监测仪，可以监视和管理网络，并且能诊断网络故障；2.为特定类型的数据帧指定转发策略。

交换机只能为同一个重定向源端口内的同一类流指定一个唯一的重定向目的端口，为同一个重定向源端口内的不同流指定一个不同的重定向目的端口；同一类流也可以应用到不同的源端口。

4.2 基于流的重定向配置任务序列

1. 基于流的重定向配置
2. 查看当前的基于流的重定向配置

1.基于流的重定向配置

命令	解释
物理接口配置模式	
access-group <aclname> redirect to interface [ethernet <IFNAME> <IFNAME>] no access-group <aclname> redirect	为端口指定基于流的重定向； 本命令的 no 操作为删除基于流的重定向

2.查看当前的基于流的重定向配置

命令	解释
全局配置模式/特权用户配置模式	
show flow-based-redirect {interface [ethernet <IFNAME> <IFNAME>]}	显示当前系统/端口中配置的基于流的重定向信息

4.3 基于流的重定向举例

案例：

用户有如下的配置需求：将 1 端口收到的源 IP 为 192.168.1.111 的帧重定向到 6 端口，即从 1 端口收到的源 IP 为 192.168.1.111 的帧通过 6 端口转发出去。

配置修改：

- 1: 配置一条 ACL，匹配条件：源 IP 为 192.168.1.111；
- 2: 将基于该流的重定向应用到端口 1。

配置步骤如下：

```
Switch(config)#access-list 1 permit host 192.168.1.111
```

```
Switch(config)#interface ethernet 1/0/1
```

```
Switch(Config-If-Ethernet1/0/1)# access-group 1 redirect to interface ethernet 1/0/6
```

4.4 基于流的重定向排错帮助

当配置基于流的重定向功能出现问题时，请检查是否是如下原因：

- ☞ 流的类型（ACL）只能为数字标准 IP 访问列表、数字扩展 IP 访问列表、命名标准 IP 访问列表、命名扩展 IP 访问列表、数字标准 IPv6 访问列表和命名标准 IPv6 访问列表；
- ☞ ACL 中不能配置 **Timerange** 和 **Portrange** 参数，ACL 类型必须为 Permit。
- ☞ 基于流的重定向功能，其重定向目的端口必须为千兆口。
- ☞ 不能实现流的重定向的跨 Vlan 转发。