

目 录

1 QoS简介	1-1
1.1 概述	1-1
1.2 QoS服务模型简介.....	1-1
1.2.1 Best-Effort服务模型.....	1-1
1.2.2 Int-Serv服务模型	1-1
1.2.3 Diff-Serv服务模型	1-1
1.3 QoS技术综述.....	1-2
1.3.1 QoS技术在网络中的位置	1-2
2 QoS配置方式	2-1
2.1 配置方式介绍.....	2-1
2.1.1 非QoS策略配置方式.....	2-1
2.1.2 QoS策略配置方式.....	2-1
2.2 QoS策略配置方式的步骤.....	2-1
2.2.1 定义类.....	2-2
2.2.2 定义流行为.....	2-4
2.2.3 定义策略.....	2-4
2.2.4 应用策略.....	2-5
2.2.5 QoS策略显示和维护.....	2-7
3 优先级映射配置	3-1
3.1 优先级映射简介.....	3-1
3.1.1 概述.....	3-1
3.1.2 优先级映射表.....	3-1
3.1.3 优先级信任模式.....	3-2
3.1.4 优先级映射过程.....	3-2
3.2 优先级映射配置任务简介.....	3-3
3.3 配置优先级映射.....	3-4
3.3.1 配置优先级映射表.....	3-4
3.3.2 配置端口优先级信任模式.....	3-4
3.3.3 配置端口优先级.....	3-5
3.4 优先级映射显示和维护.....	3-5
3.5 优先级映射典型配置举例.....	3-6
3.5.1 优先级映射配置举例.....	3-6

3.5.2 优先级映射表和重标记配置举例	3-8
4 流量整形和端口限速配置	4-1
4.1 流量整形	4-1
4.2 端口限速	4-2
4.3 流量整形配置	4-2
4.3.1 配置基于队列的流量整形	4-3
4.3.2 配置适配所有流的流量整形	4-3
4.4 端口限速配置	4-3
4.4.1 端口限速配置过程	4-3
4.4.2 端口限速配置举例	4-4
4.5 流量整形/端口限速显示和维护	4-4
5 拥塞管理配置	5-1
5.1 拥塞管理简介	5-1
5.1.1 拥塞的产生、影响和对策	5-1
5.1.2 拥塞管理策略	5-1
5.2 拥塞管理配置任务简介	5-5
5.3 拥塞管理配置	5-5
5.3.1 配置SP队列	5-5
5.3.2 配置WRR队列	5-6
5.3.3 配置SP+WRR队列	5-7
6 流量过滤配置	6-1
6.1 流量过滤简介	6-1
6.2 配置流量过滤	6-1
6.3 流量过滤配置举例	6-2
6.3.1 流量过滤配置举例	6-2
7 重标记配置	7-1
7.1 重标记简介	7-1
7.2 配置重标记	7-1
7.3 重标记配置举例	7-2
7.3.1 重标记优先级配置举例	7-2
8 流量重定向配置	8-1
8.1 流量重定向简介	8-1
8.2 配置流量重定向	8-1
9 Burst功能配置	9-1
9.1 Burst功能简介	9-1

9.2 配置Burst功能.....	9-1
9.2.1 配置准备.....	9-1
9.2.2 配置过程.....	9-1
9.3 Burst功能配置举例.....	9-1
9.3.1 Burst功能配置举例.....	9-1
10 附录 A缺省优先级映射表	10-1
11 附录 B 各种优先级介绍.....	11-1
11.1 IP优先级和DSCP优先级.....	11-1
11.2 802.1p优先级.....	11-2

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，Int-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。Int-Serv 模型可扩展性很差，难以在 Internet 核心网络实施。

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。

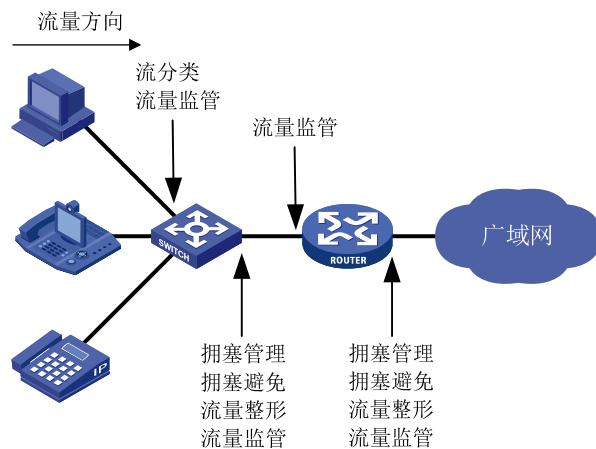
本文提到的技术都是基于 Diff-Serv 服务模型。

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。

2 QoS配置方式

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。

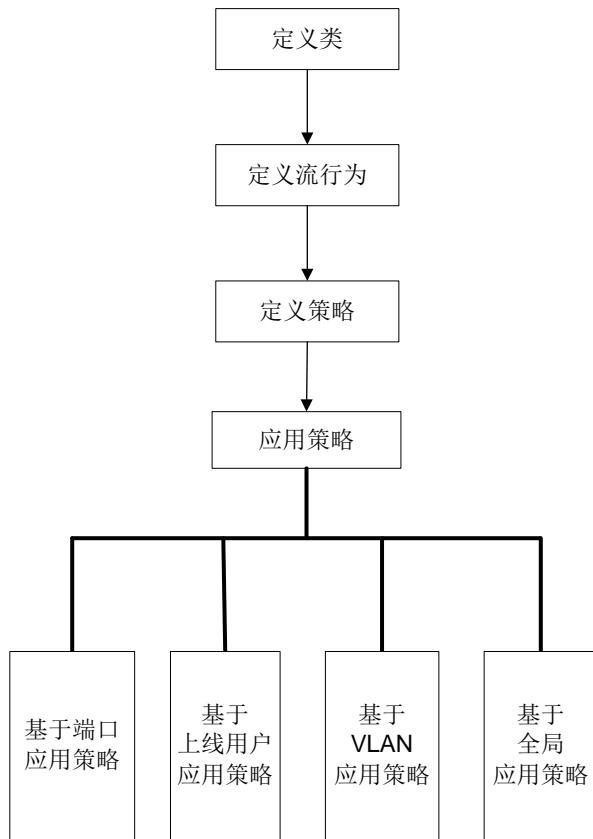
策略的要素包括：策略名称、绑定在一起的类和流行为的名称。

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 <ul style="list-style-type: none"> • 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 重复执行该命令可以配置多条匹配规则

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] { <i>acl-number</i> name <i>acl-name</i> }	定义匹配ACL的规则 <i>acl-number</i> 是ACL的序号，IPv4 ACL序号的取值范围是2000~3999，IPv6 ACL序号的取值范围是2000~3999，二层ACL序号的取值范围是4000~4999 <i>acl-name</i> 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 <i>8021p-list</i>	定义匹配用户网络 802.1p 优先级的规则， <i>8021p-list</i> 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 <i>vlan-id-list</i>	定义匹配用户网络 VLAN ID 的规则， <i>vlan-id-list</i> 为 VLAN ID 的列表，形式可以为 <i>vlan-id to vlan-id</i> ，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 <i>mac-address</i>	定义匹配目的 MAC 地址的规则
dscp <i>dscp-list</i>	定义匹配DSCP的规则， <i>dscp-list</i> 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 11-2 中的关键字
ip-precedence <i>ip-precedence-list</i>	定义匹配 IP 优先级的规则， <i>ip-precedence-list</i> 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 <i>protocol-name</i>	定义匹配协议的规则， <i>protocol-name</i> 取值为 IP 或 IPv6
service-dot1p <i>8021p-list</i>	定义匹配运营商网络 802.1p 优先级的规则， <i>8021p-list</i> 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 <i>vlan-id-list</i>	定义匹配运营商网络 VLAN ID 的规则， <i>vlan-id-list</i> 为 VLAN ID 的列表，形式可以为 <i>vlan-id to vlan-id</i> ，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 <i>mac-address</i>	定义匹配源 MAC 地址的规则



说明

如果流分类中各规则之间的逻辑关系为 **and**，在定义匹配规则时，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，对应该类的流行为将会无法正常执行：

- **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)

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**，然后再通过多次执行 **if-match** 命令的方式来配置匹配多个值的规则。



说明

当一个流分类中规则之间的逻辑关系为 **and** 时：

- 在一个流分类中，不能同时配置匹配 DSCP 优先级和匹配 IP 优先级的规则。
- 如果已经存在匹配 DSCP 优先级或匹配 IP 优先级的规则，则在指定匹配协议的规则时，只能匹配 IP 协议，不能匹配 IPv6 协议。

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 <i>behavior-name</i>	必选
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，例如流量过滤、流量重定向、重标记等，具体情况请参见相关章节	

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 <i>policy-name</i>	必选
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>	必选



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 **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。

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 内所有端口接收的流量生效。
- 基于全局应用 QoS 策略：QoS 策略对所有流量生效。



说明

- 当 QoS 策略应用到端口、VLAN、全局或未激活的 User Profile 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。但当流分类规则中匹配的是 ACL 时，不能删除或修改该 ACL（包括向该 ACL 中添加、删除和修改规则）。
- 如果 User Profile 处于激活状态，既不能修改变策略的内容（包括流分类引用的 ACL 规则），也不能删除已经应用到此 User Profile 的策略。

1. 基于端口应用QoS策略

一个策略可以应用于多个端口。每个端口只能在入方向上应用一个策略。

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	-

操作		命令	说明
进入以太网端口视图或端口组视图	进入以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	二者必选其一 进入以太网端口视图后，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 <i>port-group-name</i>	
在端口上应用关联的策略		qos apply policy <i>policy-name</i> inbound	必选

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。每个上线用户的入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 <i>profile-name</i>	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 <i>policy-name</i> inbound	必选 inbound 是对设备接收的上线用户流量（即上线用户发送的流量）应用策略
退回系统视图	quit	-
激活User Profile	user-profile <i>profile-name</i> enable	必选 缺省情况下，User Profile处于未激活状态



说明

- user-profile 视图下应用的策略中的流行为只支持 **remark** 和 **filter** 两种动作。
- 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。
- 上线用户目前支持 802.1X 和 Portal 两种接入认证方式。

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 上所有接收的流量进行管理。

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 <i>policy-name</i> vlan <i>vlan-id-list</i> inbound	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。

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所有接收的流量进行管理。

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 <i>policy-name</i> global inbound	必选

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2-9 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 [<i>tcl-name</i>] [[{ begin exclude include } <i>regular-expression</i>]]
显示配置的流行为信息	display traffic behavior user-defined [<i>behavior-name</i>] [[{ begin exclude include } <i>regular-expression</i>]]
显示用户定义策略的配置信息	display qos policy user-defined [<i>policy-name</i> [classifier <i>tcl-name</i>]] [[{ begin exclude include } <i>regular-expression</i>]]
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 [<i>interface-type interface-number</i>] [inbound] [[{ begin exclude include } <i>regular-expression</i>]]
显示VLAN应用QoS策略的信息	display qos vlan-policy { name <i>policy-name</i> vlan <i>vlan-id</i> } [slot <i>slot-number</i>] [inbound] [[{ begin exclude include } <i>regular-expression</i>]]
显示全局应用QoS策略的信息	display qos policy global [slot <i>slot-number</i>] [inbound] [[{ begin exclude include } <i>regular-expression</i>]]
清除VLAN应用QoS策略的统计信息	reset qos vlan-policy [vlan <i>vlan-id</i>] [inbound]
清除全局应用QoS策略的统计信息	reset qos policy global [inbound]

3 优先级映射配置



说明

各种优先级的相关介绍请参见 [11 附录 B 各种优先级介绍](#)。

3.1 优先级映射简介

3.1.1 概述

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。

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两种：

- 本地优先级：设备为报文分配的一种具有本地意义的优先级，是设备进行队列调度的直接依据。每个本地优先级对应一个队列，队列的优先级越高，越能够获得优先的调度。本地优先级与队列的对应关系如 [表 3-1](#) 所示：

表3-1 本地优先级与队列的对应关系

本地优先级	对应的队列编号
0, 1	0
2, 3	1
4, 5	2
6, 7	3

- 丢弃优先级：交换机在丢弃报文时参考的优先级，丢弃优先级值大的报文被优先丢弃。

优先级映射就是在报文携带优先级与设备调度优先级之间建立的对应关系，它可以将标准的优先级体系体现到设备实际的转发调度过程中。用户可以根据需要配置优先级映射规则，从而使报文的调度更适合网络的实际情况，达到灵活控制报文传输的效果。

3.1.2 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-dot1p**: 802.1p 优先级到 802.1p 优先级映射表；
- **dot1p-dscp**: 802.1p 优先级到 DSCP 映射表；
- **dot1p-ip**: 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-dscp**: DSCP 到 DSCP 映射表，仅对 IP 报文生效；
- **dscp-ip**: DSCP 到本地优先级映射表，仅对 IP 报文生效；

通常情况下，设备可以通过查找缺省优先级映射表（请参见 [10 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。

3.1.3 优先级信任模式

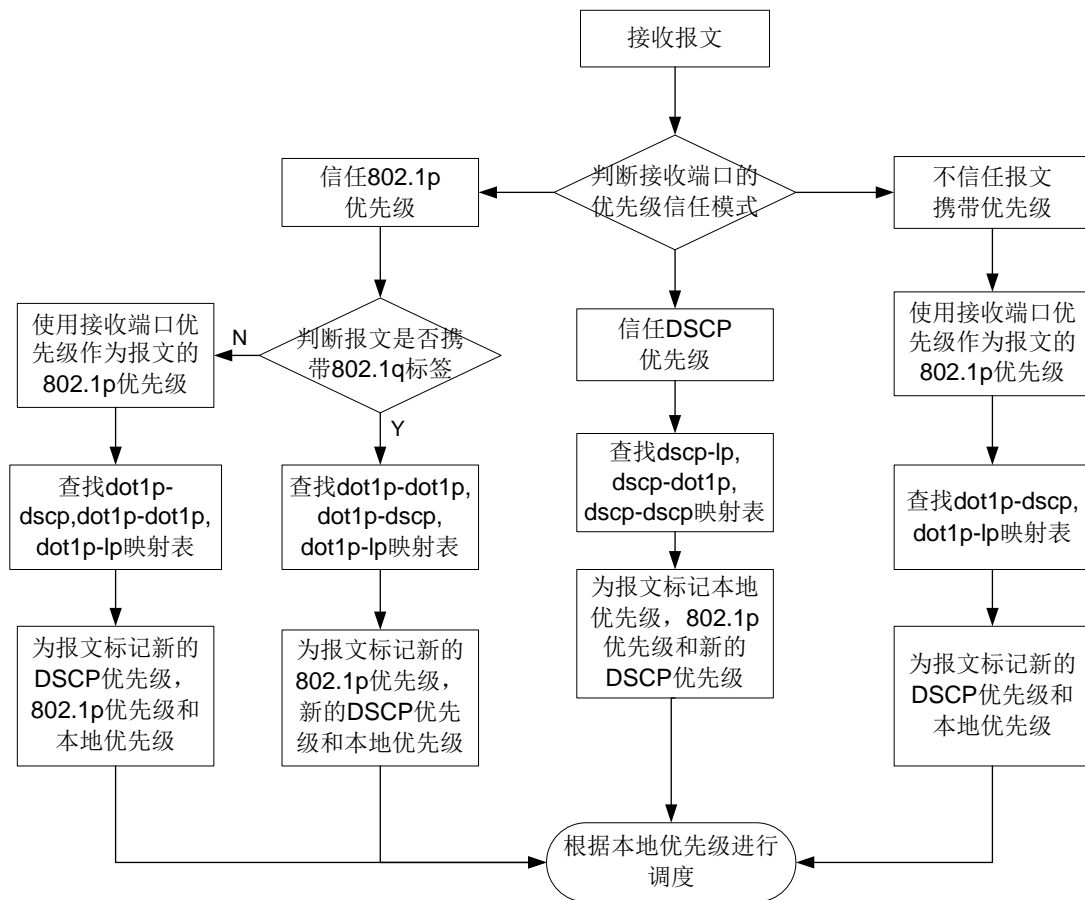
通常情况下，报文可能会携带有多种优先级，设备在进行优先级映射时，需要首先确定采用哪种优先级作为参考，再通过优先级映射表映射出调度优先级。优先级信任模式就是用来指定设备进行优先级映射时作为参考的报文携带优先级，本系列交换机支持以下三种优先级信任模式：

- 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。

3.1.4 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



 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

我们常用的方式有三种：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。

如果配置了优先级信任模式，即表示设备信任当前进来流量的报文优先级，会自动解析报文的优先级或者标志位，然后按照映射表映射到报文的优先级参数。

如果没有配置优先级信任模式，并且配置了端口优先级值，则表明设备不信任所接收报文的优先级，而是使用端口优先级，按照映射表映射到报文的优先级参数。

建议进行各项配置的时候先整体规划网络 QoS。

表3-2 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

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

表3-3 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-dot1p dot1p-dscp dot1p-lp dscp-dot1p dscp-dscp dscp-lp }	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 配置端口优先级信任模式

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3-4 配置端口优先级信任模式

操作	命令	说明
进入系统视图	system-view	-

操作		命令	说明
进入以太网端口视图或端口组视图	进入以太网端口视图	interface <i>interface-type interface-number</i>	二者必选其一 进入端口视图后，下面进行的配置只在当前接口生效；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 <i>port-group-name</i>	
配置端口信任报文的DSCP优先级		qos trust dscp	三者选其一 缺省情况下，设备不信任报文携带的优先级
配置信任报文的802.1p优先级		qos trust dot1p	
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3-5 配置端口优先级

操作		命令	说明
进入系统视图		system-view	-
进入以太网端口视图或端口组视图	进入以太网端口视图	interface <i>interface-type interface-number</i>	二者必选其一 进入端口视图后，下面进行的配置只在当前接口生效；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 <i>port-group-name</i>	
配置端口优先级		qos priority <i>priority-value</i>	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3-6 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 [<i>dot1p-dot1p</i> <i>dot1p-dscp</i> <i>dot1p-lp</i> <i>dscp-dot1p</i> <i>dscp-dscp</i> <i>dscp-lp</i>]
显示端口优先级信任模式信息	display qos trust interface [<i>interface-type interface-number</i>] [[{ <i>begin</i> <i>exclude</i> <i>include</i> } <i>regular-expression</i>]

3.5 优先级映射典型配置举例

3.5.1 优先级映射配置举例

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。

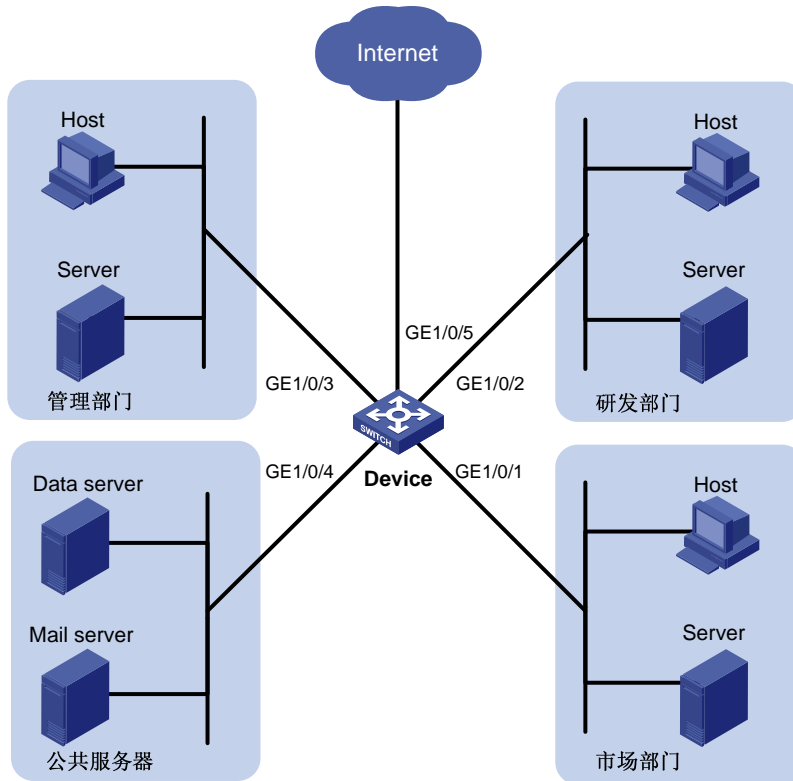
实现如下需求：

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映射到本地优先级 6，放入出队列 3 中优先进行处理；
- 通过优先级映射将管理部门发出的报文映射到本地优先级 4，放入出队列 2 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映射到本地优先级 2，放入出队列 1 中最后进行处理。

2. 组网图

图3-2 优先级映射配置举例组网图



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-1p] import 4 export 6
[Device-maptbl-dot1p-1p] import 5 export 4
[Device-maptbl-dot1p-1p] 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。

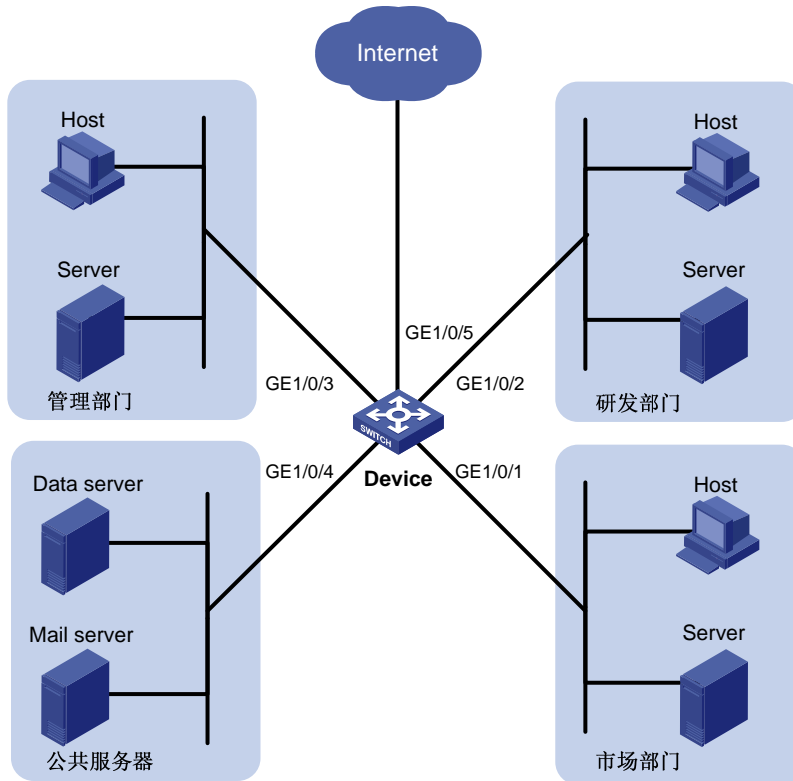
- 通过优先级映射将研发部门发出的报文映射到本地优先级 6，放入出队列 3 中优先进行处理；
- 通过优先级映射将管理部门发出的报文映射到本地优先级 4，放入出队列 2 中次优先进行处理；
- 通过优先级映射将市场部门发出的报文映射到本地优先级 2，放入出队列 1 中最后进行处理。

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，进入队列 3 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，进入队列 2 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，进入队列 1 最后进行处理。

2. 组网图

图3-3 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 流量整形和端口限速配置

4.1 流量整形



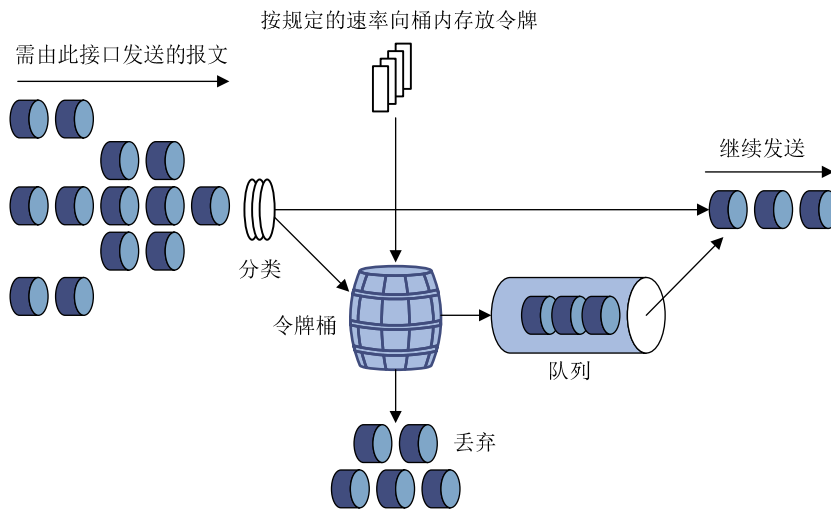
说明

流量整形只针对设备的出方向。

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。

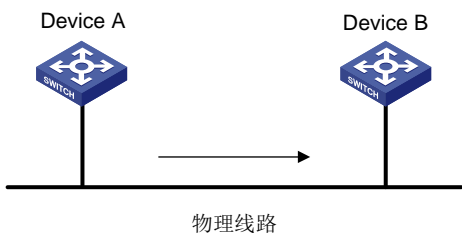
流量整形与流量监管的主要区别在于，流量整形对流量监管中需要丢弃的报文进行缓存——通常是把它们放入缓冲区或队列内，如 [图 4-1](#) 所示。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

图4-1 流量整形示意图



例如，在 [图 4-2](#) 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，对超出规格流量直接丢弃。

图4-2 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。

4.2 端口限速



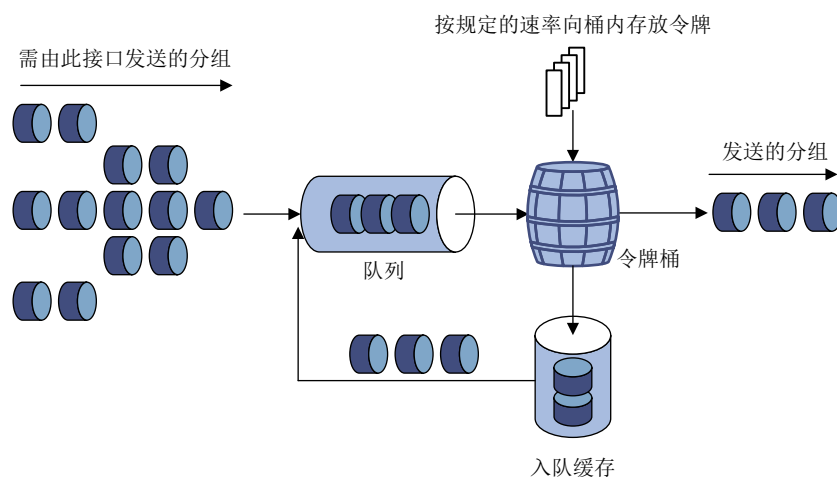
说明

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4-3 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。

4.3 流量整形配置

本系列交换机的流量整形可以通过以下两种方式配置：

- 基于队列的流量整形：针对某一个队列的数据包设置整形参数。
- 适配所有流的流量整形：为所有的流设置整形参数。

如果一个端口下同时配置了两种方式的流量整形，则设备在处理数据流时，将比较基于数据流所在队列和基于所有流的两条流量整形配置，选择 CIR 值较小的配置对数据流进行整形。

4.3.1 配置基于队列的流量整形

表4-1 基于队列的流量整形配置

操作		命令	说明
进入系统视图		system-view	-
进入端口视图或端口组视图	进入端口视图	interface <i>interface-type interface-number</i>	二者必选其一 进入端口视图后，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 <i>port-group-name</i>	
在端口配置流量整形		qos gts queue <i>queue-number cir committed-information-rate</i> [cbs <i>committed-burst-size</i>]	必选

4.3.2 配置适配所有流的流量整形

表4-2 适配所有流的流量整形配置

操作		命令	说明
进入系统视图		system-view	-
进入端口视图或端口组视图	进入端口视图	interface <i>interface-type interface-number</i>	二者必选其一 进入端口视图后，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 <i>port-group-name</i>	
在端口配置流量整形		qos gts any cir <i>committed-information-rate</i> [cbs <i>committed-burst-size</i>]	必选

4.4 端口限速配置

4.4.1 端口限速配置过程

配置端口限速就是限制接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	-
进入以太网端口视图或端口组视图	进入以太网端口视图	interface <i>interface-type interface-number</i>	二者必选其一 进入端口视图后，下面进行的配置只在当前接口生效；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 <i>port-group-name</i>	

操作	命令	说明
配置端口限速	qos lr { inbound outbound } cir <i>committed-information-rate</i>	必选

4.4.2 端口限速配置举例

把端口 GigabitEthernet1/0/1 的出速度限制为 1280kbps。

进入系统视图。

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

进入端口视图。

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

配置限速参数，端口出速率限制为 1280kbps。

```
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 1280
```

4.5 流量整形/端口限速显示和维护

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 [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]
显示端口限速配置和统计信息	display qos lr interface [<i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]

5 拥塞管理配置

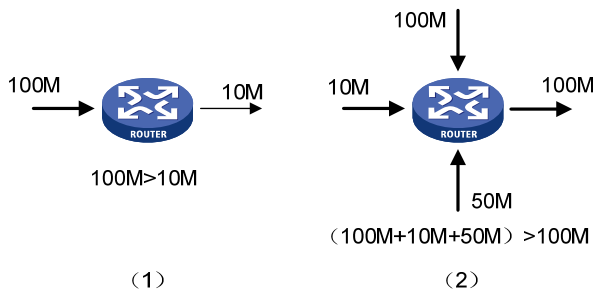
5.1 拥塞管理简介

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

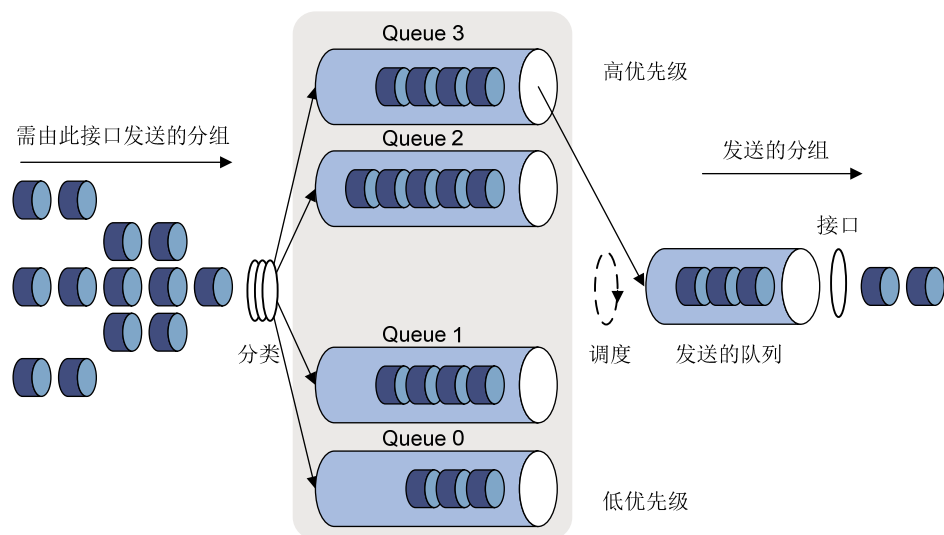
对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级别算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

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。本系列交换机的端口上共有编号分别为 3、2、1、0 的四个队列，其中分别包含了本地优先级为 6~7、4~5、2~3 和 0~1 的报文。

这里介绍三种常用的队列调度方式：严格优先级 SP (Strict-Priority) 队列、加权轮询 WRR (Weighted Round Robin) 队列和 SP+WRR 队列。

1. SP队列

图5-2 SP 队列示意图



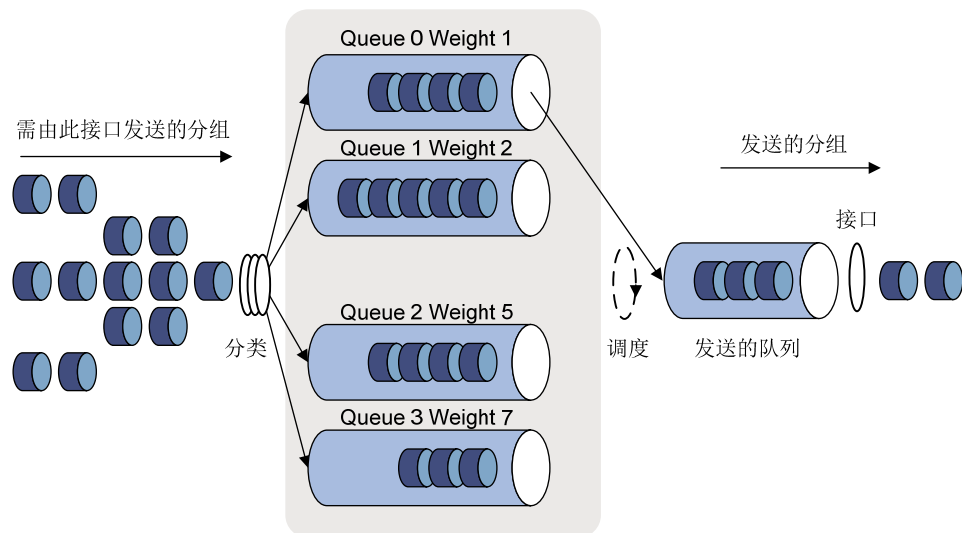
SP队列是针对关键业务类型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以图5-2为例，优先队列将端口的4个输出队列分成4类，依次为3、2、1、0队列，它们的优先级依次降低。

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



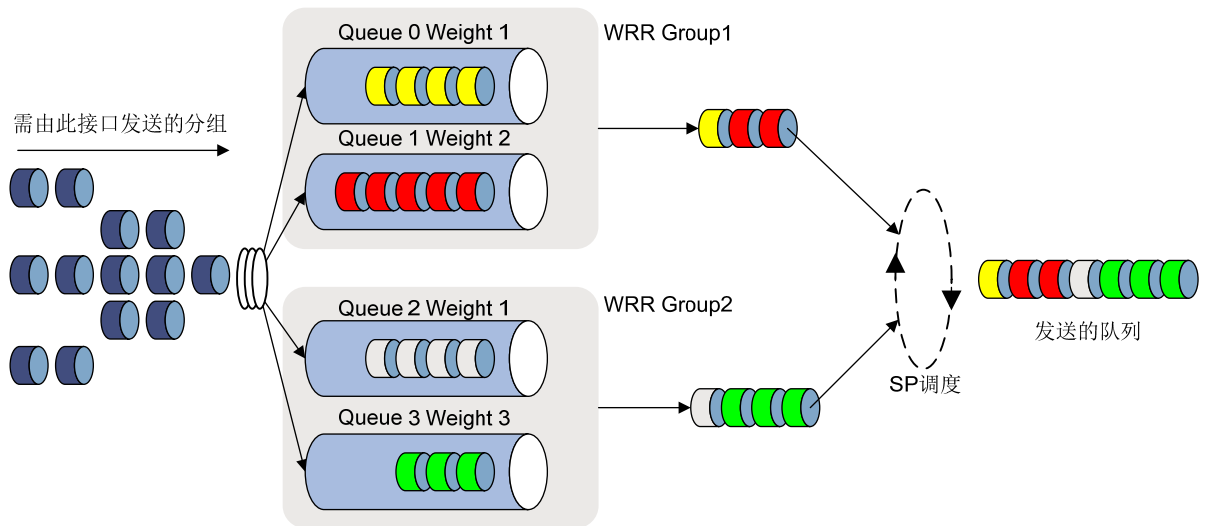
WRR 队列在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 4 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w_3 、 w_2 、 w_1 、 w_0 ），加权值表示获取资源的比重。如一个 100Mbps 的端口，配置它的 WRR 队列的加权值为 50、25、25、25（依次对应 w_3 、 w_2 、 w_1 、 w_0 ），这样可以保证最低优先级队列至少获得 20Mbps 的带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

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。

本系列交换机支持的 WRR 队列为分组 WRR 队列，用户可以根据需要将输出队列划分为 WRR 队列组 1 和 WRR 队列组 2。进行队列调度时，两个调度组先按照队列权重配置对各自组内的队列进行调度，两组调度的结果之间再按照 SP 队列算法进行调度。

例如，将队列 0 和 1 加入 WRR 队列组 1，权重分别为 1 和 2；将队列 2 和 3 加入 WRR 队列组 2，权重分别为 1 和 3，调度过程如 [图 5-4](#) 所示：

图5-4 两个 WRR 组实现队列调度示意图

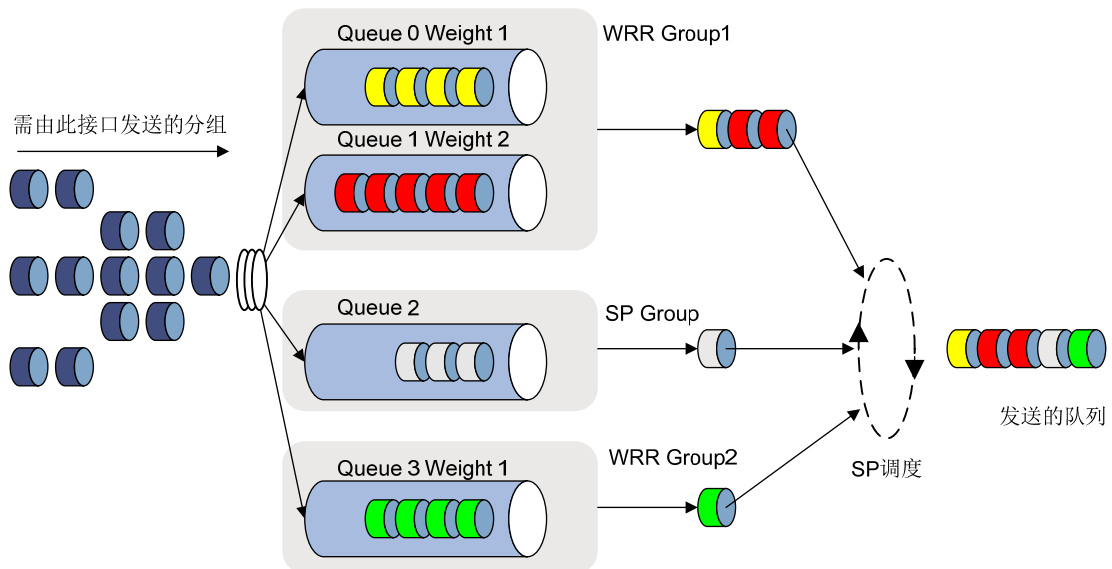


3. SP+WRR队列

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（WRR 有两个调度组：group 1 和 group 2），实现 SP+WRR 的调度功能。在队列调度时，两个 WRR 调度组先按照队列权重的配置对各自组内的队列进行调度，完成后，两组调度结果再与 SP 组之间使用 SP 算法进行队列调度。

例如，将队列 0 和 1 加入 WRR 队列组 1，权重分别为 1 和 2；将队列 3 加入 WRR 队列组 2，权重为 1；将队列 2 加入 SP 队列组，调度过程如 [图 5-5](#) 所示：

图5-5 SP+WRR 队列调度示意图



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	可选	5.3.1
配置WRR队列	可选	5.3.2
配置SP+WRR队列	可选	5.3.3

5.3 拥塞管理配置

5.3.1 配置SP队列

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	-
进入端口视图 或端口组视图	interface <i>interface-type</i> <i>interface-number</i>	二者必选其一 进入端口视图后，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
	port-group manual <i>port-group-name</i>	
配置SP队列	undo qos wrr	可选 缺省情况下，端口使用SP队列进行调度

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] undo qos wrr
```

5.3.2 配置WRR队列

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	-
进入端口视图或端口组视图	进入以太网端口视图 interface interface-type interface-number	二者必选其一 进入端口视图后，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WRR队列	qos wrr queue-id group group-id weight schedule-value	必选 缺省情况下，端口使用SP队列进行调度
显示WRR队列的配置	display qos wrr interface [interface-type interface-number]	可选 display 命令可以在任意视图下执行



说明

为保证 WRR 队列能够按用户配置的权重按比例进行调度，在使用 WRR 分组调度时，建议在各个 WRR 组中加入编号连续的队列。

2. 配置举例

(1) 组网需求

- 配置端口 GigabitEthernet 1/0/1 上的队列为 WRR 队列
- 配置队列 0、1 属于为 WRR 分组 1，权重分别为 10、20
- 配置队列 2、3 属于为 WRR 分组 2，权重分别为 30、50

(2) 配置步骤

进入系统视图。

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

配置 GigabitEthernet1/0/1 的 WRR 队列。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 10
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group 1 weight 20
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group 2 weight 30
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group 2 weight 50
```


5.3.3 配置SP+WRR队列

1. 配置过程

表5-4 SP+WRR 队列配置过程

操作		命令	说明
进入系统视图		system-view	-
进入端口视图或端口组视图	进入以太网端口视图	interface <i>interface-type</i> <i>interface-number</i>	二者必选其一 进入端口视图后，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 <i>port-group-name</i>	
配置SP队列		qos wrr <i>queue-id</i> group sp	必选
配置WRR队列		qos wrr <i>queue-id</i> group <i>group-id</i> weight <i>schedule-value</i>	必选



说明

为保证 WRR 队列能够按用户配置的权重按比例进行调度，在使用 SP+WRR 调度方式时，建议在 WRR 组中加入编号连续的队列。

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 队列属于 SP 调度组
- 配置端口 GigabitEthernet 1/0/1 上的 1 队列属于 WRR 调度组 1，权重为 20
- 配置端口 GigabitEthernet 1/0/1 上的 2、3 队列属于 WRR 调度组 2，权重分别为 10、50

(2) 配置步骤

进入系统视图。

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

配置 GigabitEthernet1/0/1 的 SP+WRR 队列。

```
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp  
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group 1 weight 20  
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group 2 weight 10  
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group 2 weight 50
```

6 流量过滤配置

6.1 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 地址或某个 MAC 地址发送的报文通过，也可以通过 ACL 时间段来实现定期执行的流量过滤动作。



说明

用户也可以选择通过在端口应用 ACL 的方式来实现流量过滤功能，详细的介绍和配置请参见“ACL 配置”。

6.2 配置流量过滤

表6-1 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 <i>tcl-name</i> [operator { and or }]	-	
定义匹配数据包的规则	if-match <i>match-criteria</i>	-	
退出类视图	quit	-	
定义一个流行为并进入流行为视图	traffic behavior <i>behavior-name</i>	-	
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 <i>policy-name</i>	-	
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>	-	
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	-

操作	命令	说明
显示流量过滤的相关配置信息	display traffic behavior user-defined [<i>behavior-name</i>] [{ begin exclude include } <i>regular-expression</i>]	可选 display 命令可以在任意视图下执行



说明

由于丢弃数据包的动作与对数据包采取其它操作的动作之间存在冲突，因此，如果在流行为中同时配置了 **filter deny** 命令和其他动作，则引用该流行为的策略不能成功下发。

6.3 流量过滤配置举例

6.3.1 流量过滤配置举例

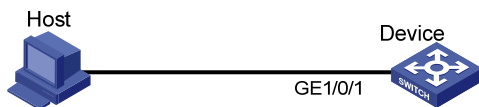
1. 组网需求

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6-1 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
```

7 重标记配置

7.1 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。

7.2 配置重标记

表7-1 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 <i>tcl-name</i> [operator { and or }]	-
定义匹配数据包的规则	if-match <i>match-criteria</i>	-
退出类视图	quit	-
定义一个流行为并进入流行为视图	traffic behavior <i>behavior-name</i>	-
配置标记报文的DSCP值	remark dscp <i>dscp-value</i>	可选
配置标记报文的802.1p优先级	remark dot1p <i>8021p</i>	可选
配置标记报文的IP优先级值	remark ip-precedence <i>ip-precedence-value</i>	可选
配置标记报文的本地优先级	remark local-precedence <i>local-precedence</i>	可选
重标记运营商VLAN ID	remark service-vlan-id <i>vlan-id</i>	可选
退出流行为视图	quit	-
定义策略并进入策略视图	qos policy <i>policy-name</i>	-
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>	-
退出策略视图	quit	-
应用QoS	基于端口	2.2.4 1. 基于端口应用QoS策略

操作		命令	说明
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	-
显示重标记的相关配置信息		display traffic behavior user-defined [<i>behavior-name</i>] [{ begin exclude include } <i>regular-expression</i>]	可选 display 命令可以在任意视图下执行

7.3 重标记配置举例

7.3.1 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：

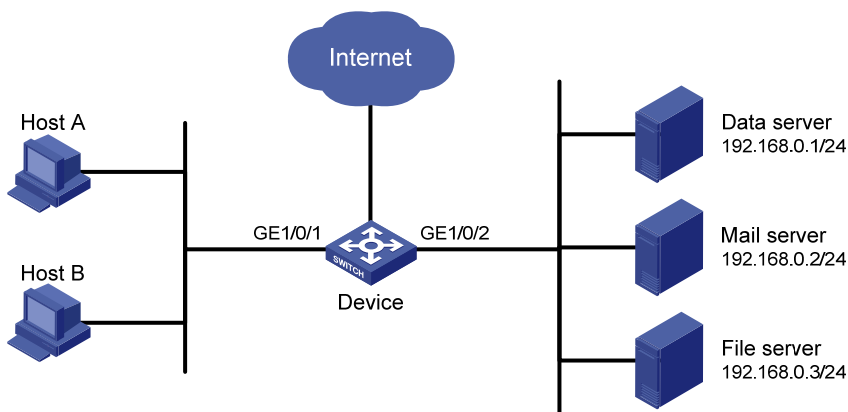
- Host A 和 Host B 通过端口 GigabitEthernet1/0/1 接入 Device；
- 数据库服务器、邮件服务器和文件服务器通过端口 GigabitEthernet1/0/2 接入 Device。

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7-1 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 6。
[Device] traffic behavior behavior_dbserver
[Device-behavior-behavior_dbserver] remark local-precedence 6
[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 4。
[Device] traffic behavior behavior_mserver
[Device-behavior-behavior_mserver] remark local-precedence 4
[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 流量重定向配置

8.1 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。

本系列交换机支持将流量重定向到指定端口，当收到需要由某个端口处理的报文时，可以通过此配置将报文重定向到此端口。流量重定向只针对二层转发报文。

8.2 配置流量重定向

表8-1 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 <i>tcl-name</i> [operator { and or }]	-	
定义匹配数据包的规则	if-match <i>match-criteria</i>	-	
退出类视图	quit	-	
定义一个流行为并进入流行为视图	traffic behavior <i>behavior-name</i>	必选	
配置流量重定向动作	redirect interface <i>interface-type</i> <i>interface-number</i>	必选 用户可根据需要选择重定向的方向	
退出流行为视图	quit	-	
定义策略并进入策略视图	qos policy <i>policy-name</i>	-	
在策略中为类指定采用的流行为	classifier <i>tcl-name</i> behavior <i>behavior-name</i>	-	
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	-

9 Burst功能配置

9.1 Burst功能简介

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设备，由低速链路转发出去；或者报文从相同速率的多个接口同时进入设备，由一个相同速率的接口转发出去。

用户可以通过使能 Burst 功能，降低设备在上述特定环境中的报文丢包率，提高对报文的处理能力。需要注意的是，使能 Burst 功能后，设备的 QoS 性能可能会受到影响，建议用户根据自己的具体网络环境进行配置。

9.2 配置Burst功能

9.2.1 配置准备

已确定实际网络环境需要启动 Burst 功能。

9.2.2 配置过程

表9-1 配置 Burst 功能

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

9.3 Burst功能配置举例

9.3.1 Burst功能配置举例

1. 组网需求

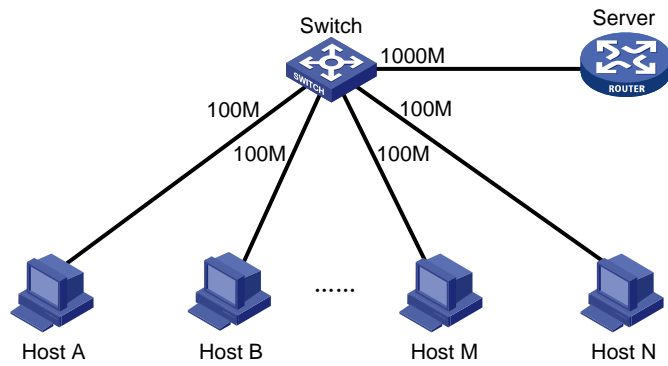
用户网络描述如下：

- Server 通过 1000Mbps 以太网接口接入 Switch，Server 会不定时发送大流量的广播或者组播报文给 Host。
- Host 通过 100Mbps 以太网卡接入 Switch。

通过 Switch 对 Server 发出的大流量报文进行处理，保证报文可以到达 Host。

2. 组网图

图9-1 配置 Burst 功能组网图



3. 配置步骤

进入系统视图。

```
<Switch> system-view
```

配置 Burst 功能。

```
[Switch] burst-mode enable
```

10 附录 A 缺省优先级映射表



说明

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

表10-1 dot1p-ip、dot1p-dscp 缺省映射关系

映射输入索引	dot1p-ip 映射	dot1p-dscp 映射
802.1p 优先级(dot1p)	本地优先级(ip)	dscp
0	2	0
1	0	8
2	1	16
3	3	24
4	4	32
5	5	40
6	6	48
7	7	56

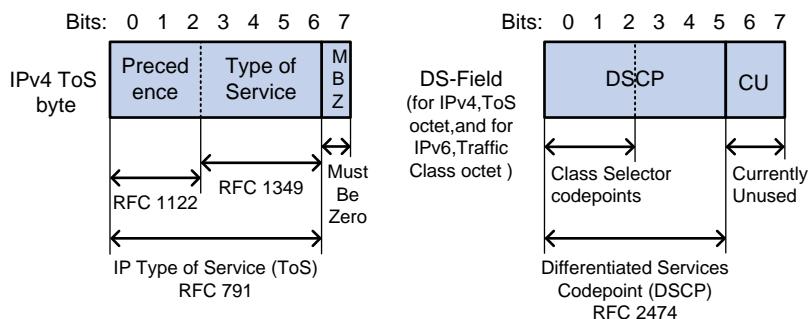
表10-2 dscp-ip、dscp-dot1p 缺省映射关系

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

11 附录 B 各种优先级介绍

11.1 IP优先级和DSCP优先级

图11-1 ToS 和 DS 域



如 图 11-1 所示，IPv4 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；IPv6 报文头的Traffic Classes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IPv4 报文头部的ToS域和IPv6 报文头部的Traffic Classes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11-1 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11-2 DSCP 优先级说明

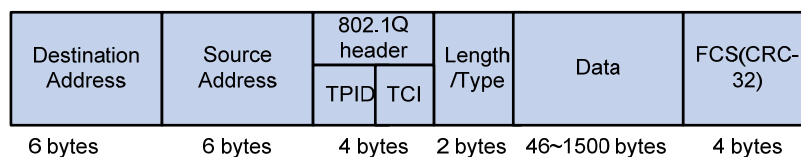
DSCP 优先级（十进制）	DSCP 优先级（二进制）	关键字
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13

DSCP 优先级（十进制）	DSCP 优先级（二进制）	关键字
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)

11.2 802.1p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11-2 带有 802.1Q 标签头的以太网帧



如 [图 11-2](#) 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 11-3](#) 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11-3 802.1Q 标签头

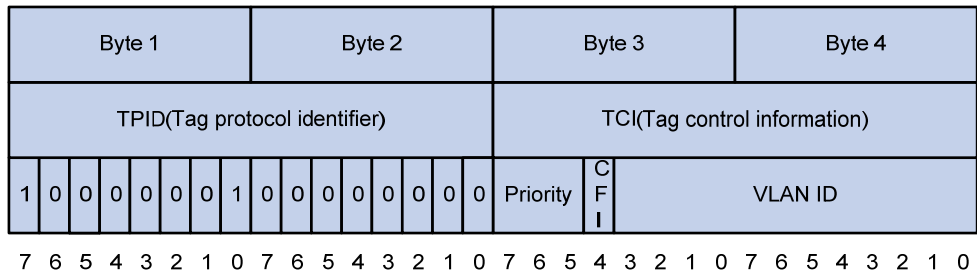


表11-3 802.1p 优先级说明

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