目 录

1 QoS 简介

1.1 概述

QoS（Quality of Service）即服务质量。对于网络业务，服务质量包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

网络资源总是有限的，只要存在抢夺网络资源的情况，就会出现服务质量的要求。服务质量是相对网络业务而言的，在保证某类业务的服务质量的同时，可能就是在损害其它业务的服务质量。例如，在网络总带宽固定的情况下，如果某类业务占用的带宽越多，那么其他业务能使用的带宽就越少，可能会影响其他业务的使用。因此，网络管理者需要根据各种业务的特点来对网络资源进行合理的规划和分配，从而使网络资源得到高效利用。

下面从 QoS 服务模型出发，对目前使用最多、最成熟的一些 QoS 技术逐一进行描述。在特定的环境下合理地使用这些技术，可以有效地提高服务质量。

1.2 QoS 服务模型简介

通常 QoS 提供以下三种服务模型：

- Best-Effort service（尽力而为服务模型）
- Integrated service（综合服务模型，简称 Int-Serv）
- Differentiated service（区分服务模型，简称 Diff-Serv）

1.2.1 Best-Effort 服务模型

Best-Effort 是一个单一的服务模型，也是最简单的服务模型。对 Best-Effort 服务模型，网络尽最大的可能性来发送报文。但对时延、可靠性等性能不提供任何保证。

Best-Effort 服务模型是网络的缺省服务模型，通过 FIFO 队列来实现。它适用于绝大多数网络应用，如 FTP、E-Mail 等。

1.2.2 Int-Serv 服务模型

Int-Serv 是一个综合服务模型，它可以满足多种 QoS 需求。该模型使用资源预留协议（RSVP），RSVP 运行在从源端到目的端的每个设备上，可以监视每个流，以防止其消耗资源过多。这种体系能够明确区分并保证每一个业务流的服务质量，为网络提供最细粒度化的服务质量区分。

但是，Inter-Serv 模型对设备的要求很高，当网络中的数据流数量很大时，设备的存储和处理能力会遇到很大的压力。Inter-Serv 模型可扩展性很差，难以在 Internet 核心网络实施。

说明

RSVP 的相关内容请参见“MPLS 配置指导”中的“MPLS TE 配置”。

1.2.3 Diff-Serv 服务模型

Diff-Serv 是一个多服务模型，它可以满足不同的 QoS 需求。与 Int-Serv 不同，它不需要通知网络为每个业务预留资源。区分服务实现简单，扩展性较好。

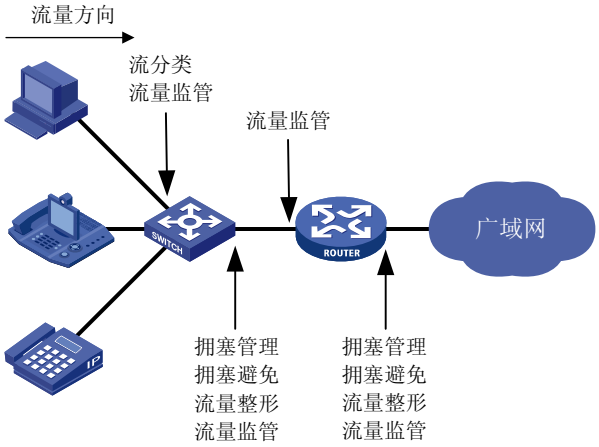
本文提到的技术都是基于 Diff-Serv 服务模型。

1.3 QoS 技术综述

QoS 技术包括流分类、流量监管、流量整形、端口限速、拥塞管理、拥塞避免等。下面对常用的技术简单进行一下介绍。

1.3.1 QoS 技术在网络中的位置

图1-1 常用 QoS 技术在网络中的位置

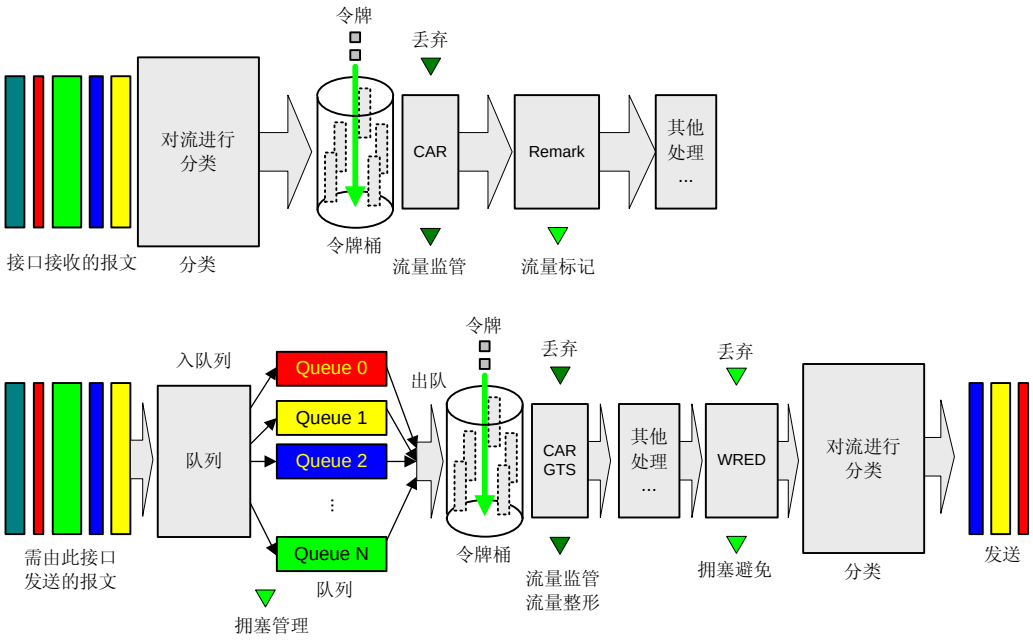


如 图 1-1所示，流分类、流量监管、流量整形、拥塞管理和拥塞避免主要完成如下功能：

- 流分类：采用一定的规则识别符合某类特征的报文，它是对网络业务进行区分服务的前提和基础。
- 流量监管：对进入或流出设备的特定流量进行监管。当流量超出设定值时，可以采取限制或惩罚措施，以保护网络资源不受损害。可以作用在接口入方向和出方向。
- 流量整形：一种主动调整流的输出速率的流量控制措施，用来使流量适配下游设备可供给的网络资源，避免不必要的报文丢弃，通常作用在接口出方向。
- 拥塞管理：就是当拥塞发生时如何制定一个资源的调度策略，以决定报文转发的处理次序，通常作用在接口出方向。
- 拥塞避免：监督网络资源的使用情况，当发现拥塞有加剧的趋势时采取主动丢弃报文的策略，通过调整队列长度来解除网络的过载，通常作用在接口出方向。

1.3.2 QoS 技术在设备中的处理顺序

图1-2 各 QoS 技术在同一网络设备中的处理顺序



2 QoS 配置方式

说明

本章中提到的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

2.1 配置方式介绍

QoS 的配置方式分为 QoS 策略配置方式和非 QoS 策略配置方式两种。

有些 QoS 功能只能使用其中一种方式来配置，有些使用两种方式都可以进行配置。在实际应用中，两种配置方式也可以结合起来使用。

2.1.1 非 QoS 策略配置方式

非 QoS 策略配置方式是指不通过 QoS 策略来进行配置。例如，端口限速功能可以通过直接在接口上配置来实现。

2.1.2 QoS 策略配置方式

QoS 策略配置方式是指通过配置 QoS 策略来实现 QoS 功能。

QoS 策略包含了三个要素：类、流行为、策略。用户可以通过 QoS 策略将指定的类和流行为绑定起来，灵活地进行 QoS 配置。

1. 类

类的要素包括：类的名称和类的规则。

用户可以通过命令定义一系列的规则来对报文进行分类。

2. 流行为

流行为用来定义针对报文所做的 QoS 动作。

流行为的要素包括：流行为的名称和流行为中定义的动作。

用户可以通过命令在一个流行为中定义多个动作。

3. 策略

策略用来将指定的类和流行为绑定起来，对分类后的报文执行流行为中定义的动作。

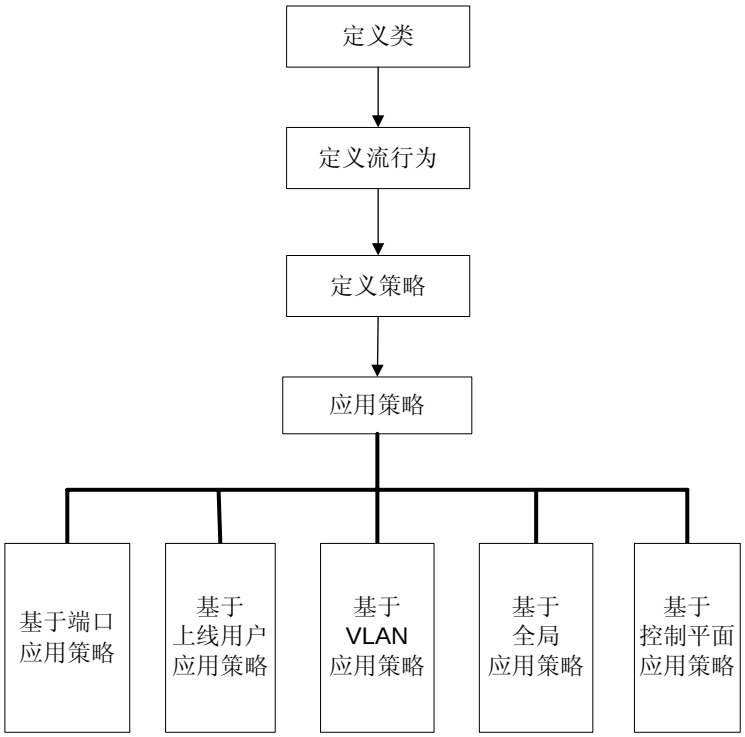
策略的要素包括：策略名称、绑定在一起的类和流行为的名称。

用户可以在一个策略中定义多个类与流行为的绑定关系。

2.2 QoS 策略配置方式的步骤

如 图 2-1所示：

图2-1 QoS 策略配置方式的步骤



2.2.1 定义类

定义类首先要创建一个类名称，然后在此类视图下配置其匹配规则。

表2-1 定义类

操作	命令	说明
进入系统视图	**system-view**	-
定义类并进入类视图	**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	必选 缺省为 **and**，即类视图下各匹配规则之间的关系为逻辑与 • **and**：报文只有匹配了所有的规则，设备才认为报文属于这个类 • **or**：报文只要匹配了类中的任何一个规则，设备就认为报文属于这个类
定义匹配数据包的规则	**if-match** *match-criteria*	必选

match-criteria：匹配规则，取值如 表 2-2所示。

表2-2 匹配规则

取值	描述
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	定义匹配 ACL 的规则 *acl-number* 是 ACL 的序号，IPv4 ACL 序号的取值范围是 2000～4999，IPv6 ACL 序号的取值范围是 2000～3999 *acl-name* 是 ACL 的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头，为避免混淆，ACL 的名称不可以使用英文单词 all
any	定义匹配所有报文的规则
customer-dot1p *8021p-list*	定义匹配用户网络 802.1p 优先级的规则，*8021p-list* 为 CoS 取值的列表，最多可以输入 8 个 CoS 取值，用空格隔开，CoS 的取值范围为 0～7
customer-vlan-id *vlan-id-list*	定义匹配用户网络 VLAN ID 的规则，*vlan-id-list* 为 VLAN ID 的列表，形式可以为 *vlan-id* **to** *vlan-id*，也可以输入多个不连续的 VLAN ID，用空格隔开，设备最多允许用户同时指定 8 个 VLAN ID；VLAN ID 的取值范围为 1～4094
destination-mac *mac-address*	定义匹配目的 MAC 地址的规则
dscp *dscp-list*	定义匹配DSCP的规则，*dscp-list*为DSCP取值的列表，最多可以输入 8 个DSCP取值，用空格隔开，DSCP的取值范围为 0～63 或表 14-2中的关键字
ip-precedence *ip-precedence-list*	定义匹配 IP 优先级的规则，*ip-precedence-list* 为 IP 优先级取值的列表，最多可以输入 8 个 IP 优先级取值，用空格隔开，IP 优先级的取值范围为 0～7
protocol *protocol-name*	定义匹配协议的规则，*protocol-name* 取值为 IP 或 IPv6
qos-local-id *local-id-value*	定义匹配 qos-local-id 的规则，*local-id-value* 为 QoS 本地 ID，取值范围为 1～4095 在 CE3000-32F-EI 交换机上，能够支持的 *local-id-value* 值为 1～3999
service-dot1p *8021p-list*	定义匹配运营商网络 802.1p 优先级的规则，*8021p-list* 为 CoS 取值的列表，最多可以输入 8 个 CoS 取值，用空格隔开，CoS 的取值范围为 0～7
service-vlan-id *vlan-id-list*	定义匹配运营商网络 VLAN ID 的规则，*vlan-id-list* 为 VLAN ID 的列表，形式可以为 *vlan-id* **to** *vlan-id*，也可以输入多个不连续的 VLAN ID，用空格隔开，设备最多允许用户同时指定 8 个 VLAN ID；VLAN ID 的取值范围为 1～4094
source-mac *mac-address*	定义匹配源 MAC 地址的规则
system-index *index-value-list*	定义规则来匹配预定义的上送控制平面报文类型，*index-value-list* 为系统预定义匹配字段索引号（system-index）的列表，最多可以输入 8 个 system-index 值，system-index 值的取值范围为 1～128

说明

如果指定类的逻辑关系为 **and**，使用 **if-match** 命令定义匹配规则时，有如下注意事项：

- 匹配规则含有 **acl** 或 **acl ipv6** 时，如果在类中配置了多条这样的匹配规则，在应用策略时，匹配 **acl** 或 **acl ipv6** 的规则之间的逻辑关系实际为 **or**。
- 匹配规则含有 **customer-vlan-id** 或 **service-vlan-id** 时，如果在类中配置了多条这样的匹配规则，在应用策略时，匹配 **customer-vlan-id** 或 **service-vlan-id** 的规则之间的逻辑关系实际为 **or**。

说明

当流分类中各规则之间的逻辑关系为 **and** 时，对于以下匹配条件，用户虽然可以通过重复执行 **if-match** 命令来配置多条匹配不同取值的规则，或在一条规则中使用 *list* 形式输入多个匹配值，但在应用使用该类的 QoS 策略时，将会无法正常下发：

- **customer-dot1p** *8021p-list*
- **destination-mac** *mac-address*（不支持 list 形式）
- **dscp** *dscp-list*
- **ip-precedence** *ip-precedence-list*
- **service-dot1p** *8021p-list*
- **source-mac** *mac-address*（不支持 list 形式）
- **system-index** *index-value-list*

如果用户需要创建匹配以上某一字段多个取值的规则，需要在创建流分类时指定各规则之间的逻辑关系为 **or**，然后再配置匹配多个值的规则。

说明

如果使用 **customer-dot1p** 规则作为流分类的匹配条件，则使用该流分类的 QoS 策略将不能在出方向进行应用。

2.2.2 定义流行为

定义流行为首先需要创建一个流行为名称，然后可以在此流行为视图下根据需要配置相应的流行为。每个流行为由一组 QoS 动作组成。

表2-3 定义流行为

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	必选

操作	命令	说明
配置流行为	流行为就是对应符合流分类的报文做出相应的 QoS 动作，例如流量监管、流量过滤、流量重定向、重标记、流量统计等，具体情况请参见本文相关章节	

2.2.3 定义策略

在策略视图下为使用的类指定对应的流行为。以某种匹配规则将流区分为不同的类，再结合不同的流行为就能很灵活的实现各种 QoS 功能。

表2-4 在策略中为类指定流行为

操作	命令	说明
进入系统视图	**system-view**	-
定义策略并进入策略视图	**qos policy** *policy-name*	必选
在策略中为类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name* [**mode** { **dcbx** | **dot1q-tag-manipulation** }]	必选 **mode dcbx**：表示该策略为 DCBX（Data Center Bridge Capability Exchange Protocol，数据中心桥能力交换协议）模式。有关 DCBX 的介绍，请参见“二层技术－以太网交换配置指导”中的“LLDP 配置”。 **mode dot1q-tag-manipulation** 用来设置 VLAN 映射功能中的类和流行为对应关系。有关 N:1 VLAN 映射功能的介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN 映射配置”。

说明

- 如果 QoS 策略在定义流分类规则时引用了 ACL，则忽略 ACL 规则的动作，以流行为中定义的动作为准，报文匹配只使用 ACL 中的分类域。
- 当用户在策略下配置了多组类和流行为的对应关系时，如果某个流行为中配置了 **nest**、**remark customer-vlan-id** 或 **remark service-vlan-id** 动作，建议用户不要在此流行为中配置其他动作，以保证应用策略后实际的运行结果与用户的配置意图一致。有关 **nest**、**remark customer-vlan-id** 或 **remark service-vlan-id** 动作的介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN 映射配置”。
- **do1q-tag-manipulation** 参数仅在配置 N:1 VLAN 映射功能时需要使用，在配置其它用途的 QoS 策略时请不要使用该参数。

2.2.4 应用策略

QoS 策略支持以下应用方式：

- 基于端口应用 QoS 策略：QoS 策略对通过端口接收（发送）的流量生效。

- 基于上线用户应用 QoS 策略：QoS 策略对通过上线用户接收（发送）的流量生效。
- 基于 VLAN 应用 QoS 策略：QoS 策略对通过同一个 VLAN 内所有端口接收（发送）的流量生效。
- 基于全局应用 QoS 策略：QoS 策略对所有流量生效。
- 基于控制平面应用 QoS 策略：QoS 策略对通过控制平面接收的流量生效。

说明

- 当在端口和全局同时应用了 QoS 策略时，端口上应用的策略优先级较高，优先生效。
- 除基于上线用户应用的 QoS 策略外，当 QoS 策略应用后，用户仍然可以修改 QoS 策略中的流分类规则和流行为，以及二者的对应关系。当流分类规则中匹配的是 ACL 时，允许删除或修改该 ACL（包括向该 ACL 中添加、删除和修改规则）。

1. 基于端口应用 QoS 策略

一个策略可以应用于多个端口。端口的每个方向（出/入两个方向）只能应用一个策略。

表2-5 在端口上应用策略

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
在端口上应用关联的策略		**qos apply policy** *policy-name* { **inbound** | **outbound** }	必选

说明

如果 QoS 策略应用在端口的出方向，则 QoS 策略对本地协议报文不起作用。本地协议报文是设备内部发起的某些报文，它是维持设备正常运行的重要协议报文。为了确保这些报文能够被不受影响的发送出去，即便在端口的出方向应用了 QoS 策略，本地协议报文也不会受到 QoS 策略的限制，从而降低了因配置 QoS 而误将这些报文丢弃或进行其他处理的风险。一些常见的本地协议报文如下：链路维护报文、IS-IS、OSPF、RIP、BGP、LDP、RSVP、SSH 等。

2. 基于上线用户应用 QoS 策略

一个策略可以应用于多个上线用户。上线用户的每个方向（发送/接收报文两个方向）只能应用一个策略，如果用户想修改某方向上应用的策略，必须先取消原先的配置，然后再配置新的策略。

表2-6 基于上线用户应用 QoS 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入 user-profile 视图	**user-profile** *profile-name*	必选 进入 user-profile 视图后，下面进行的配置只在 User Profile 处于激活状态，且用户成功上线后才生效 关于 User Profile 的相关介绍以及配置，请参见“安全配置指导”中的“User Profile 配置”
应用关联的策略	**qos apply policy** *policy-name* { **inbound** | **outbound** }	必选 **inbound** 是对设备入方向的上线用户流量（即上线用户发送的流量）应用策略；**outbound** 是对设备出方向的上线用户流量（即上线用户接收到的流量）应用策略
退回系统视图	**quit**	-
激活 User Profile	**user-profile** *profile-name* **enable**	必选 缺省情况下，User Profile 处于未激活状态

说明

- 如果 User Profile 处于激活状态，则除了可以修改策略引用的 ACL 外，既不能修改策略的其他内容，也不能删除已经应用到此 User Profile 的策略。如果 User Profile 对应的用户已经上线，则策略引用的 ACL 规则内容也不能修改。
- user-profile 视图下应用的策略中的流行为只支持 **remark**、**car**、**filter** 三种动作。
- user-profile 视图下应用的策略不能为空策略，因为应用空策略的 User Profile 不能被激活。

3. 基于 VLAN 应用 QoS 策略

基于 VLAN 应用 QoS 策略可以方便对某个 VLAN 上的所有流量进行管理。

表2-7 基于 VLAN 应用的 QoS 策略

操作	命令	说明
进入系统视图	**system-view**	-
应用 QoS 策略到指定的 VLAN	**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }	必选

说明

- 基于 VLAN 应用的 QoS 策略不能应用在动态 VLAN 上。例如，在运行 GVRP 协议的情况下，设备可能会动态创建 VLAN，QoS 策略不能应用在该动态 VLAN 上。
- 建议用户不要在 VLAN 上和此 VLAN 内的端口上同时应用 QoS 策略。

4. 基于全局应用 QoS 策略

基于全局应用 QoS 策略可以方便对设备上的所有流量进行管理。

表2-8 基于全局应用 QoS 策略

操作	命令	说明
进入系统视图	**system-view**	-
基于全局应用 QoS 策略	**qos apply policy** *policy-name* **global** { **inbound** | **outbound** }	必选

5. 基于控制平面应用 QoS 策略

我们将处理报文的设备单元抽象为数据平面与控制平面两个部分：

- 数据平面（DP，Data Plane）：是指对报文进行收发、交换的处理单元，它的主要工作是转发报文。在设备上，与之相对应的核心物理实体就是各种专用转发芯片，它们有极高的处理速度和很强的数据吞吐能力。
- 控制平面（CP，Control Plane）：是指运行大部分路由交换协议进程的处理单元，它的主要工作是进行协议报文的解析和协议的计算。在设备上，与之相对应的核心物理实体就是 CPU，它具备灵活的报文处理能力，但数据吞吐能力有限。

数据平面接收到无法识别或处理的报文会送到控制平面进行进一步处理。如果上送控制平面的报文速率超过了控制平面的处理能力，那么上送控制平面的正常报文会得不到正确转发或及时处理，从而影响协议的正常运行，例如设备受到 DoS（Denial of Service，拒绝服务）攻击。

为了解决此问题，用户可以把 QoS 策略应用在控制平面上，通过对上送控制平面的报文进行过滤、限速等 QoS 处理，达到保护控制平面正常报文的收发、维护控制平面正常处理状态的目的。

表2-9 应用控制平面策略

操作	命令	说明
进入系统视图	**system-view**	-
进入控制平面视图	**control-plane slot** *slot-number*	必选
应用 QoS 策略	**qos apply policy** *policy-name* **inbound**	必选

注意

- 缺省情况下，设备会在控制平面上应用预定义的 QoS 策略，并默认生效。预定义的 QoS 策略中通过 system-index 来标识各种上送控制平面的报文类型，用户也可以在流分类视图下通过 **if-match** 命令引用这些 system-index 来进行报文分类，然后根据需要为这些报文重新配置流行为。系统预定义的 QoS 策略信息可以通过 **display qos policy control-plane pre-defined** 命令查看。
- 在控制平面上应用 QoS 策略时，如果流分类的匹配条件是 **system-index**，则流行为的动作只能为 **car** 或 **accounting**，且当配置流行为为 **car** 时，只有 **cir** 参数的取值可以被正常应用。
- 在控制平面上应用 QoS 策略时，如果流分类的匹配条件不是 **system-index**，则流行为中的动作将对该控制平面所在单板上的数据流量也将生效。

2.2.5 QoS 策略显示和维护

在任意视图下执行 **display** 命令可以显示 QoS 策略的运行情况，通过查看显示信息验证配置的效果。

表2-10 QoS 策略显示和维护

操作	命令
显示配置的类信息	**display traffic classifier user-defined** [*tcl-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示配置的流行为信息	**display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示用户定义策略的配置信息	**display qos policy user-defined** [*policy-name* [**classifier** *tcl-name*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示指定端口或所有端口上策略的配置信息和运行情况	**display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示 VLAN 应用 QoS 策略的信息	**display qos vlan-policy** { **name** *policy-name* | **vlan** *vlan-id* } [**slot** *slot-number*] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示全局应用 QoS 策略的信息	**display qos policy global** [**slot** *slot-number*] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示控制平面应用 QoS 策略的信息	**display qos policy control-plane slot** *slot-number* [**inbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示预定义控制平面应用 QoS 策略的信息	**display qos policy control-plane pre-defined** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除 VLAN 应用 QoS 策略的统计信息	**reset qos vlan-policy** [**vlan** *vlan-id*] [**inbound** | **outbound**]
清除全局应用 QoS 策略的统计信息	**reset qos policy global** [**inbound** | **outbound**]
清空控制平面应用 QoS 策略的统计信息	**reset qos policy control-plane slot** *slot-number* [**inbound**]

3 优先级映射配置

说明

本章中提到的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

3.1 优先级映射简介

3.1.1 概述

报文在进入设备以后，设备会根据自身情况和相应规则分配或修改报文的各种优先级的值，为队列调度和拥塞控制服务。

优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值，就可以获得各种用以决定报文调度能力的各种优先级字段，从而可以全面有效的控制报文的转发调度能力。

3.1.2 优先级介绍

优先级用于标识报文传输的优先程度，可以分为两类：报文携带优先级和设备调度优先级。

报文携带优先级包括：802.1p优先级、DSCP优先级、IP优先级、EXP优先级等。这些优先级都是根据公认的标准和协议生成，体现了报文自身的优先等级。相关介绍请参见 14 附录 B 各种优先级介绍。

设备调度优先级是指报文在设备内转发时所使用的优先级，只对当前设备自身有效。设备调度优先级包括以下几种：

- 本地优先级（LP）：设备为报文分配的一种具有本地意义的优先级，每个本地优先级对应一个队列，本地优先级值越大的报文，进入的队列优先级越高，从而能够获得优先的调度。
- 丢弃优先级（DP）：在进行报文丢弃时参考的参数，丢弃优先级值越大的报文越被优先丢弃。

3.1.3 优先级映射表

优先级映射功能通过优先级映射表来进行，设备提供了多张优先级映射表，分别对应相应的优先级映射关系：

- **dot1p-dp**：802.1p 优先级到丢弃优先级映射表；
- **dot1p-exp**：802.1p 优先级到 EXP 映射表；
- **dot1p-lp**：802.1p 优先级到本地优先级映射表；
- **dscp-dot1p**：DSCP 到 802.1p 优先级映射表，仅对 IP 报文生效；
- **dscp-dp**：DSCP 到丢弃优先级映射表，仅对 IP 报文生效；
- **dscp-dscp**：DSCP 到 DSCP 映射表，仅对 IP 报文生效；
- **exp-dot1p**：EXP 到 802.1p 优先级映射表；
- **exp-dp**：EXP 到丢弃优先级映射表；

通常情况下，可以通过查找缺省优先级映射表（附录 A 缺省优先级映射表）来为报文分配相应的优先级。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

3.1.4 优先级信任模式

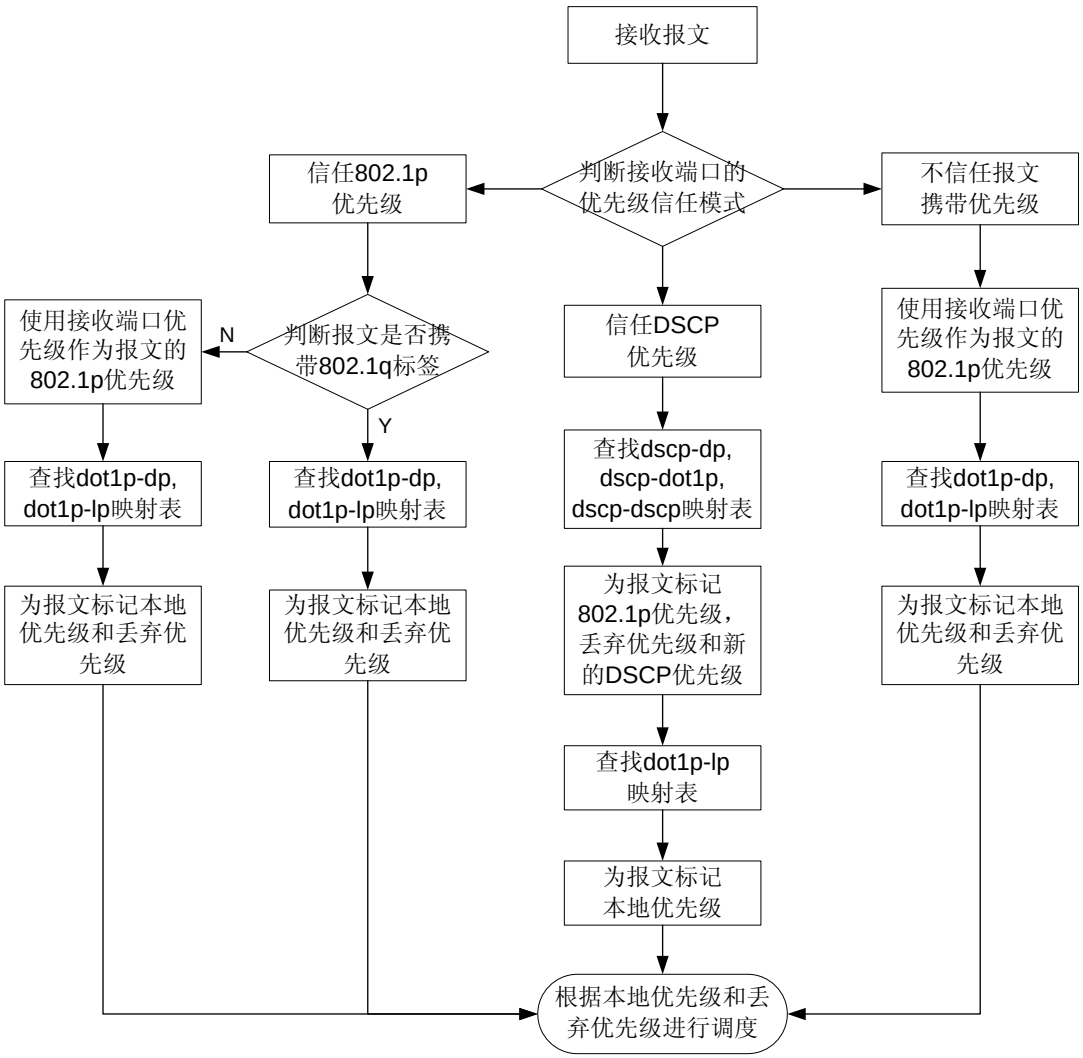
通常情况下，报文可能会携带有多种优先级，设备在进行优先级映射时，需要首先确定采用哪种优先级作为参考，再通过优先级映射表映射出调度优先级。优先级信任模式就是用来指定设备进行优先级映射时作为参考的报文携带优先级，CE3000-32F-EI 交换机支持以下三种优先级信任模式：

- 信任 DSCP 优先级：设备将根据报文携带的 DSCP 优先级查找映射表进行优先级映射。
- 信任 802.1p 优先级：设备将根据报文携带的 802.1p 优先级查找映射表进行优先级映射。
- 不信任报文优先级：设备将使用接收报文的端口的端口优先级作为报文的 802.1p 优先级，并通过映射表进行优先级映射。

3.1.5 优先级映射过程

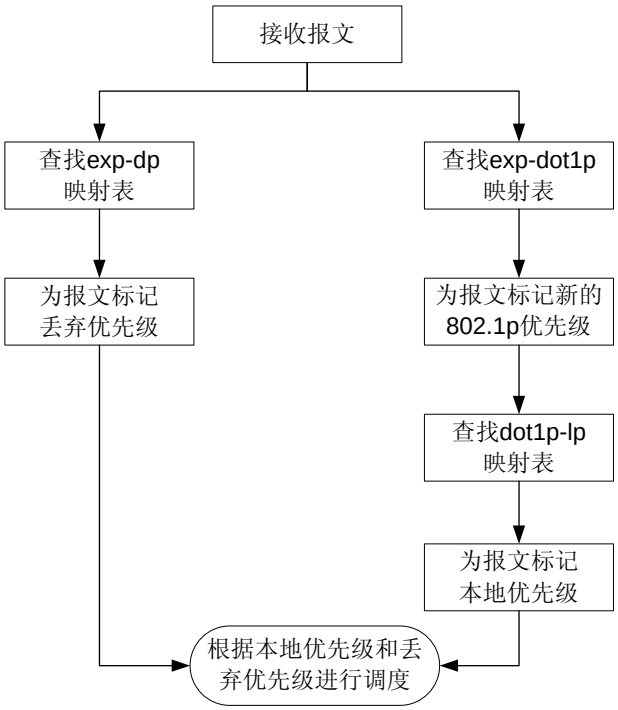
对于接收到的以太网报文，交换机根据优先级信任模式和报文的 802.1q标签状态，将采用不同的方式为其标记调度优先级。如 图 3-1所示：

图3-1 以太网报文优先级映射过程



对于接收到的MPLS报文，将采用以下方式为其标记优先级，如 图 3-2所示。

图3-2 MPLS 报文优先级映射过程



说明

上面介绍的过程适用于没有配置重标记功能的情况，如果已经配置了重标记功能，设备将根据重标记后的报文携带优先级查找映射表，为报文分配调度优先级，或者直接采用重标记后的调度优先级进行调度。此时端口的信任模式和端口优先级的配置均不生效。

3.2 优先级映射配置任务简介

修改优先级映射关系的方式有三种：配置优先级映射表、配置优先级信任模式和配置端口优先级。建议进行各项配置之前先整体规划网络的 QoS 方案。

表3-1 优先级映射配置任务简介

配置任务	说明	详细配置
配置优先级映射表	可选	3.3.1
配置优先级信任模式	可选	3.3.2
配置端口优先级	可选	3.3.3

3.3 配置优先级映射

3.3.1 配置优先级映射表

表3-2 配置优先级映射表

操作	命令	说明
进入系统视图	**system-view**	-
进入指定的优先级映射表视图	**qos map-table** { **dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** | **exp-dp** }	必选 用户根据需要进入相应的优先级映射表视图
配置指定优先级映射表参数，定义优先级映射关系	**import** *import-value-list* **export** *export-value*	必选 新配置的映射项将覆盖原有映射项

3.3.2 配置优先级信任模式

根据报文自身的优先级，查找优先级映射表，为报文分配优先级参数，可以通过配置优先级信任模式的方式来实现。

在配置端口/端口组上的优先级模式时，用户可以选择下列信任模式：

- **dot1p**：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。
- **dscp**：信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射。
- **untrust**：不信任报文携带的优先级。

表3-3 配置优先级信任模式

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口的优先级信任模式		**qos trust** { **dot1p** | **dscp** }	二者选其一 缺省情况下，设备不信任报文携带的优先级
配置不信任报文携带的优先级		**undo qos trust**	

3.3.3 配置端口优先级

表3-4 配置端口优先级

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口优先级		**qos priority** *priority-value*	必选 端口优先级的缺省值为 0

3.4 优先级映射显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后优先级映射的运行情况，通过查看显示信息验证配置的效果。

表3-5 优先级映射显示和维护

操作	命令
显示指定优先级映射表配置情况	**display qos map-table** [**dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** | **exp-dp**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口优先级信任模式信息	**display qos trust interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

3.5 优先级映射典型配置举例

3.5.1 优先级信任模式和端口优先级配置举例

1. 组网需求

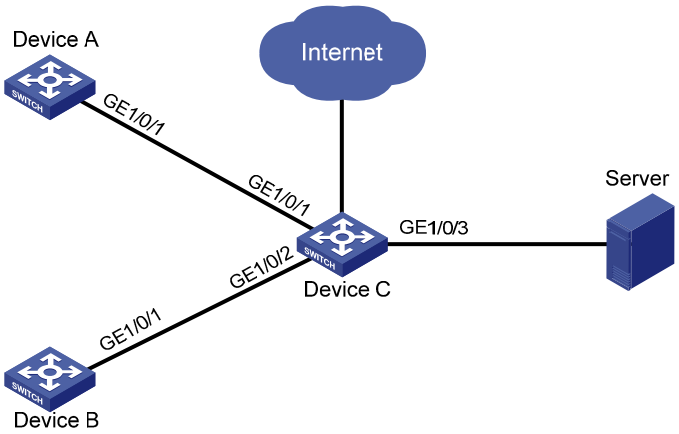
Device A 和 Device B 通过 Device C 实现互连。网络环境描述如下：

- Device A 通过端口 GigabitEthernet1/0/1 接入 Device C；
- Device B 通过端口 GigabitEthernet1/0/2 接入 Device C。

要求通过配置实现如下需求：如果 Device C 在 GigabitEthernet1/0/3 端口发生拥塞，则优先处理 Device A 发出的报文（优先让 Device A 访问 Server）。

2. 组网图

图3-3 优先级信任模式和端口优先级配置举例组网图



3. 配置步骤

在 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 端口上分别配置端口优先级，GigabitEthernet1/0/1 上配置的端口优先级值要高于 GigabitEthernet1/0/2 上配置的端口优先级值。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] qos priority 3
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] qos priority 1
[DeviceC-GigabitEthernet1/0/2] quit
```

3.5.2 优先级映射表和重标记配置举例

说明

关于重标记功能的介绍，请参见 重标记配置。

---

1. 组网需求

公司企业网通过 Device 实现各部门之间的互连。网络环境描述如下：

- 市场部门通过端口 GigabitEthernet1/0/1 接入 Device，标记市场部门发出的报文的 802.1p 优先级为 3；
- 研发部门通过端口 GigabitEthernet1/0/2 接入 Device，标记研发部门发出的报文的 802.1p 优先级为 4；
- 管理部门通过端口 GigabitEthernet1/0/3 接入 Device，标记管理部门发出的报文的 802.1p 优先级为 5。

实现如下需求：

访问公共服务器的时候，研发部门 > 管理部门 > 市场部门。

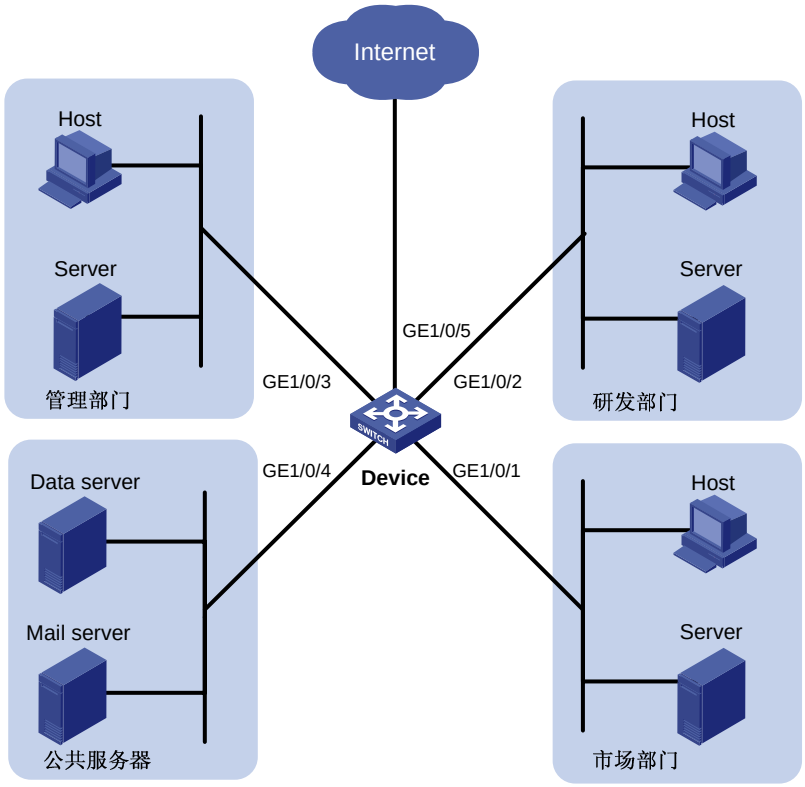
- 通过优先级映射将研发部门发出的报文放入出队列 6 中，优先进行处理；
- 通过优先级映射将管理部门发出的报文放入出队列 4 中，次优先进行处理；
- 通过优先级映射将市场部门发出的报文放入出队列 2 中，最后进行处理。

通过 HTTP 方式访问 Internet 的时候，管理部门 > 市场部门 > 研发部门。

- 管理部门发出的报文本地优先级为 6，优先进行处理；
- 重标记市场部门发出的报文的本地优先级为 4，次优先进行处理；
- 重标记研发部门发出的报文的本地优先级为 2，最后进行处理。

2. 组网图

图3-4 优先级映射表和重标记配置举例组网图



3. 配置步骤

(1) 配置端口的端口优先级

配置端口 GigabitEthernet1/0/1 的端口优先级为 3。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos priority 3
[Device-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet1/0/2 的端口优先级为 4。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos priority 4
[Device-GigabitEthernet1/0/2] quit
```

配置端口 GigabitEthernet1/0/3 的端口优先级为 5。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos priority 5
[Device-GigabitEthernet1/0/3] quit
```

(2) 配置优先级映射表

配置 802.1p 优先级到本地优先级映射表，将 802.1p 优先级 3、4、5 对应的本地优先级配置为 2、6、4。

```
[Device] qos map-table dot1p-lp
```

```
[Device-maptbl-dot1p-lp] import 3 export 2
[Device-maptbl-dot1p-lp] import 4 export 6
[Device-maptbl-dot1p-lp] import 5 export 4
[Device-maptbl-dot1p-lp] quit
```

(3) 配置重标记

将管理、市场、研发部门发出的 HTTP 报文的 802.1p 优先级分别重标记为 4、5、3，使其能根据前面配置的映射表分别映射到本地优先级 6、4、2。

创建 ACL 3000，用来匹配 HTTP 报文。

```
[Device] acl number 3000
[Device-acl-adv-3000] rule permit tcp destination-port eq 80
[Device-acl-adv-3000] quit
```

创建流分类，匹配 ACL 3000。

```
[Device] traffic classifier http
[Device-classifier-http] if-match acl 3000
[Device-classifier-http] quit
```

配置管理部门的重标记策略并应用到 GigabitEthernet1/0/3 端口的入方向。

```
[Device] traffic behavior admin
[Device-behavior-admin] remark dot1p 4
[Device-behavior-admin] quit
[Device] qos policy admin
[Device-qospolicy-admin] classifier http behavior admin
[Device-qospolicy-admin] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] qos apply policy admin inbound
```

配置市场部门的重标记策略并应用到 GigabitEthernet1/0/1 端口的入方向。

```
[Device] traffic behavior market
[Device-behavior-market] remark dot1p 5
[Device-behavior-market] quit
[Device] qos policy market
[Device-qospolicy-market] classifier http behavior market
[Device-qospolicy-market] quit
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy market inbound
```

配置研发部门的重标记策略并应用到 GigabitEthernet1/0/2 端口的入方向。

```
[Device] traffic behavior rd
[Device-behavior-rd] remark dot1p 3
[Device-behavior-rd] quit
[Device] qos policy rd
[Device-qospolicy-rd] classifier http behavior rd
[Device-qospolicy-rd] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos apply policy rd inbound
```

4 流量监管、流量整形和端口限速配置

说明

本章中提到的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

4.1 流量监管、流量整形和端口限速简介

如果不限制用户发送的流量，那么大量用户不断突发的数据只会使网络更拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的流量加以限制。比如限制每个时间间隔某个流只能得到承诺分配给它的那部分资源，防止由于过分突发所引发的网络拥塞。

流量监管、流量整形和端口限速都可以通过对流量规格的监督来限制流量及其资源的使用，它们有一个前提条件，就是要知道流量是否超出了规格，然后才能根据评估结果实施调控。一般采用令牌桶（Token Bucket）对流量的规格进行评估。

4.1.1 流量评估与令牌桶

1. 令牌桶的特点

令牌桶可以看作是一个存放一定数量令牌的容器。系统按设定的速度向桶中放置令牌，当桶中令牌满时，多出的令牌溢出，桶中令牌不再增加。

2. 用令牌桶评估流量

在用令牌桶评估流量规格时，是以令牌桶中的令牌数量是否足够满足报文的转发为依据的。如果桶中存在足够的令牌可以用来转发报文（通常用一个令牌关联一个比特的转发权限），称流量遵守或符合这个规格，否则称为不符合或超标。

评估流量时令牌桶的参数包括：

- 平均速率：向桶中放置令牌的速率，即允许的流的平均速度。通常配置为 CIR。
- 突发尺寸：令牌桶的容量，即每次突发所允许的最大的流量尺寸。通常配置为 CBS，突发尺寸必须大于最大报文长度。

每到达一个报文就进行一次评估。每次评估，如果桶中有足够的令牌可供使用，则说明流量控制在允许的范围内，此时要从桶中取走与报文转发权限相当的令牌数量；否则说明已经耗费太多令牌，流量超标了。

3. 复杂评估

为了评估更复杂的情况，实施更灵活的调控策略，可以配置两个令牌桶（简称 C 桶和 E 桶）。例如 TP 中有四个参数：

- CIR：表示向 C 桶中投放令牌的速率，即 C 桶允许传输或转发报文的平均速率；
- CBS：表示 C 桶的容量，即 C 桶瞬间能够通过的承诺突发流量；
- PIR：表示向 E 桶中投放令牌的速率，即 E 桶允许传输或转发报文的最大速率；
- EBS：表示 E 桶的容量，即 E 桶瞬间能够通过的超出突发流量。

CBS 和 EBS 是由两个不同的令牌桶承载的。每次评估时，依据下面的情况，可以分别实施不同的流控策略：

- 如果 C 桶有足够的令牌，报文被标记为 green，即绿色报文；
- 如果 C 桶令牌不足，但 E 桶有足够的令牌，报文被标记为 yellow，即黄色报文；
- 如果 C 桶和 E 桶都没有足够的令牌，报文被标记为 red，即红色报文。

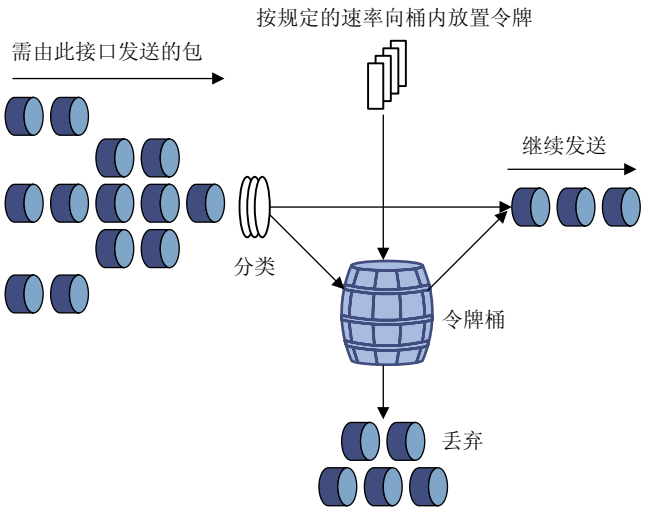
4.1.2 流量监管

说明

流量监管支持入/出两个方向，为了方便描述，下文以出方向为例。

流量监管 TP（Traffic Policing）就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，以保护网络资源和运营商的利益。例如可以限制 HTTP 报文不能占用超过 50%的网络带宽。如果发现某个连接的流量超标，流量监管可以选择丢弃报文，或重新配置报文的优先级。

图4-1 TP 示意图



流量监管广泛的用于监管进入 Internet 服务提供商 ISP 的网络流量。流量监管还包括对所监管流量的流分类服务，并依据不同的评估结果，实施预先设定好的监管动作。这些动作可以是：

- 转发：比如对评估结果为“符合”的报文继续转发。
- 丢弃：比如对评估结果为“不符合”的报文进行丢弃。
- 改变优先级并转发：比如对评估结果为“符合”的报文，将之标记为其它的优先级后再进行转发。

4.1.3 流量整形

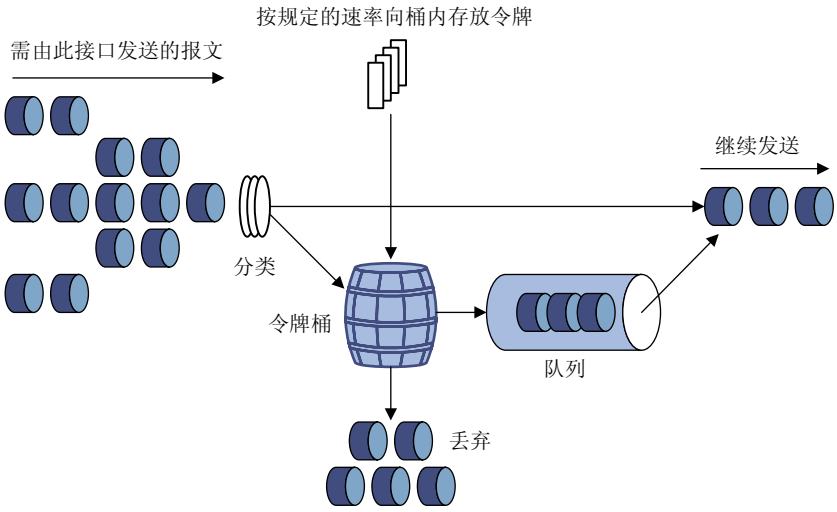
说明

流量整形仅支持出方向。

TS（Traffic Shaping，流量整形）是一种主动调整流量输出速率的措施。一个典型应用是基于下游网络节点的 TP 指标来控制本地流量的输出。

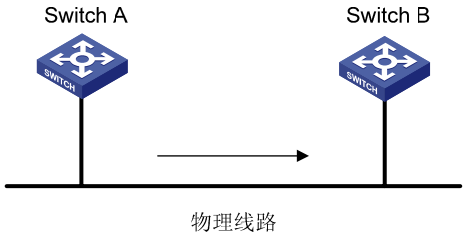
流量整形与流量监管的主要区别在于，流量整形对流量监管中需要丢弃的报文进行缓存——通常是将它们放入缓冲区或队列内，如 图 4-2所示。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

图4-2 TS 示意图



例如，在 图 4-3所示的应用中，设备Switch A向Switch B发送报文。Switch B要对Switch A发送来的报文进行TP监管，对超出规格的流量直接丢弃。

图4-3 流量整形的应用



为了减少报文的无谓丢失，可以在 Switch A 的出口对报文进行流量整形处理。将超出流量整形特性的报文缓存在 Switch A 中。当可以继续发送下一批报文时，流量整形再从缓冲队列中取出报文进行发送。这样，发向 Switch B 的报文将都符合 Switch B 的流量规定。

4.1.4 端口限速

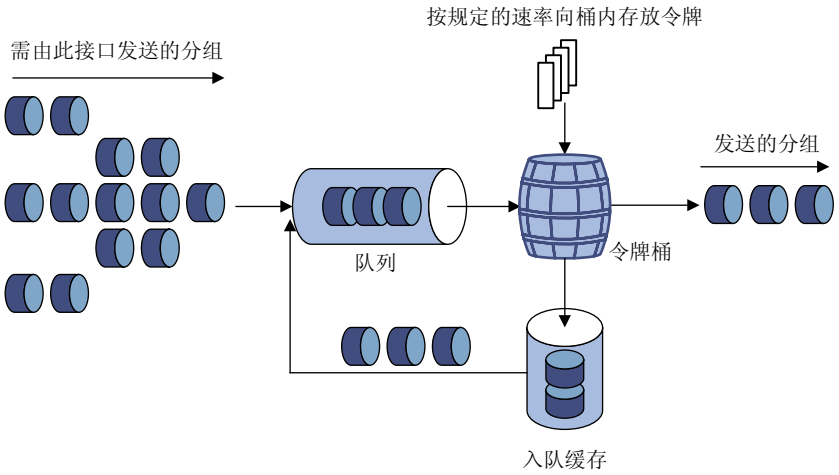
说明

端口限速支持入/出两个方向，为了方便描述，下文以出方向为例。

利用 LR（Line Rate，物理端口限速）可以在一个物理端口上限制发送报文（包括紧急报文）的总速率。

LR 也是采用令牌桶进行流量控制。如果在设备的某个端口上配置了 LR，所有经由该端口发送的报文首先要经过 LR 的令牌桶进行处理。如果令牌桶中有足够的令牌，则报文可以发送；否则，报文将进入 QoS 队列进行拥塞管理。这样，就可以对通过该物理端口的报文流量进行控制。

图4-4 LR 处理过程示意图



由于采用了令牌桶控制流量，当令牌桶中存有令牌时，可以允许报文的突发性传输；当令牌桶中没有令牌时，报文必须等到桶中生成了新的令牌后才可以继续发送。这就限制了报文的流量不能大于令牌生成的速度，达到了限制流量，同时允许突发流量通过的目的。

与流量监管相比，物理端口限速能够限制在物理端口上通过的所有报文。当用户只要求对所有报文限速时，使用物理端口限速比较简单。

4.2 流量监管配置

表4-1 流量监管配置

操作	命令	说明
进入系统视图	**system-view**	-
定义类并进入类视图	**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则	**if-match** *match-criteria*	-
退出类视图	**quit**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	-
配置流量监管动作	**car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action*] [**yellow** *action*] [**red** *action*] [**hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]]	必选 分层CAR的详细情况请参见 10.1.2 分层CAR
退出流行为视图	**quit**	-

操作		命令	说明
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用 QoS 策略	基于端口	2.2.4 1. 基于端口应用QoS策略	-
	基于上线用户	2.2.4 2. 基于上线用户应用QoS策略	-
	基于 VLAN	2.2.4 3. 基于VLAN应用QoS策略	-
	基于全局	2.2.4 4. 基于全局应用QoS策略	-
	基于控制平面	2.2.4 5. 基于控制平面应用QoS策略	-

4.3 流量整形配置

CE3000-32F-EI 交换机的流量整形为基于队列的流量整形，即针对某一个队列的数据包设置整形参数。

表4-2 流量整形配置

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
在端口配置流量整形		**qos gts queue** *queue-number* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	必选

4.4 端口限速配置

配置端口限速就是限制端口向外发送数据或者接收数据的速率。

表4-3 端口限速配置过程

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置端口限速		**qos lr** { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	必选

4.5 流量监管/流量整形/端口限速显示和维护

说明

CE3000-32F-EI交换机的流量监管功能通过QoS策略方式实现，相关显示和维护的命令请参见 2.2.5 QoS策略显示和维护。

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后流量监管/流量整形/端口限速的运行情况，通过查看显示信息验证配置的效果。

表4-4 流量监管/流量整形/端口限速显示和维护

操作	命令
显示流量整形配置运行信息	**display qos gts interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口的 LR 配置和统计信息	**display qos lr interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

5 拥塞管理配置

说明

本章中提到的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

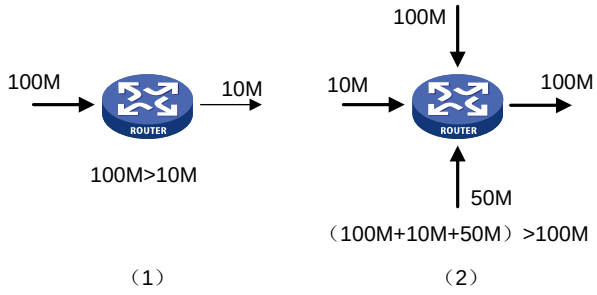
5.1 拥塞管理简介

5.1.1 拥塞的产生、影响和对策

所谓拥塞，是指当前供给资源相对于正常转发处理需要资源的不足，从而导致服务质量下降的一种现象。

在复杂的 Internet 分组交换环境下，拥塞极为常见。以下图中的两种情况为例：

图5-1 流量拥塞示意图



拥塞有可能会引发一系列的负面影响：

- 拥塞增加了报文传输的延迟和抖动，可能会引起报文重传，从而导致更多的拥塞产生。
- 拥塞使网络的有效吞吐率降低，造成网络资源的利用率降低。
- 拥塞加剧会耗费大量的网络资源（特别是存储资源），不合理的资源分配甚至可能导致系统陷入资源死锁而崩溃。

在分组交换以及多用户业务并存的复杂环境下，拥塞又是不可避免的，因此必须采用适当的方法来解决拥塞。

拥塞管理的中心内容就是当拥塞发生时如何制定一个资源的调度策略，以决定报文转发的处理次序。拥塞管理的处理包括队列的创建、报文的分类、将报文送入不同的队列、队列调度等。

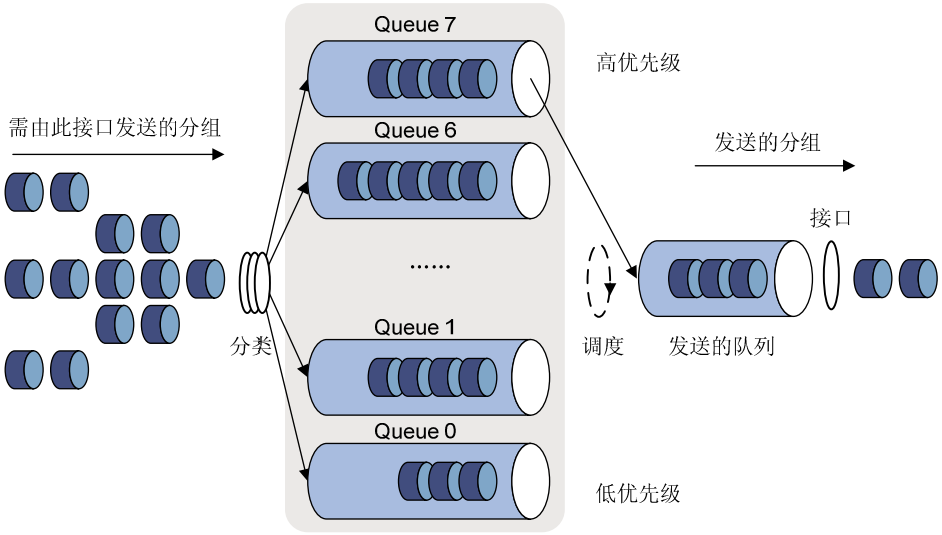
5.1.2 拥塞管理策略

对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级别算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

队列调度对不同优先级的报文进行分级处理，优先级高的会得到优先发送。这里介绍四种常用的队列：严格优先级 SP（Strict-Priority）队列、加权轮询 WRR（Weighted Round Robin）队列、加权公平队列（Weighted Fair Queuing）和 SP+WRR 队列。

1. SP 队列

图5-2 SP 队列示意图



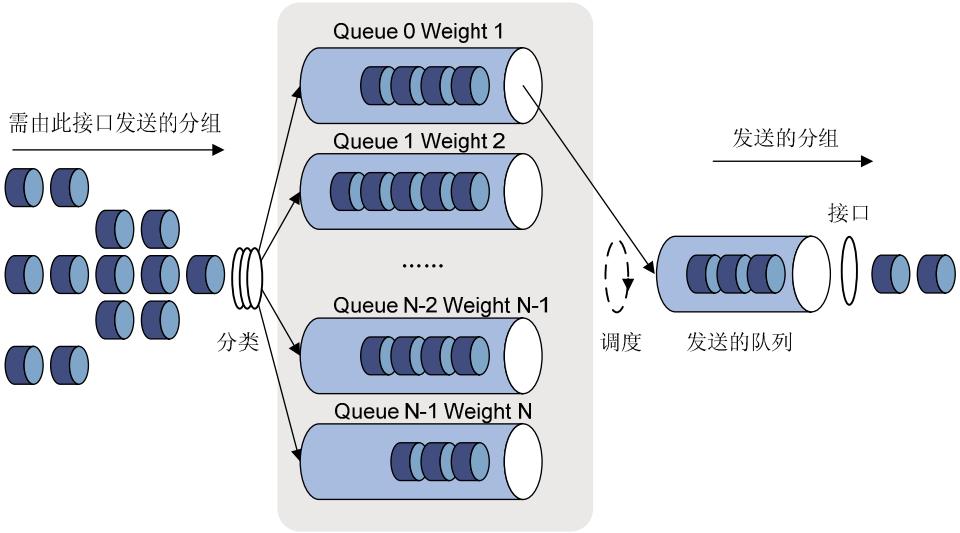
SP队列是针对关键业务类型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以 图 5-2为例，优先队列将端口的 8 个输出队列分成 8 类，依次为 7、6、5、4、3、2、1、0 队列，它们的优先级依次降低。

在队列调度时，SP 严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文将一直得不到服务。

2. WRR 队列

图5-3 WRR 队列示意图



WRR 队列是指在队列之间进行轮流调度，以保证每个队列都得到一定的服务时间。在使用 WRR 队列调度时，每个队列都拥有一个加权值，又称为调度权重。调度权重表示设备在调度该队列的报文时使用调度资源的比例。CE3000-32F-EI 交换机可以根据每次轮询调度的字节数或者报文个数来体现某个队列的调度权重，即使用字节数或报文个数作为调度单位。

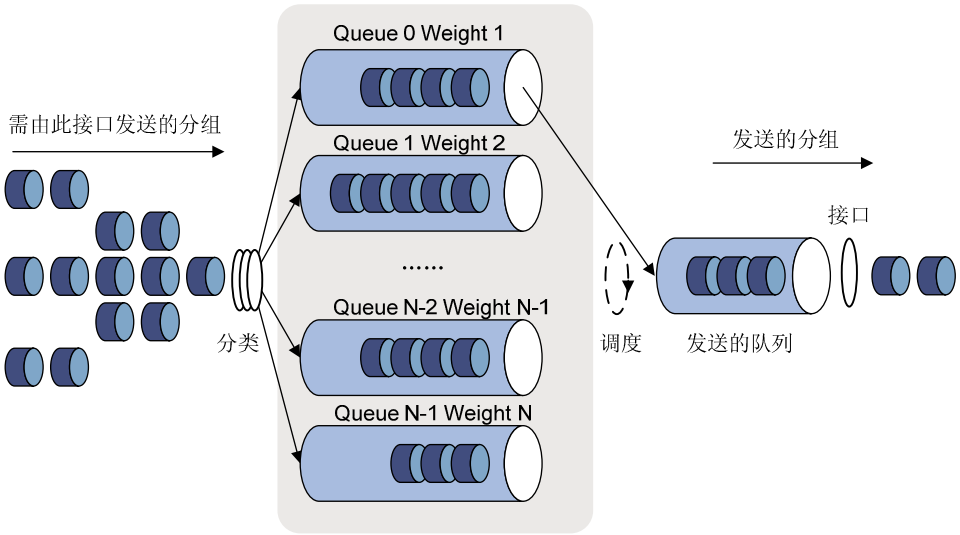
以使用字节数为调度单位的 WRR 队列为例：在一个 1000Mbps 的端口上，配置 8 个队列的调度权重分别为 5、5、3、3、1、1、1、1，这样可以保证最低优先级队列至少获得 1/(5＋5＋3＋3＋1＋1＋1＋1)×1000Mbps ＝ 50Mbps 的带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

WRR 队列还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

在使用 WRR 队列时，用户可以选择使用字节数或报文个数作为调度单位，并定制各个队列的权重，WRR 将按用户设定的参数进行加权轮询调度。

3. WFQ 队列

图5-4 WFQ 队列



WFQ 和使用报文个数作为调度单位的 WRR 队列调度效果类似，唯一的区别是 WFQ 还支持最小带宽保证机制，能够实现更灵活的调度方案：

- 通过配置最小带宽保证值，确保 WFQ 中每一个队列都拥有最小保证带宽。
- 可分配带宽（可分配带宽 ＝ 总带宽 － 各队列最小保证带宽）按照各队列优先级进行分配。

例如：端口的总带宽为 10M、端口中当前共有 5 个流，它们的优先级分别为 0、1、2、3、4；每个流的最小带宽保证分别为 128kbps、128kbps、128kbps、64kbps、64kbps。

- 可分配带宽＝10M－（128k＋128k＋128k＋64k＋64k） ＝ 9.5M。
- 可分配带宽总配额为所有（流的优先级＋1）的和。即：1＋2＋3＋4＋5 ＝ 15。
- 每个流所占可分配带宽比例为：（自己的优先级数＋1）/（所有 (流的优先级＋1) 的和）。即每个流可得的可分配带宽比分别为：1/15、2/15、3/15、4/15、5/15。
- 最终每个队列得到的带宽=最小保证带宽＋该队列从可分配带宽中分到的带宽。

由于 WFQ 在拥塞发生时能均衡各个流的延迟和抖动，所以 WFQ 在一些特殊场合得到了有效的应用。比如在使用资源预留协议 RSVP（Resource Reservation Protocol）的保证型业务中，通常就是采用 WFQ 作为调度策略；在流量整形 TS 中，也采用 WFQ 调度缓存的报文。

4. SP+WRR 队列

用户可以根据需要配置端口上的部分队列使用 SP 队列调度，部分队列使用 WRR 队列调度，通过将端口上的队列分别加入 SP 调度组和 WRR 调度组（即 group 1），实现 SP+WRR 的调度功能。在队列调度时，系统会优先保证 SP 调度组内的队列调度，当 SP 调度组内的队列中没有报文发送时，才会调度 WRR 调度组内的队列。SP 调度组内各个队列执行严格优先级调度方式，WRR 调度组内各个队列执行加权轮询调度方式。

5.2 拥塞管理配置任务简介

表5-1 拥塞管理配置任务简介

配置任务	说明	详细配置
配置 SP 队列	请根据需要选择一种拥塞管理方式	5.3
配置 WRR 队列		5.4
配置 WFQ 队列		5.5
配置 SP+WRR 队列		5.6

5.3 配置 SP 队列

5.3.1 配置过程

表5-2 SP 队列配置过程

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
配置 SP 队列		**qos sp**	必选 缺省情况下，端口采用 WRR 算法进行队列调度
显示 SP 队列		**display qos sp interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display** 命令可以在任意视图下执行

5.3.2 配置举例

(1) 组网需求

配置 GigabitEthernet1/0/1 采用 SP 队列。

(2) 配置步骤

进入系统视图

```
<Sysname> system-view
```

配置 GigabitEthernet1/0/1 的 SP 队列。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos sp
```

5.4 配置 WRR 队列

5.4.1 配置过程

表5-3 WRR 队列配置过程

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
开启端口的 WRR 队列，并指定 WRR 队列的调度单位（字节数或报文个数）		**qos wrr** [**byte-count** | **weight**]	可选 缺省情况下，端口使用 WRR 队列调度算法，并使用字节数为单位进行调度
配置 WRR 队列的调度权重	以字节数为调度单位	**qos wrr** *queue-id* **group 1 byte-count** *schedule-value*	请根据 WRR 队列的调度单位选择其中一种方法进行配置 缺省情况下，WRR 队列使用字节数为单位进行调度，8 个队列的调度权重值分别为 1、2、3、4、5、9、13、15
	以报文个数为调度单位	**qos wrr** *queue-id* **group 1 weight** *schedule-value*	
显示 WRR 队列的配置		**display qos wrr interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display** 命令可以在任意视图下执行

5.4.2 配置举例

(1) 组网需求

- 配置端口 GigabitEthernet1/0/1 的队列为 WRR 队列，并使用字节数为单位进行调度。
- 配置所有队列均属于为 WRR 分组，权重分别为 1、2、4、6、8、10、12、14。

(2) 配置步骤

进入系统视图。

```
<Sysname> system-view
```

配置端口 GigabitEthernet 1/0/1 使用 WRR 队列调度算法。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr byte-count
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 byte-count 1
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group 1 byte-count 2
```

```
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group 1 byte-count 4
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group 1 byte-count 6
[Sysname-GigabitEthernet1/0/1] qos wrr 4 group 1 byte-count 8
[Sysname-GigabitEthernet1/0/1] qos wrr 5 group 1 byte-count 10
[Sysname-GigabitEthernet1/0/1] qos wrr 6 group 1 byte-count 12
[Sysname-GigabitEthernet1/0/1] qos wrr 7 group 1 byte-count 14
```

5.5 配置 WFQ 队列

5.5.1 配置过程

表5-4 WFQ 队列配置过程

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
使能 WFQ 队列		**qos wfq**	必选 缺省情况下，端口使用 WRR 队列进行调度
配置 WFQ 队列的最小保证带宽值		**qos bandwidth queue** *queue-id* **min** *bandwidth-value*	可选 缺省情况下，使用 WFQ 队列的端口上每个队列的最小保证带宽值为 64Kbps
配置 WFQ 队列的队列调度权重值		**qos wfq** *queue-id* **weight** *schedule-value*	可选 缺省情况下，开启 WFQ 调度算法后，各个队列的权重值为 1
显示 WFQ 队列配置		**display qos wfq interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display** 命令可以在任意视图下执行

5.5.2 配置举例

(1) 组网需求

- 配置端口 GigabitEthernet 1/0/1 使用 WFQ 队列调度算法，队列 0～7 的权重分别为 1、2、4、6、8、10、12、14。
- 配置队列 0 的最小保证带宽为 128kbps。

(2) 配置步骤

进入系统视图。

```
<Sysname> system-view
```

配置端口 GigabitEthernet 1/0/1 使用 WFQ 队列调度算法。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos wfq 0 weight 1
[Sysname-GigabitEthernet1/0/1] qos wfq 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wfq 2 weight 4
[Sysname-GigabitEthernet1/0/1] qos wfq 3 weight 6
[Sysname-GigabitEthernet1/0/1] qos wfq 4 weight 8
[Sysname-GigabitEthernet1/0/1] qos wfq 5 weight 10
[Sysname-GigabitEthernet1/0/1] qos wfq 6 weight 12
[Sysname-GigabitEthernet1/0/1] qos wfq 7 weight 14
```

配置端口队列 0 的最小保证带宽为 128kbps。

```
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 0 min 128
```

5.6 配置 SP+WRR 队列

5.6.1 配置过程

表5-5 配置 SP＋WRR 队列

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	
开启端口的 WRR 队列，并指定 WRR 队列的调度单位（字节数或报文个数）		**qos wrr** [**byte-count** | **weight**]	可选 缺省情况下，端口使用 WRR 队列调度算法，并使用字节数为单位进行调度
配置 SP 调度组		**qos wrr** *queue-id* **group sp**	必选 缺省情况下，所有队列均处于 WRR 调度组中
配置 WRR 调度组的队列调度权重	以字节数为调度单位	**qos wrr** *queue-id* **group 1 byte-count** *schedule-value*	请根据 WRR 队列的调度单位选择其中一种方法进行配置 缺省情况下，WRR 队列使用字节数为单位进行调度，8 个队列的权重值分别为 1、2、3、4、5、9、13、15
	以报文个数为调度单位	**qos wrr** *queue-id* **group 1 weight** *schedule-value*	

5.6.2 配置举例

(1) 组网需求

- 配置端口 GigabitEthernet 1/0/1 使用 SP+WRR 队列调度算法
- 配置端口 GigabitEthernet 1/0/1 上的 0、1、2、3 队列属于 SP 调度组

- 配置端口 GigabitEthernet 1/0/1 上的 4、5、6、7 队列属于 WRR 调度组，调度单位为字节数，调度权重分别为 2、4、6、8

(2) 配置步骤

进入系统视图。

```
<Sysname> system-view
```

配置端口 GigabitEthernet 1/0/1 使用 SP+WRR 队列调度算法。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 4 group 1 byte-count 2
[Sysname-GigabitEthernet1/0/1] qos wrr 5 group 1 byte-count 4
[Sysname-GigabitEthernet1/0/1] qos wrr 6 group 1 byte-count 6
[Sysname-GigabitEthernet1/0/1] qos wrr 7 group 1 byte-count 8
```

6 拥塞避免配置

说明

本章中提到的三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

6.1 拥塞避免简介

过度的拥塞会对网络资源造成极大危害，必须采取某种措施加以解除。拥塞避免（Congestion Avoidance）是一种流量控制机制，它通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞产生或有加剧的趋势时主动丢弃报文，通过调整网络的流量来解除网络过载。

与端到端的流量控制相比，这里的流量控制具有更广泛的意义，它影响到设备中更多的业务流的负载。设备在丢弃报文时，需要与源端的流量控制动作（比如 TCP 流量控制）相配合，调整网络的流量到一个合理的负载状态。丢包策略和源端流控机制有效的组合，可以使网络的吞吐量和利用效率最大化，并且使报文丢弃和延迟最小化。

1. 传统的丢包策略

传统的丢包策略采用尾部丢弃（Tail-Drop）的方法。当队列的长度达到最大值后，所有新到来的报文都将被丢弃。

这种丢弃策略会引发 TCP 全局同步现象：当队列同时丢弃多个 TCP 连接的报文时，将造成多个 TCP 连接同时进入拥塞避免和慢启动状态以降低并调整流量，而后又会在某个时间同时出现流量高峰。如此反复，使网络流量忽大忽小，网络不停震荡。

2. RED 与 WRED

为避免 TCP 全局同步现象，可使用 RED（Random Early Detection，随机早期检测）或 WRED（Weighted Random Early Detection，加权随机早期检测）。

RED 和 WRED 通过随机丢弃报文避免了 TCP 的全局同步现象，使得当某个 TCP 连接的报文被丢弃、开始减速发送的时候，其他的 TCP 连接仍然有较高的发送速度。这样，无论什么时候，总有 TCP 连接在进行较快的发送，提高了线路带宽的利用率。

在 RED 类算法中，为每个队列都设定上限和下限，对队列中的报文进行如下处理：

- 当队列的长度小于下限时，不丢弃报文；
- 当队列的长度超过上限时，丢弃所有到来的报文；
- 当队列的长度在上限和下限之间时，开始随机丢弃到来的报文。队列越长，丢弃概率越高，但有一个最大丢弃概率。

与 RED 不同，WRED 生成的随机数是基于优先权的，它引入 IP 优先权区别丢弃策略，考虑了高优先权报文的利益，使其被丢弃的概率相对较小。

直接采用队列的长度和上限、下限比较并进行丢弃，将会对突发性的数据流造成不公正的待遇，不利于数据流的传输。WRED 采用平均队列和设置的队列上限、下限比较来确定丢弃的概率。

队列平均长度既反映了队列的变化趋势，又对队列长度的突发变化不敏感，避免了对突发性数据流的不公正待遇。计算队列平均长度的公式为：平均队列长度=上一时刻平均队列长度＋（当前队列

长度 - 上一时刻平均队列长度）/ 2^n。其中 n 可以通过命令 **qos wred weighting-constant** 进行配置。

6.2 WRED 配置的说明

6.2.1 WRED 的配置方式

CE3000-32F-EI 交换机的 WRED 功能采用 WRED 表的配置方式，即在系统视图下配置 WRED 表，然后在端口上应用 WRED 表。

6.2.2 WRED 的参数说明

在进行 WRED 配置时，需要事先确定如下参数：

- 队列上限和下限：当平均队列长度小于下限时，不丢弃报文。当平均队列长度在上限和下限之间时，设备随机丢弃报文，队列越长，丢弃概率越高。当平均队列长度超过上限时，丢弃所有到来的报文。
- 丢弃优先级：在进行报文丢弃时参考的参数，0 对应绿色报文、1 对应黄色报文、2 对应红色报文，红色报文将被优先丢弃。
- 计算平均队列长度的指数：指数越大，计算队列平均长度时对队列的实时变化越不敏感。
- 丢弃概率：以百分数的形式表示丢弃报文的概率，取值越大，报文被丢弃的机率越大。

6.3 配置 WRED

WRED 表是一个基于队列的表，拥塞时根据报文所在队列进行随机丢弃。

同一个表可以同时在多个端口应用。WRED 表被应用到端口后，用户可以对 WRED 表的取值进行修改，但是不能删除该 WRED 表。

6.3.1 配置过程

表6-1 WRED 表的配置和应用过程

操作		命令	说明
进入系统视图		**system-view**	-
配置 WRED 表		**qos wred queue table** *table-name*	-
配置计算平均队列长度的指数		**queue** *queue-id* **weighting-constant** *exponent*	可选 缺省情况下，该指数取值为 9
配置 WRED 表的其它参数		**queue** *queue-id* [**drop-level** *drop-level*] **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]	可选 缺省情况下，*low-limit* 为 100，*high-limit* 为 1000，*discard-prob* 为 10
进入二层以太网端口视图、三层以太网端口视图或端口组视图	进入二层以太网端口视图/三层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图/三层以太网端口视图后，下面进行的配置只在当前端口生效；进入端口组视图后，下面进行的配置将在端口组中的所有端口生效
	进入端口组视图	**port-group manual** *port-group-name*	

操作	命令	说明
在端口上应用 WRED 表	**qos wred apply** *table-name*	必选

6.3.2 配置举例

1. 组网需求

配置 WRED 表，对队列 1 中的黄色报文，丢弃队列上限为 100，下限为 30，丢弃概率为百分之 50，并将此 WRED 表应用到端口 GigabitEthernet 1/0/1 上。

2. 配置步骤

进入系统视图

```
<Sysname> system-view
```

根据组网需求创建 WRED 表并配置相应的参数。

```
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 30 high-limit 100 discard-probability 50
[Sysname-wred-table-queue-table1] quit
```

进入端口视图。

```
[Sysname] interface gigabitethernet 1/0/1
```

在端口上应用 WRED 表。

```
[Sysname-GigabitEthernet1/0/1] qos wred apply queue-table1
```

6.4 WRED 显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 WRED 的运行情况，通过查看显示信息验证配置的效果。

表6-2 WRED 显示和维护

操作	命令
显示端口的 WRED 配置情况和统计信息	**display qos wred interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示 WRED 表配置情况	**display qos wred table** [*table-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

7 流量过滤配置

7.1 流量过滤简介

流量过滤就是将符合流分类的流配置流量过滤动作。

例如，可以根据网络的实际情况禁止从某个源 IP 地址发送的报文通过。

7.2 配置流量过滤

表7-1 配置流量过滤

操作		命令	说明
进入系统视图		**system-view**	-
定义类并进入类视图		**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则		**if-match** *match-criteria*	-
退出类视图		**quit**	-
定义一个流行为并进入流行为视图		**traffic behavior** *behavior-name*	-
配置流量过滤动作		**filter** { **deny** | **permit** }	必选 **deny** 表示丢弃数据包；**permit** 表示允许数据包通过
退出流行为视图		**quit**	-
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用 QoS 策略	基于端口	**2.2.4 1.** 基于端口应用QoS策略	-
	基于上线用户	**2.2.4 2.** 基于上线用户应用QoS策略	-
	基于 VLAN	**2.2.4 3.** 基于VLAN应用QoS策略	-
	基于全局	**2.2.4 4.** 基于全局应用QoS策略	-
	基于控制平面	**2.2.4 5.** 基于控制平面应用QoS策略	-
显示流量过滤的相关配置信息		**display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display** 命令可以在任意视图下执行

说明

如果配置了 **filter deny** 命令，那么其他流行为（除流量统计）都不会生效。

7.3 流量过滤配置举例

7.3.1 流量过滤配置举例

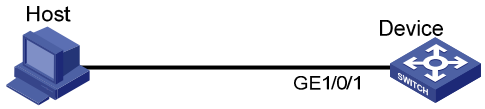
1. 组网需求

Host 通过端口 GigabitEthernet1/0/1 接入设备 Device。

配置流量过滤功能，对端口 GigabitEthernet1/0/1 接收的源端口号等于 21 的 TCP 报文进行丢弃。

2. 组网图

图7-1 配置流量过滤组网图



3. 配置步骤

定义高级 ACL 3000，匹配源端口号等于 21 的数据流。

```
<DeviceA> system-view
[DeviceA] acl number 3000
[DeviceA-acl-basic-3000] rule 0 permit tcp source-port eq 21
[DeviceA-acl-basic-3000] quit
```

定义类 classifier_1，匹配高级 ACL 3000。

```
[DeviceA] traffic classifier classifier_1
[DeviceA-classifier-classifier_1] if-match acl 3000
[DeviceA-classifier-classifier_1] quit
```

定义流行为 behavior_1，动作为流量过滤（**deny**），表示对数据包进行丢弃。

```
[DeviceA] traffic behavior behavior_1
[DeviceA-behavior-behavior_1] filter deny
[DeviceA-behavior-behavior_1] quit
```

定义策略 policy，为类 classifier_1 指定流行为 behavior_1。

```
[DeviceA] qos policy policy
[DeviceA-qospolicy-policy] classifier classifier_1 behavior behavior_1
[DeviceA-qospolicy-policy] quit
```

将策略 policy 应用到端口 GigabitEthernet1/0/1 的入方向上。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy policy inbound
```

8 重标记配置

8.1 重标记简介

说明

重标记可以和优先级映射功能配合使用，具体请参见优先级映射章节 3.5.2 。

重标记是将报文的优先级或者标志位进行设置，重新定义流量的优先级等。例如，对于 IP 报文来说，所谓重标记就是对 IP 报文中的 IP 优先级或 DSCP 值进行重新设置，改变 IP 报文在网络传输中状态。

重标记动作的配置，可以通过与类关联，将原来报文的优先级或标志位重新进行标记。

8.2 根据报文颜色进行优先级重标记

8.2.1 报文颜色的标记方式

报文的颜色用来表示设备对报文传输优先等级的评估结果，CE3000-32F-EI 交换机可以根据以下两种方式为报文标记颜色：

- 流量监管功能
- 映射丢弃优先级

1. 流量监管功能

流量监管是一种常用的流量控制技术，它可以通过令牌桶机制来对设备接收或发送的流量进行评估，并根据评估结果对报文标记不同的颜色。用户通过为不同颜色的报文配置不同的流控策略，来实现对不同流量的差异化服务，从而保证网络资源的有效利用。

CE3000-32F-EI 交换机支持双令牌桶评估方式（C 桶和 E 桶），可以根据令牌桶中令牌的使用情况来标记报文的颜色：

- 如果 C 桶有足够的令牌，报文被标记为 green，即绿色报文；
- 如果 C 桶令牌不足，但 E 桶有足够的令牌，报文被标记为 yellow，即黄色报文；
- 如果 C 桶和 E 桶都没有足够的令牌，报文被标记为 red，即红色报文。

说明

CE3000-32F-EI交换机支持使用普通CAR以及聚合CAR两种流量监管功能为报文标记颜色，有关这两种功能的详细介绍和配置方法，请参见 流量监管、流量整形和端口限速配置以及 全局CAR配置。

2. 映射丢弃优先级

在没有配置流量监管功能的情况下，CE3000-32F-EI交换机根据报文的802.1p优先级以及dot1p-dp映射表，映射出报文的丢弃优先级，并根据丢弃优先级为报文标记颜色。丢弃优先级 0 对应绿色报文、1 对应黄色报文、2 对应红色报文。

说明

关于优先级映射表以及调整优先级映射关系的详细介绍和配置，请参见 优先级映射配置。

8.2.2 根据报文颜色进行优先级重标记

1. 基于流量监管的评估结果进行优先级重标记

在得到流量监管的评估结果之后，CE3000-32F-EI 交换机可以为不同颜色的报文重新标记各种优先级值，包括 DSCP 优先级、802.1p 优先级和本地优先级，您可以通过以下两种方式进行配置：

- 在流量监管动作中指定对不同颜色的报文采取的重标记动作
- 在流量监管动作所属的流行为中创建重标记动作，为不同颜色的报文标记各种优先级值

说明

- 您可以同时采用这两种方式为同一颜色报文的多种优先级进行重标记。但两种方式中不能包含对同一种优先级的不同标记动作，否则采用流行为的 QoS 策略将无法正常应用。
- 关于在流量监管动作中指定重标记动作的配置，请参见 流量监管配置以及 配置聚合CAR。

2. 基于丢弃优先级的映射结果进行优先级重标记

在使用丢弃优先级为报文标记颜色的情况下，您可以通过在流行为中创建重标记动作，为不同颜色的报文标记各种优先级值，包括 DSCP 优先级、802.1p 优先级和本地优先级。

8.3 配置重标记

表8-1 配置重标记

操作	命令	说明
进入系统视图	**system-view**	-
定义类并进入类视图	**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则	**if-match** *match-criteria*	-
退出类视图	**quit**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	-
配置标记报文的 DSCP 值	**remark** [**green** | **red** | **yellow**] **dscp** *dscp-value*	可选 如果是对通过流量监管标记颜色的报文进行优先级重标记，需要注意重标记动作中的标记策略不能与流量监管中的标记策略冲突，否则 QoS 策略将无法正常应用

操作		命令	说明
配置标记报文的802.1p优先级		**remark** [**green** | **red** | **yellow**] **dot1p** *802.1p*	可选 如果是对通过流量监管标记颜色的报文进行优先级重标记，需要注意重标记动作中的标记策略不能与流量监管中的标记策略冲突，否则QoS策略将无法正常应用
配置内外层标签优先级复制功能		**remark dot1p customer-dot1p-trust**	可选
配置标记报文的丢弃优先级		**remark drop-precedence** *drop-precedence-value*	可选 仅应用在出方向
配置标记报文的IP优先级值		**remark ip-precedence** *ip-precedence-value*	可选
配置标记报文的本地优先级		**remark** [**green** | **red** | **yellow**] **local-precedence** *local-precedence*	可选 如果是对通过流量监管标记颜色的报文进行优先级重标记，需要注意重标记动作中的标记策略不能与流量监管中的标记策略冲突，否则QoS策略将无法正常应用 在使用聚合CAR方式标记报文颜色时，不支持根据报文颜色重标记本地优先级。
配置标记报文的qos-local-id		**remark qos-local-id** *local-id-value*	可选 qos-local-id是设备为报文重新标记的一种属性，用户可以根据不同的需求给报文标记不同的qos-local-id。标记qos-local-id主要用于对匹配多个流分类的报文进行重分类，再对这个重分类进行流行为动作，以达到对多种报文进行同一种处理方式的效果
退出流行为视图		**quit**	-
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用QoS策略	基于端口	2.2.4 1. 基于端口应用QoS策略	-
	基于上线用户	2.2.4 2. 基于上线用户应用QoS策略	-
	基于VLAN	2.2.4 3. 基于VLAN应用QoS策略	-
	基于全局	2.2.4 4. 基于全局应用QoS策略	-
	基于控制平面	2.2.4 5. 基于控制平面应用QoS策略	-
显示重标记的相关配置信息		**display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display** 命令可以在任意视图下执行

应用重标记的 QoS 策略时 **inbound** 和 **outbound** 方向的支持情况如下表所示。

表8-2 inbound 和 outbound 方向的支持情况

动作	inbound 方向	outbound 方向
标记报文的 802.1p 优先级	支持	支持
标记报文的 DSCP 优先级	支持	支持
标记报文的丢弃优先级	支持	不支持
标记报文的 IP 优先级	不支持	支持
标记报文的本地优先级	支持	不支持
标记报文的 qos-local-id	支持	不支持

8.4 重标记配置举例

8.4.1 重标记优先级配置举例

1. 组网需求

公司企业网通过 Device 实现互连。网络环境描述如下：

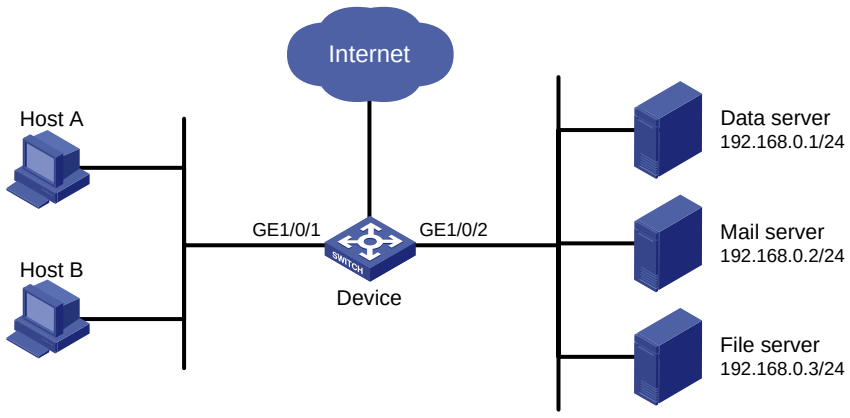
- Host A 和 Host B 通过端口 GigabitEthernet1/0/1 接入 Device；
- 数据库服务器、邮件服务器和文件服务器通过端口 GigabitEthernet1/0/2 接入 Device。

通过配置重标记功能，Device 上实现如下需求：

- 优先处理 Host A 和 Host B 访问数据库服务器的报文；
- 其次处理 Host A 和 Host B 访问邮件服务器的报文；
- 最后处理 Host A 和 Host B 访问文件服务器的报文。

2. 组网图

图8-1 配置重标记组网图



3. 配置步骤

定义高级 ACL 3000，对目的 IP 地址为 192.168.0.1 的报文进行分类。

```
<Device> system-view
[Device] acl number 3000
```

```
[Device-acl-adv-3000] rule permit ip destination 192.168.0.1 0
[Device-acl-adv-3000] quit
```
定义高级 ACL 3001，对目的 IP 地址为 192.168.0.2 的报文进行分类。
```
[Device] acl number 3001
[Device-acl-adv-3001] rule permit ip destination 192.168.0.2 0
[Device-acl-adv-3001] quit
```
定义高级 ACL 3002，对目的 IP 地址为 192.168.0.3 的报文进行分类。
```
[Device] acl number 3002
[Device-acl-adv-3002] rule permit ip destination 192.168.0.3 0
[Device-acl-adv-3002] quit
```
定义类 classifier_dbserver，匹配高级 ACL 3000。
```
[Device] traffic classifier classifier_dbserver
[Device-classifier-classifier_dbserver] if-match acl 3000
[Device-classifier-classifier_dbserver] quit
```
定义类 classifier_mserver，匹配高级 ACL 3001。
```
[Device] traffic classifier classifier_mserver
[Device-classifier-classifier_mserver] if-match acl 3001
[Device-classifier-classifier_mserver] quit
```
定义类 classifier_fserver，匹配高级 ACL 3002。
```
[Device] traffic classifier classifier_fserver
[Device-classifier-classifier_fserver] if-match acl 3002
[Device-classifier-classifier_fserver] quit
```
定义流行为 behavior_dbserver，动作为重标记报文的本地优先级为 4。
```
[Device] traffic behavior behavior_dbserver
[Device-behavior-behavior_dbserver] remark local-precedence 4
[Device-behavior-behavior_dbserver] quit
```
定义流行为 behavior_mserver，动作为重标记报文的本地优先级为 3。
```
[Device] traffic behavior behavior_mserver
[Device-behavior-behavior_mserver] remark local-precedence 3
[Device-behavior-behavior_mserver] quit
```
定义流行为 behavior_fserver，动作为重标记报文的本地优先级为 2。
```
[Device] traffic behavior behavior_fserver
[Device-behavior-behavior_fserver] remark local-precedence 2
[Device-behavior-behavior_fserver] quit
```
定义策略 policy_server，为类指定流行为。
```
[Device] qos policy policy_server
[Device-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[Device-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[Device-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[Device-qospolicy-policy_server] quit
```
将策略 policy_server 应用到端口 GigabitEthernet1/0/1 上。
```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy_server inbound
[Device-GigabitEthernet1/0/1] quit
```

8.4.2 重标记 qos-local-id 配置举例

重标记 qos-local-id 功能主要用于将匹配多种分类条件的报文进行重分类，再对这个重分类进行流行为的情况。

例如：需要对源 MAC 地址为 0001-0001-0001，或者源 IP 地址为 1.1.1.1 的这两种报文的总流量限速为 128Kbps，如果采用匹配源 MAC 地址的分类和匹配源 IP 地址的流分类分别与流量监管的流行为进行关联的 QoS 策略配置方式，则最后的配置结果会是两种报文的限速分别为 128Kbps，无法达到预期效果。

而通过使用 qos-local-id 就可以解决这个问题。首先将匹配源 MAC 地址和源 IP 地址的报文标记统一的 qos-local-id，然后再以 qos-local-id 为新的分类条件，创建流量监管的动作，这样就可以对这两种报文的总流量进行限速。配置步骤如下：

创建 ACL 2000，匹配源 IP 地址为 1.1.1.1 的报文。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2000] quit
```

创建流分类 class_a，匹配源 MAC 地址为 0001-0001-0001 或源 IP 地址为 1.1.1.1 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class_a operator or
[Sysname-classifier-class_a] if-match source-mac 1-1-1
[Sysname-classifier-class_a] if-match acl 2000
[Sysname-classifier-class_a] quit
```

创建流行为 behavior_a，对匹配 class_a 分类的报文将 qos-local-id 标记为 100。

```
[Sysname] traffic behavior behavior_a
[Sysname-behavior-behavior_a] remark qos-local-id 100
[Sysname-behavior-behavior_a] quit
```

创建流分类 class_b，匹配 qos-local-id 为 100 的报文。

```
[Sysname] traffic classifier class_b
[Sysname-classifier-class_b] if-match qos-local-id 100
[Sysname-classifier-class_b] quit
```

创建流行为 behavior_b，对匹配 class_b 分类的报文限速为 128Kbps。

```
[Sysname] traffic behavior behavior_b
[Sysname-behavior-behavior_b] car cir 128
[Sysname-behavior-behavior_b] quit
```

创建 QoS 策略 car_policy，并将 class_a 和 behavior_a 进行关联，将 class_b 和 behavior_b 进行关联。

```
[Sysname] qos policy car_policy
[Sysname-qospolicy-car_policy] classifier class_a behavior behavior_a
[Sysname-qospolicy-car_policy] classifier class_b behavior behavior_b
```

将通过上面步骤创建的 QoS 策略应用到端口后，即可实现组网需求。

8.4.3 基于流量监管的颜色标记进行优先级重标记配置举例

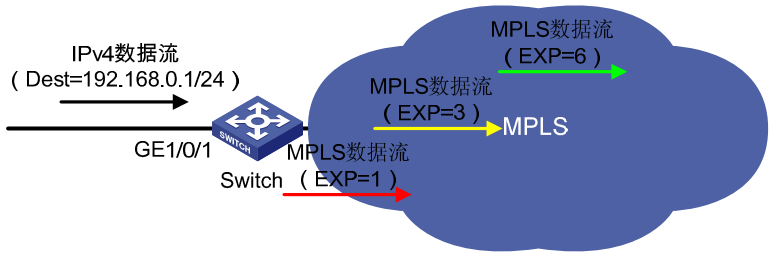
1. 组网需求

Switch 作为 MPLS 域的边缘设备，通过 GigabitEthernet1/0/1 端口接入 IPv4 网络，负责为进入 MPLS 域的报文封装 MPLS 标签。

现需要对 GigabitEthernet1/0/1 端口接收到的目的为 192.168.0.1/24 网段的报文进行限速并标记颜色。限速参数为：CIR=1024Kbps，CBS=8000bytes，EBS=8000bytes，PIR=2048Kbps。对经过流量监管评估后的报文全部采取发送的操作，但在封装 MPLS 标签时，对绿色报文标记 EXP 优先级为 6；对黄色报文标记 EXP 优先级为 3；对红色报文标记 EXP 优先级为 1。

2. 组网图

图8-2 基于流量监管的评估结果进行重标记组网示意图



3. 配置步骤

(1) 配置 MPLS 基本功能

关于 MPLS 基本功能的配置，请参见“MPLS 配置指导”中的“MPLS 基本配置”，这里不再赘述。

(2) 配置流量监管策略

创建高级 ACL3000，匹配目的地址为 192.168.0.1/24 网段的报文。

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip destination 192.168.1.0 0.0.0.255
[Sysname-acl-adv-3000] quit
```

创建流分类 class1，匹配规则为 ACL3000。

```
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3000
[Sysname-classifier-class1] quit
```

配置流行为 behavior1，动作为流量监管，并根据组网需求配置相关参数。同时，由于默认情况下 802.1p 和 EXP 优先级是 1:1 映射关系，因此可以为不同颜色报文标记不同的 802.1p 优先级，802.1p 优先级将通过 dot1p-exp 映射表映射到 MPLS 标签中的 EXP 优先级，从而实现在不同颜色报文的 MPLS 标签中标记不同的 EXP 优先级值。

```
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] car cir 1024 cbs 8000 ebs 8000 pir 2048 green remark-dot1p-pass
6 red remark-dot1p-pass 1 yellow remark-dot1p-pass 3
[Sysname-behavior-behavior1] quit
```

创建 QoS 策略 policy1，将上面创建的流分类和流行为进行绑定。

```
[Sysname] qos policy policy1
[Sysname-qospolicy-policy1] classifier class1 behavior behavior1
[Sysname-qospolicy-policy1] quit
```

将 QoS 策略 policy1 应用到 GigabitEthernet1/0/1 端口的入方向。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy policy1 inbound
```

9 流量重定向配置

9.1 流量重定向简介

流量重定向就是将符合流分类的流重定向到其他地方进行处理。

目前支持的流量重定向包括以下几种：

- 重定向到 CPU：对于需要 CPU 处理的报文，可以通过配置上送给 CPU。
- 重定向到端口：对于收到需要由某个端口处理的报文时，可以通过配置重定向到此端口。只针对二层转发报文，端口为二层以太网端口。
- 重定向到下一跳：对于收到需要由某个接口处理的报文时，可以通过配置重定向到此接口。只针对三层转发报文。

9.2 配置流量重定向

表9-1 配置流量重定向

操作		命令	说明
进入系统视图		**system-view**	-
定义类并进入类视图		**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则		**if-match** *match-criteria*	-
退出类视图		**quit**	-
定义一个流行为并进入流行为视图		**traffic behavior** *behavior-name*	必选
配置流量重定向动作		**redirect** { **cpu** | **interface** *interface-type interface-number* | **next-hop** { *ipv4-add1* [*ipv4-add2*] | *ipv6-add1* [*interface-type interface-number*] [*ipv6-add2* [*interface-type interface-number*]] } [**fail-action** { **discard** | **forward** }] }	可选
退出流行为视图		**quit**	-
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用 QoS 策略	基于端口	**2.2.4 1.** 基于端口应用QoS策略	-
	基于 VLAN	**2.2.4 3.** 基于VLAN应用QoS策略	-
	基于全局	**2.2.4 4.** 基于全局应用QoS策略	-
	基于控制平面	**2.2.4 5.** 基于控制平面应用QoS策略	-

说明

- 在配置重定向动作时，同一个流行为中重定向类型只能为重定向到 CPU、重定向到端口、重定向到下一跳中的一种。
- 在配置重定向下一跳失败的处理动作时，如果不配置处理动作，默认的处理动作是转发。
- 可以通过命令 **display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]查看流量重定向的相关配置信息。

10 全局 CAR 配置

10.1 全局 CAR 简介

全局 CAR 是在全局创建的一种策略，所有应用该策略的数据流将共同接受全局 CAR 的监管。

目前全局 CAR 支持聚合 CAR 和分层 CAR 两种。

10.1.1 聚合 CAR

聚合 CAR 是指能够对多个业务流使用同一个 CAR 进行流量监管，即如果多个端口应用同一聚合 CAR，则这多个端口的流量之和必须在此聚合 CAR 设定的流量监管范围之内。

10.1.2 分层 CAR

分层 CAR 是一种更灵活的流量监管策略，用户可以在为每个流单独配置 CAR 动作（或聚合 CAR）的基础上，再通过分层 CAR 对多个流的流量总和进行限制。

分层 CAR 与普通 CAR（或聚合 CAR）的结合应用有两种模式：

- and：在该模式下，对于多条数据流应用同一个分层 CAR，必须每条流满足各自的普通 CAR（或聚合 CAR）配置，同时各流量之和又满足分层 CAR 的配置，流量才能正常通过。and 模式适用于严格限制流量带宽的环境，分层 CAR 的限速配置通常小于各流量自身 CAR 的限速值之和。例如对于 Internet 流量，可以使用普通 CAR 将数据流 1 和数据流 2 各自限速为 128kbps，再使用分层 CAR 限制总流量为 192kbps。当不存在数据流 1 时，数据流 2 可以用达到自身限速上限的速率访问 Internet，如果存在数据流 1，则两个数据流不能超过各自限速且总速率不能超过 192kbps。
- or：在该模式下，对于多条数据流应用同一个分层 CAR，只要每条流满足各自的普通 CAR（或聚合 CAR）配置或者各流量之和满足分层 CAR 配置，流量即可正常通过。or 模式适用于保证高优先级业务带宽的环境，分层 CAR 的限速值通常等于或大于各流量自身的限速值之和。例如对于视频流量，使用普通 CAR 将数据流 1 和数据流 2 各自限速 128kbps，再使用分层 CAR 限制总流量为 512kbps，则当数据流 1 的流量不足 128kbps 时，即使数据流 2 的流量达到了的 384kbps，仍然可以正常通过。

两种模式可以结合起来使用，达到合理利用带宽的效果。例如，存在一条视频流和一条数据流，使用普通 CAR 将数据流限速 1024kbps、视频流限速 2048kbps。连接视频流接口采用 or 模式 CAR 限速 3072kbps，因为可能存在多台视频设备同时上线出现的突发流量，当视频设备流量速率超出 2048kbps 时，如果总体流量资源仍有剩余（即数据流速率在 1024kbps 以内），这时视频流可以临时借用数据流的带宽；同时，连接数据流接口采用 and 模式 CAR 限速 3072kbps，确保数据流量不能超出自身限速的 1024kbps。

10.2 配置聚合 CAR

10.2.1 配置过程

表10-1 配置聚合 CAR

操作	命令	说明
进入系统视图	**system-view**	-
配置聚合 CAR 的各个参数	**qos car** *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peek-information-rate*] [**red** *action*]	必选
进入流行为视图	**traffic behavior** *behavior-name*	必选
在流行为中引用聚合 CAR	**car name** *car-name*	必选
显示配置的流行为信息	**display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display** 命令可以在任意视图下执行
显示指定聚合 CAR 的 CAR 配置和统计信息	**display qos car name** [*car-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	

10.2.2 配置举例

配置聚合 CAR aggcar-1 采取的 CAR 参数取值，cir 取值为 256，cbs 取值为 2000，对于红色报文采取丢弃的动作，并在流行为 be1 中引用 aggcar-1。

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 256 cbs 2000 red discard
[Sysname] traffic behavior be1
[Sysname-behavior-be1] car name aggcar-1
```

10.3 配置分层 CAR

表10-2 配置分层 CAR

操作	命令	说明
进入系统视图	**system-view**	-
配置分层 CAR 的各个参数	**qos car** *car-name* **hierarchy cir** *committed-information-rate* [**cbs** *committed-burst-size*]	必选
进入流行为视图	**traffic behavior** *behavior-name*	必选
在流行为中引用分层 CAR（和聚合 CAR 配合使用）	**car name** *car-name* **hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]	二者必选其一 普通CAR的相关内容请参见 4.2 流量

操作	命令	说明
在流行为中引用分层 CAR（和普通 CAR 配合使用）	**car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action*] [**yellow** *action*] [**red** *action*] **hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]	监管配置
显示配置的流行为信息	**display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display** 命令可以在任意视图下执行
显示指定全局 CAR 的 CAR 配置和统计信息	**display qos car name** [*car-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	

10.4 全局 CAR 显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后全局 CAR 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除全局 CAR 统计信息。

表10-3 全局 CAR 显示和维护

操作	命令
显示全局 CAR 的配置和统计信息	**display qos car name** [*car-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除全局 CAR 的统计信息	**reset qos car name** [*car-name*]

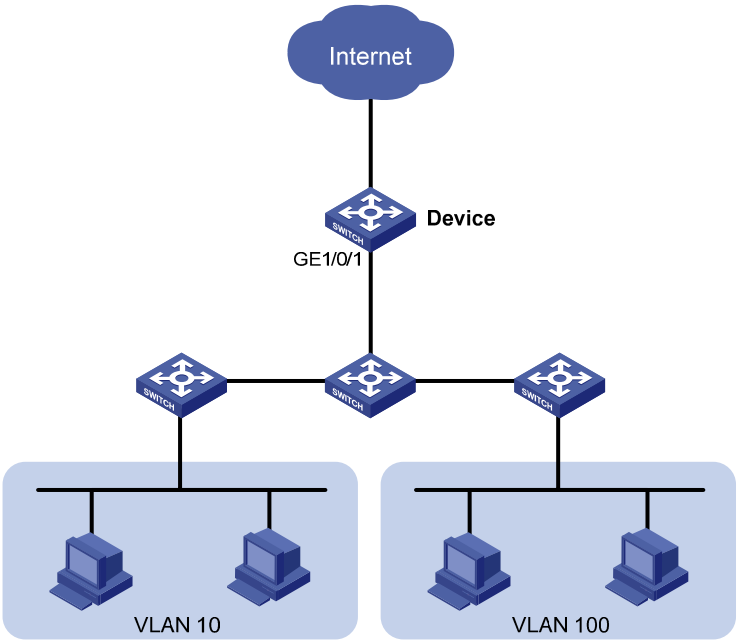
10.5 全局 CAR 配置举例

10.5.1 聚合 CAR 配置举例

1. 组网需求

通过配置聚合 CAR，对端口 GigabitEthernet1/0/1 接收的 VLAN10 和 VLAN100 的报文流量之和进行限制，cir 为 2560，cbs 为 20000，对于红色报文，采取丢弃策略。

2. 组网图



3. 配置步骤

按流量限制需求配置聚合 CAR。

```
<Device> system-view
[Device] qos car aggcar-1 aggregative cir 2560 cbs 20000 red discard
```

配置流分类和流行为，对 VLAN10 的报文采用聚合 CAR 的限速配置。

```
[Device] traffic classifier 1
[Device-classifier-1] if-match customer-vlan-id 10
[Device-classifier-1] quit
[Device] traffic behavior 1
[Device-behavior-1] car name aggcar-1
[Device-behavior-1] quit
```

配置流分类和流行为，对 VLAN100 的报文采用聚合 CAR 的限速配置。

```
[Device] traffic classifier 2
[Device-classifier-2] if-match customer-vlan-id 100
[Device-classifier-2] quit
[Device] traffic behavior 2
[Device-behavior-2] car name aggcar-1
[Device-behavior-2] quit
```

配置 QoS 策略，将流分类与流行为进行绑定。

```
[Device] qos policy car
[Device-qospolicy-car] classifier 1 behavior 1
[Device-qospolicy-car] classifier 2 behavior 2
[Device-qospolicy-car] quit
```

将 QoS 策略应用到端口 GigabitEthernet1/0/1 的入方向。

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1]qos apply policy car inbound
```

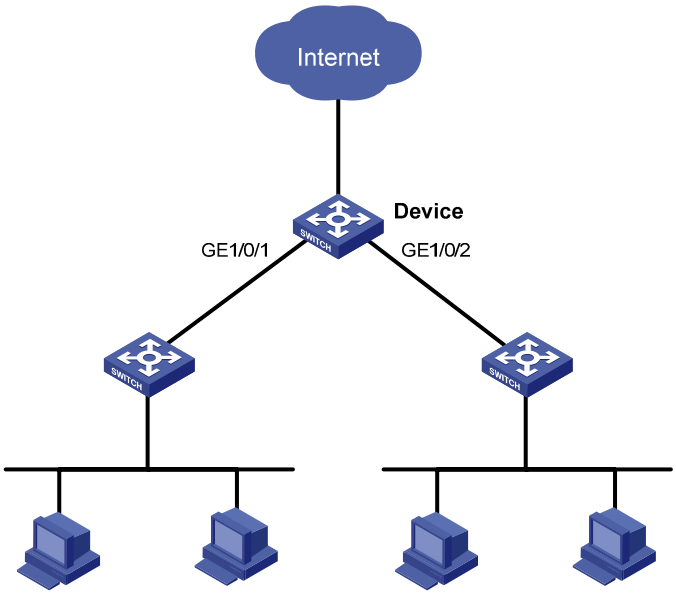
10.5.2 and 模式分层 CAR 配置举例

1. 组网需求

对端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 接收的 HTTP 报文流量进行限速，要求每个端口接收到的HTTP报文速率不能超过192kbps。同时，使用分层CAR来限制这两个端口接收的HTTP总流量不能超过 256kbps，丢弃超过流量上限的报文。

2. 组网图

图10-1 and 模式配置举例组网图



3. 配置步骤

按流量限制需求配置分层 CAR。

```
<Device> system-view
[Device] qos car http hierarchy cir 256 red discard
```

配置 ACL 3000，匹配 HTTP 报文。

```
[Device] acl number 3000
[Device-acl-basic-3000] rule permit tcp destination-port eq 80
[Device-acl-basic-3000] quit
```

配置流分类和流行为，对 HTTP 报文进行 CAR 限速，并与分层 CAR 结合使用。

```
[Device] traffic classifier 1
[Device-classifier-1] if-match acl 3000
[Device-classifier-1] quit
[Device] traffic behavior 1
[Device-behavior-1] car cir 192 hierarchy-car http mode and
[Device-behavior-1] quit
```

配置 QoS 策略，将流分类与流行为进行绑定。

```
[Device] qos policy http
[Device-qospolicy-http] classifier 1 behavior 1
[Device-qospolicy-http] quit
```

将 QoS 策略应用到端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的入方向。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy http inbound
```

```
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] qos apply policy http inbound
```

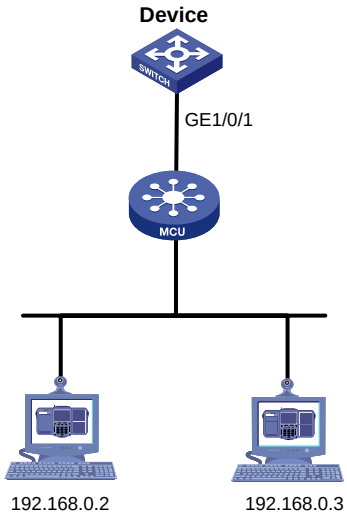
10.5.3 or 模式配置举例

1. 组网需求

对端口 GigabitEthernet1/0/1 接收的来自 192.168.0.2 和 192.168.0.3 的视频报文流量进行限速，根据日常视频应用的流量速率，配置 cir 为 256kbps。同时为保证可能出现的大流量视频应用能够顺利通过，使用分层 CAR 为视频报文限定总流量上限为 640kbps，丢弃超出流量上限的报文。

2. 组网图

图10-2 or 模式配置举例组网图



3. 配置步骤

按流量限制需求配置分层 CAR。

```
<Device> system-view
[Device] qos car video hierarchy cir 640 red discard
```

配置流分类和流行为，对来自视讯终端（192.168.0.2）的报文进行普通 CAR 限速，并与分层 CAR 结合使用。

```
[Device] acl number 2000
[Device-acl-basic-2000] rule permit source 192.168.0.2 0.0.0.0
[Device-acl-basic-2000] quit
[Device] traffic classifier 1
[Device-classifier-1] if-match acl 2000
[Device-classifier-1] quit
[Device] traffic behavior 1
[Device-behavior-1] car cir 256 hierarchy-car video mode or
[Device-behavior-1] quit
```

配置流分类和流行为，对来自视讯终端（192.168.0.3）的报文进行普通 CAR 限速，并与分层 CAR 结合使用。

```
[Device] acl number 2001
[Device-acl-basic-2001] rule permit source 192.168.0.3 0.0.0.0
[Device-acl-basic-2001] quit
[Device] traffic classifier 2
```

```
[Device-classifier-2] if-match acl 2001
[Device-classifier-2] quit
[Device] traffic behavior 2
[Device-behavior-2] car cir 256 hierarchy-car video mode or
[Device-behavior-2] quit
```

配置 QoS 策略，将流分类与流行为进行绑定。

```
[Device] qos policy video
[Device-qospolicy-video] classifier 1 behavior 1
[Device-qospolicy-video] classifier 2 behavior 2
[Device-qospolicy-video] quit
```

将 QoS 策略应用到端口 GigabitEthernet1/0/1 的入方向。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy video inbound
```

11 流量统计配置

11.1 流量统计简介

流量统计就是通过与类关联，对符合匹配规则的流进行统计。例如，可以统计从某个源 IP 地址发送的报文，然后管理员对统计信息进行分析，根据分析情况采取相应的措施。

11.2 配置流量统计

表11-1 配置流量统计

操作		命令	说明
进入系统视图		**system-view**	-
定义类并进入类视图		**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则		**if-match** *match-criteria*	-
退出类视图		**quit**	-
定义一个流行为并进入流行为视图		**traffic behavior** *behavior-name*	必选
配置统计动作		**accounting { byte | packet }**	可选 **byte** 表示报文基于字节为最小单位进行统计；**packet** 表示报文基于包为最小单位进行统计
退出流行为视图		**quit**	-
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用 QoS 策略	基于端口	**2.2.4 1.** 基于端口应用QoS策略	-
	基于 VLAN	**2.2.4 3.** 基于VLAN应用QoS策略	-
	基于全局	**2.2.4 4.** 基于全局应用QoS策略	-
	基于控制平面	**2.2.4 5.** 基于控制平面应用QoS策略	-

11.3 流量统计显示和维护

在完成上述配置后，用户可以根据 QoS 的应用范围在任意视图下执行 **display qos policy global**、**display qos policy interface** 或 **display qos vlan-policy** 命令来显示流量统计的情况，通过查看显示信息验证配置的效果。

11.4 流量统计配置举例

11.4.1 流量统计配置举例

1. 组网需求

用户网络描述如下：Host 通过端口 GigabitEthernet1/0/1 接入设备 Device。

配置流量统计功能，对端口 GigabitEthernet1/0/1 接收的源 IP 地址为 1.1.1.1/24 的报文进行统计。

2. 组网图

图11-1 配置流量统计组网图

3. 配置步骤

定义基本 ACL 2000，对源 IP 地址为 1.1.1.1 的报文进行分类。

```
<DeviceA> system-view
[DeviceA] acl number 2000
[DeviceA-acl-basic-2000] rule permit source 1.1.1.1 0
[DeviceA-acl-basic-2000] quit
```

定义类 classifier_1，匹配基本 ACL 2000。

```
[DeviceA] traffic classifier classifier_1
[DeviceA-classifier-classifier_1] if-match acl 2000
[DeviceA-classifier-classifier_1] quit
```

定义流行为 behavior_1，动作为流量统计。

```
[DeviceA] traffic behavior behavior_1
[DeviceA-behavior-behavior_1] accounting
[DeviceA-behavior-behavior_1] quit
```

定义策略 policy，为类 classifier_1 指定流行为 behavior_1。

```
[DeviceA] qos policy policy
[DeviceA-qospolicy-policy] classifier classifier_1 behavior behavior_1
[DeviceA-qospolicy-policy] quit
```

将策略 policy 应用到端口 GigabitEthernet1/0/1 的入方向上。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos apply policy policy inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

查看配置后流量统计的情况。

```
[DeviceA] display qos policy interface gigabitethernet 1/0/1

  Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: policy
   Classifier: classifier_1
     Operator: AND
```

```
Rule(s) : If-match acl 2000
Behavior: behavior_1
 Accounting Enable:
   28529 (Packets)
```

12 配置数据缓冲区

12.1 数据缓冲区简介

12.1.1 数据缓冲区

CE3000-32F-EI 交换机提供的数据缓冲区用来缓存从所有端口发送的报文，防止在出现突发流量时由于拥塞而产生的丢包现象。

交换机通过分配 **cell** 资源和 **packet** 资源（统称为缓冲资源）来控制各端口对数据缓冲区的使用：

- cell 资源是指缓存报文时使用的设备存储芯片容量。端口上分配到的 cell 资源表示该端口最多可以在缓冲区中占用的缓存空间。
- packet 资源是一种逻辑上的计数资源，它表示设备发送的数据包个数。设备每发送一个数据包，无论该数据包的长度是多少，均占用 1 个 packet 资源。端口上分配到的 packet 资源表示该端口最多可以在缓冲区中缓存的报文个数。

两种资源相互独立，但又共同作用，当端口需要缓存报文时，既使用相当于报文长度的 **cell** 资源，同时也使用相当于报文数量的 **packet** 资源，如果其中一种资源耗尽，则端口将不能再缓存报文，未进入缓冲区的报文将被丢弃。在完成报文发送后，端口将所使用的资源释放，等待下次缓存报文时再次使用。

12.1.2 缓冲资源的分配

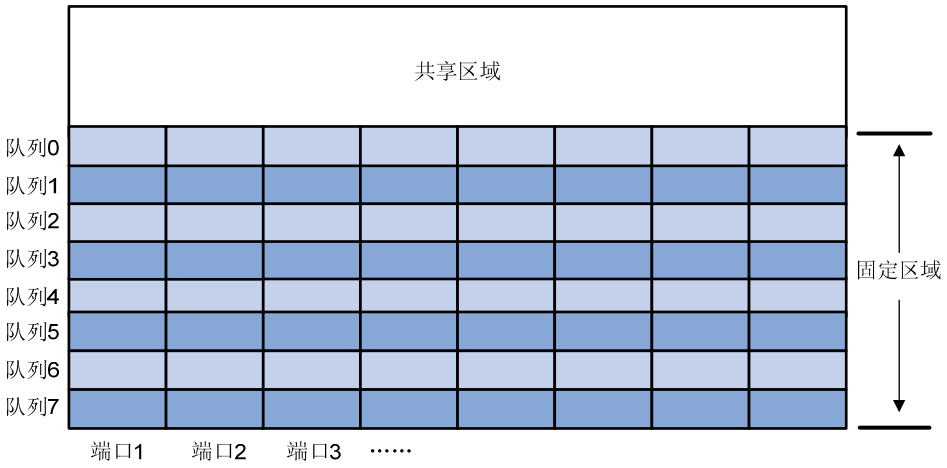
为了灵活应对网络中可能出现的突发流量，CE3000-32F-EI 交换机的 **cell** 和 **packet** 资源采用固定区域和共享区域的划分方式，资源耗尽的端口可以临时使用共享区域的资源来完成报文发送。用户可以手工设置 **cell** 资源和 **packet** 资源中共享区域所占的比例，其余部分将自动成为固定区域。

说明

cell 资源和 **packet** 资源均采用本节中介绍的划分方式，但二者可以具有不同的划分比例。

在CE3000-32F-EI交换机上，缓冲资源的划分方式如 图 12-1所示：

图12-1 CE3000-32F-EI 交换机缓冲资源划分示意图



如 图 12-1所示，固定区域的划分可以通过两个方向来进行：

- 基于端口划分：如图中纵向线条的划分示意，交换机自动将固定区域平均分配给每个端口，即每个端口有独享的端口资源。
- 基于队列划分：如图中横向线条的划分示意，表示每个队列所能使用当前端口独享资源的比例（以下称为队列的最小保证资源比），这个比例在所有端口上都保持一致。

12.1.3 共享区域的使用

如果端口在短时间内需要发送超长的报文或者是数量较多的报文，将会使端口独享的 **cell** 资源或 **packet** 资源消耗殆尽。

cell 资源和 **packet** 资源的共享区域可以为端口上的突发流量提供应急的缓存能力，共享区域为所有端口的所有队列共用，即：当某个端口（或某个队列）有突发流量产生时，可以临时占用共享区域的资源，在完成突发流量的发送后，再释放其所占用的共享区域资源，供其它端口（或队列）使用。

1. 队列对共享区域的使用

当端口上的某个队列出现拥塞时（无可用的独享 **cell** 资源或 **packet** 资源），可以配置该队列在一定的比例之内动态使用 **cell** 或 **packet** 资源的共享区域，该比例称为队列的最大共享资源占用比。例如，配置队列 0 在无可用的独享 **cell** 资源时，最多可以占用 **cell** 资源的共享区域中 6%的资源。

2. 端口对共享区域的使用

当端口上所有队列都出现拥塞时，端口独享的 **cell** 或 **packet** 资源已全部耗尽，此时可以配置该端口在一定比例内动态使用 **cell** 或 **packet** 资源的共享区域，该比例称为端口的最大共享资源占用比。例如，配置端口 1 最多可以占用 **packet** 资源的共享区域中 30%的资源。

说明

端口的最大共享资源占用比相当于对此端口下所有队列占用共享资源之和的限制，即每个队列可以有单独的最大共享资源占用比，但同一时刻 8 个队列占用共享资源的比例之和不能超过端口的最大共享资源占用比。

12.2 数据缓冲区配置

12.2.1 数据缓冲区的配置方式

用户可以使用以下两种方式配置 CE3000-32F-EI 交换机的数据缓冲区：

- 由交换机自动配置（Burst 功能）
- 由用户手工配置

说明

以上两种数据缓冲区的配置方式不能同时使用，如果已经使用某一种方式进行了配置，则必须先取消该方式的配置之后，才能使用另外一种方式进行配置。

12.2.2 通过 Burst 功能配置数据缓冲区

配置了 Burst 功能后，交换机将自动分配 **cell** 资源和 **packet** 资源的共享区域比例、队列的最小保证资源比、队列和端口的最大共享资源占用比。

在下列情况下，Burst 功能可以提供更好的报文缓存功能和流量转发性能：

- 广播或者组播报文流量密集，瞬间突发大流量的网络环境中；
- 报文从高速链路进入交换机，由低速链路转发出去；或者报文从相同速率的多个端口同时进入交换机，由一个相同速率的端口转发出去。

表12-1 通过 Burst 功能配置端口缓冲区

操作	命令	说明
进入系统视图	**system-view**	-
使能 Burst 功能	**burst-mode enable**	必选 缺省情况下，Burst 功能处于关闭状态

12.2.3 手工配置数据缓冲区

说明

数据缓冲区的配置比较复杂，而且对设备的转发功能有重要的影响，建议用户不要轻易修改数据缓冲区的参数。在需要较大的缓存空间时，建议使用 Burst 功能来自动分配缓冲区。

1. 手工配置数据缓冲区配置任务简介

表12-2 手工配置数据缓冲区配置任务简介

配置任务	说明	详细配置
配置缓冲资源中共享区域的比例	请根据需要进行相应的配置	12.2.3 2.
配置队列的最小保证资源比		12.2.3 3.

配置任务	说明	详细配置
配置队列的最大共享资源占用比		12.2.3 4.
配置端口的最大共享资源占用比		12.2.3 5.
应用数据缓冲区配置	必选	12.2.3 6.

2. 配置缓冲资源中共享区域的比例

表12-3 配置缓冲资源中共享区域的比例

操作	命令	说明
进入系统视图	**system-view**	-
配置 **cell** 资源中共享区域所占比例	**buffer egress** [**slot** *slot-number*] **cell total-shared ratio** *ratio*	至少配置其中一项 缺省情况下，**cell** 资源中共享区域所占比例为 73%，**packet** 资源中共享区域所占比例为 74%
配置**packet**资源中共享区域所占比例	**buffer egress** [**slot** *slot-number*] **packet total-shared ratio** *ratio*	

3. 配置队列的最小保证资源比

表12-4 配置队列的最小保证资源比

操作	命令	说明
进入系统视图	**system-view**	-
配置队列在 **cell** 缓冲区中的最小保证资源比	**buffer egress** [**slot** *slot-number*] **cell queue** *queue-id* **guaranteed ratio** *ratio*	至少配置其中一项 缺省情况下，队列在**cell**资源和**packet**资源的最小保证资源比均为 12%
配置队列在**packet**缓冲区中的最小保证资源比	**buffer egress** [**slot** *slot-number*] **packet queue** *queue-id* **guaranteed ratio** *ratio*	

说明

- 由于端口的独享资源是由 8 个队列共同使用，因此当用户修改了某个队列的最小保证资源比之后，其它队列的最小保证资源比将随之自动变化，自动变化的原则为：除用户手工配置的最小保证资源比之外，剩余比例将平均分配给未进行手工配置的队列。例如，如果配置一个队列的最小保证资源比为 30%，则剩余 7 个队列的最小保证资源比将自动变化为 10%。
- 队列的最小保证资源比对全局生效，即配置后每个端口上的该队列均能以相同的比例占用当前端口的独享资源。

4. 配置队列的最大共享资源占用比

表12-5 配置队列的最大共享资源占用比

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置队列在 **cell** 资源中的最大共享资源占用比	**buffer egress** [**slot** *slot-number*] **cell queue** *queue-id* **shared ratio** *ratio*	至少配置其中一项 缺省情况下，队列在 **cell** 资源和 **packet** 资源中的最大共享资源占用比均为 33%
配置队列在 **packet** 资源中的最大共享资源占用比	**buffer egress** [**slot** *slot-number*] **packet queue** *queue-id* **shared ratio** *ratio*	

说明

队列的最大共享资源占用比对全局生效，即配置后每个端口上的该队列均能以相同的最大共享资源占用比来动态使用共享区域的资源。

5. 配置端口的最大共享资源占用比

表12-6 配置端口的最大共享资源占用比

操作	命令	说明
进入系统视图	**system-view**	-
配置端口在 **cell** 资源中的最大共享资源占用比	**buffer egress** [**slot** *slot-number*] **cell shared ratio** *ratio*	至少配置其中一项 缺省情况下，每个端口在 **cell** 资源和 **packet** 资源中的最大共享资源占用比均为 33%
配置端口在 **packet** 资源中的最大共享资源占用比	**buffer egress** [**slot** *slot-number*] **packet shared ratio** *ratio*	

说明

端口的最大共享资源占用比对所有端口生效，即配置后每个端口均能够以相同的最大共享资源占用比来动态使用共享区域资源。

6. 应用数据缓冲区的配置

用户在完成对数据缓冲区的手工配置后，必须使用下面的步骤将所作的修改进行应用，之前的配置才能生效。

表12-7 应用数据缓冲区的配置

操作	命令	说明
进入系统视图	**system-view**	-
应用数据缓冲区的配置	**buffer apply**	必选

13 附录 A 缺省优先级映射表

说明

dot1p-exp、**dscp-dscp** 和 **exp-dot1p** 映射表的缺省映射关系为：映射输出值等于输入值。

表13-1 dot1p-lp、dot1p-dp 缺省映射关系

映射输入索引	dot1p-lp 映射	dot1p-dp 映射
802.1p 优先级(dot1p)	本地优先级(lp)	丢弃优先级(dp)
0	2	0
1	0	0
2	1	0
3	3	0
4	4	0
5	5	0
6	6	0
7	7	0

表13-2 dscp-dp、dscp-dot1p 缺省映射关系

映射输入索引	dscp-dp 映射	dscp-dot1p 映射
dscp	丢弃优先级(dp)	802.1p 优先级(dot1p)
0～7	0	0
8～15	0	1
16～23	0	2
24～31	0	3
32～39	0	4
40～47	0	5
48～55	0	6
56～63	0	7

表13-3 exp-dp 缺省映射关系

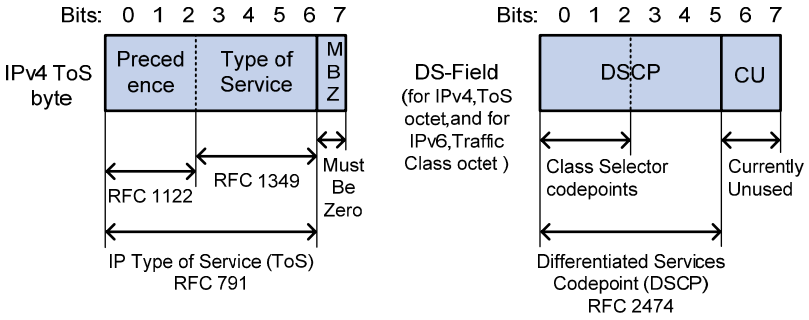
映射输入索引	exp-dp 映射
exp 优先级	丢弃优先级(dp)
0	0

映射输入索引	exp-dp 映射
1	0
2	0
3	0
4	0
5	0
6	0
7	0

14 附录 B 各种优先级介绍

14.1 IP 优先级和 DSCP 优先级

图14-1 ToS 和 DS 域



如 图 14-1所示，IP报文头的ToS字段有 8 个bit，其中前 3 个bit表示的就是IP优先级，取值范围为 0～7。RFC 2474 中，重新定义了IP报文头部的ToS域，称之为DS（Differentiated Services，差分服务）域，其中DSCP优先级用该域的前 6 位（0～5 位）表示，取值范围为 0～63，后 2 位（6、7 位）是保留位。

表14-1 IP 优先级说明

IP 优先级（十进制）	IP 优先级（二进制）	关键字
0	000	routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

表14-2 DSCP 优先级说明

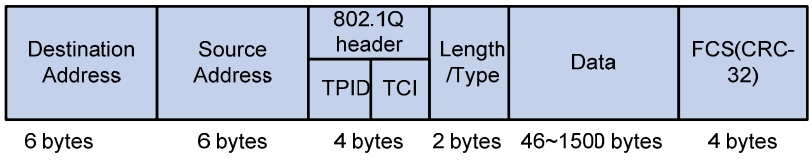
DSCP 优先级（十进制）	DSCP 优先级（二进制）	关键字
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23

DSCP 优先级（十进制）	DSCP 优先级（二进制）	关键字
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be（default）

14.2 802.1p 优先级

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。

图14-2 带有 802.1Q 标签头的以太网帧



如 图 14-2所示，4 个字节的 802.1Q标签头包含了 2 个字节的TPID（Tag Protocol Identifier，标签协议标识，取值为 0x8100）和 2 个字节的TCI（Tag Control Information，标签控制信息），图 14-3 显示了 802.1Q标签头的详细内容，Priority字段就是 802.1p优先级。之所以称此优先级为 802.1p 优先级，是因为有关这些优先级的应用是在 802.1p规范中被详细定义。

图14-3 802.1Q 标签头

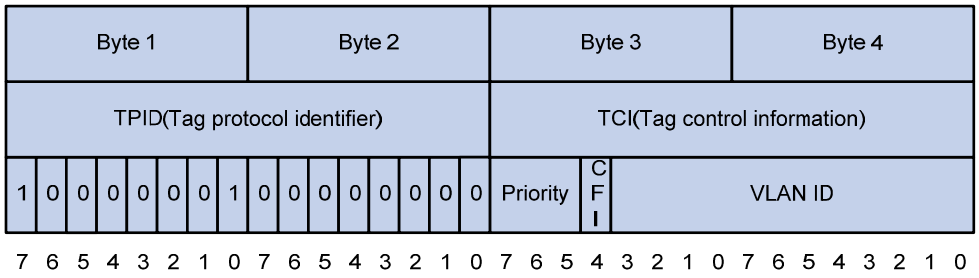


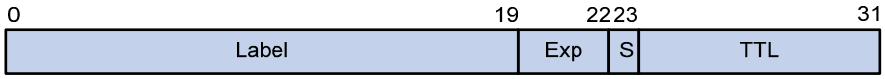
表14-3 802.1p 优先级说明

802.1p 优先级（十进制）	802.1p 优先级（二进制）	关键字
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

14.3 EXP 优先级

EXP 优先级位于 MPLS 标签内，用于标记 MPLS QoS。

图14-4 MPLS 标签的封装结构



在 图 14-4中，Exp字段就是EXP优先级。它由 3 个bit组成，取值范围为 0～7。