# 目 录

# 1 QoS 概述

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、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，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。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。

## 1.1 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 IntServ）
- Differentiated service（区分服务模型，简称 DiffServ）

### 1.1.1 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。

### 1.1.2 IntServ 服务模型

IntServ 是一个综合服务模型，它可以满足多种 QoS 需求。该模型使用 RSVP 协议，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，IntServ 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。IntServ 模型可扩展性很差，难以在 Internet 核心网络实施。

### 1.1.3 DiffServ 服务模型

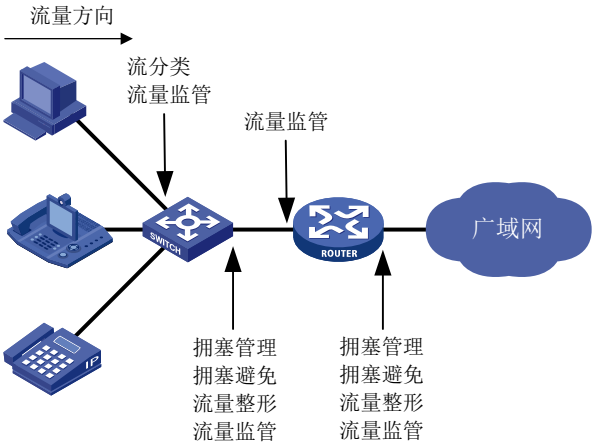
DiffServ 是一个多服务模型，它可以满足不同的 QoS 需求。与 IntServ 不同，它不需要通知网络为每个业务预留资源。区分服务实现简单，扩展性较好。

本文提到的技术都是基于 DiffServ 服务模型。

## 1.2 QoS技术在网络中的位置

QoS 技术包括流分类、流量监管、流量整形、限速、拥塞管理、拥塞避免等。下面对常用的技术进行简单地介绍。

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，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：当拥塞发生时制定一个资源的调度策略，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。

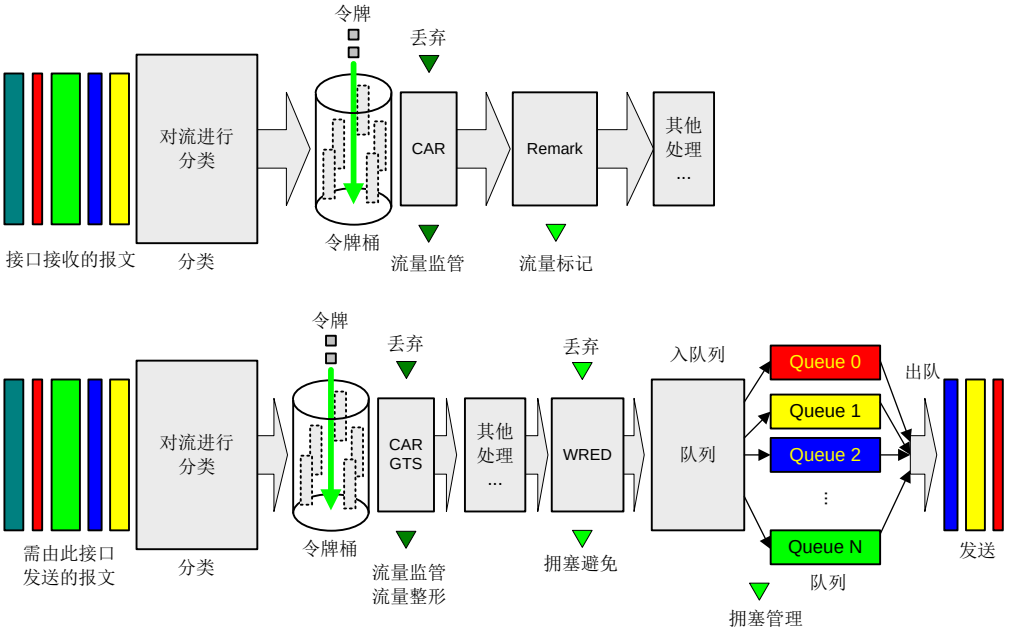
## 1.3 QoS技术在设备中的处理顺序

图 1-2 简要描述了各种 QoS 技术在网络设备中的处理顺序。

(1) 首先通过流分类对各种业务进行识别和区分，它是后续各种动作的基础；

(2) 通过各种动作对特定的业务进行处理。这些动作需要和流分类关联起来才有意义。具体采取何种动作，与所处的阶段以及网络当前的负载状况有关。例如，当报文进入网络时进行流量监管；流出节点之前进行流量整形；拥塞时对队列进行拥塞管理；拥塞加剧时采取拥塞避免措施等。

图1-2 各 QoS 技术在同一网络设备中的处理顺序




## 1.4 QoS配置方式

QoS 的配置方式分为 MQC 方式（模块化 QoS 配置，Modular QoS Configuration）和非 MQC 方式。

MQC 方式通过 QoS 策略定义不同类别的流量要采取的动作，并将 QoS 策略应用到不同的目标位置（例如接口）来实现对业务流量的控制。

非 MQC 方式则通过直接在目标位置上配置 QoS 参数来实现对业务流量的控制。例如，在接口上配置限速功能来达到限制接口流量的目的。

# 2 QoS 策略

## 2.1 QoS策略简介

QoS 策略由如下部分组成：

- 类，定义了对报文进行识别的规则。
- 流行为，定义了一组针对类识别后的报文所做的 QoS 动作。

通过将类和流行为关联起来，QoS 策略可对符合分类规则的报文执行流行为中定义的动作。

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策略配置任务简介

QoS 策略配置任务如下：

(1) 定义类

(2) 定义流行为

(3) 定义策略

(4) 应用策略

- 基于接口应用 QoS 策略
- 基于 VSI 应用 QoS 策略
- 基于 VLAN 应用 QoS 策略
- 基于全局应用 QoS 策略
- 基于上线用户应用 QoS 策略

## 2.3 定义类

(1) 进入系统视图。

**system-view**

(2) 创建类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

(3) （可选）配置类的描述信息。

**description** *text*

缺省情况下，未配置类的描述信息。

(4) 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

## 2.4 定义流行为

(1) 进入系统视图。

**system-view**

(2) 创建流行为，并进入流行为视图。

**traffic behavior** *behavior-name*

(3) 配置流行为的动作。

缺省情况下，未配置流行为的动作。

流行为动作就是对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、重标记、流量统计等，具体情况请参见本文相关章节。

## 2.5 定义策略

(1) 进入系统视图。

**system-view**

(2) 创建 QoS 策略，并进入策略视图。

**qos policy** *policy-name*

(3) 为类指定流行为。

**classifier** *classifier-name* **behavior** *behavior-name* [ **mode dcbx** | **insert-before** *before-classifier-name* ]

缺省情况下，未指定类对应的流行为。

| 参数 | 说明 |
| --- | --- |
| **dcbx** | 表示该策略为DCBX（Data Center Bridging 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” |

## 2.6 应用策略

### 2.6.1 设备支持的策略应用位置

QoS 策略支持应用在如下位置：

- 基于以太网服务实例应用 QoS 策略，QoS 策略对以太网服务实例接收或发送的流量生效。
- 基于接口应用 QoS 策略，QoS 策略对通过接口接收或发送的流量生效。
- 基于 VSI 应用 QoS 策略，QoS 策略仅对 VSI 上入方向流量生效。
- 基于 VLAN 应用 QoS 策略，QoS 策略对通过同一个 VLAN 内所有接口接收或发送的流量生效。
- 基于全局应用 QoS 策略，QoS 策略对所有流量生效。
- 基于上线用户应用 QoS 策略，QoS 策略对通过上线用户接收或发送的流量生效。

### 2.6.2 策略应用限制和指导

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。当流分类规则中使用 ACL 匹配报文时，允许删除或修改该 ACL（包括向该 ACL 中添加、删除和修改匹配规则）。

### 2.6.3 基于以太网服务实例应用 QoS 策略

#### 1. 配置限制和指导

关于以太网服务实例的相关配置命令，请参见“VXLAN 命令参考”。

#### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。请选择其中一项进行配置。

- 进入二层以太网接口视图。

  **interface** *interface-type interface-number*

- 进入二层聚合接口视图。

  **interface bridge-aggregation** *interface-number*

(3) 创建以太网服务实例，并进入以太网服务实例视图。

**service-instance** *instance-id*

(4) 在以太网服务实例上应用已创建的 QoS 策略。

**qos apply policy** *policy-name* **inbound**

缺省情况下，未在以太网服务实例上应用 QoS 策略。

### 2.6.4 基于接口应用 QoS 策略

#### 1. 配置限制和指导

基于接口应用 QoS 策略时需要注意的是：

- 一个 QoS 策略可以应用于多个接口，但在接口的每个方向（出和入两个方向）只能应用一个策略。
- QoS 策略应用在出方向时，对设备发出的协议报文不起作用，以确保这些报文在策略误配置时仍然能够正常发出，维持设备的正常运行。常见的本地协议报文如下：链路维护报文、RIP、LDP、SSH 等。

本节中的“接口”指的是二层以太网接口和三层以太网接口。三层以太网接口是指在以太网接口视图下通过 **port link-mode route** 命令切换为三层模式的以太网接口，有关以太网接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“以太网接口配置”。

#### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 在接口上应用已创建的 QoS 策略。

**qos apply policy** *policy-name* { **inbound** | **outbound** }

缺省情况下，未在接口上应用 QoS 策略。

### 2.6.5 基于 VSI 应用 QoS 策略

#### 1. 配置限制和指导

关于 VSI 的相关配置命令，请参见“VXLAN 命令参考”。

#### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入 VSI 视图。

**vsi** *vsi-name* [ **hub-spoke** ]

(3) 在 VSI 上应用已创建的 QoS 策略。

**qos apply policy** *policy-name* **inbound**

缺省情况下，未在 VSI 上应用 QoS 策略。

### 2.6.6 基于 VLAN 应用 QoS 策略

#### 1. 功能简介

基于 VLAN 应用 QoS 策略可以对属于某个 VLAN 内的所有接口上的流量进行管理。

#### 2. 配置限制和指导

基于 VLAN 应用的 QoS 策略时需要注意的是：

- 不能应用在动态 VLAN 上，例如 GVRP 协议创建的 VLAN。
- 基于 VLAN 应用 QoS 策略时，该 QoS 策略会被所有成员设备上的 VLAN 应用，如果某个成员设备 QACL 资源不足，将导致 QoS 策略应用失败。此时需要先执行 **undo qos vlan-policy vlan** 命令删除基于 VLAN 应用的 QoS 策略，待预留足够资源后，再将 QoS 策略应用到该 VLAN 上。

#### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 在指定 VLAN 上应用已创建的 QoS 策略。

**qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

缺省情况下，未在指定 VLAN 上应用 QoS 策略。

### 2.6.7 基于全局应用 QoS 策略

#### 1. 功能简介

基于全局应用 QoS 策略后可以对设备所有接口上的流量进行管理。

#### 2. 配置限制和指导

基于全局应用 QoS 策略时，该 QoS 策略会被所有成员设备应用，如果某个成员设备 QACL 资源不足，将导致 QoS 策略应用失败。此时需要先执行 **undo qos apply policy global** 命令删除基于全局应用的 QoS 策略，待预留足够资源后，再将 QoS 策略应用到全局。

#### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 全局应用已创建的 QoS 策略。

**qos apply policy** *policy-name* **global { inbound| outbound }**

缺省情况下，未在全局应用 QoS 策略。

### 2.6.8 基于上线用户应用 QoS 策略

#### 1. 功能简介

用户通过身份认证后，认证服务器会将与用户帐户绑定的 User Profile 名称下发给设备，设备可以通过 User Profile 视图下配置 QoS 策略来对上线用户的流量进行管理。User Profile 视图下的 QoS 策略只有在用户成功上线后才生效。

#### 2. 配置限制和指导

一个策略可以应用于多个上线用户。上线用户的每个方向（发送和接收两个方向）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。

#### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入 User Profile 视图。

**user-profile** *profile-name*

(3) 在 User Profile 下应用 QoS 策略。

**qos apply policy** *policy-name* **{ inbound | outbound }**

缺省情况下，未在 User Profile 下应用 QoS 策略。

| 参数 | 说明 |
| --- | --- |
| **inbound** | 表示对设备接收上线用户的流量（即上线用户发送的流量）应用策略 |
| **outbound** | 表示对设备发送给上线用户的流量（即上线用户接收的流量）应用策略 |

## 2.7 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。

在用户视图下执行 **reset** 命令可以清除 QoS 策略的统计信息。

表2-1 QoS 策略显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示QoS策略的配置信息 | **display qos policy user-defined** [ *policy-name* [ **classifier** *classifier-name* ] ] [ **slot** *slot-number* ] |
| 显示L2VPN AC承载的以太网服务实例上QoS策略的配置信息和运行情况 | **display qos policy l2vpn-ac** [ **interface** *interface-type interface-number* [ **service-instance** *instance-id* ] [ **slot** *slot-number* ] ] [ **inbound** ] |
| 显示VSI上QoS策略的配置信息和运行情况 | **display qos policy vsi** [ **name** *vsi-name* ] [ **inbound** ] [ **slot** *slot-number* ] |
| 显示基于全局应用QoS策略的信息 | **display qos policy global** [ **slot** *slot-number* ] [ **inbound** \| **outbound** ] |
| 显示接口上QoS策略的配置信息和运行情况 | **display qos policy interface** [ *interface-type interface-number* ] [ **inbound** \| **outbound** ] |
| 显示用户上线后User Profile下应用的QoS策略的信息和运行情况 | **display qos policy user-profile** [ **name** *profile-name* ] [ **user-id** *user-id* ] [ **slot** *slot-number* ] [ **inbound** \| **outbound** ] |
| 显示基于VLAN应用QoS策略的信息 | **display qos vlan-policy** { **name** *policy-name* \| **vlan** [ *vlan-id* ] } [ **slot** *slot-number* ] [ **inbound** \| **outbound** ] |
| 显示QoS和ACL资源的使用情况 | **display qos-acl resource** [ **slot** *slot-number* ] |
| 显示流行为的配置信息 | **display traffic behavior user-defined** [ *behavior-name* ] [ **slot** *slot-number* ] |
| 显示类的配置信息 | **display traffic classifier user-defined** [ *classifier-name* ] [ **slot** *slot-number* ] |
| 清除全局应用QoS策略的统计信息 | **reset qos policy global** [ **inbound** \| **outbound** ] |
| 清除VLAN应用QoS策略的统计信息 | **reset qos vlan-policy** [ **vlan** *vlan-id* ] [ **inbound** \| **outbound** ] |

# 3 优先级映射

## 3.1 优先级映射简介

优先级映射可以将报文携带的优先级字段映射成指定优先级字段值，设备根据映射后的优先级字段，为报文提供有差别的 QoS 服务，从而为全面有效的控制报文的转发调度等级提供依据。

### 3.1.1 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“12.3 附录 C 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。
- 用户优先级（UP）：设备对于进入的流量，会自动获取报文的优先级作为后续转发调度的参数，这种报文优先级称为用户优先级。对于不同类型的报文，用户优先级所代表的优先级字段不同。对于二层报文，用户优先级取自 802.1p 优先级；对于三层报文，用户优先级取自 IP 优先级；对于 MPLS 报文，用户优先级取自 EXP。

设备仅支持以本地优先级（LP）和丢弃优先级（DP）作为设备调度优先级。

### 3.1.2 优先级映射表

设备提供了多张优先级映射表，分别对应不同的优先级映射关系。

通常情况下，设备可以通过查找缺省优先级映射表（12.2 附录 B 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。

### 3.1.3 优先级映射配置方式

优先级映射配置方式包括：优先级信任模式方式、端口优先级方式。

#### 1. 优先级信任模式方式

配置端口的优先级信任模式后，设备将信任报文自身携带的优先级。通过优先级映射表，使用所信任的报文携带优先级进行优先级映射，根据映射关系完成对报文优先级的修改，以及实现报文在设备内部的调度。

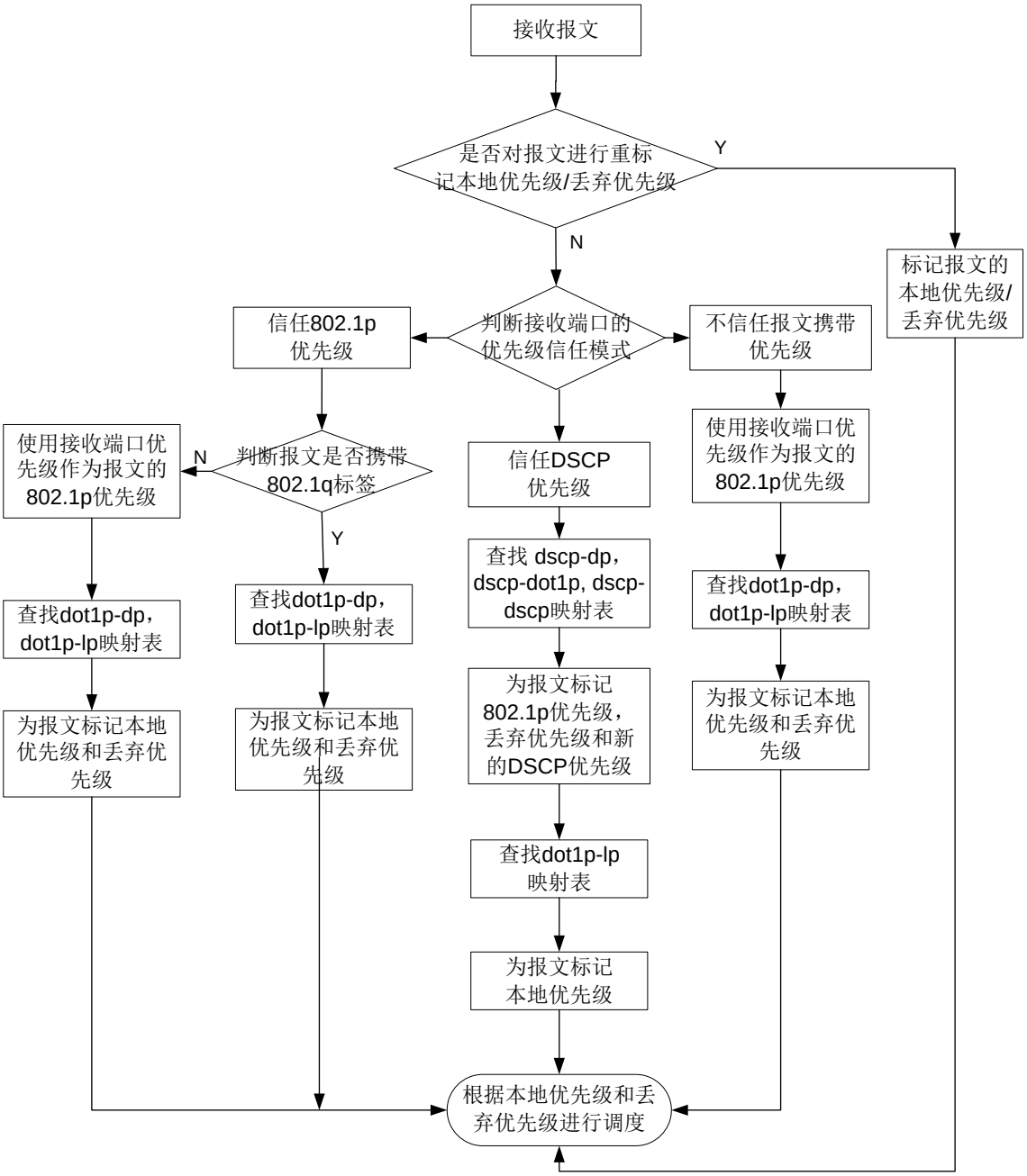
### 2. 端口优先级方式

未配置端口的优先级信任模式时，设备会将端口优先级作为报文自身的优先级。通过优先级映射表，对报文进行映射。用户可以配置端口优先级，通过优先级映射，使不同端口收到的报文进入对应的队列，以此实现对不同端口收到报文的差异化调度。

## 3.1.4 优先级映射过程

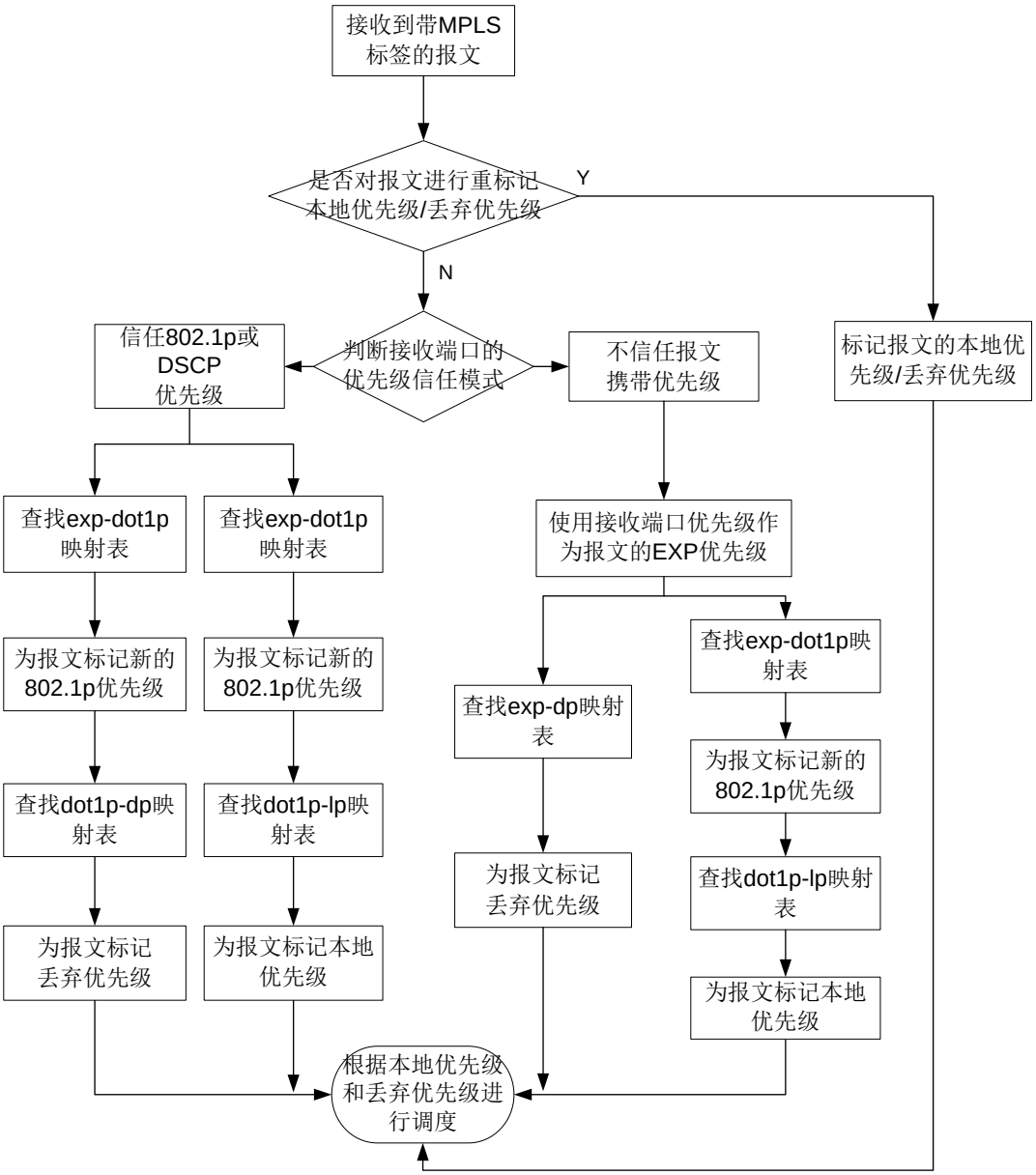
对于接收到的以太网报文，根据优先级信任模式和报文的 802.1Q 标签状态，设备将采用不同的方式为其标记调度优先级。如图 3-1 所示：

图3-1 以太网报文优先级映射过程



对于接收到的 MPLS 报文，根据优先级信任模式和报文的 EXP 优先级状态，设备将采用不同的方式为其标记调度优先级。如图 3-2 所示：

图3-2 MPLS 报文优先级映射过程




说明

关于重标记优先级功能的介绍，请参见重标记。

## 3.2 优先级映射配置任务简介

优先级映射配置任务如下：

(1) （可选）配置优先级映射表

(2) 配置优先级映射方式。

- 配置优先级信任模式
- 配置端口优先级

## 3.3 配置优先级映射表

(1) 进入系统视图。

**system-view**

(2) 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** }

(3) 配置指定优先级映射表的映射关系。

**import** *import-value-list* **export** *export-value*

缺省情况下，优先级映射表的映射关系请参见“12.2 附录 B 缺省优先级映射表”。

多次执行本命令，最后一次执行的命令生效。

## 3.4 配置优先级信任模式

### 1. 功能简介

配置优先级信任模式后，设备将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。

在配置接口上的优先级模式时，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。

### 2. 配置限制和指导

本节中的“接口”指的是二层以太网接口和三层以太网接口。三层以太网接口是指在以太网接口视图下通过 **port link-mode route** 命令切换为三层模式的以太网接口，有关以太网接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“以太网接口配置”。

### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 配置优先级信任模式。

**qos trust** { **dot1p** | **dscp** }

设备不信任报文携带的优先级，会使用端口优先级作为报文的 802.1p 优先级进行优先级映射。

## 3.5 配置端口优先级

### 1. 功能简介

按照接收端口的端口优先级，设备通过一一映射为报文分配相应的优先级。

### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 配置端口优先级。

**qos priority** *priority-value*

缺省情况下，端口优先级为 0。

## 3.6 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3-1 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** ] |
| 显示端口优先级信任模式信息 | **display qos trust interface** [ *interface-type interface-number* ] |

## 3.7 优先级映射典型配置举例

### 3.7.1 优先级信任模式和端口优先级配置举例

#### 1. 组网需求

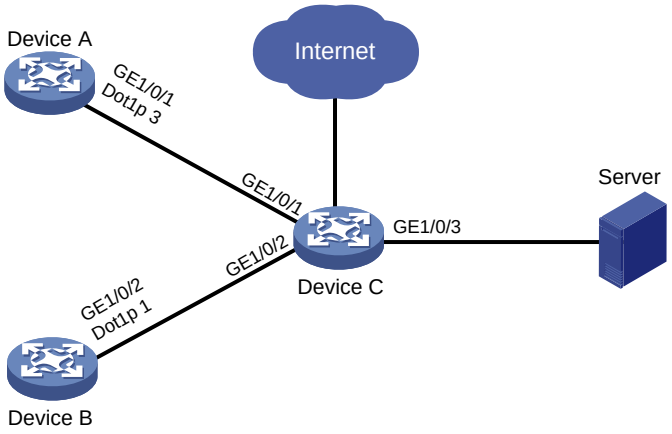
Device A 和 Device B 通过 Device C 实现互连。网络环境描述如下：

- Device A 通过端口 GigabitEthernet1/0/1 接入 Device C，向 Device C 发送 dot1p 值为 3 的报文；
- Device B 通过端口 GigabitEthernet1/0/2 接入 Device C，向 Device C 发送 dot1p 值为 1 的报文。

要求通过配置实现如下需求：如果 Device C 在接口 GigabitEthernet1/0/3 的出方向发生拥塞，则优先让 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组网图




### 3. 配置步骤

(1) 方法一

# 在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上分别配置优先级信任模式为 **dot1p**。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] qos trust dot1p
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] qos trust dot1p
[DeviceC-GigabitEthernet1/0/2] quit
```

(2) 方法二

# 在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 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。（同时保证在接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上没有配置信任模式。）

```
<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
```

## 3.7.2 优先级映射表和重标记配置举例

### 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。

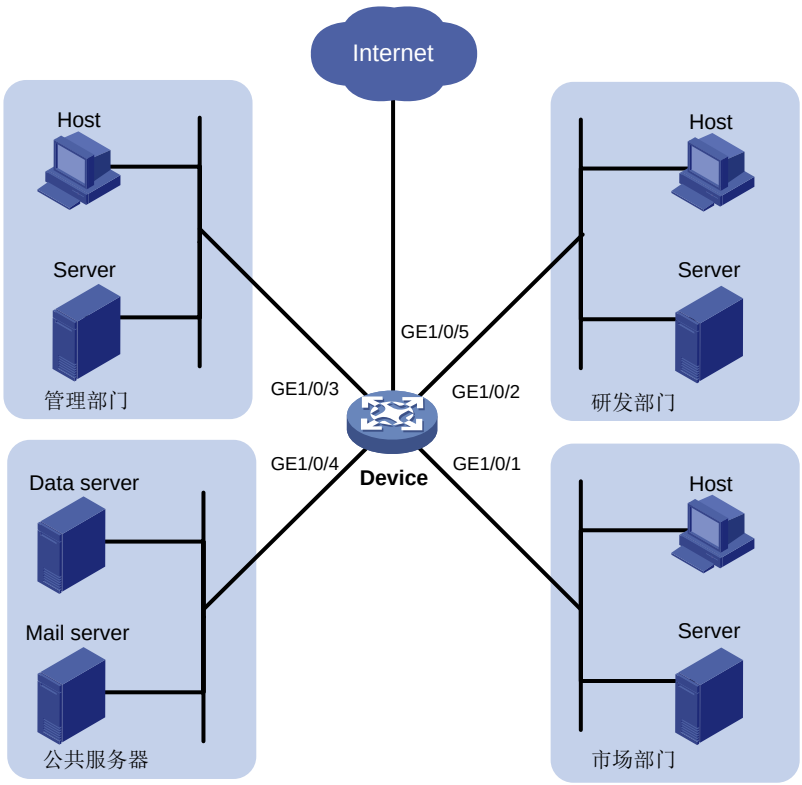
- 通过优先级映射将研发部门发出的报文放入出队列 6 中，优先进行处理；
- 通过优先级映射将管理部门发出的报文放入出队列 4 中，次优先进行处理；
- 通过优先级映射将市场部门发出的报文放入出队列 2 中，最后进行处理。

访问 Internet 的时候，管理部门 > 市场部门 > 研发部门。

- 重标记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。保证访问服务器的优先级为研发部门（6）>管理部门（4）>市场部门（2）。

```
[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 advanced 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接口 GigabitEthernet1/0/3 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接口 GigabitEthernet1/0/1 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接口 GigabitEthernet1/0/2 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、流量整形和限速

## 4.1 流量监管、流量整形和限速简介

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。流量监管、流量整形和限速可以实现流量的速率限制功能，而要实现此功能就必须对通过设备的流量进行度量。一般采用令牌桶（Token Bucket）对流量进行度量。

### 4.1.1 流量评估与令牌桶

#### 1. 令牌桶

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，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，此时要从桶中取走满足报文的转发的令牌；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，可以使用两个令牌桶（分别称为 C 桶和 E 桶）对流量进行评估。主要有如下三种算法。

(1) 单速率单桶双色算法

- 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。

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，报文被标记为 red，即红色报文。

(2) 单速率双桶三色算法

- 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；
- EBS：表示 E 桶的容量的增量，即 E 桶瞬间能够通过的超出突发流量，取值不为 0。E 桶的容量等于 CBS 与 EBS 的和。

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。

(3) 双速率双桶三色算法

- 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。

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：

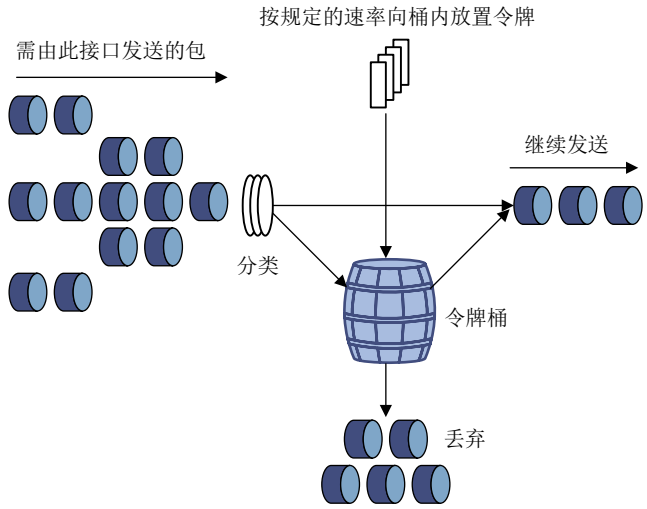
- 如果 C 桶有足够的令牌，报文被标记为 green，即绿色报文；
- 如果 C 桶令牌不足，但 E 桶有足够的令牌，报文被标记为 yellow，即黄色报文；
- 如果 C 桶和 E 桶都没有足够的令牌，报文被标记为 red，即红色报文。

### 4.1.2 流量监管

流量监管分为入和出两个方向，为了方便描述，下文以出方向为例。

流量监管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，将其优先级进行重标记后再进行转发。

### 4.1.3 流量整形

说明

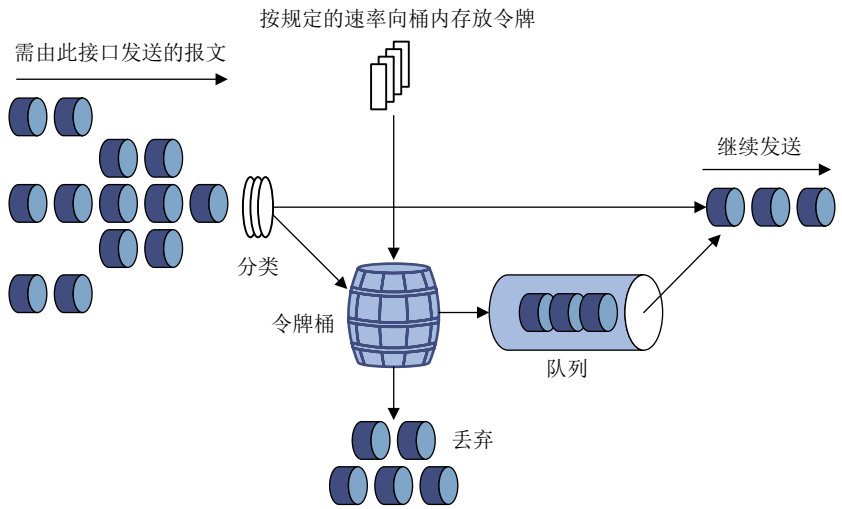
流量整形目前只支持出方向。

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流量监管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：

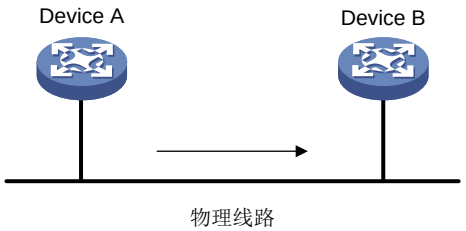
- 流量整形对流量监管中需要丢弃的报文进行缓存——通常是将它们放入缓冲区或队列内，如图 4-2 所示。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。
- 流量整形可能会增加延迟，而流量监管几乎不引入额外的延迟。

图4-2 流量整形示意图




例如，在图 4-3 所示的应用中，设备 Device A 向 Device B 发送报文。Device B 要对 Device A 发送来的报文进行流量监管，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 Device 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 Device 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 Device B 的报文将都符合 Device B 的流量规定。

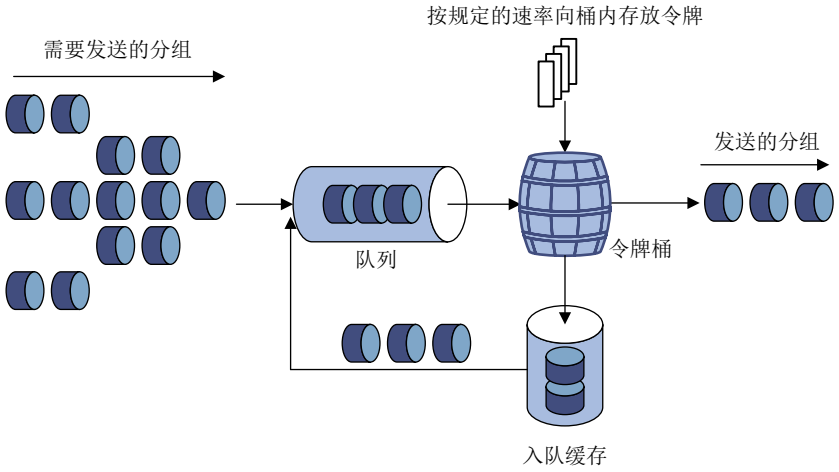
### 4.1.4 限速

限速分为入和出两个方向，为了方便描述，下文以出方向为例。

利用限速可以在一个接口上限制发送报文（除紧急报文）的总速率。

限速也是采用令牌桶进行流量控制。假如在设备的某个接口上配置了限速，所有经由该接口发送的报文首先要经过限速的令牌桶进行处理。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，就可以对该接口的报文流量进行控制。

图4-4 限速处理过程示意图




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，限速能够限制所有报文。当用户只要求对所有报文限速时，使用限速比较简单。

## 4.2 流量监管、流量整形和限速配置限制和指导

相邻的数据帧之间存有一定的间隙，即帧间隙。帧间隙主要有如下作用：

- 便于设备区分不同的数据帧。
- 设备收到数据帧后有一定的时间处理当前数据帧并预接收下一数据帧。

流量监管、流量整形和限速中配置的承诺信息速率为剔除帧间隙后的单位时间的流量大小，所以流量监管、流量整形和限速实际生效的数值要略大于配置的承诺信息速率的数值。

## 4.3 配置流量监管

#### 1. 配置限制和指导

设备支持基于接口、VLAN、全局和上线用户应用 QoS 策略配置流量监管。

### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 定义类。

a. 创建类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

b. 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

**quit**

(3) 定义流行为。

a. 创建一个流行为并进入流行为视图。

**traffic behavior** *behavior-name*

b. 配置流量监管动作。

**car cir** *committed-information-rate* [ **cbs** *committed-burst-size* [ **ebs** *excess-burst-size* ] ] [ **green** *action* | **red** *action* | **yellow** *action* ] *

**car cir** *committed-information-rate* [ **cbs** *committed-burst-size* ] **pir** *peak-information-rate* [ **ebs** *excess-burst-size* ] [ **green** *action* | **red** *action* | **yellow** *action* ] *

缺省情况下，未配置流量监管动作。

c. 退回系统视图。

**quit**

(4) 定义策略。

a. 创建策略并进入策略视图。

**qos policy** *policy-name*

b. 在策略中为类指定采用的流行为。

**classifier** *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

**quit**

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

## 4.4 配置流量整形

1.

### 2. 配置限制和指导

本节中的“接口”指的是二层以太网接口和三层以太网接口。三层以太网接口是指在以太网接口视图下通过 **port link-mode route** 命令切换为三层模式的以太网接口，有关以太网接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“以太网接口配置”。

### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 配置基于队列的流量整形。

**qos gts queue** *queue-id* **cir** *committed-information-rate* [ **cbs** *committed-burst-size* ]

**undo qos gts queue** *queue-id*

缺省情况下，接口上未配置流量整形。

## 4.5 配置限速

1.

### 2. 配置限制和指导

本节中的“接口”指的是二层以太网接口和三层以太网接口。三层以太网接口是指在以太网接口视图下通过 port link-mode route 命令切换为三层模式的以太网接口，有关以太网接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“以太网接口配置”。

### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 配置接口限速。

**qos lr** { **inbound** | **outbound** } **cir** *committed-information-rate* [ **cbs** *committed-burst-size* ]

缺省情况下，接口上未配置接口限速。

## 4.6 流量监管、流量整形和限速显示和维护

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、流量整形和接口限速的运行情况，通过查看显示信息验证配置的效果。

表4-1 流量监管、流量整形和限速显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示接口的流量整形配置情况和统计信息 | **display qos gts interface** [ *interface-type interface-number* ] |
| 显示限速配置情况和统计信息 | **display qos lr interface** [ *interface-type interface-number* ] |
| 显示QoS和ACL资源的使用情况（本命令的详细介绍，请参见“ACL和QoS命令参考”中的“ACL”） | **display qos-acl resource** [ **slot** *slot-number* ] |
| 显示流量监管的相关配置信息 | **display traffic behavior user-defined** [ *behavior-name* ] |

# 4.7 流量监管、流量整形和限速典型配置举例

## 4.7.1 流量监管与流量整形典型配置举例

### 1. 配置需求

- 设备 Device A 通过接口 GigabitEthernet1/0/3 和设备 Device B 的接口 GigabitEthernet1/0/1 互连；
- Server、Host A、Host B 可经由 Device A 和 Device B 访问 Internet；
- Server、Host A 与 Device A 的 GigabitEthernet1/0/1 接口在同一网段；
- Host B 与 Device A 的 GigabitEthernet1/0/2 接口在同一网段。

要求在设备 Device A 上对接口 GigabitEthernet1/0/1 接收到的源自 Server 和 Host A 的报文流分别实施流量控制如下：

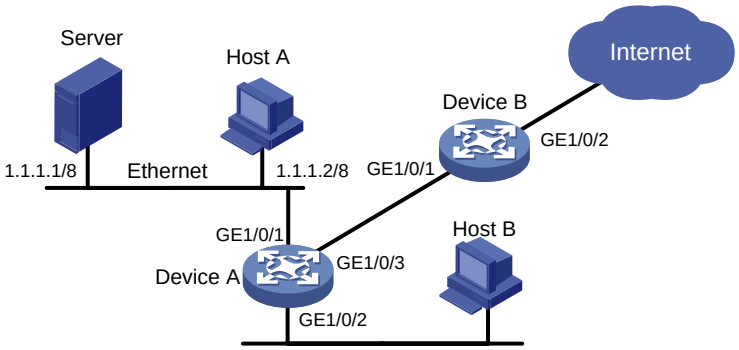
- 来自 Server 的报文流量约束为 10240kbps，流量小于 10240kbps 时可以正常发送，流量超过 10240kbps 时则将违规报文的优先级设置为 0 后进行发送；
- 来自 Host A 的报文流量约束为 2560kbps，流量小于 2560kbps 时可以正常发送，流量超过 2560kbps 时则丢弃违规报文；

对设备 Device B 的 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 接口收发报文有如下要求：

- Device B 的 GigabitEthernet1/0/1 接口接收报文的总流量限制为 20480kbps，如果超过流量限制则将违规报文丢弃；
- 经由 Device B 的 GigabitEthernet1/0/2 接口进入 Internet 的报文流量限制为 10240kbps，如果超过流量限制则将违规报文丢弃。

## 2. 组网图

图4-5 流量监管、流量整形配置组网图




## 3. 配置步骤

(1) 配置设备 Device A

# 配置 ACL 规则列表，分别匹配来源于 Server 和 Host A 的报文流。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[DeviceA-acl-ipv4-basic-2001] quit
[DeviceA] acl basic 2002
[DeviceA-acl-ipv4-basic-2002] rule permit source 1.1.1.2 0
[DeviceA-acl-ipv4-basic-2002] quit
```

# 创建流分类 server，匹配 Server 发出的报文流。

```
[DeviceA] traffic classifier server
[DeviceA-classifier-server] if-match acl 2001
[DeviceA-classifier-server] quit
```

# 创建流分类 host，匹配 Host 发出的报文流。

```
[DeviceA] traffic classifier host
[DeviceA-classifier-host] if-match acl 2002
[DeviceA-classifier-host] quit
```

# 创建流行为 server，动作为流量监管，cir 为 10240kbps，对超出限制的报文（红色报文）将其 DSCP 优先级设置为 0 后发送。

```
[DeviceA] traffic behavior server
[DeviceA-behavior-server] car cir 10240 red remark-dscp-pass 0
[DeviceA-behavior-server] quit
```

# 创建流行为 host，动作为流量监管，cir 为 2560kbps，由于默认对红色报文的处理方式就是丢弃，因此无需配置。

```
[DeviceA] traffic behavior host
[DeviceA-behavior-host] car cir 2560
[DeviceA-behavior-host] quit
```

# 创建 QoS 策略，命名为 car，将流分类 server 和流行为 server 进行关联；将流分类 host 和流行为 host 进行关联。

```
[DeviceA] qos policy car
[DeviceA-qospolicy-car] classifier server behavior server
```

```
[DeviceA-qospolicy-car] classifier host behavior host
[DeviceA-qospolicy-car] quit
```

# 将 QoS 策略 car 应用到接口 GigabitEthernet1/0/1 的入方向上。

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

(2) 配置设备 Device B

# 配置高级 ACL3001，匹配 HTTP 报文。

```
<DeviceB> system-view
[DeviceB] acl advanced 3001
[DeviceB-acl-adv-3001] rule permit tcp destination-port eq 80
[DeviceB-acl-adv-3001] quit
```

# 创建流分类 http，匹配 ACL 3001。

```
[DeviceB] traffic classifier http
[DeviceB-classifier-http] if-match acl 3001
[DeviceB-classifier-http] quit
```

# 创建流分类 class，匹配所有报文。

```
[DeviceB] traffic classifier class
[DeviceB-classifier-class] if-match any
[DeviceB-classifier-class] quit
```

# 创建流行为 car_inbound，动作为流量监管，cir 为 20480kbps，由于默认对红色报文的处理方式就是丢弃，因此无需配置。

```
[DeviceB] traffic behavior car_inbound
[DeviceB-behavior-car_inbound] car cir 20480
[DeviceB-behavior-car_inbound] quit
```

# 创建流行为 car_outbound，动作为流量监管，cir 为 10240kbps。

```
[DeviceB] traffic behavior car_outbound
[DeviceB-behavior-car_outbound] car cir 10240
[DeviceB-behavior-car_outbound] quit
```

# 创建 QoS 策略，命名为 car_inbound，将流分类 class 和流行为 car_inbound 进行关联。

```
[DeviceB] qos policy car_inbound
[DeviceB-qospolicy-car_inbound] classifier class behavior car_inbound
[DeviceB-qospolicy-car_inbound] quit
```

# 创建 QoS 策略，命名为 car_outbound，将流分类 http 和流行为 car_outbound 进行关联。

```
[DeviceB] qos policy car_outbound
[DeviceB-qospolicy-car_outbound] classifier http behavior car_outbound
[DeviceB-qospolicy-car_outbound] quit
```

# 将 QoS 策略 car_inbound 应用到接口 GigabitEthernet1/0/1 的入方向上。

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

# 将 QoS 策略 car_outbound 应用到接口 GigabitEthernet1/0/2 的出方向上。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] qos apply policy car_outbound outbound
```

# 5 拥塞管理

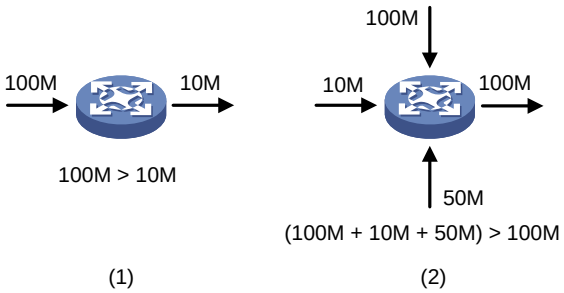
## 5.1 拥塞管理简介

### 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 设备支持的拥塞管理方法

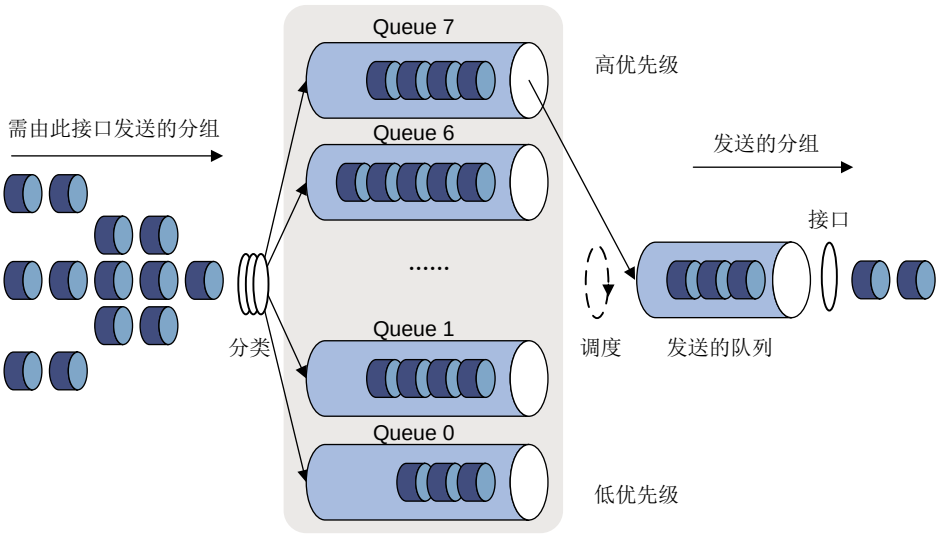
对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级别算法将这些流量发送出去。

目前设备支持如下几种队列：

- SP 队列
- WRR 队列

### 1. SP 队列

图5-2 SP 队列示意图



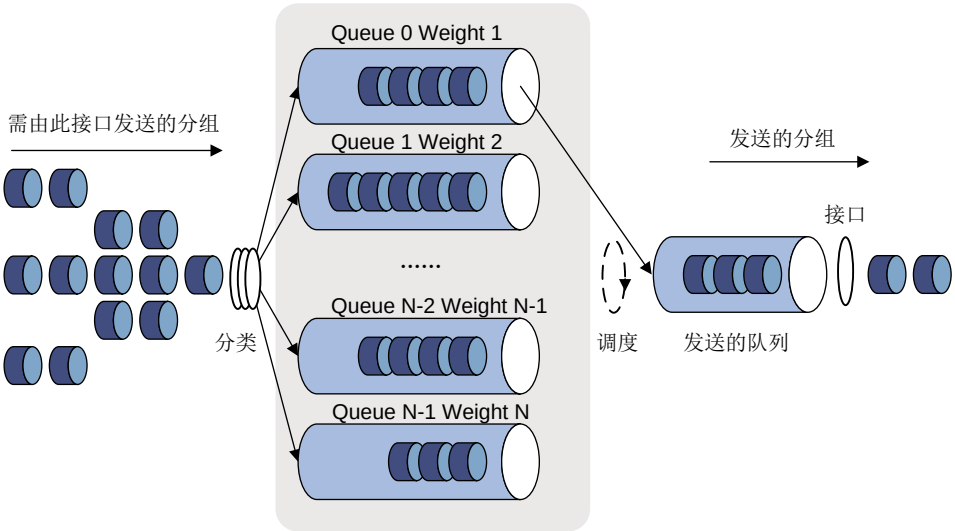

SP 队列是针对关键业务类型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以图 5-2 为例，优先队列将端口的 8 个输出队列分成 8 类，依次为 7、6、5、4、3、2、1、0 队列，它们的优先级依次降低。

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 队列在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 8 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w7、w6、w5、w4、w3、w2、w1、w0），加权值表示获取资源的比重。如一个 100Mbps 的端口，配置它的 WRR 队列的加权值为 50、50、30、30、10、10、10、10（依次对应 w7、w6、w5、w4、w3、w2、w1、w0），这样可以保证最低优先级队列至少获得 5Mbps 的带宽，解决了采用 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问题。

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。

用户还可以根据需要将输出队列划分为 WRR 优先级队列组 1 和 SP 优先级队列组。进行队列调度时遵循如下规则：

- 只有 WRR 组时，各队列之间按照 WRR 方式调度。
- SP 组和 WRR 组同时存在时：
  - 如果 SP 组中的最高优先级低于 WRR 组中的最低优先级，优先调度 WRR 组。例如队列 0 和 1 属于 SP 组，队列 2～7 属于 WRR 组，则优先调度队列 2～7。队列 2～7 为空时调度队列 1 和 0。
  - 其他情况下，优先调度 SP 组中优先级高于 WRR 组中最低优先级的队列，然后调度 WRR 组，最后调度 SP 组中剩余队列。例如队列 0、1、3 和 4 属于 SP 组，队列 2、5、6 和 7 属于 WRR 组，则优先调度队列 3 和 4。队列 3 和 4 为空时调度队列 2、5、6 和 7。队列 2、5、6 和 7 也为空时调度队列 0 和 1。

## 5.2 拥塞管理配置任务简介

拥塞管理配置任务如下：

- 配置接口队列

  请选择以下一项任务进行配置：
  - 配置 SP 队列
  - 配置 WRR 队列
  - 配置 SP+WRR 队列
- 配置队列调度策略

## 5.3 配置接口队列

### 5.3.1 配置限制和指导

本节中的“接口”指的是二层以太网接口和三层以太网接口。三层以太网接口是指在以太网接口视图下通过 **`port link-mode route`** 命令切换为三层模式的以太网接口，有关以太网接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“以太网接口配置”。

### 5.3.2 配置 SP 队列

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 配置 SP 队列。

**qos sp**

缺省情况下，接口采用 WRR 调度算法，各队列按照每次轮询可发送的字节数进行计算。

### 5.3.3 配置 WRR 队列

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 开启 WRR 队列。

**qos wrr weight**

接口采用 WRR 调度算法，各队列按照每次轮询可发送的报文个数进行计算。

(4) 配置分组 WRR 队列的参数。

**qos wrr** *queue-id* **group 1 weight** *schedule-value*

所有队列都处于 WRR 调度组 1 中，调度权重从队列 0 到 7 分别为 1、2、3、4、5、9、13、15，各队列按照每次轮询可发送的报文个数进行计算。

### 5.3.4 配置 SP+WRR 队列

#### 1. 配置限制和指导

在配置 WRR 队列的调度权重值时需要注意的是，选择的调度单位（字节数或报文个数）需要与使能 WRR 时使用的调度单位保持一致，否则将无法正常配置。

#### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 开启 WRR 队列。

**qos wrr weight**

缺省情况下，接口采用 WRR 调度算法，各队列按照每次轮询可发送的报文个数进行计算。

(4) 配置队列加入 SP 组，采用严格优先级调度算法。

**qos wrr** *queue-id* **group sp**

当接口使用 WRR 队列时，所有队列均处于 WRR 调度组 1 中。

(5) 配置队列加入 WRR 调度组。

**qos wrr** *queue-id* **group 1 weight** *schedule-value*

当接口使用 WRR 队列时，所有队列都处于 WRR 调度组 1 中，调度权重从队列 0 到 7 分别为 1、2、3、4、5、9、13、15，各队列按照每次轮询可发送的报文个数进行计算。

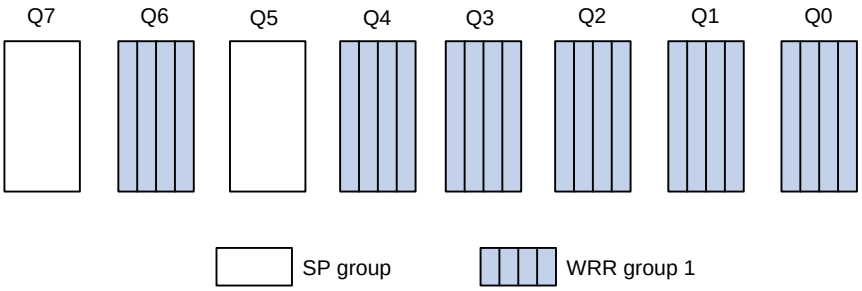
# 5.4 配置队列调度策略

## 5.4.1 队列调度策略简介

队列调度策略配置是在一个策略中配置各个队列的调度参数，最后通过在接口应用该策略来实现拥塞管理功能。

队列调度策略中的队列支持两种调度方式：SP 和 WRR。在一个队列调度策略中支持 SP 和 WRR 的混合配置。具体调度方式，可参见 5.1.2 设备支持的拥塞管理方法中介绍的内容。以 SP 和 WRR 分组混合配置为例，调度关系如图 5-4 所示。

图5-4 SP 和 WRR 混合配置图




- 设备优先调度 SP 组队列中的报文。
- 队列 7（即图中的 Q7，下同）在 SP 组中优先级最高，该队列的报文优先发送。
- 队列 5 在 SP 组中优先级次之，队列 7 为空时发送本队列的报文。
- 队列 6、4、3、2、1、0 之间按照权重轮询调度，在队列 7、5 为空时调度 WRR 分组 1。

## 5.4.2 配置限制和指导

在配置队列调度策略时需要注意的是：

- 队列调度策略中队列的调度参数支持动态修改，从而方便修改已经应用的队列调度策略。
- 本节中的“接口”指的是二层以太网接口和三层以太网接口。三层以太网接口是指在以太网接口视图下通过 **port link-mode route** 命令切换为三层模式的以太网接口，有关以太网接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“以太网接口配置”。

## 5.4.3 创建队列调度策略

(1) 进入系统视图。

**system-view**

(2) 创建队列调度策略，并进入相应的队列调度策略视图。

**qos qmprofile** *profile-name*

(3) （可选）配置队列调度参数。请选择其中一项进行配置。

- 配置严格优先级调度：

**queue** *queue-id* **sp**

- 配置加权轮询调度：

  **queue** *queue-id* **wrr group** *group-id* { **weight** | **byte-count** } *schedule-value*

缺省情况下，队列调度策略的内容是所有队列均采用 SP 方式调度。

### 5.4.4 应用队列调度策略

(1) 进入系统视图。

**system-view**

(2) 进入已创建的队列调度策略视图。

**qos qmprofile** *profile-name*

(3) 请依次执行以下命令在接口出方向上应用队列调度策略。

**interface** *interface-type interface-number*

**qos apply qmprofile** *profile-name*

缺省情况下，接口上未应用队列调度策略。

### 5.4.5 队列调度策略典型配置举例

#### 1. 配置需求

接口 GigabitEthernet1/0/1 的队列调度方式如下：

- 队列 7 优先级最高，该队列报文优先发送。
- 队列 0～6 之间按照权重轮询调度，属于 WRR 分组，使用报文个数作为调度权重，分别为 2、1、2、4、6、8、10，在队列 7 为空时调度 WRR 分组。

#### 2. 配置步骤

# 进入系统视图。

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

# 创建队列调度策略 qm1。

```
[Sysname] qos qmprofile qm1
[Sysname-qmprofile-qm1]
```

# 配置队列 7 为 SP 队列。

```
[Sysname-qmprofile-qm1] queue 7 sp
```

# 配置队列 0～6 属于 WRR 分组 1，使用报文个数作为调度权重，分别为 2、1、2、4、6、8、10。

```
[Sysname-qmprofile-qm1] queue 0 wrr group 1 weight 2
[Sysname-qmprofile-qm1] queue 1 wrr group 1 weight 1
[Sysname-qmprofile-qm1] queue 2 wrr group 1 weight 2
[Sysname-qmprofile-qm1] queue 3 wrr group 1 weight 4
[Sysname-qmprofile-qm1] queue 4 wrr group 1 weight 6
[Sysname-qmprofile-qm1] queue 5 wrr group 1 weight 8
[Sysname-qmprofile-qm1] queue 6 wrr group 1 weight 10
[Sysname-qmprofile-qm1] quit
```

# 把队列调度策略 qm1 应用到接口 GigabitEthernet1/0/1 上。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply qmprofile qm1
```

配置完成后，接口 GigabitEthernet1/0/1 按指定方式进行队列调度。

## 5.5 拥塞管理显示和维护

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队列的运行情况，通过查看显示信息验证配置的效果。

表5-1 拥塞管理的显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示队列调度策略的配置信息 | **display qos qmprofile configuration** [ *profile-name* ] [ **slot** *slot-number* ] |
| 显示接口的队列调度策略应用信息 | **display qos qmprofile interface** [ *interface-type interface-number* ] |
| 显示端口队列出方向的统计信息 | **display qos queue-statistics interface outbound** |
| 显示SP队列 | **display qos queue sp interface** [ *interface-type interface-number* ] |
| 显示WRR队列的配置 | **display qos queue wrr interface** [ *interface-type interface-number* ] |

# 6 流量过滤

## 6.1 流量过滤简介

流量过滤是指对符合流分类的流进行过滤的动作。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。

## 6.2 流量过滤配置限制和指导

设备支持基于接口、VLAN、全局和上线用户应用 QoS 策略配置流量过滤。

## 6.3 配置流量过滤

(1) 进入系统视图。

**system-view**

(2) 定义类。

a. 创建一个类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

b. 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

**quit**

(3) 定义流行为。

a. 创建一个流行为，并进入流行为视图。

**traffic behavior** *behavior-name*

b. 配置流量过滤动作。

**filter** { **deny** | **permit** }

缺省情况下，未配置流量过滤动作。

c. 退回系统视图。

**quit**

(4) 定义策略。

a. 创建策略并进入策略视图。

**qos policy** *policy-name*

b. 在策略中为类指定采用的流行为。

**classifier** *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

**quit**

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

(6) （可选）显示流量过滤的相关配置信息。

**display traffic behavior user-defined** [ *behavior-name* ]

# 6.4 流量过滤典型配置举例

## 6.4.1 流量过滤基本组网配置举例

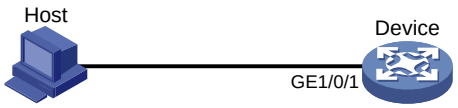
### 1. 组网需求

Host 通过接口 GigabitEthernet1/0/1 接入设备 Device。

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

### 2. 组网图

图6-1 流量过滤基本组网图




### 3. 配置步骤

# 定义高级 ACL 3000，匹配源端口号不等于 21 的数据流。

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 permit tcp source-port neq 21
[Device-acl-ipv4-adv-3000] quit
```

# 定义类 classifier_1，匹配高级 ACL 3000。

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

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

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

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

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

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

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

# 7 重标记

## 7.1 重标记简介

重标记是将报文的优先级或者标志位进行设置，重新定义报文的优先级等。例如，对于 IP 报文来说，可以利用重标记对 IP 报文中的 IP 优先级或 DSCP 值进行重新设置，控制 IP 报文的转发。

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。

重标记可以和优先级映射功能配合使用，具体请参见“3 优先级映射”。

## 7.2 配置重标记

### 1. 配置限制和指导

设备支持基于接口、VLAN、全局和上线用户应用 QoS 策略配置重标记。

### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 定义类。

a. 创建一个类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

b. 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

**quit**

(3) 定义流行为

a. 创建一个流行为，并进入流行为视图。

**traffic behavior** *behavior-name*

b. 重新标记报文的动作。

具体重标记动作的介绍，请查看“QoS 命令”中的 **remark** 命令。

c. 退回系统视图。

**quit**

(4) 定义策略。

a. 创建一个策略，并进入策略视图。

**qos policy** *policy-name*

b. 在策略中为类指定采用的流行为。

**classifier** *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

**quit**

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

(6) （可选）显示重标记的相关配置信息。

**display traffic behavior user-defined** [ *behavior-name* ]

# 7.3 重标记典型配置举例

## 7.3.1 重标记基本组网配置举例

### 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：

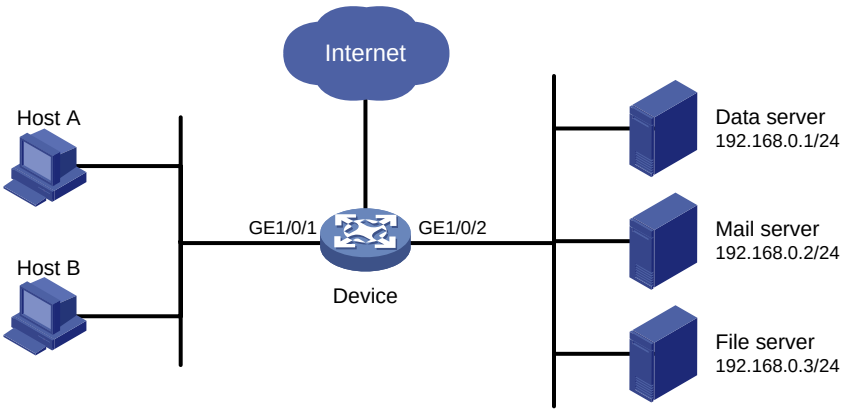
- Host A 和 Host B 通过端口 GigabitEthernet1/0/1 接入 Device；
- 数据库服务器、邮件服务器和文件服务器通过端口 GigabitEthernet1/0/2 接入 Device。

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7-1 重标记基本组网图




### 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 advanced 3000
[Device-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.1 0
[Device-acl-ipv4-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 advanced 3001
[Device-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
[Device-acl-ipv4-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 advanced 3002
[Device-acl-ipv4-adv-3002] rule permit ip destination 192.168.0.3 0
[Device-acl-ipv4-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 Nest

## 8.1 Nest简介

Nest 用来为符合流分类的流添加一层 VLAN Tag，使携带该 VLAN Tag 的报文通过对应 VLAN。例如，为从用户网络进入运营商网络的 VLAN 报文添加外层 VLAN Tag，使其携带运营商网络分配的 VLAN Tag 穿越运营商网络。

## 8.2 Nest配置限制和指导

设备支持基于接口入方向应用 QoS 策略配置 Nest。

如果该接口已使能 QinQ 功能，且 QoS 策略中配置了匹配 VLAN Tag VLAN ID 的规则，则该接口必须允许 VLAN ID 匹配的报文带 Tag 通过，才能保证 QinQ 功能和 Nest 同时生效，否则 Nest 将不会生效。

## 8.3 配置Nest

(1) 进入系统视图。

**system-view**

(2) 定义类。

a. 创建一个类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

b. 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

**quit**

(3) 定义流行为

a. 创建一个流行为，并进入流行为视图。

**traffic behavior** *behavior-name*

b. 配置添加报文的外层 VLAN Tag 动作。

**nest top-most vlan** *vlan-id*

缺省情况下，未配置添加外层 VLAN Tag 动作。

c. 退回系统视图。

**quit**

(4) 定义策略。

a. 创建一个策略，并进入策略视图。

**qos policy** *policy-name*

b. 在策略中为类指定采用的流行为。

**classifier** *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

**quit**

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

(6) （可选）显示 Nest 的相关配置信息。

**display traffic behavior user-defined** [ *behavior-name* ]

# 8.4 Nest典型配置举例

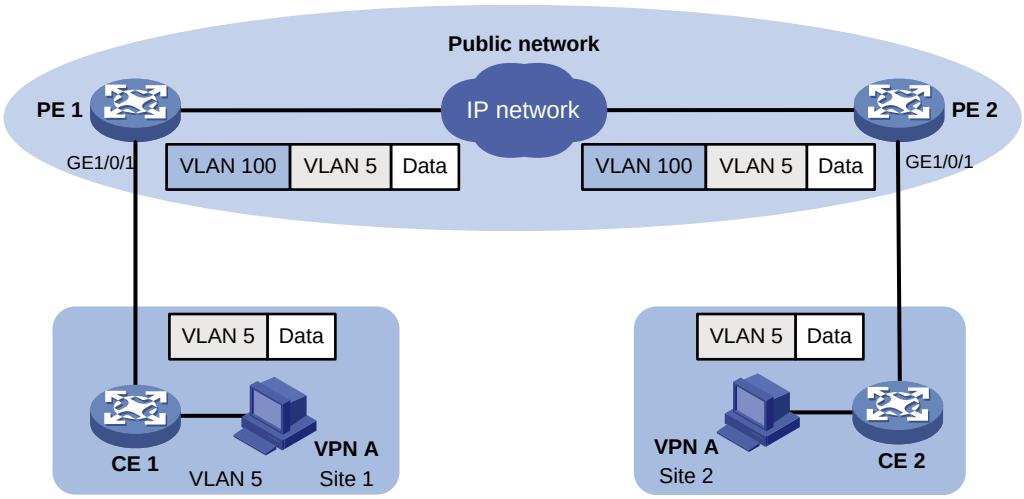
## 8.4.1 Nest 基本功能配置举例

### 1. 组网需求

- VPN A 中的 Site 1 和 Site 2 是某公司的两个分支机构，利用 VLAN 5 承载业务。由于分处不同地域，这两个分支机构采用了服务提供商（SP）所提供的 VPN 接入服务，SP 将 VLAN 100 分配给这两个分支机构使用。
- 该公司希望其下属的这两个分支机构可以跨越 SP 的网络实现互通。

### 2. 组网图

图8-1 Nest 基本功能组网图




### 3. 配置步骤

(1) 配置 PE 1

# 定义类 test 的匹配规则为：匹配从 GigabitEthernet1/0/1 收到的 VLAN ID 值为 5 的报文。

```
<PE1> system-view
```

```
[PE1] traffic classifier test
[PE1-classifier-test] if-match service-vlan-id 5
[PE1-classifier-test] quit
```

# 在流行为 test 上配置如下动作：添加 VLAN ID 为 100 的外层 VLAN Tag。

```
[PE1] traffic behavior test
[PE1-behavior-test] nest top-most vlan 100
[PE1-behavior-test] quit
```

# 在策略 test 中为类 test 指定采用流行为 test。

```
[PE1] qos policy test
[PE1-qospolicy-test] classifier test behavior test
[PE1-qospolicy-test] quit
```

# 配置下行端口 GigabitEthernet1/0/1 为 Hybrid 端口且允许 VLAN 100 的报文不携带 VLAN Tag 通过。

```
[PE1] interface gigabitethernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type hybrid
[PE1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

# 在下行端口 GigabitEthernet1/0/1 的入方向上应用上行策略 test。

```
[PE1-GigabitEthernet1/0/1] qos apply policy test inbound
[PE1-GigabitEthernet1/0/1] quit
```

# 配置上行端口 GigabitEthernet1/0/2 为 Trunk 端口且允许 VLAN 100 通过。

```
[PE1] interface gigabitethernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 100
[PE1-GigabitEthernet1/0/2] quit
```

(2) 配置 PE 2

PE 2 的配置与 PE 1 完全一致，这里不再赘述。

# 9 流量重定向

## 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。
- 重定向到接口：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。

## 9.2 流量重定向配置限制和指导

配置流量重定向时需要注意的是：

- 设备支持基于接口、VLAN、全局和上线用户的入方向应用 QoS 策略配置流量重定向。
- 在配置重定向动作时，同一个流行为中，多次配置重定向命令，最后一次配置的生效。
- 配置重定向到指定的以太网接口后，如果该以太网接口所在的接口板或接口模块扩展卡被拔出，设备将不显示流行为下的重定向到该以太网接口的配置，重定向动作失效；当接口板或接口模块扩展卡重新插回设备后，此时设备可以显示流行为下的重定向到该以太网接口的配置，重定向动作会继续生效。

## 9.3 配置流量重定向

(1) 进入系统视图。

**system-view**

(2) 定义类。

a. 创建一个类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

b. 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

**quit**

(3) 定义流行为

a. 创建一个流行为，并进入流行为视图。

**traffic behavior** *behavior-name*

b. 配置流量重定向动作。

**redirect** { **cpu** | **interface** *interface-type interface-number* }

缺省情况下，未配置流量重定向动作。

c. 退回系统视图。

**quit**

(4) 定义策略。

a. 创建一个策略，并进入策略视图。

**qos policy** *policy-name*

b. 在策略中为类指定采用的流行为。

**classifier** *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

**quit**

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

(6) （可选）显示流量重定向的相关配置信息。

**display traffic behavior user-defined** [ *behavior-name* ]

# 9.4 流量重定向典型配置举例

## 9.4.1 重定向至接口配置举例

### 1. 组网需求

网络环境描述如下：

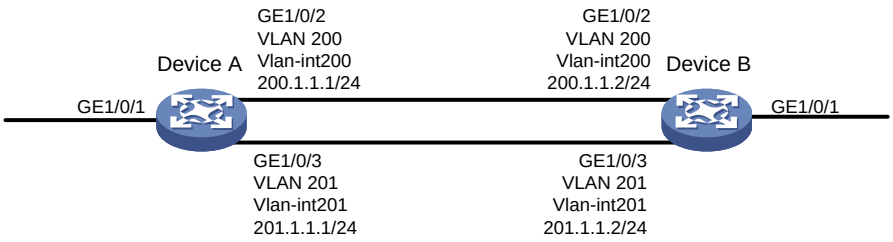
- Device A 通过两条链路与 Device B 连接，同时 Device A 和 Device B 各自连接其他的设备；
- Device A 上的端口 GigabitEthernet1/0/1 的链路类型为 Trunk 类型，且允许 VLAN200 和 VLAN201 的报文通过；
- Device A 上的端口 GigabitEthernet1/0/2 和 Device B 上的端口 GigabitEthernet1/0/2 属于 VLAN 200；
- Device A 上的端口 GigabitEthernet1/0/3 和 Device B 上的端口 GigabitEthernet1/0/3 属于 VLAN 201；
- Device A 上接口 Vlan-interface200 的 IP 地址为 200.1.1.1/24，接口 Vlan-interface201 的 IP 地址为 201.1.1.1/24；
- Device B 上接口 Vlan-interface200 的 IP 地址为 200.1.1.2/24，接口 Vlan-interface201 的 IP 地址为 201.1.1.2/24。

配置重定向至接口，满足如下需求：

- 将 Device A 的端口 GigabitEthernet1/0/1 接收到的源 IP 地址为 2.1.1.1 的报文转发至 GigabitEthernet1/0/2；
- 将 Device A 的端口 GigabitEthernet1/0/1 接收到的源 IP 地址为 2.1.1.2 的报文转发至 GigabitEthernet1/0/3；
- 对于 Device A 的端口 GigabitEthernet1/0/1 接收到的其它报文，按照查找路由表的方式进行转发。

## 2. 组网图

图9-1 重定向至接口配置组网图




## 3. 配置步骤

# 定义基本 ACL 2000，对源 IP 地址为 2.1.1.1 的报文进行分类。

```
<DeviceA> system-view
[DeviceA] acl basic 2000
[DeviceA-acl-ipv4-basic-2000] rule permit source 2.1.1.1 0
[DeviceA-acl-ipv4-basic-2000] quit
```

# 定义基本 ACL 2001，对源 IP 地址为 2.1.1.2 的报文进行分类。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 2.1.1.2 0
[DeviceA-acl-ipv4-basic-2001] 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
```

# 定义类 classifier_2，匹配基本 ACL 2001。

```
[DeviceA] traffic classifier classifier_2
[DeviceA-classifier-classifier_2] if-match acl 2001
[DeviceA-classifier-classifier_2] quit
```

# 定义流行为 behavior_1，动作为重定向至 GigabitEthernet1/0/2。

```
[DeviceA] traffic behavior behavior_1
[DeviceA-behavior-behavior_1] redirect interface gigabitethernet 1/0/2
[DeviceA-behavior-behavior_1] quit
```

# 定义流行为 behavior_2，动作为重定向至 GigabitEthernet1/0/3。

```
[DeviceA] traffic behavior behavior_2
[DeviceA-behavior-behavior_2] redirect interface gigabitethernet 1/0/3
[DeviceA-behavior-behavior_2] quit
```

# 定义策略 policy，为类 classifier_1 指定流行为 behavior_1，为类 classifier_2 指定流行为 behavior_2。

```
[DeviceA] qos policy policy
[DeviceA-qospolicy-policy] classifier classifier_1 behavior behavior_1
[DeviceA-qospolicy-policy] classifier classifier_2 behavior behavior_2
[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
```

# 10 全局 CAR

## 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。全局 CAR 分为聚合 CAR 和分层 CAR。

### 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 240kbps，再使用分层 CAR 限制总流量为 320kbps。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 320kbps。
- 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 240kbps，再使用分层 CAR 限制总流量为 560kbps，则当数据流 1 的流量不足 240kbps 时，即使数据流 2 的流量达到了 320kbps，仍然可以正常通过。

## 10.2 全局CAR配置限制和指导

当前设备仅支持聚合 CAR。

当前设备支持基于接口、VLAN、全局和上线用户入方向应用 QoS 策略配置聚合 CAR。

## 10.3 配置聚合CAR

(1) 进入系统视图。

**system-view**

(2) 定义类。

a. 创建一个类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

b. 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

**quit**

(3) 配置聚合 CAR。

**qos car** *car-name* **aggregative cir** *committed-information-rate* [ **cbs** *committed-burst-size* [ **ebs** *excess-burst-size* ] ] [ **green** *action* | **red** *action* | **yellow** *action* ] *

**qos car** *car-name* **aggregative cir** *committed-information-rate* [ **cbs** *committed-burst-size* ] **pir** *peak-information-rate* [ **ebs** *excess-burst-size* ] [ **green** *action* | **red** *action* | **yellow** *action* ] *

缺省情况下，未配置聚合 CAR。

(4) 定义流行为。

a. 进入流行为视图。

**traffic behavior** *behavior-name*

b. 在流行为中应用聚合 CAR 动作。

**car name** *car-name*

缺省情况下，流行为中未应用聚合 CAR 动作。

(5) 定义策略。

a. 创建一个策略，并进入策略视图。

**qos policy** *policy-name*

b. 在策略中为类指定采用的流行为。

**classifier** *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

**quit**

(6) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

## 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10-1 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* ] |
| 清除全局CAR的统计信息 | **reset qos car name** [ *car-name* ] |

# 11 流量统计

## 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 流量统计配置限制和指导

设备支持基于接口、VLAN、全局和上线用户应用 QoS 策略配置流量统计。

## 11.3 配置流量统计

(1) 进入系统视图。

**system-view**

(2) 定义类。

a. 创建一个类，并进入类视图。

**traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ]

b. 定义匹配数据包的规则。

**if-match** *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

**quit**

(3) 定义流行为。

a. 创建一个流行为，并进入流行为视图。

**traffic behavior** *behavior-name*

b. 为流行为配置流量统计动作。

**accounting** { **byte** | **packet** }

缺省情况下，未配置流量统计动作。

c. 退回系统视图。

**quit**

(4) 定义策略。

a. 创建一个策略，并进入策略视图。

**qos policy** *policy-name*

b. 在策略中为类指定采用的流行为。

**classifier** *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

**quit**

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

(6) （可选）显示流量统计的相关配置信息。

**display traffic behavior user-defined** [ *behavior-name* ]

# 11.4 流量统计典型配置举例

## 11.4.1 流量统计基本组网配置举例

### 1. 组网需求

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

配置流量统计功能，对接口 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 流量统计基本组网图


### 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。

```
<Device> system-view
[Device] acl basic 2000
[Device-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Device-acl-ipv4-basic-2000] quit
```

# 定义类 classifier_1，匹配基本 ACL 2000。

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

# 定义流行为 behavior_1，动作为流量统计。

```
[Device] traffic behavior behavior_1
[Device-behavior-behavior_1] accounting packet
[Device-behavior-behavior_1] quit
```

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

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

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

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

```
[Device-GigabitEthernet1/0/1] qos apply policy policy inbound
[Device-GigabitEthernet1/0/1] quit
```

# 查看配置后流量统计的情况。

```
[Device] 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 附录

## 12.1 附录 A 缩略语表

表12-1 附录 A 缩略语表

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
| AF | Assured Forwarding | 确保转发 |
| BE | Best Effort | 尽力转发 |
| BQ | Bandwidth Queuing | 带宽队列 |
| CAR | Committed Access Rate | 承诺访问速率 |
| CBQ | Class Based Queuing | 基于类的队列 |
| CBS | Committed Burst Size | 承诺突发尺寸 |
| CBWFQ | Class Based Weighted Fair Queuing | 基于类的加权公平队列 |
| CE | Customer Edge | 用户边缘设备 |
| CIR | Committed Information Rate | 承诺信息速率 |
| CQ | Custom Queuing | 定制队列 |
| DAR | Deeper Application Recognition | 深度应用识别 |
| DCBX | Data Center Bridging Exchange Protocol | 数据中心桥能力交换协议 |
| DiffServ | Differentiated Service | 区分服务 |
| DoS | Denial of Service | 拒绝服务 |
| DSCP | Differentiated Services Code Point | 区分服务编码点 |
| EACL | Enhanced ACL | 增强型ACL |
| EBS | Excess Burst Size | 超出突发尺寸 |
| ECN | Explicit Congestion Notification | 显示拥塞通知 |
| EF | Expedited Forwarding | 加速转发 |
| FEC | Forwarding Equivalance Class | 转发等价类 |
| FIFO | First in First out | 先入先出 |
| FQ | Fair Queuing | 公平队列 |
| GMB | Guaranteed Minimum Bandwidth | 最小带宽保证队列 |
| GTS | Generic Traffic Shaping | 通用流量整形 |
| IntServ | Integrated Service | 综合服务 |
| ISP | Internet Service Provider | 互联网服务提供商 |
| LFI | Link Fragmentation and Interleaving | 链路分片与交叉 |

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
| LLQ | Low Latency Queuing | 低时延队列 |
| LR | Line Rate | 限速 |
| LSP | Label Switched Path | 标签交换路径 |
| MPLS | Multiprotocol Label Switching | 多协议标签交换 |
| P2P | Peer-to-Peer | 对等 |
| PE | Provider Edge | 服务提供商网络边缘 |
| PHB | Per-hop Behavior | 单中继段行为 |
| PIR | Peak Information Rate | 峰值信息速率 |
| PQ | Priority Queuing | 优先队列 |
| PW | Pseudowire | 伪线 |
| QoS | Quality of Service | 服务质量 |
| QPPB | QoS Policy Propagation Through the Border Gateway Protocol | 通过BGP传播QoS策略 |
| RED | Random Early Detection | 随机早期检测 |
| RSVP | Resource Reservation Protocol | 资源预留协议 |
| RTP | Real-time Transport Protocol | 实时传输协议 |
| SLA | Service Level Agreement | 服务水平协议 |
| SP | Strict Priority | 严格优先级队列 |
| TE | Traffic Engineering | 流量工程 |
| ToS | Type of Service | 服务类型 |
| TP | Traffic Policing | 流量监管 |
| TS | Traffic Shaping | 流量整形 |
| VoIP | Voice over IP | 在IP网络上传送语音 |
| VPN | Virtual Private Network | 虚拟专用网络 |
| VSI | Virtual Station Interface | 虚拟服务器接口 |
| WFQ | Weighted Fair Queuing | 加权公平队列 |
| WRED | Weighted Random Early Detection | 加权随机早期检测 |
| WRR | Weighted Round Robin | 加权轮询队列 |

## 12.2 附录 B 缺省优先级映射表

说明

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

表12-2 dot1p-lp、dot1p-dp、dot1p-dscp 缺省映射关系

| 映射输入索引 | dot1p-lp 映射 | dot1p-dp 映射 | dot1p-dscp 映射 |
|---|---|---|---|
| dot1p | lp | dp | dscp |
| 0 | 2 | 0 | 0 |
| 1 | 0 | 0 | 8 |
| 2 | 1 | 0 | 16 |
| 3 | 3 | 0 | 24 |
| 4 | 4 | 0 | 32 |
| 5 | 5 | 0 | 40 |
| 6 | 6 | 0 | 48 |
| 7 | 7 | 0 | 56 |

表12-3 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 | dp | 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12-4 exp-dp 缺省映射关系

| 映射输入索引 | exp-dp 映射 |
|---|---|
| exp优先级 | dp |
| 0 | 0 |
| 1 | 0 |

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

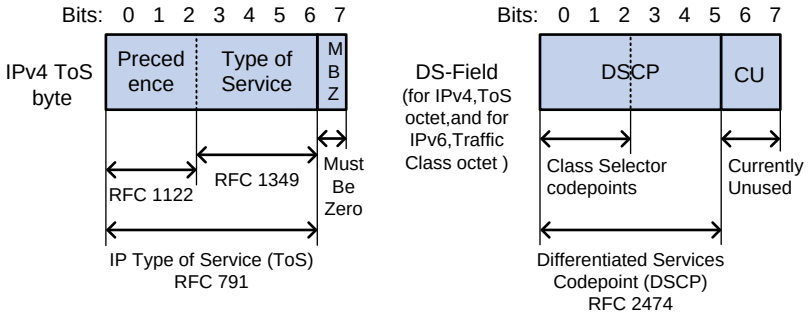
表12-5 端口优先级和 LP 映射关系

| 端口优先级 | LP |
| --- | --- |
| 0 | 0 |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

# 12.3 附录 C 各种优先级介绍

## 12.3.1 IP 优先级和 DSCP 优先级

图12-1 ToS 和 DS 域




如图 12-1 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12-6 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 |

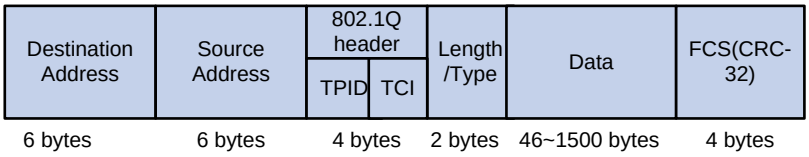
表12-7 DSCP 优先级说明

| 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 |
| 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） |

## 12.3.2 802.1p 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12-2 带有 802.1Q 标签头的以太网帧




如图 12-2 所示，4 个字节的 802.1Q 标签头包含了 2 个字节的 TPID（Tag Protocol Identifier，标签协议标识符）和 2 个字节的 TCI（Tag Control Information，标签控制信息），TPID 取值为 0x8100，图 12-3 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 规范中被详细定义的。

图12-3 802.1Q 标签头

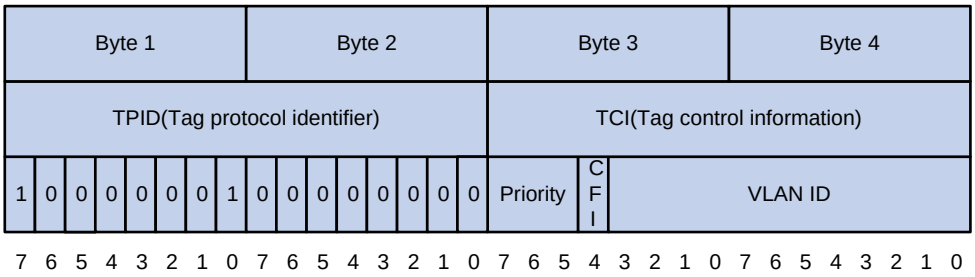



表12-8 802.1p 优先级说明

| 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 |

## 12.3.3 EXP 优先级

EXP 优先级位于 MPLS 标签内，用于标记 MPLS QoS。

图12-4 MPLS 标签的封装结构


在图 12-4 中，Exp 字段就是 EXP 优先级，长度为 3 比特，取值范围为 0～7。