

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	1-7
1.3 QoS举例	1-11
1.4 QoS排错帮助	1-14
第 2 章 基于流的重定向	2-1
2.1 基于流的重定向介绍	2-1
2.2 基于流的重定向配置任务序列	2-1
2.3 基于流的重定向举例	2-2
2.4 基于流的重定向排错帮助	2-2
第 3 章 Egress QoS配置	3-1
3.1 Egress QoS介绍	3-1
3.1.1 Egress QoS术语.....	3-1
3.1.2 Egress QoS基本模型	3-1
3.2 Egress QoS配置	3-2
3.3 Egress QoS举例	3-5
3.4 Egress QoS排错帮助	3-7
第 4 章 灵活QinQ操作	4-1
4.1 灵活QinQ功能介绍	4-1
4.1.1 QinQ技术	4-1
4.1.2 基本QinQ.....	4-1
4.1.3 灵活QinQ.....	4-1
4.2 灵活QinQ配置	4-1
4.3 灵活QinQ举例	4-3
4.4 灵活QinQ排错帮助	4-4

第1章 QoS配置

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。

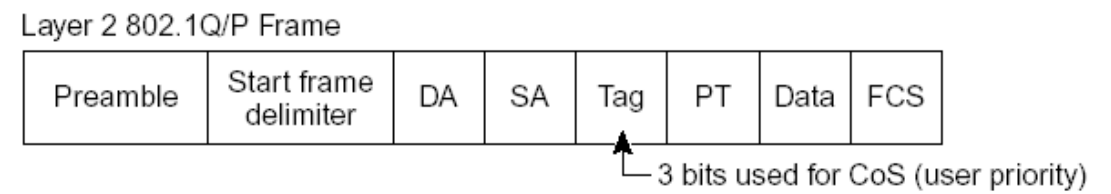


图 1-1 CoS 优先级

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。

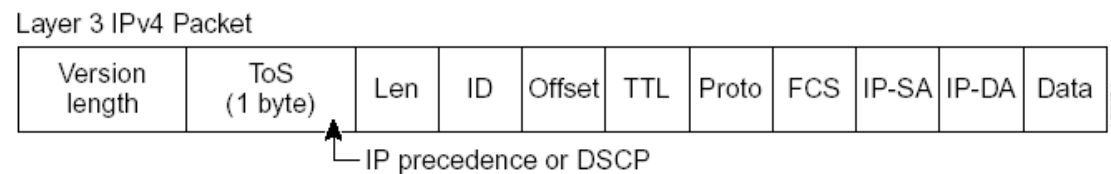


图 1-2 ToS 优先级

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。

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，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，根据数据包的内部优先级（internal priority），将其归入相应的出口队列。然后根据报文本身的 Drop Precedence、所在的出口队列的发送算法和队列权重，进行发送和丢弃决定。

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。

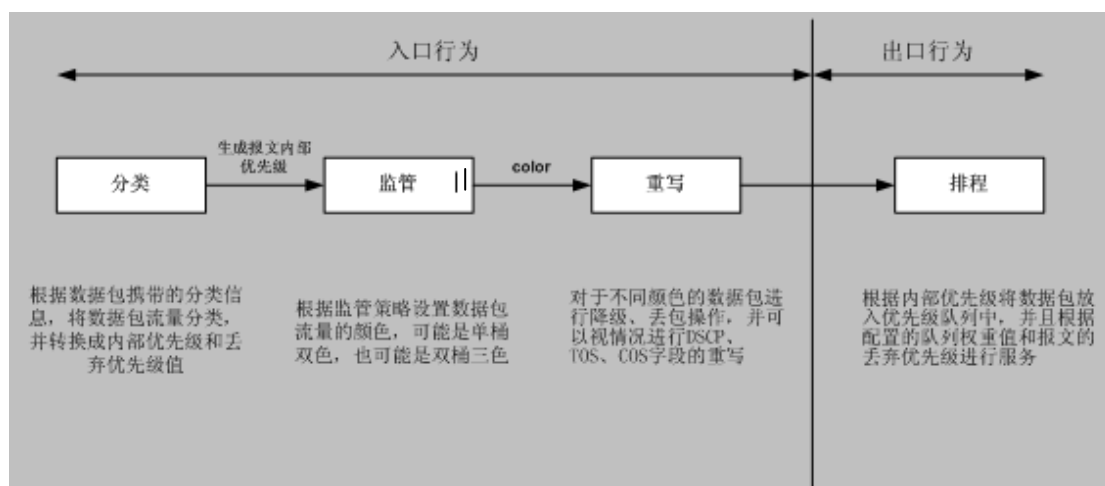


图 1-3 QoS 基本模型

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。对于不同类型的数据包，分类有不同的处理方式，由下面的流程图详细说明：

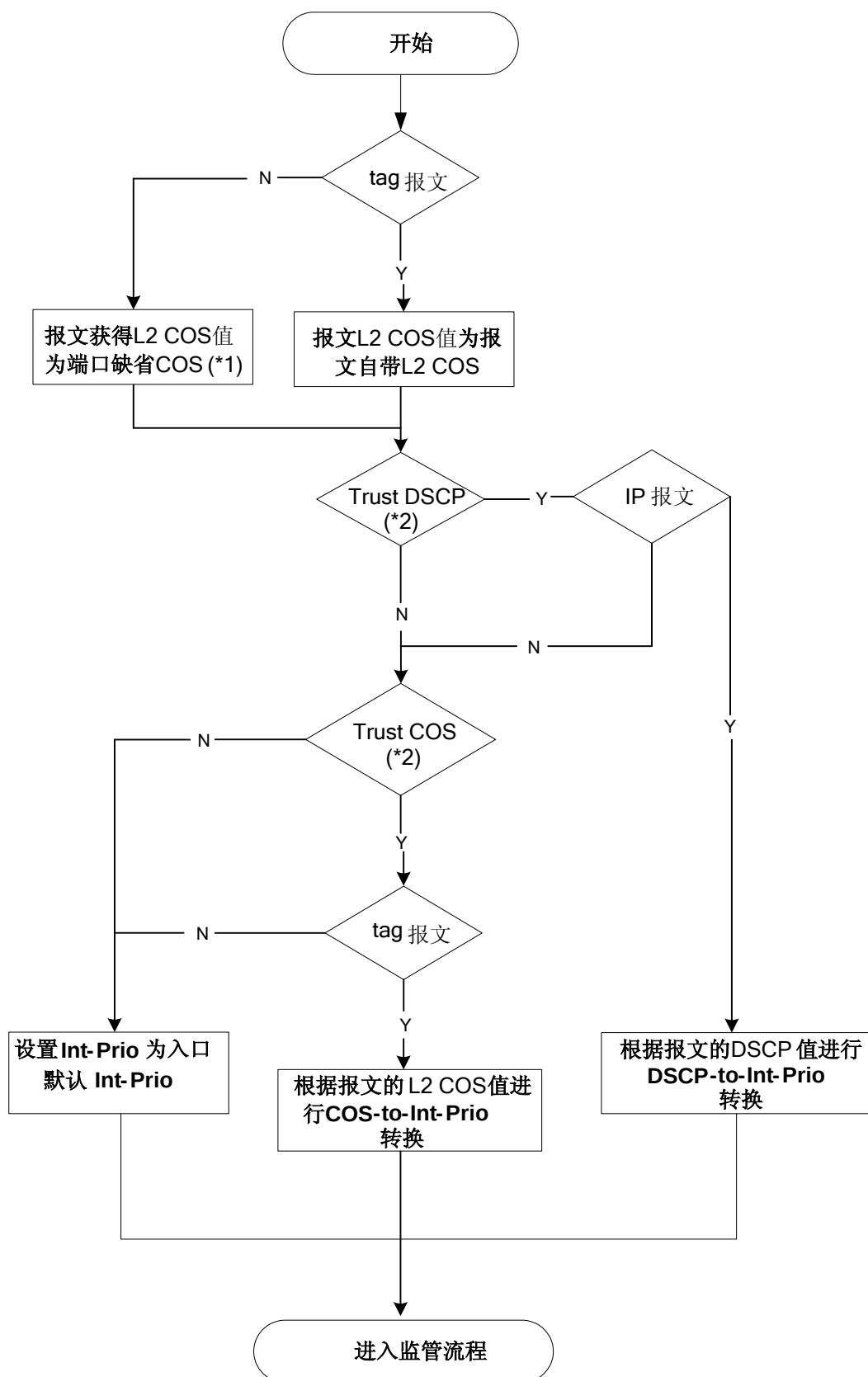


图 1-4 分类流程

注 1：该 L2 CoS 值用作报文的一个属性，与下面流程中的内部优先级的获取无关；

注 2: Trust DSCP 和 Trust COS 可以同时配置，他们之间的优先级如下：DSCP>COS。

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单桶双色，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。重写行为首先用一个新的优先级别较低的 Int-Prio 值来代替数据包原有的级别较高的 Int-Prio 值，在出口时，将根据新的 Int-Prio 修改数据包 COS 和 DSCP 字段。监管和重写的具体行为，由下面的流程图详细说明：

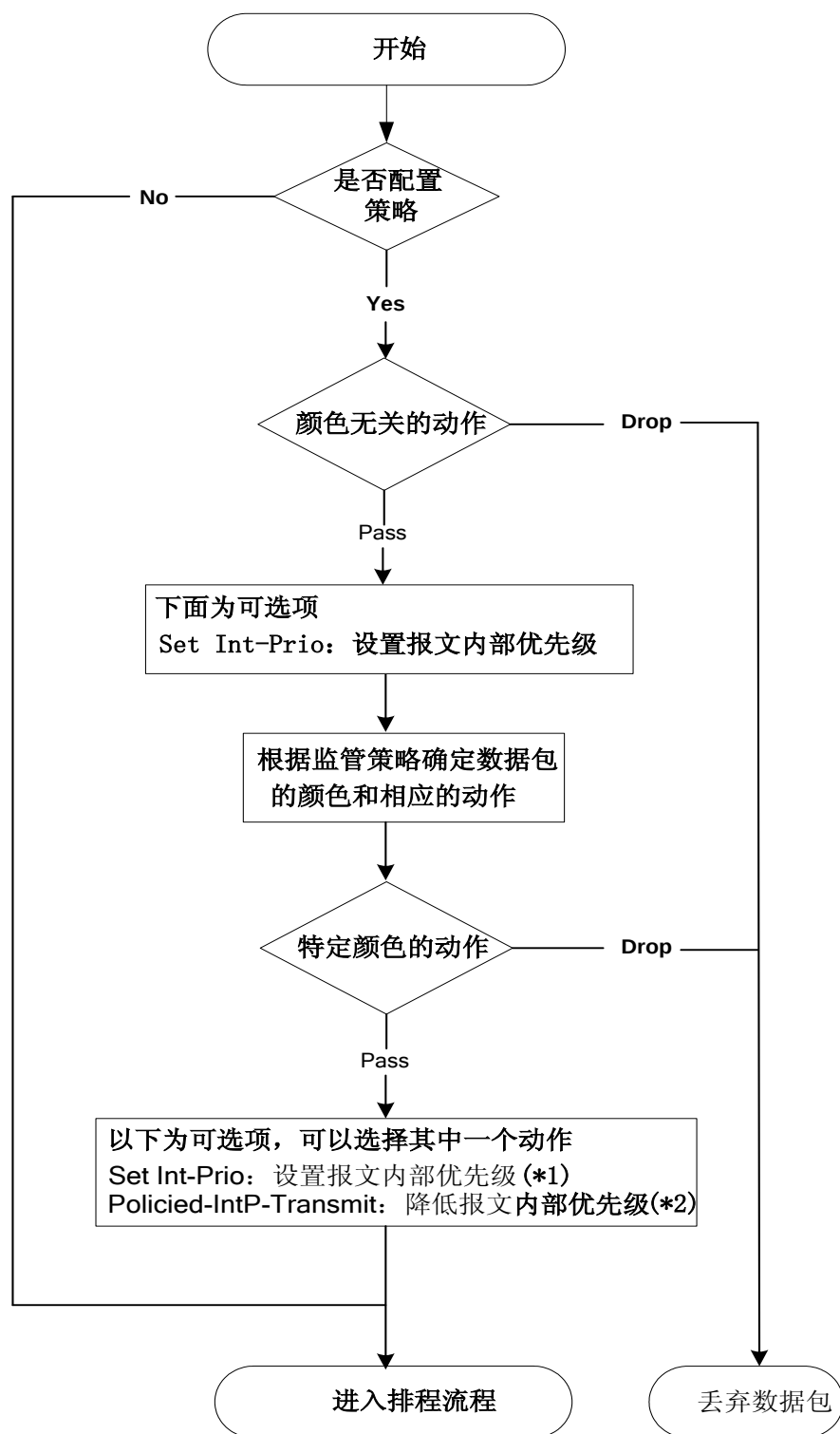


图 1-5 监管和重写流程

注 1: Int-Prio 会被后续的设置覆盖，特定颜色动作的 Set Int-Prio 会覆盖颜色无关动作的 Set Int-Prio;

注 2: 根据 IntP-to-IntP map 降低报文内部优先级，源 Int-Prio 是指监管流程之前获取的 Int-Prio，具体指分类流程中获取的 Int-Prio 或颜色无关动作中设置的 Int-Prio。

整形和排程: 出口的数据包会都具有内部优先级值，排程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，然后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。排程的具体行为，由下面的流程图详细说明：

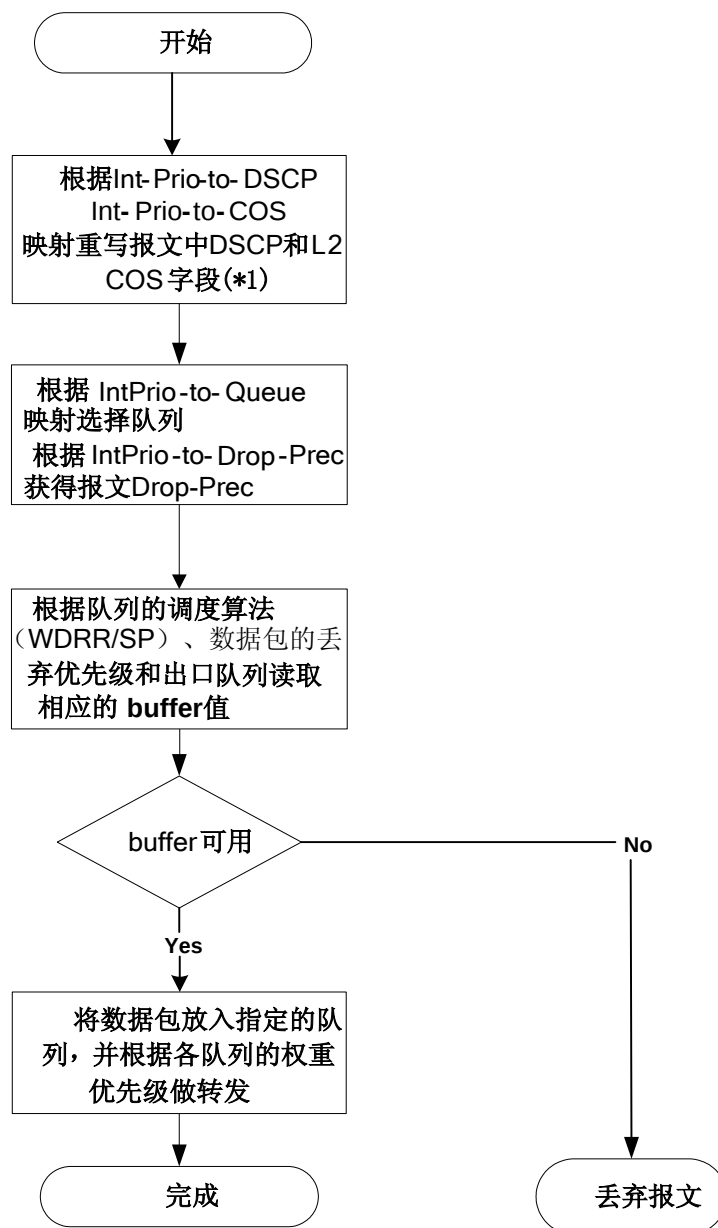


图 1-6 整形和排程流程

注 1: 入口处可以配置 `pass-through-cos`、`pass-through-dscp` 以禁止报文 L2 Cos 优先级和 dscp 值的重写，在出口处，将根据报文最终的 Int-Prio 获得报文的 L2 Cos 优先级、dscp 值，并根据 `pass-through-cos`、`pass-through-dscp` 决定是否重写报文的 L2 Cos 优先级、dscp 值。

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（**policy-map**）

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**，若在 VLAN 和属于该 VLAN 的端口上同时使用了 **policy map** 则以端口上绑定的 **policy map** 优先。

配置端口队列调度算法

设定端口队列调度算法，如 **sp**，**wrr** 等。

配置 QoS 映射关系

配置 **cos** 到 **intp**，**dscp** 到 **intp**，**intp** 到 **dscp** 或 **cos** 或 **intp** 或 **dp** 或 **queue** 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> vlan range <vlan-list>} no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp ipv6 flowlabel vlan [cos vlan range]}	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（**policy-map**）

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>]	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

no class <class-map-name>	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 internal priority <new-intp> no set internal priority	为分类后的流量分配一个新的内部优先级; 本命令的 no 操作为取消分配新的值。
单桶模式: policy <bits_per_second> <normal_burst_bytes> {{exceed-action ACTION}} 双桶模式: policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] <maximum_burst_bytes> [[exceed-action ACTION violate-action ACTION]] ACTION 定义: drop transmit set-internal-priority <intp_value> policed-intp-transmit no policy	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。
policy aggregate <aggregate-policy-name> no policy aggregate	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。
accounting no accounting	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 green 表示绿色, red 表示红色; 双桶模式下, 会有三种颜色的报文, green 表示绿色, yellow 表示黄色, red 表示红色。
策略分类表配置模式	
drop no drop transmit no transmit	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 {cos dscp} no mls qos trust {cos 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	配置交换机端口的默认 CoS 值；本命令的 no 操作为恢复缺省情况。
mls qos internal-priority {<default-intp>} no mls qos internal-priority	配置交换机端口的默认内部优先级值；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。
pass-through-cos no pass-through-cos	禁止从本端口进入的报文在出口时重写 L2 CoS 值；本命令的 no 操作为恢复允许从本端口进入的报文在出口时重写 L2 CoS 值
pass-through-dscp no pass-through-dscp	禁止从本端口进入的报文在出口时重写 dscp 值；本命令的 no 操作为恢复允许从本端口进入的报文在出口时重写 dscp 值
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 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 wdr。
全局配置模式	
mls qos queue wdr weight <weight0..weight7> no mls qos queue wdr weight	全局配置所有端口的 wdr 队列权重。缺省队列权重为 1 1 1 1 1 1 1 1。

5. 配置 QoS 映射关系

命令	解释
全局配置模式	
mls qos map {cos-intp <intp1...intp8> dscp-intp <in-dscp list> to <intp> intp-cos <intp list> to <out-cos> intp-dp <intp list> to <out-dp> intp-dscp <intp list> to <out-dscp> intp-intp <color> <intp list> to <intp> intp-queue <intp list> to <out-queue> } no mls qos map {cos-intp dscp-intp intp-cos intp-dp intp-dscp intp-intp <color> intp-queue}	设置 QoS 的优先级映射，no 命令恢复缺省映射值。

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-intp dscp-intp intp-intp intp-cos intp-dscp intp-dp intp-queue]	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 aggregate-policy [<aggregate-policy-name>]	显示 QoS 的集合策略配置信息。
show mls qos interface [<interface-id> [policy queuing]	显示 QoS 在交换机端口上的配置信息。
show mls qos vlan <v-id>	显示 QoS 在交换机 vlan 接口上的配置信息。

1.3 QoS 举例

案例 1:

启动 QoS 功能，将交换机全局出口队列的权重改为 1:1:2:2:4:4:8:8，端口 ethernet 1/0/1

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)# mls qos queue weight 1 1 2 2 4 4 8 8
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet 1/0/1)#mls qos trust cos
Switch(Config-If-Ethernet 1/0/1)#pass-through-dscp
Switch(Config-If-Ethernet1/0/1)#mls qos cos 5
```

配置结果：

全局启动了 QoS 功能，各端口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 值到内部优先级的映射关系，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-c1)# 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：

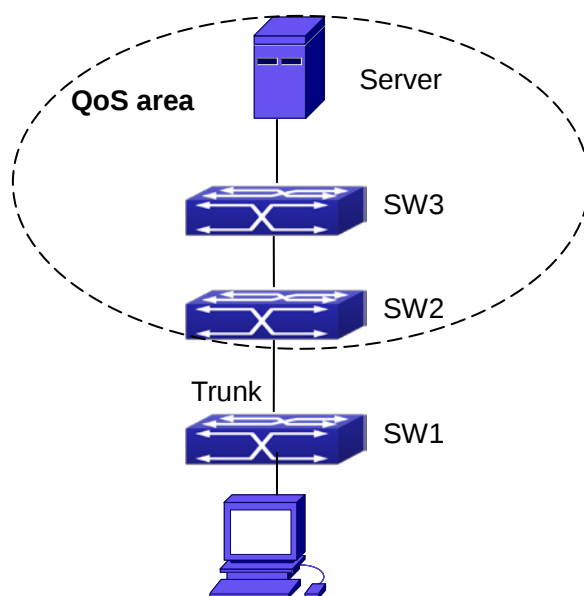


图 1-7 QoS 典型拓扑

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（通过设置内部优先级为 40，默认 intp-dscp 的映射关系为 40-40，相对应的 IP 优先级为 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 dscp。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 40
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
Switch(Config-If-Ethernet1/0/1)#mls qos trust dscp
```

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。

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

第2章 基于流的重定向

2.1 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。

2.2 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
3. 配置端口的 vlan 重定向功能
4. 设置每个端口 redirect 的 vlan 数最大值

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

3. 配置端口的 vlan 重定向功能

命令	解释
端口模式	
match vlan <1-4096> redirect interface (ethernet) IFNAME no match vlan <1-4096> redirect	配置端口的 vlan 重定向功能。
port-redirect match vlan <1-4094> source-port	配置端口的 vlan 重定向功能。

<pre> interface (ethernet) IFNAME destination-port interface (ethernet) IFNAME no port-redirect match vlan <1-4094> source-port interface (ethernet) IFNAME destination-port interface (ethernet) IFNAME </pre>	
---	--

4. 设置每个端口 redirect 的 vlan 数最大值

命令	解释
全局模式	
<pre> vlan-port-redirect vlan maximum <1-1000> no vlan-port-redirect vlan maximum </pre>	设置每个端口 redirect 的 vlan 数最大值。

2.3 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
```

2.4 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。

第3章 Egress QoS配置

3.1 Egress QoS介绍

在传统的 IP 网络中，所有的报文都被无区别的等同对待，每个网络设备对所有的报文均采用先入先出的策略进行处理，它尽最大的努力（Best-Effort）将报文送到目的地，但对报文传送的可靠性、传送延迟等性能不提供任何保证。网络发展日新月异，随着 IP 网络上新应用的不断出现，对 IP 网络的服务质量也提出了新的要求。例如 VoIP 和视频等时延敏感业务对报文的传输时延提出了较高要求。如果报文传送延时太长，将是用户所不能接受的（相对而言，E-Mail 和 FTP 业务对时间延迟并不敏感）。为了支持具有不同服务需求的语音、视频以及数据等业务，要求网络能够区分出不同的通信，进而为之提供相应的服务。传统 IP 网络的尽力服务不可能识别和区分出网络中的各种通信类别，而具备通信类别的区分能力正是为不同的通信提供差异化服务的前提，所以说传统网络的尽力服务模式已不能满足应用的需要。QoS 技术的出现便致力于解决这个问题。

Egress Polycymap 即出口 QoS 策略，Egress PolicyMap 可以在出口方向对报文进行 QoS 控制，通过利用各种各样的技术为选定的网络通信提供更好的服务的能力。Egress PolicyMap 包括 class-map、policy-map 两大部分，class-map 用于选定操作的数据包，policy-map 用于设定使用何种操作。目前仅部分设备支持 Egress QoS。

3.1.1 Egress QoS术语

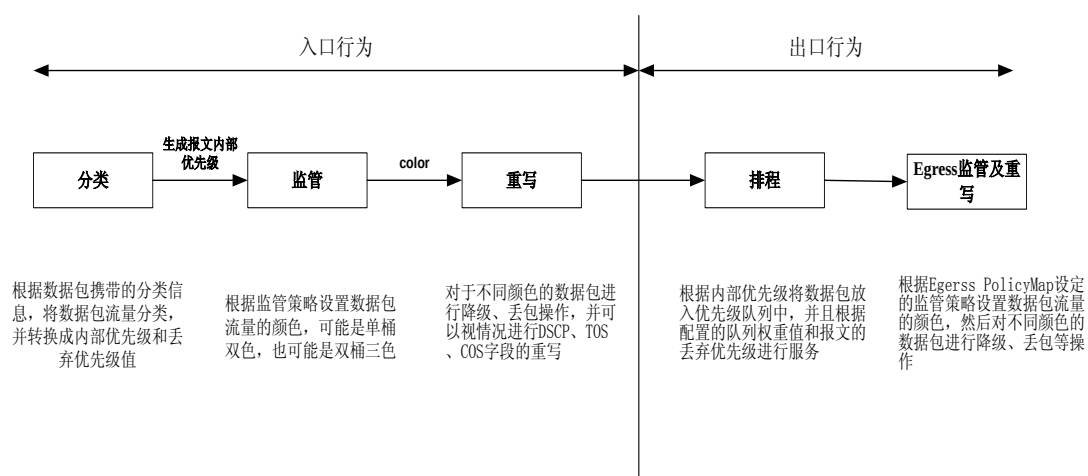
Egress QoS: 在端口出方向实现 QoS 功能。

Inner_vid: 双 TAG 的时候，靠近网络层头的 TAG 所带的 vlan id。

Outer_vid: 双 TAG 的时候，靠近网络链路层包头的 TAG 所带的 vlan id。一个 TAG 就默认为 outer tag。

Outer_tpid: 网络链路层包头的协议类型，表示 outer tag 的类型。

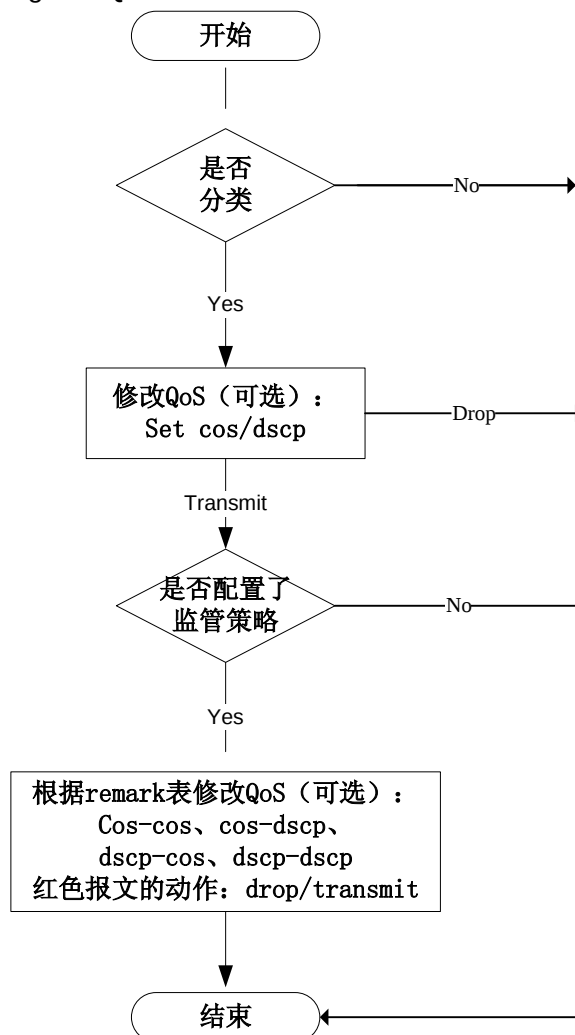
3.1.2 Egress QoS基本模型



Egress 监管及重写根据上游报文的特点（包括：CoS、DSCP 等域值），在报文出口之

前，对报文进行最后一次 QoS 修改。

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。下面的流程图详细说明 Egress QoS 流程：



上图中根据出口 remark 表修改 QoS 属性的动作解释：

cos-cos：根据报文自身 cos 值按照 QoS remarking 的 cos 表修改报文的 cos 值；

cos-dscp：根据报文自身 cos 值按照 QoS remarking 的 cos 表修改报文的 dscp 值；

dscp-cos：根据报文自身 dscp 值按照 QoS remarking 的 dscp 表修改报文的 cos 值；

dscp-dscp：根据报文自身 dscp 值按照 QoS remarking 的 dscp 表修改报文的 dscp 值。

3.2 Egress QoS配置

Egress 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 DSCP 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、分配新的 DSCP 值等等。

将 Egress 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。

设置 Egress QoS remark 映射表

如果 policy 中使用了 Egress QoS remark 表进行 QoS 属性修改，就要设置相应的映射表；如果要对绿色报文生效，还要打开绿色报文的修改开关；同时入口还要 trust 相应的 QoS 属性(qos/dscp/exp)。

1. 配置分类表（class-map）

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 dscp <dscp-list> vlan <vlan-list> cos <cos-list> ipv6 access-group <acl-index-or-name>} no match {access-group ip dscp ip precedence ipv6 dscp vlan cos ipv6 access-group}	设置分类表中的匹配标准，可以根据 ACL、CoS、VLAN ID、IPv4 Precedence、DSCP、IPv6 DSCP 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（policy-map）

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> cos <new-cos> c-vid <new-c-vid> s-vid <new-s-vid> s-tpid <new-s-tpid>} no set {ip dscp ip precedence cos c-vid 	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。

s-vid s-tpid}	
单桶模式: <pre>policy <bits_per_second> <normal_burst_bytes> [{action ACTION} exceed-action drop transmit}]</pre> 双桶模式: <pre>policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] <maximum_burst_bytes> [{action ACTION violate-action drop transmit}]</pre> ACTION 定义: <pre>policied-cos-to-cos-transmit policied-cos-to-dscp-transmit policied-dscp-exp-to-cos-transmit policied-dscp-exp-to-dscp-transmit 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>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。

3. 策略应用到端口或 vlan 出方向

命令	解释
接口配置模式	
<pre>service-policy output <policy-map-name> no service-policy output {<policy-map-name>}</pre>	在端口出方向上应用一个策略表; 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出方向应用的所有策略表。
全局配置模式	
<pre>service-policy output <policy-map-name> vlan <vlan-list> no service-policy output {<policy-map-name>} vlan <vlan-list></pre>	在交换机 VLAN 出方向上应用一个策略表; 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 接口出方向应用的所有策略表。

4. 设置 Egress QoS remark 映射表

命令	解释
全局配置模式	
mls qos map {cos-cos cos-dscp} {green yellow red} <value1> <value2>...<value8> no mls qos map {cos-cos cos-dscp} {green yellow red}	设置 Egress cos 映射表；本命令的 no 操作为回复默认配置。
mls qos map {dscp-cos dscp-dscp} {green yellow red} <dscp list> to <value> no mls qos map {dscp-cos dscp-dscp} {green yellow red}	设置 Egress dscp 映射表，<dscp-list>表示 1-8 个 dscp 值；本命令的 no 操作为回复默认配置。
mls qos egress green remark no mls qos egress green remark	设置 Egress QoS remark 映射对绿色报文生效；no 操作表示不对绿色报文生效。

5. 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。

6. 显示 QoS 的配置信息

命令	解释
特权配置模式	
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。
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 maps {cos-cos cos-dscp dscp-cos dscp-exp} {green yellow red }	显示 Egress QoS remark 表映射关系。

3.3 Egress QoS 举例

案例 1:

在端口 1 的出口方向，对于 dscp 值为 0 的报文，选取的动作为将该报文 cos 值改为 4。
创建一个分类表

```
Switch(config)#class-map c1
```

```
switch(config-classmap-c1)#match ip dscp 0
```

```
switch(config-classmap-c1)#exit
```

创建一个策略表

```

switch(config)#policy-map p1
switch(config-policy-map-p1)#class c1
switch(config-policy-map-p1-class-c1)#set cos 4
switch(config-policy-map-p1-class-c1)#exit
switch(config-policy-map-p1)#exit
将策略绑定在端口
switch(config)#in e 1/0/1
switch(config-if-ethernet1/0/1)#service-policy output p1

```

案例 2:

在 vlan 10 的出方向，对于 ipv6 dscp 值为 7 的报文，选取的动作为将该报文 cos 值修改为 4。

创建一个分类表

```

switch(config)#class-map c1
switch(config-classmap-c1)#match ipv6 dscp 7
switch(config-classmap-c1)#exit

```

创建一个策略表

```

switch(config)#policy-map p1
switch(config-policy-map-p1)#class c1
switch(config-policy-map-p1-class-c1)#set cos 4
switch(config-policy-map-p1-class-c1)#exit
switch(config-policy-map-p1)#exit

```

将策略绑定在 vlan

```

switch(config)#service-policy output p1 vlan 10

```

案例 3:

在端口 1 的出口方向限速，带宽限制为 1M 比特/秒，约定突发值设为 1M 字节，最大突发值设为 4M，同时将 dscp 值为 1 的绿色报文的 dscp 值改为 10，黄色报文的 dscp 值改为 9，红色报文丢弃。

创建一个分类表

```

switch(config)#class-map c1
switch(config-classmap-c1)#match ip dscp 1
switch(config-classmap-c1)#exit

```

创建一个策略表

```

switch(config)#policy-map p1
switch(config-policy-map-p1)#class c1
switch(config-policy-map-p1-class-c1)#policy      1000      1000      4000      action
policed-dscp-exp-to-dscp-transmit violate-action drop
switch(config-policy-map-p1-class-c1)#exit
switch(config-policy-map-p1)#exit

```

设置 Egress dscp remark 映射表

```

switch(config)#mls qos map dscp-dscp green 1 to 10

```

```

switch(config)#mls qos map dscp-dscp yellow 1 to 9

```

设置 Egress remark 对绿色报文生效

```
switch(config)#mls qos egress green remark  
在入端口设置 trust dscp 模式  
switch(config-if-port-range)#mls qos trust dscp  
将策略绑定在 1 端口的出口方向  
switch(config-if-ethernet1/0/1)#service-policy output p1
```

3.4 Egress QoS排错帮助

- ☞ 目前仅部分设备支持 Egress QoS，请确认当前设备支持该功能
- ☞ 如果配置的 policy 无法绑定到端口或 VLAN，请确认分类表中 match 的选项当前设备是否支持
- ☞ 如果终端打印提示资源不足，请确认有足够的资源下发当前配置的 policy
- ☞ 如果配置了 match acl 的 policy 无法绑定到端口或 VLAN，请确认 ACL 中存在规则并且包含有 permit 规则
- ☞ 如果使用了 Egress QoS remark 修改报文的 QoS 属性没有生效，请确认入口是否设置 trust 相关的 QoS 属性。
- ☞ 如果出口策略即设置了修改所有报文（不区分颜色）的 QoS 属性（set cos/ip dscp），同时又使用 Egress remark 表针对报文颜色修改 QoS 属性，那么报文先按照前者修改，再根据修改后的值按照后者修改。

第4章 灵活QinQ操作

4.1 灵活QinQ功能介绍

4.1.1 QinQ技术

Dot1q-tunnel 也称 QinQ (802.1Q-in-802.1Q)，是对 802.1Q 的扩展，其核心思想是将用户私网 VLAN 标签 (CVLAN tag) 封装到公网 VLAN 标签 (SPVLAN tag) 上，报文带着两层 VLAN 标签穿越服务商的骨干网络，从而为用户提供一种较为简单的二层隧道。它简单而易于管理，仅仅通过静态配置即可实现，特别适用于小型的以三层交换机为骨干的企业网或小规模城域网。

QinQ 分为两种，基本 QinQ 和灵活 QinQ，两者优先级关系为：灵活 QinQ 优先级大于基本 QinQ。

4.1.2 基本QinQ

基本 QinQ 是基于端口的：当端口上配置了 QinQ 后，不论从该端口收到的报文是否带 tag，设备都会为该报文打上本端口缺省的 VLAN tag。基本 QinQ 使用起来比较简单，但设置 VLAN tag 的方式欠缺灵活。

4.1.3 灵活QinQ

灵活 QinQ 是基于数据流的：通过匹配具体的流来选择是否打上外层 VLAN Tag，打上何种外层 VLAN Tag：如根据用户 VLAN tag，MAC 地址，IPv4/IPv6 地址，IPv4/IPv6 协议，应用程序端口号等实施灵活 QinQ 特性。这样可以根据不同用户，不同业务等对报文进行外层 VLAN Tag 封装，对多种业务实施不同的承载方案。

4.2 灵活QinQ配置

灵活 QinQ 配置任务序列

灵活 QinQ 数据流的匹配采用 QOS 的 policy map 规则下发，配置序列如下：

- 1、创建分类表，对不同的数据流进行分类
- 2、创建灵活 QinQ 策略表，与分类表进行关联，并设置相应的操作
- 3、绑定灵活 QinQ 策略表到端口

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。

<pre>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> vlan <vlan-list> c-vlan <vlan-list> cos <cos-list>} no match {access-group ip dscp ip precedence ipv6 access-group ipv6 dscp vlan c-vlan cos }</pre>	设置分类表中的匹配标准，可以根据 ACL、CoS、VLAN ID、IPV4 Precedent、DSCP 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. 配置灵活 QinQ 策略表（policymap）

命令	解释
全局配置模式	
<pre>policy-map <policy-map-name> no policy-map <policy-map-name></pre>	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。
<pre>class <class-map-name> [insert-before <class-map-name>] no class <class-map-name></pre>	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。
<pre>set s-vid <vid> no set s-vid</pre>	为分类后的流量修改外层 VLAN Tag；本命令的 no 操作为取消对 VLAN Tag 的操作。
<pre>add s-vid <vid> no add s-vid <vid></pre>	为分类后的流量增加外层 VLAN Tag；本命令的 no 操作为取消对 VLAN Tag 的操作。

3. 绑定灵活 QinQ 策略表到端口

命令	解释
端口配置模式	
<pre>service-policy input<policy-map-name> no service-policy input<policy-map-name></pre>	在端口上应用策略表；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。
全局配置模式	
<pre>service-policy input<policy-map-name> vlan<vid> no service-policy input<policy-map-name> vlan <vid></pre>	在 vlan 上应用策略表；本命令的 no 操作为删除应用到交换机 vlan 的某个指定策略表。

4. 显示端口绑定的灵活 QinQ 策略表

命令	解释
特权配置模式	
show mls qos {interface [<interface-id>]	显示灵活 QinQ 在交换机端口上的配置信息。

4.3 灵活QinQ举例

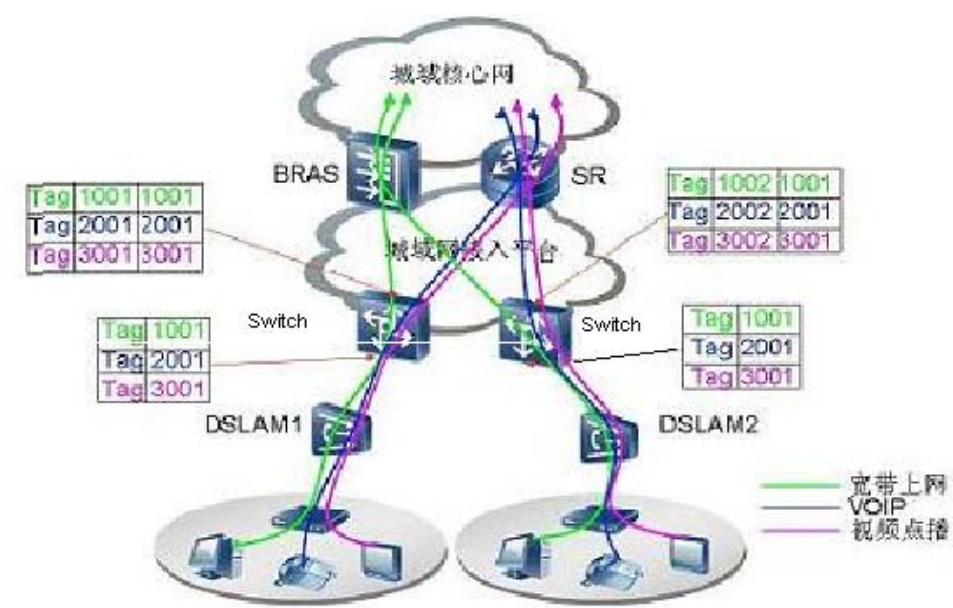


图 4-1 灵活 QinQ 应用拓扑

如上所示：比如 DSLAM1 下的用户甲，分配三个 VLAN，VLAN 标签值分别为 1001，2001，3001，VLAN1001 对应宽带上网，VLAN2001 对应 VOIP 业务，VLAN3001 对应 VOD 业务，在业务进入 Switch 交换机的下行端口后，下行端口启用灵活 QINQ 功能，根据用户 VLAN ID 分别打上不同的外层标签，如果用户数据外层标签为 1001，直接在外层增加一层标签 1001（该标签在公网唯一），业务进入 Switch 上的宽带上网 VLAN1001，数据分流到 BRAS 设备，如果标签为 2001，根据流规则，外层增加 VLAN TAG2001，业务分流到 SR 设备，同理，标签为 3001 的数据会增加一层外层标签 3001，然后分流到 SR。同理，在 DSLAM2 下的乙用户，其不同的业务可以分配不同的 VLAN 标签，注意，这里分配的 VLAN 标签可以和甲用户分配的标签相同，在进入 Switch 后根据内层标签增加一个外层标签，注意，外层标签和甲用户分配的不同，主要是为了区分 DSLAM 的位置，也是为了最终定位用户。

配置步骤如下：

假如 DSLAM1 流量业务进入 Switch 交换机下行端口为端口 1，此 Switch 配置如下：

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match vlan 1001
Switch(config-classmap-c1)#exit
Switch(config)#class-map c2
```

```
Switch(config-classmap-c2)#match vlan 2001
Switch(config-classmap-c2)#exit
Switch(config)#class-map c3
Switch(config-classmap-c3)#match vlan 3001
Switch(config-classmap-c3)#exit
Switch(config)#policy-map p1
Switch(config-policy-map-p1)#class c1
Switch(config-policy-map-p1-class-c1)#set s-vid 1001
Switch(config-policy-map-p1)#class c2
Switch(config-policy-map-p1-class-c2)#set s-vid 2001
Switch(config-policy-map-p1)#class c3
Switch(config-policy-map-p1-class-c3)#set s-vid 3001
Switch(config-policy-map-p1-class-c3)#exit
Switch(config-policy-map-p1)#exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#service-policy input p1
```

DSLAM2 流量业务进入 Switch 交换机下行端口为端口 1，此 Switch 配置如下：

```
Switch(config)#class-map c1
Switch(config-classmap-c1)#match vlan 1001
Switch(config-classmap-c1)#exit
Switch(config)#class-map c2
Switch(config-classmap-c2)#match vlan 2001
Switch(config-classmap-c2)#exit
Switch(config)#class-map c3
Switch(config-classmap-c3)#match vlan 3001
Switch(config-classmap-c3)#exit
Switch(config)#policy-map p1
Switch(config-policy-map-p1)#class c1
Switch(config-policy-map-p1-class-c1)#set s-vid 1002
Switch(config-policy-map-p1)#class c2
Switch(config-policy-map-p1-class-c2)#set s-vid 2002
Switch(config-policy-map-p1)#class c3
Switch(config-policy-map-p1-class-c3)#set s-vid 3002
Switch(config-policy-map-p1-class-c3)#exit
Switch(config-policy-map-p1)#exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#service-policy input p1
```

4.4 灵活 QinQ 排错帮助

- ☞ 如果配置的灵活 QinQ 策略无法绑定到端口，请确认灵活 QinQ 支持所配置的分类表和策略表动作
- ☞ 如果配置的灵活 QinQ 策略无法绑定到端口，如果分类表匹配的是 ACL 规则，请确认

ACL 中包含有 permit 规则

- ☞ 如果配置的灵活 QinQ 策略无法绑定到端口，请确认交换机中存在足够的 VFP 资源下发绑定
- ☞ 灵活 QinQ 与 vlan ingress 过滤对报文处理的优先级顺序如下：灵活 QinQ > vlan ingress 过滤