H3C S5500-HI 系列以太网交换机

ACL 和 QoS 配置指导

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W102-20131220
产品版本：Release 52xx 系列

前 言

H3C S5500-HI 系列以太网交换机配置指导共分为十一本手册，介绍了 S5500-HI 系列以太网交换机 Release52xx 系列软件版本各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《ACL 和 QoS 配置指导》主要介绍 ACL 和 QoS 技术的原理和配置，包括创建 IPv4 ACL 和 IPv6 ACL，通过 ACL 进行报文过滤、使用 QoS 策略对流量进行控制，以及端口限速、拥塞管理、流量重标记等常用的 QoS 技术。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

新增及修改特性说明

本手册对应 S5500-HI 系列以太网交换机的 Release52xx 系列软件版本，各版本间特性差异如下：

- Release5206 与 Release5203 版本相比，无新增、修改特性。
- Release5203 与Release5101 版本相比，新增、修改了部分特性，具体请参见 表 1。

表1 Release5203 与 Release5101 版本间特性差异

配置指导	新增及修改特性
ACL	新增特性：报文过滤高级日志功能
QoS	新增特性：显示端口队列统计信息
HQoS	无

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

产品配套资料

H3C S5500-HI 系列以太网交换机的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	产品彩页	帮助您了解产品的主要规格参数及亮点
	技术白皮书	帮助您了解产品和特性功能，对于特色及复杂技术从细节上进行介绍
硬件介绍及安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	H3C 设备防雷安装指导手册	帮助您了解防雷接地设计和工程安装方法，以保证交换机具有良好的抗雷击性能
	快速安装指南	指导您对设备进行初始安装，通常针对最常用的情况，减少您的检索时间
	安装指导	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
	风扇安装手册	帮助您了解产品支持的可插拔风扇模块的外观、功能、规格、安装及拆卸方法
	电源手册	帮助您了解产品支持的可插拔电源模块的外观、功能、规格、安装及拆卸方法
	RPS电源用户手册	帮助您了解产品支持的RPS电源的外观、功能、规格
	H3C低端系列以太网交换机RPS电源选购指南	帮助您了解各种RPS电源适用的交换机产品型号及RPS电源配套电缆的相关规格
	接口模块扩展卡用户手册	帮助您了解该接口模块扩展卡的外观、规格、安装及拆卸方法
	H3C低端系列以太网交换机可插拔模块手册	帮助您了解产品支持的可插拔模块类型、外观和规格
	H3C可插拔SFP[SFP+][XFP]模块安装指南	帮助您掌握SFP/SFP+/XFP模块的正确安装方法，避免因操作不当而造成器件损坏

大类	资料名称	内容介绍
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	详细介绍设备的命令，相当于命令字典，方便您查阅各个命令的功能
运行维护	故障处理手册	指导您快速定位并处理软件故障
	版本说明书	帮助您了解产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

010-62982107

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL配置

说明

本文将用于 IPv4 和 IPv6 的 ACL 分别简称为 IPv4 ACL 和 IPv6 ACL。若非特别指明，本文所指的 ACL 均包括 IPv4 ACL 和 IPv6 ACL。

1.1 ACL简介

1.1.1 ACL概述

ACL（Access Control List，访问控制列表）是一或多条规则的集合，用于识别报文流。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。网络设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

1.1.2 ACL在交换机上的应用方式

当 ACL 被其他功能引用时，根据设备在实现该功能时的处理方式（硬件处理或者软件处理），ACL 可以被分为基于硬件的应用和基于软件的应用。

典型的基于硬件的应用包括：报文过滤、QoS 策略；基于软件的应用包括：路由、对登录用户（Telnet、SNMP、WEB）进行控制等。

在某些应用方式下（例如 QoS 策略），ACL 仅用于匹配报文，ACL 规则中的动作（**deny** 或 **permit**）被忽略，不作为对报文进行丢弃或转发的依据，类似情况请参见相应功能中的说明。

说明

- 当 ACL 被 QoS 策略引用进行流分类时，如果报文没有与 ACL 中的规则匹配，此时交换机不会使用流行为中定义的动作对此类报文进行处理。
- 当 ACL 被用于对 Telnet、SNMP 和 WEB 登录用户进行控制时，如果报文没有与 ACL 中的规则匹配，此时交换机对此类报文采取的动作为 deny，即拒绝报文通过。
- 关于应用ACL对报文进行过滤的介绍和配置，请参见 1.3.6 应用ACL进行报文过滤。

1.1.3 ACL的编号和名称

用户在创建ACL时必须为其指定编号，不同的编号对应不同类型的ACL，如 表 1-1 所示；同时，为了便于记忆和识别，用户在创建ACL时还可选择是否为其设置名称。ACL一旦创建，便不允许用户再为其设置名称、修改或删除其原有名称。

当 ACL 创建完成后，用户就可以通过指定编号或名称的方式来指定该 ACL，以便对其进行操作。

说明

二层 ACL 的编号和名称全局唯一；IPv4 基本和高级 ACL 的编号和名称只在 IPv4 中唯一；IPv6 基本和高级 ACL 的编号和名称也只在 IPv6 中唯一。

1.1.4 ACL的分类

根据规则制订依据的不同，可以将ACL分为如 表 1-1 所示的几种类型。

表1-1 ACL 的分类

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
基本ACL	2000～2999	IPv4	报文的源IP地址
		IPv6	报文的源IPv6地址
高级ACL	3000～3999	IPv4	报文的源IP地址、目的IP地址、报文优先级、IP承载的协议类型及特性等三、四层信息
		IPv6	报文的源IPv6地址、目的IPv6地址、报文优先级、IPv6承载的协议类型及特性等三、四层信息
二层ACL	4000～4999	IPv4和IPv6	报文的源MAC地址、目的MAC地址、802.1p优先级、链路层协议类型等二层信息

1.1.5 ACL的规则匹配顺序

由于 ACL 中每条规则的报文匹配条件不同，导致这些规则之间可能存在重复甚至矛盾的地方，因此在将一个报文与 ACL 的各条规则进行匹配时，需要有明确的匹配顺序来确定规则执行的优先级，一旦匹配上某条规则就不会再继续匹配下去，系统将依据该规则对该报文执行相应的操作。ACL 的规则匹配顺序有以下两种：

- 配置顺序：按照规则编号由小到大进行匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，各类型ACL的“深度优先”排序法则如 表 1-2 所示。

表1-2 各类型 ACL 的“深度优先”排序法则

ACL 类型	“深度优先”排序法则
IPv4基本ACL	(1) 先判断规则中是否携带有 VPN 实例，携带 VPN 实例者优先 (2) 如果 VPN 实例的携带情况相同，再比较源 IPv4 地址范围，范围较小者优先 (3) 如果源 IP 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv4高级ACL	(1) 先判断规则中是否携带有 VPN 实例，携带 VPN 实例者优先 (2) 如果 VPN 实例的携带情况相同，再比较协议范围，指定有 IPv4 承载的协议类型者优先 (3) 如果协议范围也相同，再比较源 IPv4 地址范围，较小者优先 (4) 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先 (5) 如果目的 IPv4 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号范围，较小者优先 (6) 如果四层端口号范围也相同，再比较配置的先后次序，先配置者优先

ACL 类型	“深度优先”排序法则
IPv6基本ACL	(1) 先判断规则中是否携带有 VPN 实例，携带 VPN 实例者优先 (2) 如果 VPN 实例的携带情况相同，再比较源 IPv6 地址范围，范围较小者优先 (3) 如果源 IPv6 地址范围也相同，再比较配置的先后次序，先配置者优先
IPv6高级ACL	(1) 先判断规则中是否携带有 VPN 实例，携带 VPN 实例者优先 (2) 如果 VPN 实例的携带情况相同，再比较协议范围，指定有 IPv6 承载的协议类型者优先 (3) 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 (4) 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 (5) 如果目的 IPv6 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号范围，较小者优先 (6) 如果四层端口号范围也相同，再比较配置的先后次序，先配置者优先
二层ACL	(1) 先比较源 MAC 地址范围，较小者优先 (2) 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 (3) 如果目的 MAC 地址范围也相同，再比较配置的先后次序，先配置者优先

说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少：“0”位越多，范围越小。通配符掩码（又称反向掩码）以点分十进制表示，并以二进制的“0”表示“匹配”，“1”表示“不关心”，这与子网掩码恰好相反，譬如子网掩码 255.255.255.0 对应的通配符掩码就是 0.0.0.255。此外，通配符掩码中的“0”或“1”可以是不连续的，这样可以更加灵活地进行匹配，譬如 0.255.0.255 就是一个合法的通配符掩码。
- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

1.1.6 ACL的规则描述和注释

在一个 ACL 中用户可以创建多条规则，为了方便标识这些规则的用途，用户可以为单条规则添加描述信息，也可以在各条规则之间插入注释信息来对前一段或后一段规则进行统一描述。

1. 规则描述信息

规则描述信息主要用于对单条规则进行单独标识。当需要对各条规则进行不同的标识或对某条规则进行特别标识时，适用此方式。

2. 规则注释信息

规则注释信息主要用于对一段规则进行统一标识。当需要对一段规则进行相同的标识时，如果采用对每条规则都添加相同描述信息的方式，需要进行大量配置，效率会非常低下。在这种情况下，可以在这段规则的前、后插入注释信息的方式来提高标识效率，即：在这段规则的首条规则之前以及末条规则之后分别插入一条注释信息，通过首、尾这两条注释信息就可以标识整段规则的用途。

说明

在不同的规则匹配顺序下，“首条规则”和“末条规则”的确定方法不同：

- 在配置顺序下：规则的显示将按照规则编号由小到大排列，因此应通过规则的编号来确定；
- 在自动排序下：规则的显示将按照“深度优先”原则由深到浅排列，因此应通过“深度优先”原则来确定。

1.1.7 ACL的步长

ACL 中的每条规则都有自己的编号，这个编号在该 ACL 中是唯一的。在创建规则时，可以手工为其指定一个编号，如未手工指定编号，则由系统为其自动分配一个编号。由于规则的编号可能影响规则匹配的顺序，因此当由系统自动分配编号时，为了方便后续在已有规则之前插入新的规则，系统通常会在相邻编号之间留下一定的空间，这个空间的大小（即相邻编号之间的差值）就称为 ACL 的步长。譬如，当步长为 5 时，系统会将编号 0、5、10、15……依次分配给新创建的规则。

系统为规则自动分配编号的方式如下：系统从 0 开始，按照步长自动分配一个大于现有最大编号的最小编号。譬如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，此时如果创建一条规则且不指定编号，那么系统将自动为其分配编号 15。

如果步长发生了改变，ACL 内原有全部规则的编号都将自动从 0 开始按新步长重新排列。譬如，某 ACL 内原有编号为 0、5、9、10 和 15 的五条规则，当修改步长为 2 之后，这些规则的编号将依次变为 0、2、4、6 和 8。

1.1.8 ACL对分片报文的处理

传统的报文过滤并不处理所有的分片报文，只对首个分片进行匹配处理，而对后续分片一律放行。这样，网络攻击者可以构造后续的分片报文进行流量攻击，从而带来了安全隐患。为提高网络安全性，ACL 规则缺省会匹配所有的非分片报文以及分片报文的每个分片。同时，为了提高匹配效率，用户也可以对此匹配策略进行修改，譬如可指定规则仅对非首片分片报文有效等。

1.2 ACL配置任务简介

表1-3 ACL 配置任务简介

配置任务	说明	详细配置
配置ACL的生效时间段	可选 本配置任务适用于IPv4和IPv6	1.3.1
配置IPv4基本ACL	至少选择一项	1.3.2 1.
配置IPv6基本ACL		1.3.2 2.
配置IPv4高级ACL		1.3.3 1.
配置IPv6高级ACL		1.3.3 2.
配置二层ACL		1.3.4

配置任务	说明	详细配置
复制ACL	可选 本配置任务适用于IPv4和IPv6	1.3.5
应用ACL进行报文过滤	可选 本配置任务适用于IPv4和IPv6	1.3.6

1.3 配置ACL

1.3.1 配置ACL的生效时间段

当 ACL 规则只需在某个或某些特定的时间段内生效时，可以设置基于时间段的 ACL 过滤。为此，用户可以先配置一个或多个时间段，然后在规则中引用这些时间段，那么该规则将只在指定的时间段内生效。ACL 的生效时间段可分为以下两种：

- 周期时间段：表示规则以一周为周期（如每周一的 8 至 12 点）循环生效。
- 绝对时间段：表示规则在指定时间范围内（如 2011 年 1 月 1 日 8 点至 2011 年 1 月 3 日 18 点）生效。

用户使用同一名称可以配置内容不同的多条时间段，所配置的各周期时间段之间以及各绝对时间段之间分别取并集之后，各并集的交集将成为最终生效的时间范围。

表1-4 配置 ACL 的生效时间段

操作	命令	说明
进入系统视图	**system-view**	-
创建时间段	**time-range** *time-range-name* { *start-time* **to** *end-time* *days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }	必选 缺省情况下，不存在任何时间段

说明

用户最多可以创建 256 个不同名称的时间段，而同一名称下最多可以配置 32 条周期时间段和 12 条绝对时间段。

1.3.2 配置基本ACL

1. 配置IPv4 基本ACL

IPv4 基本 ACL 根据报文的源 IP 地址来制订规则，对 IPv4 报文进行匹配。

表1-5 配置 IPv4 基本 ACL

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建IPv4基本ACL，并进入IPv4基本ACL视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何ACL IPv4基本ACL的编号范围为2000～2999
配置ACL的描述信息	**description** *text*	可选 缺省情况下，ACL没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	必选 缺省情况下，IPv4基本ACL内不存在任何规则 需要注意的是： • 当 IPv4 基本 ACL 被 QoS 策略引用对报文进行流分类时，不支持配置 **vpn-instance** 参数，在规则中配置的 **logging** 和 **counting** 参数不会生效 • 当 IPv4 基本 ACL 被用于报文过滤时，不支持配置 **vpn-instance** 参数
为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
配置规则注释信息	**rule** [*rule-id*] **remark** *text*	可选 缺省情况下，ACL内没有任何规则注释信息
使能基于硬件应用的ACL的规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的ACL的规则匹配统计功能处于关闭状态 当ACL被QoS策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建 IPv4 基本 ACL 时为其指定了名称，则也可以使用 **acl name** *acl-name* 命令通过指定名称的方式进入其视图。

2. 配置IPv6 基本ACL

IPv6 基本 ACL 根据报文的源 IPv6 地址来制订规则，对 IPv6 报文进行匹配。

表1-6 配置 IPv6 基本 ACL

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建IPv6基本ACL，并进入IPv6基本ACL视图	**acl ipv6 number** *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何ACL IPv6基本ACL的编号范围为2000～2999
配置ACL的描述信息	**description** *text*	可选 缺省情况下，ACL没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	必选 缺省情况下，IPv6基本ACL内不存在任何规则 需要注意的是： • 当IPv6基本ACL被QoS策略引用对报文进行流分类时，不支持配置 **fragment**、**routing** 和 **vpn-instance** 参数，在规则中配置的 **logging** 和 **counting** 参数不会生效 • 当IPv6基本ACL被用于报文过滤时，不支持配置 **fragment**、**routing** 和 **vpn-instance** 参数
为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
配置规则注释信息	**rule** [*rule-id*] **remark** *text*	可选 缺省情况下，ACL内没有任何规则注释信息
使能基于硬件应用的ACL的规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的ACL的规则匹配统计功能处于关闭状态 当ACL被QoS策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建IPv6基本ACL时为其指定了名称，则也可以使用 **acl ipv6 name** *acl6-name* 命令通过指定名称的方式进入其视图。

1.3.3 配置高级ACL

1. 配置IPv4 高级ACL

IPv4 高级 ACL 可根据报文的源 IP 地址、目的 IP 地址、报文优先级、IP 承载的协议类型及特性（如 TCP/UDP 的源端口和目的端口、TCP 报文标识、ICMP 协议的消息类型和消息码等）等信息来制定规则，对 IPv4 报文进行匹配。用户可利用 IPv4 高级 ACL 制订比 IPv4 基本 ACL 更准确、丰富、灵活的规则。

表1-7 配置 IPv4 高级 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv4高级ACL，并进入IPv4高级ACL视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何ACL IPv4高级ACL的编号范围为3000～3999
配置ACL的描述信息	**description** *text*	可选 缺省情况下，ACL没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **precedence** *precedence* | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *	必选 缺省情况下，IPv4高级ACL内不存在任何规则 重复执行本命令可以创建多条规则 需要注意的是，当IPv4高级ACL用于QoS策略的流分类或用于报文过滤功能时： • 不支持配置 **vpn-instance** 参数 • 不支持配置操作符 *operator* 取值为 **neq** • 当 ACL 用于流分类时，在规则中配置的 **logging** 和 **counting** 参数不会生效
为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
配置规则注释信息	**rule** [*rule-id*] **remark** *text*	可选 缺省情况下，ACL内没有任何规则注释信息
使能基于硬件应用的ACL的规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的ACL的规则匹配统计功能处于关闭状态 当ACL被QoS策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建 IPv4 高级 ACL 时为其指定了名称，则也可以使用 **acl name** *acl-name* 命令通过指定名称的方式进入其视图。

2. 配置IPv6 高级ACL

IPv6 高级 ACL 可根据报文的源 IPv6 地址、目的 IPv6 地址、报文优先级、IPv6 承载的协议类型及特性（如 TCP/UDP 的源端口和目的端口、TCP 报文标识、ICMPv6 协议的消息类型和消息码等）等信息来制定规则，对 IPv6 报文进行匹配。用户可利用 IPv6 高级 ACL 制订比 IPv6 基本 ACL 更准确、丰富、灵活的规则。

表1-8 配置 IPv6 高级 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建IPv6高级ACL，并进入IPv6高级ACL视图	**acl ipv6 number** *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何ACL IPv6高级ACL的编号范围3000～3999
配置ACL的描述信息	**description** *text*	可选 缺省情况下，ACL没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为5
创建规则	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **source** { *source source-prefix* | *source/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *	必选 缺省情况下，IPv6高级ACL内不存在任何规则 需要注意的是，当IPv6高级ACL用于QoS策略的流分类或用于报文过滤功能时： • 不支持配置 **fragment** 和 **routing** 参数 • 不支持配置 **vpn-instance** 参数 • 不支持配置操作符 *operator* 取值为 **neq** • 如果 QoS 策略或报文过滤功能应用于出方向，则不支持配置 **flow-label** 参数 • 当 ACL 用于流分类时，在规则中配置的 **logging** 和 **counting** 参数不会生效

操作	命令	说明
为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
配置规则注释信息	**rule** [*rule-id*] **remark** *text*	可选 缺省情况下，ACL内没有任何规则注释信息
使能基于硬件应用的ACL的规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的ACL的规则匹配统计功能处于关闭状态 当ACL被QoS策略引用对报文进行流分类时，本功能不会生效

说明

- 对于带有扩展报文头的 IPv6 报文，可以通过 IPv6 高级 ACL 来匹配所有类型的扩展报文头，但如果 ACL 的匹配内容为扩展报文头内层的报文内容，则扩展报文头不能超过两层，且不能包含 IPv6 Encapsulation Header 报文头，否则 ACL 将无法进行匹配。
- 当匹配的扩展报文头类型（*protocol* 参数）取值为 43、44、51、60 时，引用该 ACL 的 QoS 策略将不能在出方向应用。
- 如果在创建 IPv6 高级 ACL 时为其指定了名称，则也可以使用 **acl ipv6 name** *acl6-name* 命令通过指定名称的方式进入其视图。

1.3.4 配置二层ACL

二层 ACL 可根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、链路层协议类型等二层信息来制订规则，对报文进行匹配。

表1-9 配置二层 ACL

操作	命令	说明
进入系统视图	**system-view**	-
创建二层ACL，并进入二层ACL视图	**acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	必选 缺省情况下，不存在任何ACL 二层ACL的编号范围为4000～4999
配置ACL的描述信息	**description** *text*	可选 缺省情况下，ACL没有任何描述信息
配置规则编号的步长	**step** *step-value*	可选 缺省情况下，规则编号的步长为5

操作	命令	说明
创建规则	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **counting** | **dest-mac** *dest-addr dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *sour-addr source-mask* | **time-range** *time-range-name*] *	必选 缺省情况下，二层ACL内不存在任何规则 需要注意的是，当二层ACL用于QoS策略的流分类或用于报文过滤功能时，不支持配置**lsap**参数
为指定规则配置描述信息	**rule** *rule-id* **comment** *text*	可选 缺省情况下，规则没有任何描述信息
配置规则注释信息	**rule** [*rule-id*] **remark** *text*	可选 缺省情况下，ACL内没有任何规则注释信息
使能基于硬件应用的ACL的规则匹配统计功能	**hardware-count enable**	可选 缺省情况下，基于硬件应用的ACL的规则匹配统计功能处于关闭状态 当ACL被QoS策略引用对报文进行流分类时，本功能不会生效

说明

如果在创建二层 ACL 时为其指定了名称，则也可以使用 **acl name** *acl-name* 命令通过指定名称的方式进入其视图。

1.3.5 复制ACL

用户可通过复制一个已存在的 ACL（即源 ACL），来生成一个新的同类型 ACL（即目的 ACL）。除了 ACL 的编号和名称不同外，新生成的目的 ACL 的匹配顺序、规则匹配统计功能的使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

1. 复制IPv4 ACL

表1-10 复制 IPv4 ACL

操作	命令	说明
进入系统视图	**system-view**	-
复制生成一个新的同类型IPv4 ACL	**acl copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }	必选

说明

目的 IPv4 ACL 要与源 IPv4 ACL 的类型相同，且目的 IPv4 ACL 必须不存在，否则将导致复制失败。

2. 复制IPv6 ACL

表1-11 复制 IPv6 ACL

操作	命令	说明
进入系统视图	**system-view**	-
复制生成一个新的同类型IPv6 ACL	**acl ipv6 copy** { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }	必选

说明

目的 IPv6 ACL 要与源 IPv6 ACL 的类型相同，且目的 IPv6 ACL 必须不存在，否则将导致复制失败。

1.3.6 应用ACL进行报文过滤

ACL 最基本的应用就是进行报文过滤，即通过将 ACL 规则应用到指定接口的入或出方向上，从而对该接口收到或发出的报文进行过滤。此外，通过配置报文过滤日志的生成与发送周期，还可周期性地生成并发送报文过滤的日志信息（信息级别为 informational），包括匹配次数以及所使用的 ACL 规则。该日志信息将被发往信息中心，有关信息中心的详细介绍，请参见“网络管理和监控配置指导”中的“信息中心”。

注意

- 应用 ACL 进行报文过滤功能中所指的“接口”包括二层以太网端口、三层以太网端口、和 VLAN 接口。三层以太网端口是指被配置为三层模式的以太网端口，有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”。
- 在 VLAN 接口上应用 ACL 进行报文过滤时，只能对通过该接口进行三层转发的报文进行过滤，而对纯二层转发的报文不进行过滤。
- 在端口上配置报文过滤时，可以同时应用 IPv4 ACL、IPv6 ACL 和二层 ACL，但在每个方向上每种类型的 ACL 最多只能应用一条。
- 系统只支持对应用基本或高级 ACL 进行报文过滤的日志进行记录，并在配置上述 ACL 规则时必须打开其日志记录功能（通过指定 **logging** 参数）和规则匹配统计功能（通过指定 **counting** 参数或使用 **hardware-count enable** 命令）。

1. 应用IPv4 ACL或二层ACL进行报文过滤

表1-12 应用 IPv4 ACL 进行报文过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
应用IPv4基本ACL、IPv4高级ACL或二层ACL进行报文过滤	**packet-filter** { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }	必选 缺省情况下，接口不对报文进行过滤
退回系统视图	**quit**	-
配置IPv4报文过滤日志的生成与发送周期	**acl logging frequence** *frequence*	必选 缺省情况下，IPv4报文过滤日志的生成与发送周期为0分钟，即不记录IPv4报文过滤的日志

2. 应用IPv6 ACL进行报文过滤

表1-13 应用 IPv6 ACL 进行报文过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
应用IPv6基本ACL或IPv6高级ACL进行报文过滤	**packet-filter ipv6** { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }	必选 缺省情况下，接口不对报文进行过滤
退回系统视图	**quit**	-
配置IPv6报文过滤日志的生成与发送周期	**acl ipv6 logging frequence** *frequence*	必选 缺省情况下，IPv6报文过滤日志的生成与发送周期为0分钟，即不记录IPv6报文过滤的日志

3. 报文过滤高级日志功能

为帮助用户对报文过滤功能的匹配情况进行监控和分析，本设备在输出报文过滤基本日志（记录匹配报文个数）的基础上，提供了高级日志记录功能，通过该功能输出的高级日志可以记录匹配过滤规则的报文的基本信息。例如下面的日志信息，可以表示报文过滤功能拒绝了 IP 地址为 10.253.23.181 的设备对 10.253.10.229 地址的 Telnet 访问。

```
*Feb   6  16:10:24:  %SEC-6-IPACCESSLOGP:  list  120  denied  tcp  10.253.23.181(1281)  ->
10.253.10.229(23), 1 packet
```

说明

S5500-28SC-HI 和 S5500-52SC-HI 交换机不支持本功能。

表1-14 配置报文过滤高级日志功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
配置IPv4报文过滤高级日志的生成与发送周期	**acl flow logging interval** *interval-value*	必选 缺省情况下，IPv4报文过滤高级日志的生成与发送周期为0分钟，即不记录IPv4报文过滤的高级日志
配置IPv6报文过滤高级日志的生成与发送周期	**acl ipv6 flow logging interval** *interval-value*	必选 缺省情况下，IPv6报文过滤高级日志的生成与发送周期为0分钟，即不记录IPv6报文过滤的高级日志

说明

报文过滤高级日志记录功能与基本日志记录功能相互独立，可以同时配置。

1.4 ACL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 ACL 配置后的运行情况，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 ACL 的统计信息。

表1-15 ACL 显示和维护

配置	命令
显示IPv4 ACL的配置和运行情况	**display acl** { *acl-number* | **all** | **name** *acl-name* } [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPv6 ACL的配置和运行情况	**display acl ipv6** { *acl6-number* | **all** | **name** *acl6-name* } [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示ACL资源的使用情况	**display acl resource** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示报文过滤策略的应用情况	**display packet-filter** { { **all** | **interface** *interface-type interface-number* } [**inbound** | **outbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示时间段的配置和状态信息	**display time-range** { *time-range-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除IPv4 ACL统计信息	**reset acl counter** { *acl-number* | **all** | **name** *acl-name* }
清除IPv6 ACL统计信息	**reset acl ipv6 counter** { *acl6-number* | **all** | **name** *acl6-name* }

1.5 ACL典型配置举例

1.5.1 在设备管理功能中应用ACL

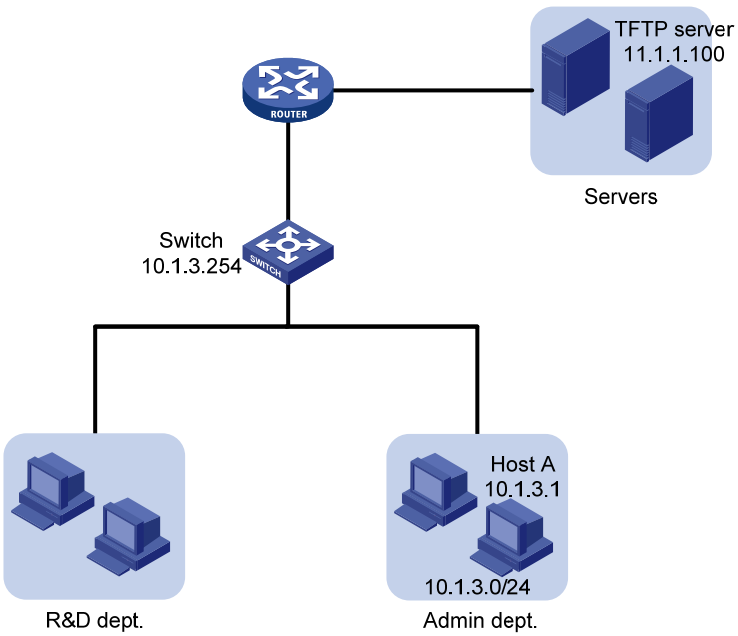
1. 组网需求

某公司的网络组网如 图 1-1 所示，现要求：

- Switch 在工作时间（8:30～18:00）可以接受管理网管工作站（Host A）的 Telnet 访问，在其余时间则不接受任何 Telnet 登录请求。
- Switch 作为 TFTP 客户端，只能从 11.1.1.100 的服务器上获取文件，以保证设备上不会保存未授权的非法文件。
- Switch 作为 FTP 服务器端，只能接受网管工作站的登录请求。

2. 组网图

图1-1 在设备管理功能中应用基本 IPv4 ACL 组网示意图



3. 配置步骤

(1) 对 Telnet 登录请求的限制

定义周期时间段 telnet，时间范围为每个工作日的 8:30～18:00。

```
<Switch> system-view
[Switch] time-range telnet 8:30 to 18:00 working-day
```

定义基本 IPv4 ACL 2000，配置两条规则，分别为允许源 IP 地址为 10.1.3.1 的报文在工作时间通过以及拒绝源 IP 地址为任意地址的报文通过。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 10.1.3.1 0 time-range telnet
[Switch-acl-basic-2000] quit
```

在所有 Telnet 用户界面下应用 ACL 2000，方向为入方向，表示对登录到本设备的 Telnet 请求进行限制。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] acl 2000 inbound
```

(2)　对 TFTP 服务器的访问限制

定义基本 IPv4 ACL 2001，配置两条规则，分别为允许源 IP 地址为 11.1.1.100 的报文通过以及拒绝源 IP 地址为任意地址的报文通过。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 11.1.1.100 0
[Switch-acl-basic-2001] quit
```

配置设备只使用 ACL 来限制可访问的 TFTP 服务器设备。

```
[Switch] tftp-server acl 2001
```

(3)　对 FTP 登录请求的限制

定义基本 IPv4 ACL 2002，配置两条规则，分别为允许源 IP 地址为 10.1.3.1 的报文通过以及拒绝源 IP 地址为任意地址的报文通过。

```
[Switch] acl number 2002
[Switch-acl-basic-2001] rule permit source 10.1.3.1 0
[Switch-acl-basic-2001] quit
```

开启设备的 FTP 服务器功能。

```
[Switch] ftp server enable
```

配置设备使用 ACL 2002 来限制 FTP 登录请求。

```
[Switch] ftp server acl 2002
```

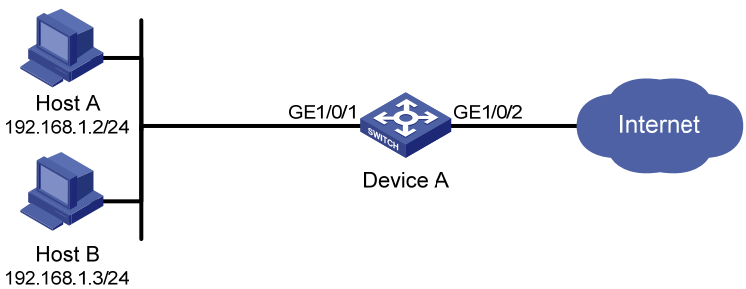
1.5.2 应用IPv4 ACL进行报文过滤配置举例

1. 组网需求

要求通过在 Device A 的端口 GigabitEthernet1/0/1 上配置 IPv4 报文过滤功能，实现在每天的 8 点到 18 点期间只允许 Host A 访问互联网，并以 10 分钟为周期记录 IPv4 报文过滤的日志信息并输出至控制台。

2. 组网图

图1-2 应用 IPv4 ACL 进行报文过滤配置组网图



3. 配置步骤

创建名为 study 的时间段，其时间范围为每天的 8 点到 18 点。

```
<DeviceA> system-view
```

```
[DeviceA] time-range study 8:0 to 18:0 daily
```

创建 IPv4 基本 ACL 2009，并制订如下规则：在名为 study 的时间段内只允许来自 Host A 的报文通过、禁止来自其它 IP 地址的报文通过，且在这些规则中对允许通过的报文记录日志信息。

```
[DeviceA] acl number 2009
[DeviceA-acl-basic-2009] rule permit source 192.168.1.2 0 time-range study logging
[DeviceA-acl-basic-2009] rule deny source any time-range study
[DeviceA-acl-basic-2009] quit
```

配置 IPv4 报文过滤日志的生成与发送周期为 10 分钟。

```
[DeviceA] acl logging frequence 10
```

配置系统信息的输出规则，将级别为 informational 的日志信息输出至控制台。

```
[DeviceA] info-center source default channel 0 log level informational
```

应用 IPv4 基本 ACL 2009 对端口 GigabitEthernet1/0/1 入方向上的报文进行过滤。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] packet-filter 2009 inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

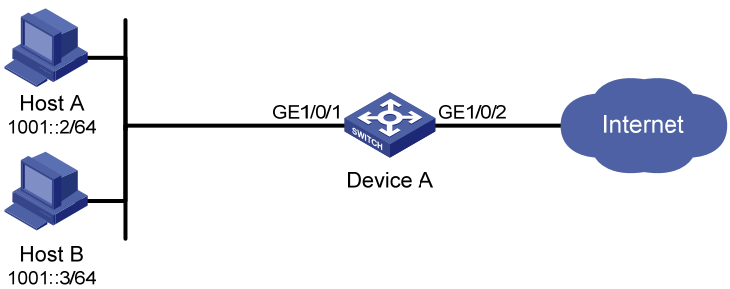
1.5.3 应用IPv6 ACL进行报文过滤配置举例

1. 组网需求

要求通过在 Device A 的端口 GigabitEthernet1/0/1 上配置 IPv6 报文过滤功能，实现在每天的 8 点到 18 点期间只允许 Host A 访问互联网，并以 10 分钟为周期记录 IPv6 报文过滤的日志信息并输出至控制台。

2. 组网图

图1-3 应用 IPv6 ACL 进行报文过滤配置组网图



3. 配置步骤

创建名为 study 的时间段，其时间范围为每天的 8 点到 18 点。

```
<DeviceA> system-view
[DeviceA] time-range study 8:0 to 18:0 daily
```

创建 IPv6 基本 ACL 2009，并制订如下规则：在名为 study 的时间段内只允许来自 Host A 的报文通过、禁止来自其它 IPv6 地址的报文通过，且在这些规则中对允许通过的报文记录日志信息。

```
[DeviceA] acl ipv6 number 2009
[DeviceA-acl6-basic-2009] rule permit source 1001::2 128 time-range study logging
[DeviceA-acl6-basic-2009] rule deny source any time-range study
[DeviceA-acl6-basic-2009] quit
```

配置 IPv6 报文过滤日志的生成与发送周期为 10 分钟。

```
[DeviceA] acl ipv6 logging frequence 10
```

配置系统信息的输出规则，将级别为 informational 的日志信息输出至控制台。

```
[DeviceA] info-center source default channel 0 log level informational
```

应用 IPv6 基本 ACL 2009 对端口 GigabitEthernet1/0/1 入方向上的报文进行过滤。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] packet-filter ipv6 2009 inbound
[DeviceA-GigabitEthernet1/0/1] quit
```

目 录

1 QoS简介

1.1 概述

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

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

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

1.2 QoS服务模型简介

通常 QoS 提供以下三种服务模型：

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

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

说明

RSVP 的相关内容请参见“MPLS 配置指导”中的“MPLS TE”。

1.2.3 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。

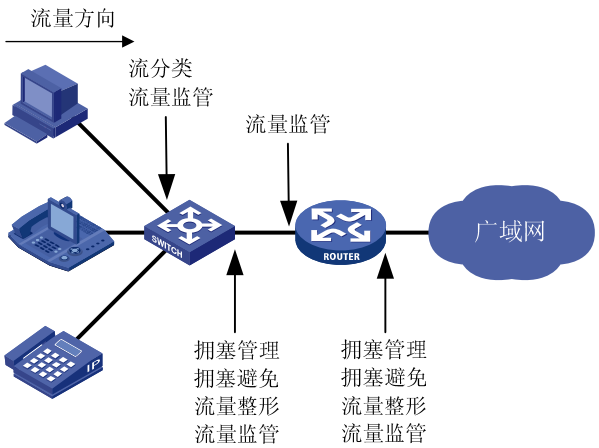
本文提到的技术都是基于 DiffServ 服务模型。

1.3 QoS技术综述

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

1.3.1 QoS技术在网络中的位置

图1-1 常用 QoS 技术在网络中的位置



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

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

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。

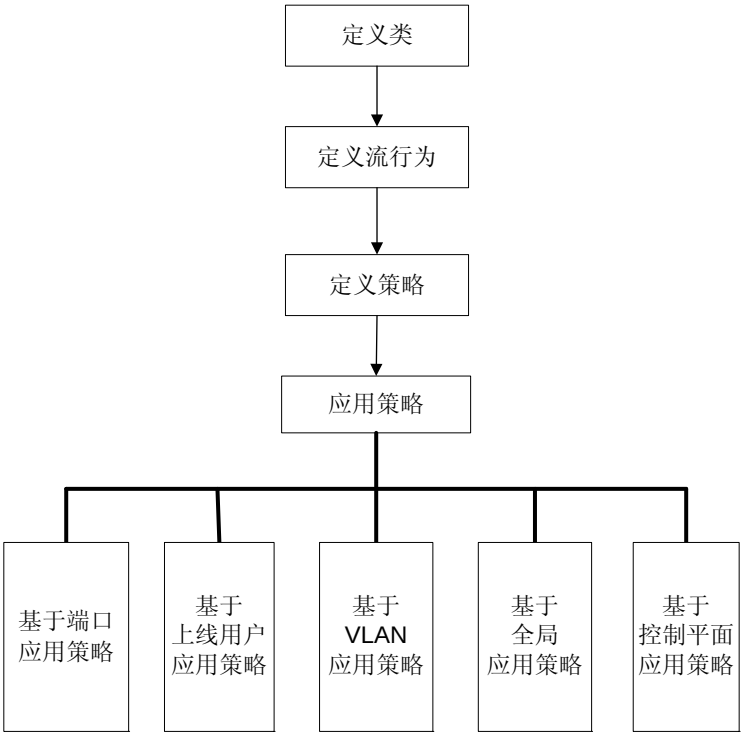
策略的要素包括：策略名称、绑定在一起的类和流行为的名称。

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 • **and**：报文只有匹配了所有的规则，设备才认为报文属于这个类 • **or**：报文只要匹配了类中的任何一个规则，设备就认为报文属于这个类
定义匹配数据包的规则	**if-match** *match-criteria*	必选

match-criteria：匹配规则，取值如 表 2-2 所示。

表2-2 类的匹配规则取值

取值	描述
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	定义匹配ACL的规则 *acl-number*是ACL的序号，IPv4 ACL序号的取值范围是2000～3999，二层ACL序号的取值范围是4000～4999，IPv6 ACL序号的取值范围是2000～3999 *acl-name*是ACL的名称，为1～63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	定义匹配所有数据包的规则
customer-dot1p *8021p-list*	定义匹配用户网络802.1p优先级的规则，*8021p-list*为CoS取值的列表，最多可以输入8个CoS取值，用空格隔开，CoS的取值范围为0～7
customer-vlan-id *vlan-id-list*	定义匹配用户网络VLAN ID的规则，*vlan-id-list*为VLAN ID的列表，形式可以为*vlan-id* **to** *vlan-id*，也可以输入多个不连续的VLAN ID，用空格隔开，设备最多允许用户同时指定8个VLAN ID；VLAN ID的取值范围为1～4094
destination-mac *mac-address*	定义匹配目的MAC地址的规则
dscp *dscp-list*	定义匹配DSCP的规则，*dscp-list*为DSCP取值的列表，最多可以输入8个DSCP取值，用空格隔开，DSCP的取值范围为0～63或表13-5中的关键字
ip-precedence *ip-precedence-list*	定义匹配IP优先级的规则，*ip-precedence-list*为IP优先级取值的列表，最多可以输入8个IP优先级取值，用空格隔开，IP优先级的取值范围为0～7
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为IP或IPv6
qos-local-id *local-id-value*	定义匹配qos-local-id的规则，*local-id-value*为QoS本地ID，取值范围为1～4095 在本系列交换机上，能够支持的*local-id-value*值为1～3999
service-dot1p *8021p-list*	定义匹配运营商网络802.1p优先级的规则，*8021p-list*为CoS取值的列表，最多可以输入8个CoS取值，用空格隔开，CoS的取值范围为0～7
service-vlan-id *vlan-id-list*	定义匹配运营商网络VLAN ID的规则，*vlan-id-list*为VLAN ID的列表，形式可以为*vlan-id* **to** *vlan-id*，也可以输入多个不连续的VLAN ID，用空格隔开，设备最多允许用户同时指定8个VLAN ID；VLAN ID的取值范围为1～4094
source-mac *mac-address*	定义匹配源MAC地址的规则
system-index *index-value-list*	定义规则来匹配预定义的上送控制平面报文类型，*index-value-list*为系统预定义匹配字段索引号（system-index）的列表，最多可以输入8个system-index值，system-index值的取值范围为1～128

说明

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

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

说明

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

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

如果用户需要创建匹配以上某一字段多个取值的规则，需要在创建流分类时指定各规则之间的逻辑关系为 **or**，然后再通过多次执行 **if-match** 命令的方式来配置匹配多个值的规则。

2.2.2 定义流行为

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

表2-3 定义流行为

操作	命令	说明
进入系统视图	**system-view**	-
定义一个流行为并进入流行为视图	**traffic behavior** *behavior-name*	必选
配置流行为	流行为就是对应符合流分类的报文做出相应的QoS动作，例如流量监管、流量过滤、流量重定向、重标记、流量统计等，具体情况请参见本文相关章节	

2.2.3 定义策略

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

表2-4 在策略中为类指定流行为

操作	命令	说明
进入系统视图	**system-view**	-
定义策略并进入策略视图	**qos policy** *policy-name*	必选
在策略中为类指定采用的流行为	**classifier** *tcl-name* **behavior** *behavior-name* [**mode dot1q-tag-manipulation**]	必选 **mode dot1q-tag-manipulation**用来设置VLAN映射功能中的类和流行为对应关系。有关VLAN映射功能的介绍，请参见“二层技术-以太网交换配置指导”中的“VLAN映射”

说明

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

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或发送的流量生效。
- 基于上线用户应用 QoS 策略：QoS 策略对通过上线用户接收或发送的流量生效。
- 基于 VLAN 应用 QoS 策略：QoS 策略对通过同一个 VLAN 内所有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。
- 基于控制平面应用 QoS 策略：QoS 策略对通过控制平面接收的流量生效。

说明

- 当 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。当流分类规则中匹配的是 ACL 时，允许删除或修改该 ACL（包括向该 ACL 中添加、删除和修改规则）。
- 如果 User Profile 处于激活状态，既不能修改策略的内容（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。
- 在基于端口、基于 VLAN 和基于全局三种应用 QoS 策略的方式中，基于端口的方式优先级高于基于 VLAN 的方式，基于全局的方式优先级最低。即设备对于接收/发送的流量，首先匹配端口上应用的 QoS 策略中的流分类条件，如果匹配则直接执行端口的 QoS 策略而不再执行 VLAN 和全局的策略。

1. 基于端口应用QoS策略

说明

本节中的端口指的是二层以太网端口和三层以太网端口。三层以太网端口是指工作模式被配置成三层模式的以太网端口，有关以太网端口工作模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口配置”部分。

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

表2-5 在端口上应用策略

操作		命令	说明
进入系统视图		**system-view**	-
进入端口视图或端口组视图	进入端口视图	**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*	
在端口上应用关联的策略		**qos apply policy** *policy-name* { **inbound** | **outbound** }	必选

说明

如果 QoS 策略应用在端口的出方向，则 QoS 策略对本地协议报文不起作用。本地协议报文是指端口所在设备自身发出的某些报文，主要是维持设备正常运行的重要协议报文。为了确保这些报文能够被不受影响的发送出去，即便在端口的出方向应用了 QoS 策略，由本设备发出的协议报文也不会受到 QoS 策略的限制，从而降低了因配置 QoS 而误将这些报文丢弃或进行其他处理的风险。一些常见的本地协议报文如下：链路维护报文、STP、LDP、RSVP 等。

2. 基于上线用户应用QoS策略

一个策略可以应用于多个上线用户。上线用户的每个方向（发送和接收两个方向）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。

表2-6 基于上线用户应用 QoS 策略

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

说明

- user-profile 视图下应用的策略中的流行为只支持 **remark**、**car**、**filter** 三种动作。
- user-profile 视图下应用的策略不能为空策略，因为应用空策略的 User Profile 不能被激活。
- 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 上的所有流量进行管理。

表2-7 基于 VLAN 应用的 QoS 策略

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

说明

基于 VLAN 应用的 QoS 策略不能应用在动态 VLAN 上。例如，在运行 GVRP 协议的情况下，设备可能会动态创建 VLAN，QoS 策略不能应用在该动态 VLAN 上。

4. 基于全局应用QoS策略

基于全局应用 QoS 策略可以方便对设备上的所有流量进行管理。

表2-8 基于全局应用 QoS 策略

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

5. 基于控制平面应用QoS策略

设备支持数据平面和控制平面：

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

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

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

表2-9 应用控制平面策略

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

注意

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

2.2.5 QoS策略显示和维护

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

表2-10 QoS 策略显示和维护

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

3 优先级映射配置

说明

优先级映射功能中的“端口”包含了二层以太网端口和三层以太网端口，三层以太网端口是指被配置为三层模式以太网端口，的有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口”。

3.1 优先级映射简介

3.1.1 概述

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

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

3.1.2 优先级介绍

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

报文携带优先级包括：802.1p优先级、DSCP优先级、IP优先级、EXP优先级等。这些优先级都是根据公认的标准和协议生成，体现了报文自身的优先等级。相关介绍请参见 13.2 附录 B 各种优先级介绍。

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

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

3.1.3 优先级映射表

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

- **dot1p-dp**：802.1p 优先级到丢弃优先级映射表；
- **dot1p-exp**：802.1p 优先级到 EXP 映射表；（S5500-28SC-HI 和 S5500-52SC-HI 不支持）
- **dot1p-lp**：802.1p 优先级到本地优先级映射表；
- **dscp-dot1p**：DSCP 到 802.1p 优先级映射表，仅对 IP 报文生效；
- **dscp-dp**：DSCP 到丢弃优先级映射表，仅对 IP 报文生效；
- **dscp-dscp**：DSCP 到 DSCP 映射表，仅对 IP 报文生效；

- **exp-dot1p**：EXP 到 802.1p 优先级映射表；（S5500-28SC-HI 和 S5500-52SC-HI 不支持）
- **exp-dp**：EXP 到丢弃优先级映射表；（S5500-28SC-HI 和 S5500-52SC-HI 不支持）

通常情况下，可以通过查找缺省优先级映射表（13.1 附录 A 缺省优先级映射表）来为报文分配相应的优先级。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

3.1.4 优先级信任模式

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

- 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。

表3-1 信任 DSCP 优先级的映射结果（优先级映射表处于缺省状态）

报文携带的 DSCP 优先级	本地优先级	队列编号
0 to 7	2	2
8 to 15	0	0
16 to 23	1	1
24 to 31	3	3
32 to 39	4	4
40 to 47	5	5
48 to 55	6	6
56 to 63	7	7

- 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。

表3-2 信任 802.1p 优先级的映射结果（优先级映射表处于缺省状态）

报文携带的 802.1p 优先级	本地优先级	队列编号
0	2	2
1	0	0
2	1	1
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

说明

在信任 802.1p优先级的情况下，如果报文未携带VLAN Tag，设备将使用端口优先级作为 802.1p 优先级，映射效果请参见 表 3-3。

- 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。

表3-3 不信任报文优先级的映射结果（优先级映射表处于缺省状态）

端口优先级	本地优先级	队列编号
0	2	2
1	0	0
2	1	1
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

另外，当端口信任 802.1p 优先级，而接收到的报文又没有携带 802.1Q 标签时，设备将使用接收端口的端口优先级作为报文的 802.1p 优先级，并依此进行优先级映射。

3.1.5 优先级映射过程

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

图3-1 以太网报文优先级映射过程

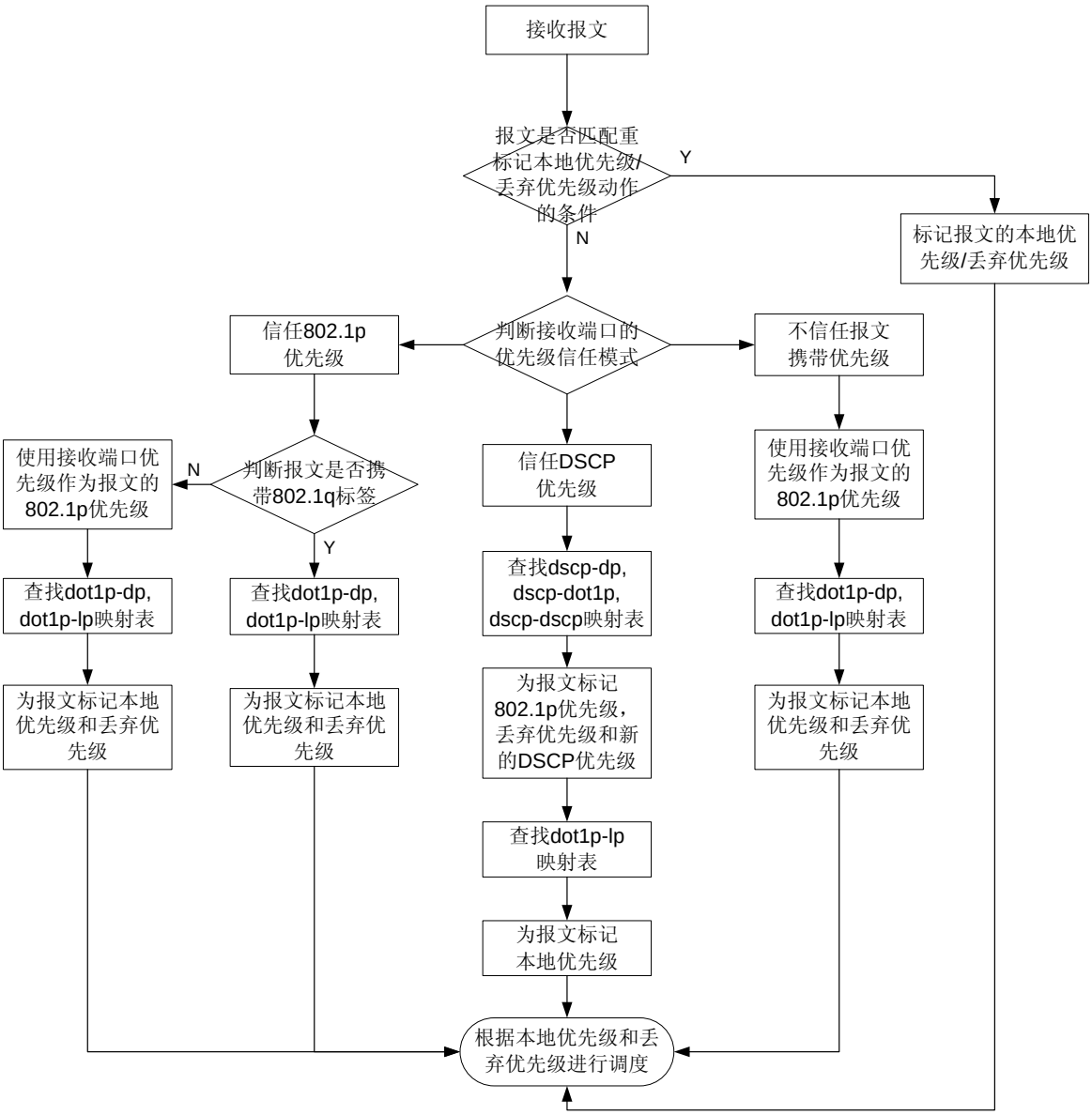
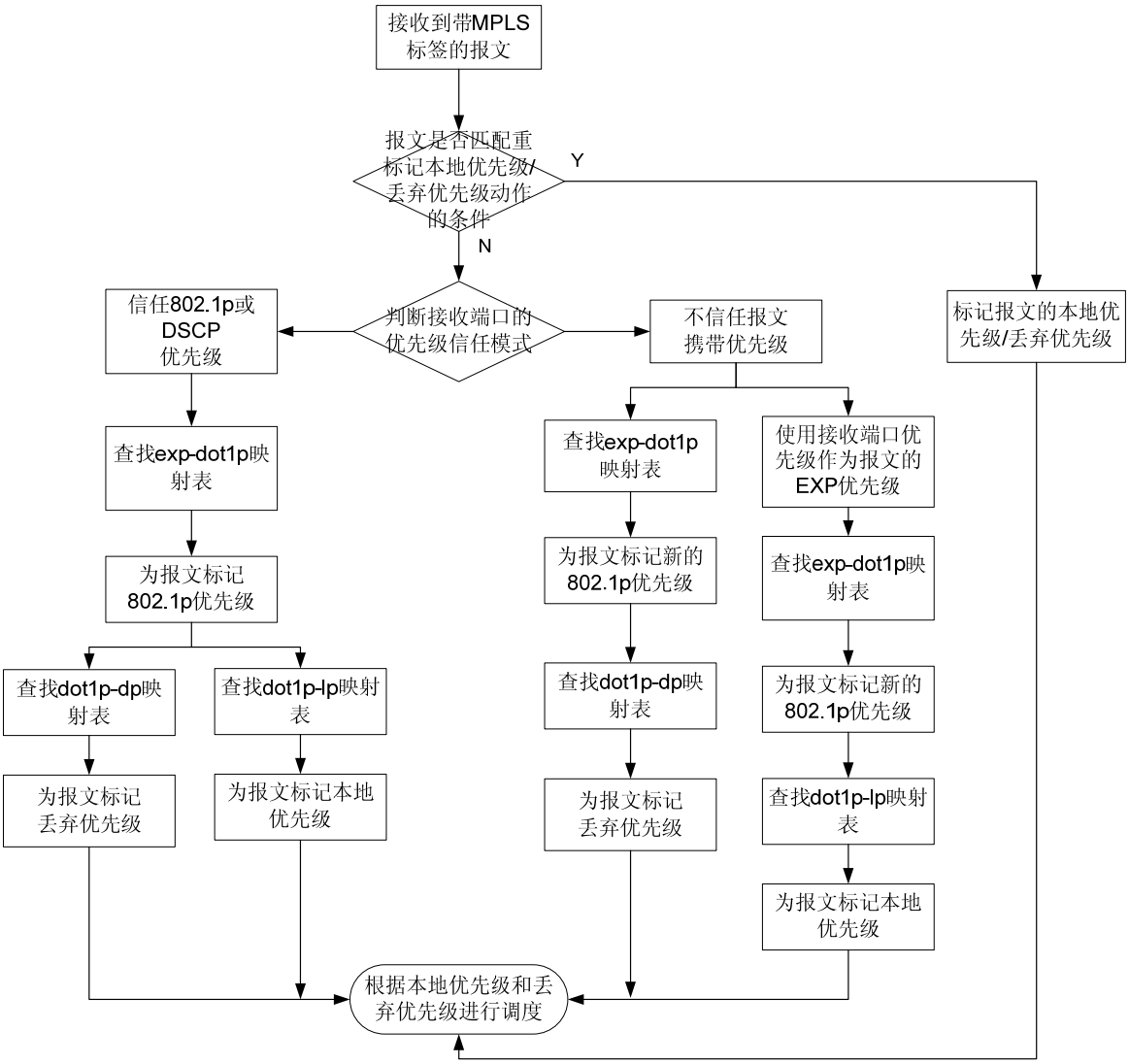


图3-2 MPLS 报文优先级映射过程（S5500-28SC-HI 和 S5500-52SC-HI 不支持）



3.2 优先级映射配置任务简介

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

表3-4 优先级映射配置任务简介

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

3.3 配置优先级映射

3.3.1 配置优先级映射表

表3-5 配置优先级映射表

操作	命令	说明
进入系统视图	**system-view**	-
进入指定的优先级映射表视图	**qos map-table** { **dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** | **exp-dp** }	必选 用户根据需要进入相应的优先级映射表视图 S5500-28SC-HI 和 S5500-52SC-HI 不支持 **dot1p-exp**、**exp-dot1p**、**exp-dp**映射表
配置指定优先级映射表参数，定义优先级映射关系	**import** *import-value-list* **export** *export-value*	必选 新配置的映射项将覆盖原有映射项

3.3.2 配置优先级信任模式

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

在配置接口/端口组上的优先级模式时，用户可以选择下列信任模式：

- 信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。
- 信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射。
- 不信任报文优先级，使用端口优先级作为报文的 802.1p 优先级进行优先级映射。

表3-6 配置优先级信任模式

操作		命令	说明
进入系统视图		**system-view**	-
进入端口视图或端口组视图	进入端口视图	**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**	

说明

在 MPLS 组网环境中，如果需要使用 EXP 优先级进行优先级映射并对 MPLS 报文进行队列调度，请将设备上转发 MPLS 报文的端口配置为信任 802.1p 优先级或 DSCP 优先级。

3.3.3 配置端口优先级

按照接收端口的端口优先级，通过一一映射为报文分配相应的优先级。

表3-7 配置端口优先级

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** *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*	
配置端口优先级		**qos priority** *priority-value*	必选 端口优先级的缺省值为0

3.4 优先级映射显示和维护

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

表3-8 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（S5500-28SC-HI和S5500-52SC-HI不支持**dot1p-exp**、**exp-dot1p**、**exp-dp**映射表）	**display qos map-table** [**dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** | **exp-dp**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口优先级信任模式信息	**display qos trust interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

3.5 优先级映射典型配置举例

3.5.1 优先级信任模式和端口优先级配置举例

1. 组网需求

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

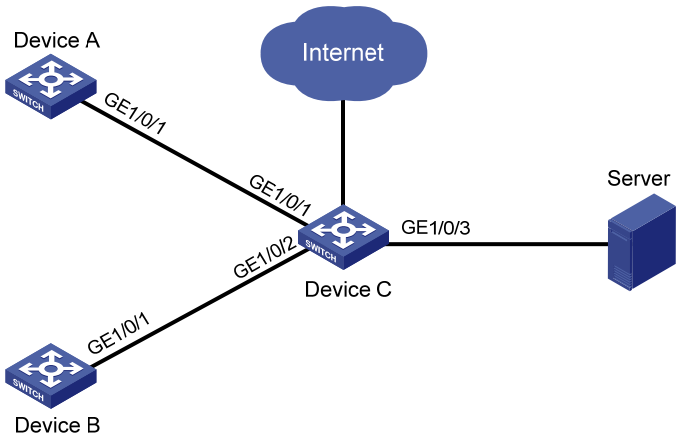
- Device A 通过端口 GigabitEthernet1/0/1 接入 Device C；

- Device B 通过端口 GigabitEthernet1/0/2 接入 Device C。
- Device A 和 Device B 向 Device C 发送的报文都不携带 VLAN Tag。

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

2. 组网图

图3-3 优先级信任模式和端口优先级配置举例组网图



3. 配置步骤

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

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

3.5.2 优先级映射表和重标记配置举例

1. 组网需求

公司企业网通过 Device 实现各部门之间的互连。网络环境描述如下：

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

实现如下需求：

访问公共服务器的时候，研发部门 > 管理部门 > 市场部门。

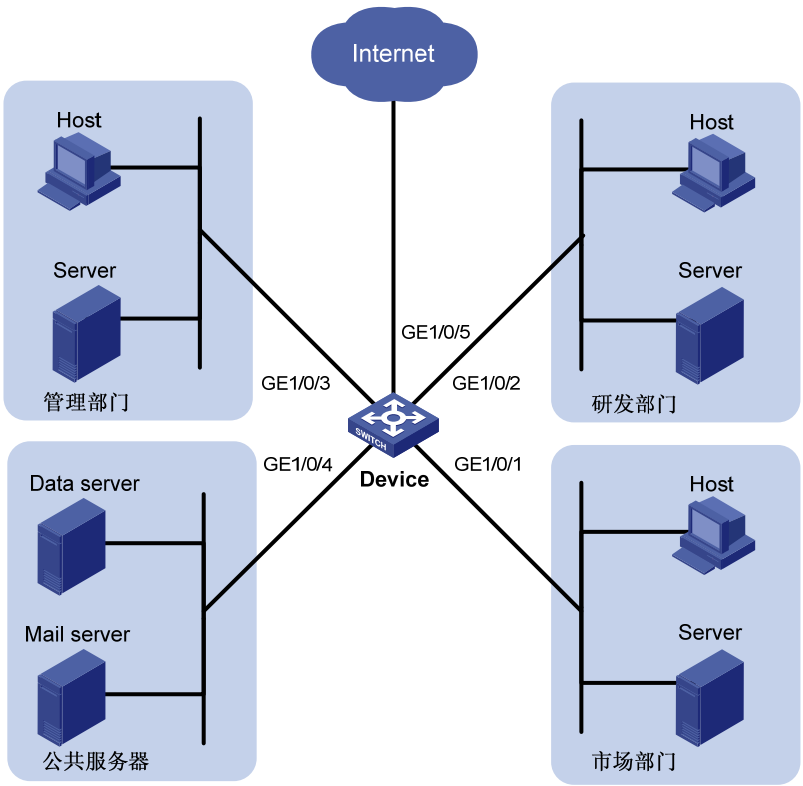
- 通过优先级映射将研发部门发出的报文放入出队列 6 中，优先进行处理；
- 通过优先级映射将管理部门发出的报文放入出队列 4 中，次优先进行处理；
- 通过优先级映射将市场部门发出的报文放入出队列 2 中，最后进行处理。

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

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

创建流分类，匹配 ACL 3000。

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

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

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

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

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

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

```
[Device] traffic behavior rd
[Device-behavior-rd] remark dot1p 3
[Device-behavior-rd] quit
[Device] qos policy rd
[Device-qospolicy-rd] classifier http behavior rd
```

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

4 流量监管、流量整形和端口限速配置

说明

流量整形和端口限速功能中的“端口”包含了二层以太网端口和三层以太网端口，三层以太网端口是指被配置为三层模式以太网端口，的有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口”。

4.1 流量监管、流量整形和端口限速简介

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

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

4.1.1 流量评估与令牌桶

1. 令牌桶的特点

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

2. 用令牌桶评估流量

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

评估流量时令牌桶的参数包括：

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

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

3. 复杂评估

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

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

- EBS：表示 E 桶的容量，即 E 桶瞬间能够通过的超出突发流量。

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

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

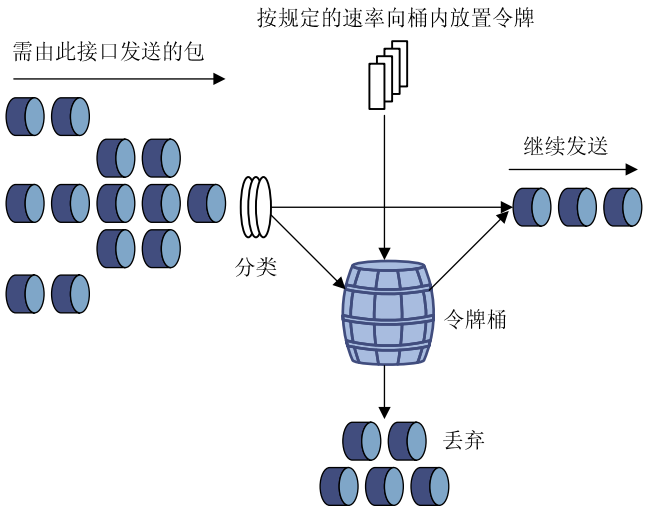
4.1.2 流量监管

说明

流量监管支持入/出两个方向，为了方便描述，下文以出方向为例。

流量监管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 流量监管示意图



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，将其优先级标记为其他值后再进行转发，可以改变的优先级包括：802.1p 优先级、DSCP 优先级、本地优先级。

4.1.3 流量整形

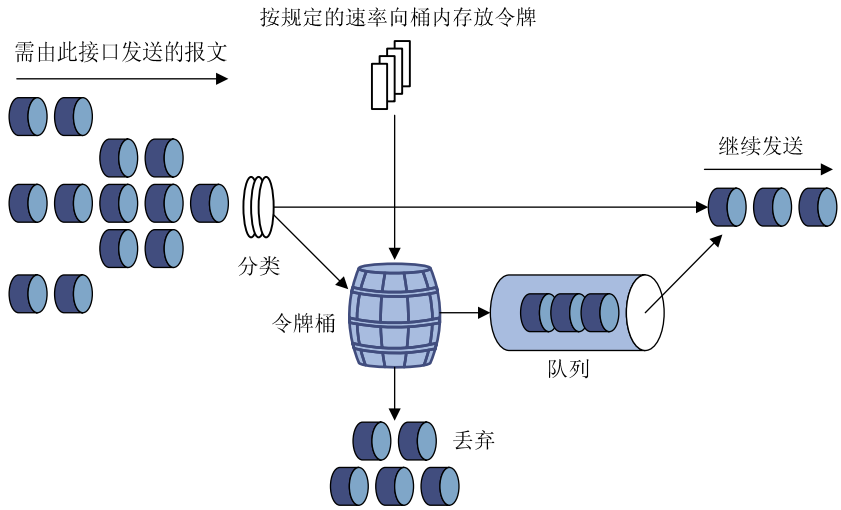
说明

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。

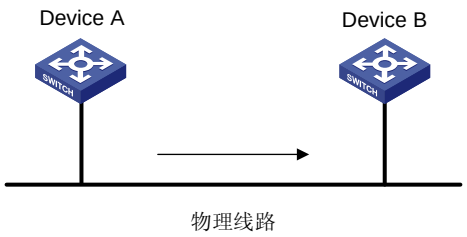
流量整形与流量监管的主要区别在于，流量整形对流量监管中需要丢弃的报文进行缓存——通常是将它们放入缓冲区或队列内，如 图 4-2 所示。当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

图4-2 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 端口限速

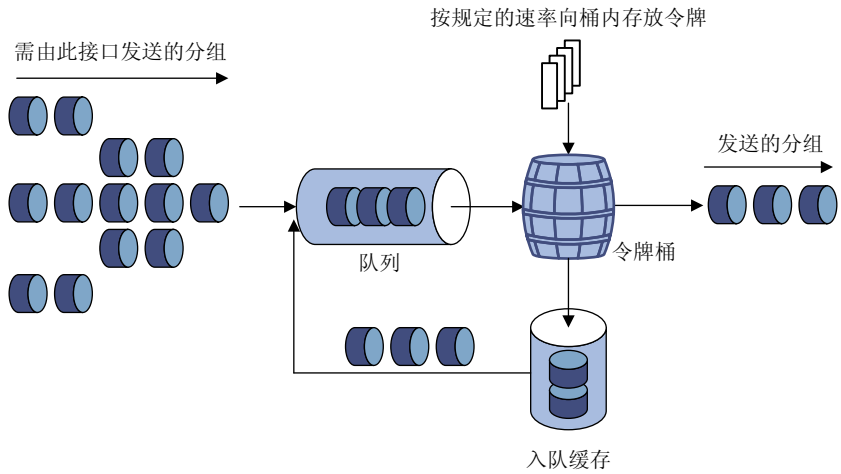
说明

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。

利用端口限速可以在一个端口上限制发送报文（包括紧急报文）的总速率。

端口限速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端口限速，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，就可以对通过该端口的报文流量进行控制。

图4-4 端口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，端口限速能够限制在端口上通过的所有报文。当用户只要求对所有报文限速时，使用端口限速比较简单。

4.2 流量监管配置

表4-1 流量监管配置

操作	命令	说明
进入系统视图	**system-view**	-
定义类并进入类视图	**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则	**if-match** *match-criteria*	-
退出类视图	**quit**	-

操作		命令	说明
定义一个流行为并进入流行为视图		**traffic behavior** *behavior-name*	-
配置流量监管动作		**car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action*] [**yellow** *action*] [**red** *action*] [**hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]]	必选 分层CAR的详细情况请参见10.1.2 分层CAR
退出流行为视图		**quit**	-
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用QoS策略	基于端口	2.2.4 1. 基于端口应用QoS策略	-
	基于上线用户	2.2.4 2. 基于上线用户应用QoS策略	-
	基于VLAN	2.2.4 3. 基于VLAN应用QoS策略	-
	基于全局	2.2.4 4. 基于全局应用QoS策略	-
	基于控制平面	2.2.4 5. 基于控制平面应用QoS策略	-

说明

在一个流行为中，流量监管动作不能与重标记优先级（包括本地优先级、丢弃优先级、802.1p优先级、DSCP优先级、IP优先级）的动作同时配置，否则会导致QoS策略不能正常应用。

4.3 流量整形配置

本系列交换机的流量整形为基于队列的流量整形，即针对某一个队列的数据包设置整形参数。

表4-2 流量整形配置

操作		命令	说明
进入系统视图		**system-view**	-
进入端口视图或端口组视图	进入端口视图	**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*	
在端口配置流量整形		**qos gts queue** *queue-number* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	必选

4.4 端口限速配置

配置端口限速就是限制端口向外发送数据或者接收数据的速率。

表4-3 端口限速配置过程

操作		命令	说明
进入系统视图		**system-view**	-
进入端口视图或端口组视图	进入端口视图	**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*	
配置端口限速		**qos lr** { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]	必选

4.5 流量监管/流量整形/端口限速显示和维护

说明

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

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

表4-4 流量监管/流量整形/端口限速显示和维护

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

4.6 流量监管典型配置举例

4.6.1 流量监管典型配置举例

1. 配置需求

- 设备 Device A 通过端口 GigabitEthernet1/0/3 和设备 Device B 的端口 GigabitEthernet1/0/1 互连
- Server、Host A、Host B 可经由 Device A 和 Device B 访问 Internet

要求在设备 Device A 上对端口 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：

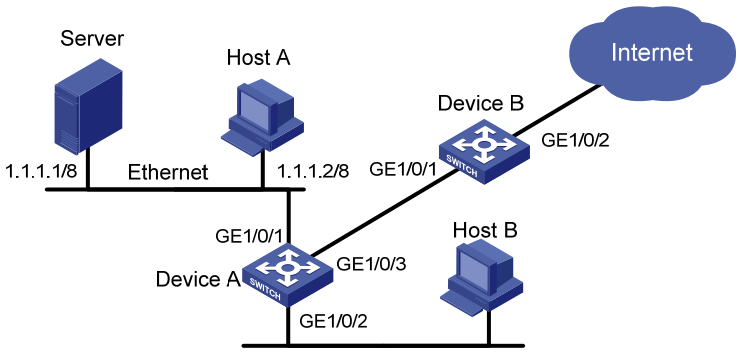
- 来自 Server 的报文流量约束为 1024kbps，流量小于 1024kbps 时可以正常发送，流量超过 1024kbps 时则将违规报文的 DSCP 优先级设置为 0 后进行发送；
- 来自 Host A 的报文流量约束为 256kbps，流量小于 256kbps 时可以正常发送，流量超过 256kbps 时则丢弃违规报文；

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 端口接收报文的总流量限制为 2048kbps，如果超过流量限制则将违规报文丢弃；
- 经由 Device B 的 GigabitEthernet1/0/2 端口进入 Internet 的 HTTP 报文流量限制为 1024kbps，如果超过流量限制则将违规报文丢弃。

2. 组网图

图4-5 流量监管配置组网图



3. 配置步骤

(1) 配置设备 Device A：

配置 ACL2001 和 2002，分别匹配来源于 Server 和 Host A 的报文流。

```
<DeviceA> system-view
[DeviceA] acl number 2001
[DeviceA-acl-basic-2001] rule permit source 1.1.1.1 0
[DeviceA-acl-basic-2001] quit
[DeviceA] acl number 2002
[DeviceA-acl-basic-2002] rule permit source 1.1.1.2 0
[DeviceA-acl-basic-2002] quit
```

创建流分类 server，匹配规则为 ACL 2001；创建流分类 host，匹配规则为 ACL 2002。

```
[DeviceA] traffic classifier server
[DeviceA-classifier-server] if-match acl 2001
[DeviceA-classifier-server] quit
[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 1024kbps，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 1024 red remark-dscp-pass 0
[DeviceA-behavior-server] quit
```

创建流行为 host，动作为流量监管，cir 为 256kbps，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 256
[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 应用到端口 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 number 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 2048kbps，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 2048
[DeviceB-behavior-car_inbound] quit
```

创建流行为 car_outbound，动作为流量监管，cir 为 1024kbps。

```
[DeviceB] traffic behavior car_outbound
[DeviceB-behavior-car_outbound] car cir 1024
[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 应用到端口 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 应用到端口 GigabitEthernet1/0/2 的入方向上。

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

5 拥塞管理配置

说明

拥塞管理功能中的“端口”包含了二层以太网端口和三层以太网端口，三层以太网端口是指被配置为三层模式以太网端口，的有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口”。

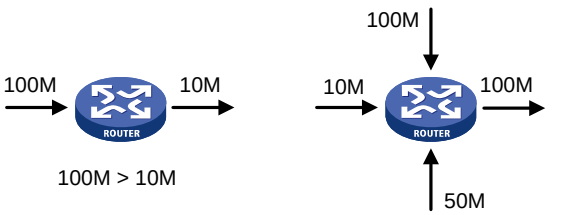
5.1 拥塞管理简介

5.1.1 拥塞的产生、影响和对策

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

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

图5-1 流量拥塞示意图



拥塞有可能会引发一系列的负面影响：

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

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

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

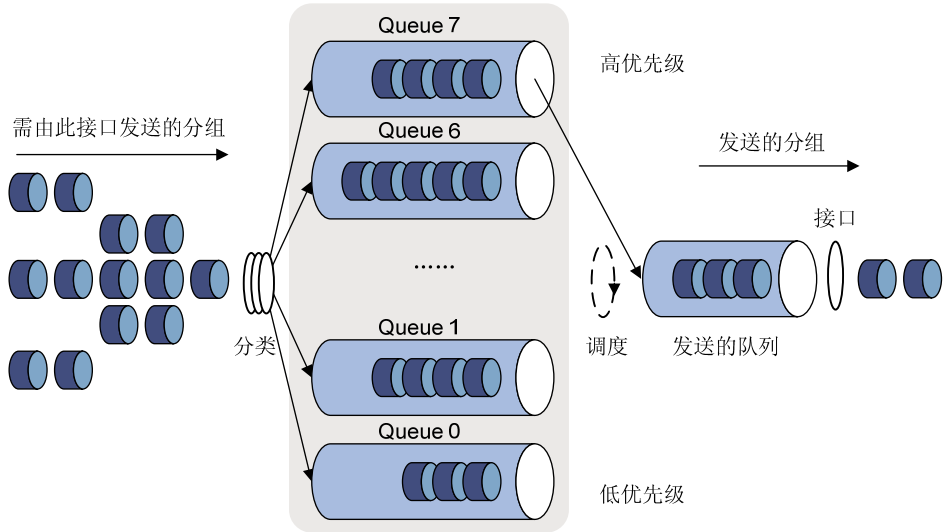
5.1.2 拥塞管理策略

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

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

1. SP队列

图5-2 SP 队列示意图



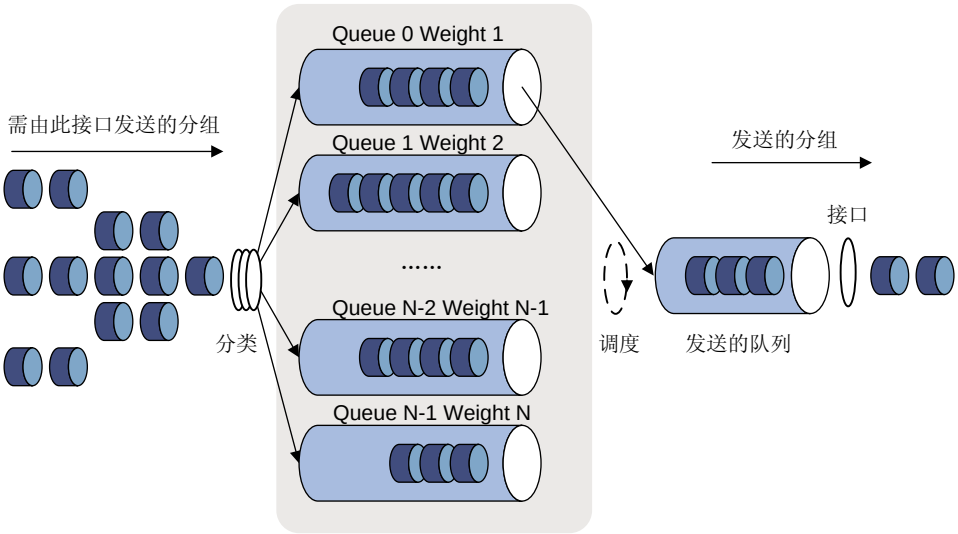
SP队列是针对关键业务类型应用设计的。关键业务有一个重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以 图 5-2 为例，优先队列将端口的 8 个输出队列分成 8 类，依次为 7、6、5、4、3、2、1、0 队列，它们的优先级依次降低。

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。

本系列交换机可以根据每次轮询调度的字节数或者报文个数来体现某个队列的调度权重，即使用字节数或报文个数作为调度单位。

以使用字节数为调度单位的 WRR 队列为例，如一个 1000Mbps 的端口，配置它的 WRR 队列的加权值为 5、5、3、3、1、1、1、1（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 50Mbps 的带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

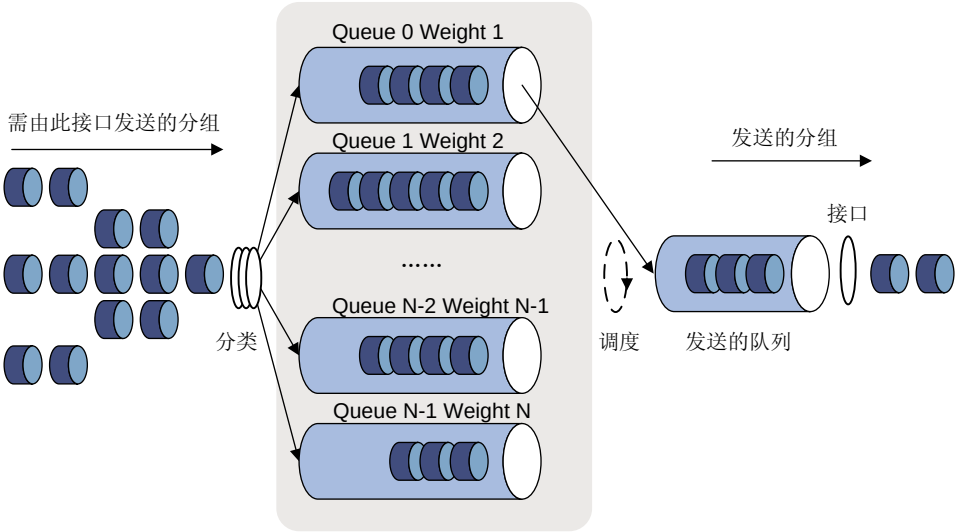
WRR 队列还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

3. WFQ队列

说明

本系列交换机中 S5500-28SC-HI 和 S5500-52SC-HI 不支持 WFQ 队列。

图5-4 WFQ 队列



WFQ 和 WRR 队列调度算法类似，在实际使用中可以与 WRR 相互替换。

WFQ 与 WRR 相比，WFQ 可以通过最小带宽保证机制与 WFQ 进行配合，具体实现如下：

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

例如：端口的总带宽为 10M、端口中当前共有 8 个队列，它们的权重分别为 1、1、1、1、3、3、5、5；每个流的最小带宽保证均为 128kbps。

- 可分配带宽=10M−（128k×8） = 9M。
- 可分配带宽总配额为所有权重的和。即：1+1+1+1+3+3+5+5 = 20。
- 每个流所占可分配带宽比例为：自身权重/所有队列权重的和。即每个流可得的可分配带宽比分别为：1/20、1/20、1/20、1/20、3/20、3/20、5/20、5/20。
- 最终每个队列得到的带宽=最小保证带宽＋该队列从可分配带宽中分到的带宽。

4. SP+WRR队列

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

5. SP+WFQ队列

说明

本系列交换机中 S5500-28SC-HI 和 S5500-52SC-HI 不支持 SP+WFQ 队列。

SP+WFQ 队列与 SP+WRR 队列的配置方式基本相同，即将部分队列加入 SP 调度组，另外的队列加入 WFQ 调度组。在进行队列调度时，首先调度 WFQ 组的队列中满足 WFQ 最小保证带宽的流量，然后按 SP 方式对 SP 组中的队列进行调度，最后再按 WFQ 组中各队列的调度权重进行轮询调度。

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
拥塞管理配置	配置SP队列	选择其中一种进行配置	5.3.1
	配置WRR队列		5.3.2
	配置WFQ队列		5.3.3
	配置SP+WRR队列		5.3.4
	配置SP+WFQ队列		5.3.5
	显示端口队列统计信息	可选	5.3.6

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	进入端口视图	**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SP队列		**qos sp**	必选 缺省情况下，端口使用WRR队列进行调度
显示SP队列		**display qos sp interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图下执行

2. 配置举例

(1) 组网需求

配置 GigabitEthernet1/0/1 采用 SP 队列。

(2) 配置步骤

进入系统视图

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

配置 GigabitEthernet1/0/1 的 SP 队列。

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

5.3.2 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*	
使能端口的WRR队列		**qos wrr** [**byte-count** | **weight**]	可选 缺省情况下，端口使用WRR队列进行调度
配置WRR队列的调度权重		**qos wrr** *queue-id* **group** *group-id* **byte-count** *schedule-value*	可选 请根据使能WRR队列时使用的调度权重选择二者之一进行配置 如果在端口上开启了WRR队列，缺省情况下使用报文个数作为调度权重，各队列的权重分别为1、2、3、4、5、9、13、15
		qos wrr *queue-id* **group** *group-id* **weight** *schedule-value*	
显示WRR队列的配置		**display qos wrr interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图下执行

说明

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

2. 配置举例

(1) 组网需求

- 配置端口 GigabitEthernet1/0/1 上的队列为 WRR 队列
- 配置所有队列均属于为 WRR 分组，权重分别为 1、2、4、6、8、10、12、14

(2) 配置步骤

进入系统视图。

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

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

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
```

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

(3) 组网需求

- 配置端口 GigabitEthernet1/0/1 的队列为 WRR 队列，使用报文个数作为调度权重。
- 配置所有队列均属于为 WRR 分组，权重分别为 1、2、4、6、8、10、12、14。

(4) 配置步骤

进入系统视图。

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

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

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

5.3.3 配置WFQ队列

说明

本系列交换机中 S5500-28SC-HI 和 S5500-52SC-HI 不支持 WFQ 队列。

1. 配置过程

表5-4 WFQ 队列配置过程

操作		命令	说明
进入系统视图		**system-view**	-
进入端口视图或端口组视图	进入端口视图	**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*	

操作	命令	说明
使能WFQ队列，并选择使用字节数或报文个数作为调度权重	**qos wfq** [**byte-count** | **weight**]	必选 缺省情况下，端口使用WRR队列进行调度
配置WFQ队列的调度权重值	**qos wfq** *queue-id* **group** *group-id* **byte-count** *schedule-value* **qos wfq** *queue-id* **group** *group-id* **weight** *schedule-value*	请根据使能WFQ队列时使用的调度权重选择二者之一进行配置 如果在端口上开启了WFQ队列，缺省情况下使用字节数作为调度权重，各队列的调度权重值均为1
配置WFQ队列的最小保证带宽值	**qos bandwidth queue** *queue-id* **min** *bandwidth-value*	可选 缺省情况下，各队列的最小保证带宽值均为64Kbps
显示WFQ队列配置	**display qos wfq interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图下执行

说明

在配置 WFQ 队列的调度权重值时，选择的调度权重（字节数或报文个数）需要与使能 WFQ 时使用的调度权重保持一致，否则将无法正常配置。

2. 配置举例

(1) 组网需求

配置端口 GigabitEthernet1/0/1 上的队列为 WFQ 队列，其中队列 1、3、4、5、6 的调度权重值分别为 2、5、10、10、10。

(2) 配置步骤

进入系统视图。

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

配置 GigabitEthernet1/0/1 的 WFQ 队列。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos wfq 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wfq 3 weight 5
[Sysname-GigabitEthernet1/0/1] qos wfq 4 weight 10
[Sysname-GigabitEthernet1/0/1] qos wfq 5 weight 10
[Sysname-GigabitEthernet1/0/1] qos wfq 6 weight 10
```

5.3.4 配置SP+WRR队列

1. 配置过程

表5-5 配置 SP＋WRR 队列

操作		命令	说明
进入系统视图		**system-view**	-
进入端口视图或端口组视图	进入端口视图	**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*	
配置端口使用WRR队列		**qos wrr** [**byte-count** | **weight**]	可选 缺省情况下，所有端口均使用WRR队列
将部分队列加入SP调度组		**qos wrr** *queue-id* **group sp**	必选 缺省情况下，当端口使用WRR队列时，所有队列均处于WRR调度组中
将部分队列加入WRR调度组		**qos wrr** *queue-id* **group** *group-id* { **weight** | **byte-count** } *schedule-value*	必选 如果在端口上开启了WRR队列，缺省情况下使用报文个数作为调度权重，队列0～7的权重分别为1、2、3、4、5、9、13、15

说明

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

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，使用报文个数作为 WRR 队列的调度权重
- 配置端口 GigabitEthernet 1/0/1 上的 0、1、2、3 队列属于 SP 调度组
- 配置端口 GigabitEthernet 1/0/1 上的 4、5、6、7 队列属于 WRR 调度组，权重分别为 2、4、6、8。

(2) 配置步骤

进入系统视图。

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

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

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr weight
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group sp
```

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

5.3.5 配置SP+WFQ队列

说明

本系列交换机中 S5500-28SC-HI 和 S5500-52SC-HI 不支持 SP+WFQ 队列。

1. 配置过程

表5-6 配置 SP＋WFQ 队列

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** *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*	
使能WFQ队列，并选择使用字节数或报文个数作为调度权重		**qos wfq** [**byte-count** | **weight**]	必选 缺省情况下，端口使用WRR队列进行调度
将部分队列加入SP调度组		**qos wfq** *queue-id* **group sp**	必选 缺省情况下，当端口使用WFQ队列时，所有队列均处于WFQ调度组中
将部分队列加入WFQ调度组		**qos wfq** *queue-id* **group** *group-id* { **weight** | **byte-count** } *schedule-value*	必选 如果在端口上开启了WFQ队列，缺省情况下使用字节数作为调度权重，各队列的调度权重值均为1
配置WFQ队列的最小保证带宽值		**qos bandwidth queue** *queue-id* **min** *bandwidth-value*	可选 缺省情况下，各队列的最小保证带宽值均为64Kbps

说明

在配置 WFQ 队列的调度权重值时，选择的调度权重（字节数或报文个数）需要与使能 WFQ 时使用的调度权重保持一致，否则将无法正常配置。

2. 配置举例

(1) 组网需求

- 配置端口 GigabitEthernet 1/0/1 使用 SP+WFQ 队列调度算法，其中 WFQ 的调度权重为报文个数
- 配置端口 GigabitEthernet 1/0/1 上的 0、1、2、3 队列属于 SP 调度组
- 配置端口 GigabitEthernet 1/0/1 上的 4、5、6、7 队列属于 WFQ 调度组，权重分别为 2、4、6、8，这四个队列的最小保证带宽值均为 128Kbps

(2) 配置步骤

进入系统视图。

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

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

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq weight
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wfq 1 group sp
[Sysname-GigabitEthernet1/0/1] qos wfq 2 group sp
[Sysname-GigabitEthernet1/0/1] qos wfq 3 group sp
[Sysname-GigabitEthernet1/0/1] qos wfq 4 group 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 4 min 128
[Sysname-GigabitEthernet1/0/1] qos wfq 5 group 1 weight 4
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 5 min 128
[Sysname-GigabitEthernet1/0/1] qos wfq 6 group 1 weight 6
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 6 min 128
[Sysname-GigabitEthernet1/0/1] qos wfq 7 group 1 weight 8
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 7 min 128
```

5.3.6 显示端口队列统计信息

通过查看端口的队列统计信息，您可以了解指定端口或全部端口的队列工作状态，包括曾经在队列中进行缓存的报文数量、以及队列中已发送和被丢弃的报文数量。

表5-7 显示端口队列统计信息

操作	命令	说明
显示端口队列统计信息	**display qos queue-statistics interface** [*interface-type interface-number*] [**outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	本命令可在任意视图下执行

6 拥塞避免

说明

拥塞避免功能中的“端口”包含了二层以太网端口和三层以太网端口，三层以太网端口是指被配置为三层模式以太网端口，的有关以太网端口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网端口”。

6.1 拥塞避免简介

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

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

1. 传统的丢包策略

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

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

2. RED与WRED

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

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

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

- 当队列的长度小于下限时，不丢弃报文；
- 当队列的长度超过上限时，丢弃所有到来的报文；
- 当队列的长度在上限和下限之间时，开始按用户配置的丢弃概率随机丢弃到来的报文。

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

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

队列平均长度既反映了队列的变化趋势，又对队列长度的突发变化不敏感，避免了对突发性数据流的不公正待遇。计算队列平均长度的公式为：平均队列长度=上一时刻平均队列长度＋（当前队列长度 - 上一时刻平均队列长度）/ 2^n。其中 n 可以通过命令 **queue weighting-constant** 进行配置。

6.2 WRED配置的说明

6.2.1 WRED的配置方式

本系列交换机的 WRED 功能采用 WRED 表的配置方式，即在系统视图下配置 WRED 表，然后在端口上应用 WRED 表。

6.2.2 WRED的参数说明

在进行 WRED 配置时，需要事先确定如下参数：

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

6.3 配置WRED

WRED 表是一个基于队列的表，发生拥塞时设备将根据报文所在队列进行随机丢弃。

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

6.3.1 配置过程

表6-1 WRED 表的配置和应用过程

操作		命令	说明
进入系统视图		**system-view**	-
配置WRED表		**qos wred queue table** *table-name*	-
配置计算平均队列长度的指数		**queue** *queue-id* **weighting-constant** *exponent*	可选 缺省情况下，该指数取值为9
配置WRED表的其它参数		**queue** *queue-id* [**drop-level** *drop-level*] **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]	可选 缺省情况下，*low-limit* 为 100，*high-limit*为1000，*discard-prob*为10
进入端口视图或端口组	进入端口视图	**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

操作		命令	说明
视图	进入端口组视图	**port-group manual** *port-group-name*	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
在端口应用WRED表		**qos wred apply** *table-name*	必选 缺省情况下，端口上没有应用WRED表

6.3.2 配置举例

配置 WRED 表，对队列 1 中的黄色报文，丢弃队列上限为 2000，下限为 500，丢弃概率为百分之 50，并将此 WRED 表应用到端口 GigabitEthernet 1/0/1 上。

进入系统视图

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

根据组网需求创建 WRED 表并配置相应的参数。

```
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 500 high-limit 2000 discard-probability 50
[Sysname-wred-table-queue-table1] quit
```

进入端口视图。

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

在端口上应用 WRED 表。

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

6.4 WRED显示和维护

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

表6-2 WRED 显示和维护

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

7 流量过滤配置

7.1 流量过滤简介

流量过滤就是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。

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 和 QoS 配置指导”中的“ACL 配置”。

7.2 配置流量过滤

表7-1 配置流量过滤

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

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

说明

如果配置了 **filter deny** 命令，则在该流行为视图下配置的其他流行为（除流量统计和流镜像）都不会生效。

7.3 流量过滤配置举例

7.3.1 流量过滤配置举例

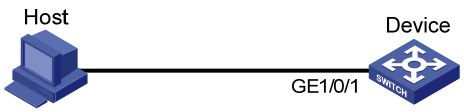
1. 组网需求

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

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

2. 组网图

图7-1 配置流量过滤组网图



3. 配置步骤

定义高级 ACL 3000，匹配源端口号等于 21 的数据流。

```
<DeviceA> system-view
[DeviceA] acl number 3000
[DeviceA-acl-adv-3000] rule 0 permit tcp source-port eq 21
[DeviceA-acl-adv-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**），对数据包进行丢弃。

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

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

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

```
[DeviceA-qospolicy-policy] quit
```

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

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

8 重标记配置

8.1 重标记简介

说明

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

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

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

8.2 根据报文颜色进行优先级重标记

8.2.1 报文颜色的标记方式

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

- 流量监管功能
- 映射丢弃优先级

1. 流量监管功能

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

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

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

说明

本系列交换机支持使用普通CAR以及聚合CAR两种流量监管功能为报文标记颜色，有关这两种功能的详细介绍和配置方法，请参见 流量监管、流量整形和端口限速配置以及 10.2 配置聚合CAR。

2. 映射丢弃优先级

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

说明

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

8.2.2 根据报文颜色进行优先级重标记

1. 基于流量监管的评估结果进行优先级重标记

在得到流量监管的评估结果之后，本系列交换机可以为不同颜色的报文重新标记各种优先级值，包括 DSCP 优先级、802.1p 优先级和本地优先级。您可以在流量监管动作中指定对不同颜色的报文采取的重标记动作，来重标记报文的优先级。

说明

关于在流量监管动作中指定重标记动作的配置，请参见 4.2 流量监管配置以及 10.2 配置聚合CAR。

2. 基于丢弃优先级的映射结果进行优先级重标记

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

说明

在一个流行为中，流量监管动作不能与重标记优先级（包括本地优先级、丢弃优先级、802.1p 优先级、DSCP 优先级、IP 优先级）的动作同时配置，否则会导致 QoS 策略不能正常应用。

8.3 配置重标记

表8-1 配置重标记

操作	命令	说明
进入系统视图	**system-view**	-
定义类并进入类视图	**traffic classifier** *tcl-name* [**operator** { **and** | **or** }]	-
定义匹配数据包的规则	**if-match** *match-criteria*	-
退出类视图	**quit**	-

操作		命令	说明
定义一个流行为并进入流行为视图		**traffic behavior** *behavior-name*	-
配置标记报文的DSCP值		**remark** [**green** | **red** | **yellow**] **dscp** *dscp-value*	可选
配置标记报文的802.1p优先级		**remark** [**green** | **red** | **yellow**] **dot1p** *8021p*	可选
配置内外层标签优先级复制功能		**remark dot1p customer-dot1p-trust**	可选
配置标记报文的丢弃优先级		**remark drop-precedence** *drop-precedence-value*	可选 仅应用在出方向
配置标记报文的IP优先级值		**remark ip-precedence** *ip-precedence-value*	可选
配置标记报文的本地优先级		**remark** [**green** | **red** | **yellow**] **local-precedence** *local-precedence*	可选
配置标记报文的本地优先级		**remark local-precedence** *local-precedence*	可选
配置标记报文的qos-local-id值		**remark qos-local-id** *local-id-value*	可选 qos-local-id是设备为报文重新标记的一种属性，用户可以根据不同的需求给报文标记不同的qos-local-id。标记qos-local-id主要用于对匹配多个流分类的报文进行重分类，再对这个重分类进行流行为动作，以达到对多种报文进行同一种处理方式的效果
退出流行为视图		**quit**	-
定义策略并进入策略视图		**qos policy** *policy-name*	-
在策略中为类指定采用的流行为		**classifier** *tcl-name* **behavior** *behavior-name*	-
退出策略视图		**quit**	-
应用QoS策略	基于端口	2.2.4 1. 基于端口应用QoS策略	-
	基于上线用户	2.2.4 2. 基于上线用户应用QoS策略	-
	基于VLAN	2.2.4 3. 基于VLAN应用QoS策略	-
	基于全局	2.2.4 4. 基于全局应用QoS策略	-
	基于控制平面	2.2.4 5. 基于控制平面应用QoS策略	-
显示重标记的相关配置信息		**display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图下执行

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

表8-2 inbound 和 outbound 方向的支持情况

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

8.4 重标记配置举例

8.4.1 重标记配置举例

1. 组网需求

公司企业网通过 Device 实现互连。网络环境描述如下：

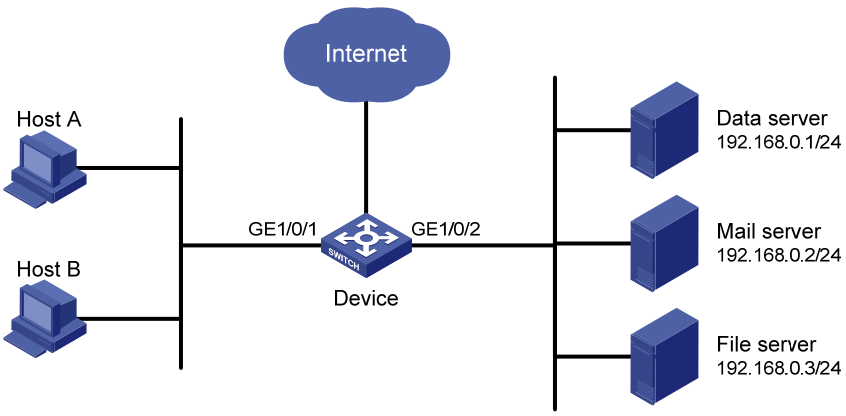
- Host A 和 Host B 通过端口 GigabitEthernet1/0/1 接入 Device；
- 数据库服务器、邮件服务器和文件服务器通过端口 GigabitEthernet1/0/2 接入 Device。

通过配置重标记功能，Device 上实现如下需求：

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

2. 组网图

图8-1 配置重标记组网图



3. 配置步骤

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

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

```
[Device-acl-adv-3000] rule permit ip destination 192.168.0.1 0
[Device-acl-adv-3000] quit
```

定义高级 ACL 3001，对目的 IP 地址为 192.168.0.2 的报文进行分类。

```
[Device] acl number 3001
[Device-acl-adv-3001] rule permit ip destination 192.168.0.2 0
[Device-acl-adv-3001] quit
```

定义高级 ACL 3002，对目的 IP 地址为 192.168.0.3 的报文进行分类。

```
[Device] acl number 3002
[Device-acl-adv-3002] rule permit ip destination 192.168.0.3 0
[Device-acl-adv-3002] quit
```

定义类 classifier_dbserver，匹配高级 ACL 3000。

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

定义类 classifier_mserver，匹配高级 ACL 3001。

```
[Device] traffic classifier classifier_mserver
[Device-classifier-classifier_mserver] if-match acl 3001
[Device-classifier-classifier_mserver] quit
```

定义类 classifier_fserver，匹配高级 ACL 3002。

```
[Device] traffic classifier classifier_fserver
[Device-classifier-classifier_fserver] if-match acl 3002
[Device-classifier-classifier_fserver] quit
```

定义流行为 behavior_dbserver，动作为重标记报文的本地优先级为 4。

```
[Device] traffic behavior behavior_dbserver
[Device-behavior-behavior_dbserver] remark local-precedence 4
[Device-behavior-behavior_dbserver] quit
```

定义流行为 behavior_mserver，动作为重标记报文的本地优先级为 3。

```
[Device] traffic behavior behavior_mserver
[Device-behavior-behavior_mserver] remark local-precedence 3
[Device-behavior-behavior_mserver] quit
```

定义流行为 behavior_fserver，动作为重标记报文的本地优先级为 2。

```
[Device] traffic behavior behavior_fserver
[Device-behavior-behavior_fserver] remark local-precedence 2
[Device-behavior-behavior_fserver] quit
```

定义策略 policy_server，为类指定流行为。

```
[Device] qos policy policy_server
[Device-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[Device-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[Device-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[Device-qospolicy-policy_server] quit
```

将策略 policy_server 应用到端口 GigabitEthernet1/0/1 上。

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

8.4.2 重标记qos-local-id配置举例

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

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

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

创建 ACL 2000，匹配源 IP 地址为 1.1.1.1 的报文。

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

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

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

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

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

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

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

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

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

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

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

将通过上面步骤创建的 QoS 策略应用到端口后，即可实现组网需求。

8.4.3 基于流量监管的颜色标记进行优先级重标记配置举例

说明

本系列交换机中 S5500-28SC-HI 和 S5500-52SC-HI 不支持本举例。

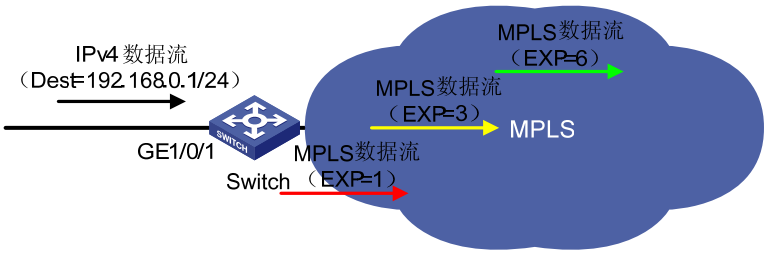
1. 组网需求

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

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

2. 组网图

图8-2 基于流量监管的评估结果进行重标记组网示意图



3. 配置步骤

(1) 配置 MPLS 基本功能

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

(2) 配置流量监管策略

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

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

创建流分类 class1，匹配规则为 ACL3000。

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

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

```
[Sysname] traffic behavior behavior1
```

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

创建 QoS 策略 policy1，将上面创建的流分类和流行为进行绑定。

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

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

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

9 流量重定向配置

9.1 流量重定向简介

流量重定向就是将符合流分类的流重定向到其他地方进行处理。

目前支持的流量重定向包括以下几种：

- 重定向到 CPU：对于需要 CPU 处理的报文，可以通过配置上送给 CPU。
- 重定向到端口：对于收到需要由某个端口处理的报文时，可以通过配置重定向到此端口。只针对二层转发报文。
- 重定向到下一跳：对于收到需要某台下游设备处理的报文时，可以通过配置重定向到该下游设备。该方式可用于实现策略路由，有关策略路由的介绍，请参见“三层技术-IP 路由配置指导”中的“策略路由配置”。

9.2 配置流量重定向

表9-1 配置流量重定向

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

说明

- 在配置重定向动作时，同一个流行为中重定向类型只能为重定向到 CPU、重定向到接口、重定向到下一跳中的一种。
- 引用重定向动作的 QoS 策略只能应用到端口、VLAN 或全局的入方向。
- 如果不配置重定向下一跳失败的处理动作，默认的处理动作是转发。
- 可以通过命令 **display traffic behavior user-defined** 查看流量重定向的相关配置信息。

9.3 流量重定向配置举例

9.3.1 重定向至下一跳配置举例

1. 组网需求

网络环境描述如下：

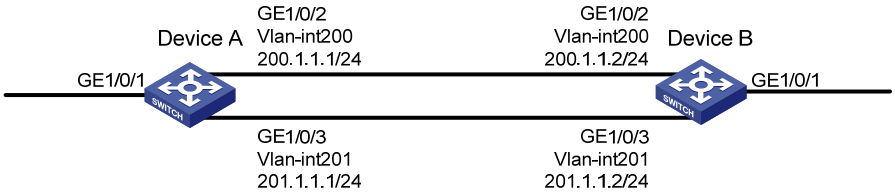
- Device A 通过两条链路与 Device B 连接，同时 Device A 和 Device B 各自连接其他的设备；
- Device A 上的端口 GigabitEthernet1/0/2 和 Device B 上的端口 GigabitEthernet1/0/2 属于 VLAN 200；
- Device A 上的端口 GigabitEthernet1/0/3 和 Device B 上的端口 GigabitEthernet1/0/3 属于 VLAN 201；
- Device A 上 VLAN 200 虚接口的 IP 地址为 200.1.1.1/24，VLAN 201 虚接口的 IP 地址为 201.1.1.1/24；
- Device B 上 VLAN 200 虚接口的 IP 地址为 200.1.1.2/24，VLAN 201 虚接口的 IP 地址为 201.1.1.2/24。

配置重定向至下一跳，实现策略路由功能，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 200.1.1.2；
- 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 201.1.1.2；
- 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 配置重定向至下一跳组网图



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 number 2000
[DeviceA-acl-basic-2000] rule permit source 2.1.1.1 0
[DeviceA-acl-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 number 2001
[DeviceA-acl-basic-2001] rule permit source 2.1.1.2 0
[DeviceA-acl-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 200.1.1.2。

```
[DeviceA] traffic behavior behavior_1
[DeviceA-behavior-behavior_1] redirect next-hop 200.1.1.2
[DeviceA-behavior-behavior_1] quit
```

定义流行为 behavior_2，动作为重定向至 201.1.1.2。

```
[DeviceA] traffic behavior behavior_2
[DeviceA-behavior-behavior_2] redirect next-hop 201.1.1.2
[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配置

10.1 全局CAR简介

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

目前全局 CAR 支持聚合 CAR 和分层 CAR 两种。

10.1.1 聚合CAR

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

10.1.2 分层CAR

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

分层 CAR 与普通 CAR（或聚合 CAR）的结合应用有两种模式：

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

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

10.2 配置聚合CAR

10.2.1 配置过程

表10-1 配置聚合 CAR

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

说明

在一个流行为中，引用聚合 CAR 的动作不能与重标记优先级（包括本地优先级、丢弃优先级、802.1p 优先级、DSCP 优先级、IP 优先级）的动作同时配置，否则会导致 QoS 策略不能正常应用。

10.3 配置分层CAR

表10-2 配置分层 CAR

操作	命令	说明
进入系统视图	**system-view**	-
配置分层CAR的各个参数	**qos car** *car-name* **hierarchy cir** *committed-information-rate* [**cbs** *committed-burst-size*]	必选

操作	命令	说明
进入流行为视图	**traffic behavior** *behavior-name*	必选
在流行为中引用分层CAR（和聚合CAR配合使用）	**car name** *car-name* **hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]	二者必选其一 普通CAR的相关内容请参见4.2 流量监管配置
在流行为中引用分层CAR（和普通CAR配合使用）	**car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action*] [**yellow** *action*] [**red** *action*] **hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]	
显示配置的流行为信息	**display traffic behavior user-defined** [*behavior-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	可选 **display**命令可以在任意视图下执行
显示指定全局CAR的CAR配置和统计信息	**display qos car name** [*car-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	

10.4 全局CAR显示和维护

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

在用户视图下执行 **reset** 命令可以清除全局 CAR 统计信息。

表10-3 全局 CAR 显示和维护

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

10.5 全局CAR配置举例

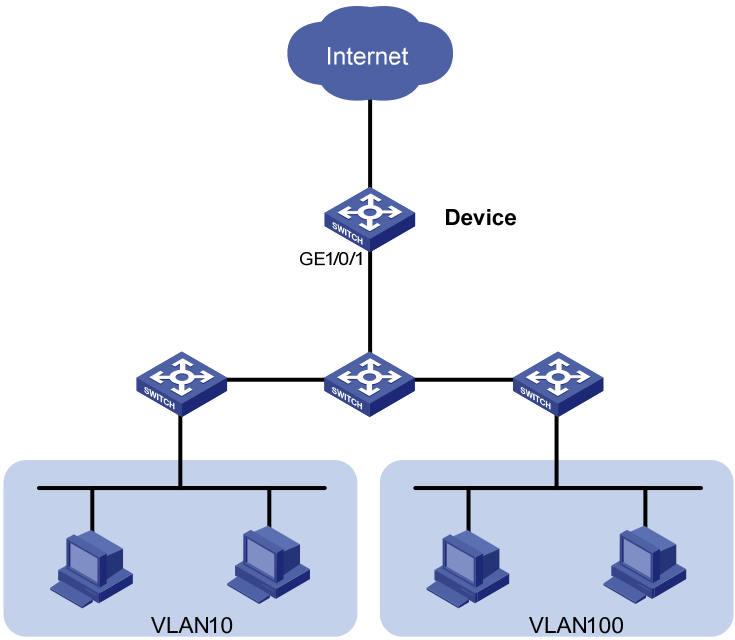
10.5.1 聚合CAR配置举例

1. 组网需求

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

2. 组网图

图10-1 聚合 CAR 配置举例组网图



3. 配置步骤

按流量限制需求配置聚合 CAR。

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

配置流分类和流行为，对 VLAN10 的报文采用聚合 CAR 的限速配置。

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

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

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

配置 QoS 策略，将流分类与流行为进行绑定。

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

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

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

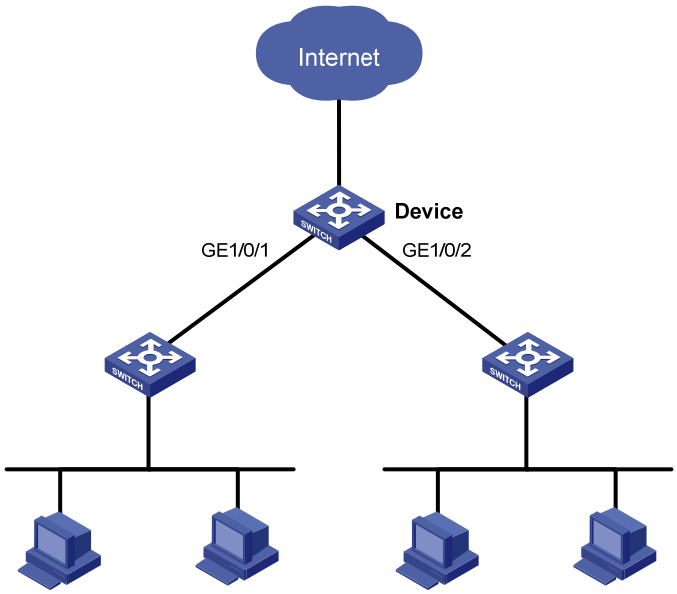
10.5.2 and模式分层CAR配置举例

1. 组网需求

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

2. 组网图

图10-2 and 模式配置举例组网图



3. 配置步骤

按流量限制需求配置分层 CAR。

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

配置 ACL 3000，匹配 HTTP 报文。

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

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

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

配置 QoS 策略，将流分类与流行为进行绑定。

```
[Device] qos policy http
```

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

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

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

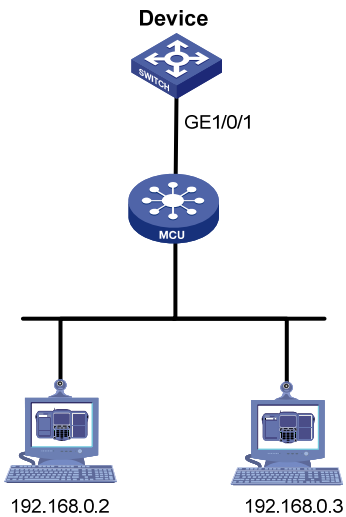
10.5.3 or模式分层CAR配置举例

1. 组网需求

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

2. 组网图

图10-3 or 模式配置举例组网图



3. 配置步骤

按流量限制需求配置分层 CAR。

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

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

```
[Device] acl number 2000
[Device-acl-basic-2000] rule permit source 192.168.0.2 0.0.0.0
[Device-acl-basic-2000] quit
[Device] traffic classifier 1
[Device-classifier-1] if-match acl 2000
[Device-classifier-1] quit
```

```
[Device] traffic behavior 1
[Device-behavior-1] car cir 256 hierarchy-car video mode or
[Device-behavior-1] quit
```

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

```
[Device] acl number 2001
[Device-acl-basic-2001] rule permit source 192.168.0.3 0.0.0.0
[Device-acl-basic-2001] quit
[Device] traffic classifier 2
[Device-classifier-2] if-match acl 2001
[Device-classifier-2] quit
[Device] traffic behavior 2
[Device-behavior-2] car cir 256 hierarchy-car video mode or
[Device-behavior-2] quit
```

配置 QoS 策略，将流分类与流行为进行绑定。

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

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

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

11 流量统计配置

11.1 流量统计简介

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

11.2 配置流量统计

表11-1 配置流量统计

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

11.3 流量统计显示和维护

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

11.4 流量统计配置举例

11.4.1 流量统计配置举例

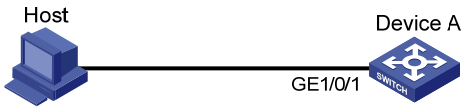
1. 组网需求

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

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

2. 组网图

图11-1 配置流量统计组网图



3. 配置步骤

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

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

定义类 classifier_1，匹配基本 ACL 2000。

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

定义流行为 behavior_1，动作为流量统计。

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

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

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

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

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

查看配置后流量统计的情况。

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

  Interface: GigabitEthernet1/0/1

  Direction: Inbound
```

```
Policy: policy
 Classifier: classifier_1
   Operator: AND
   Rule(s) : If-match acl 2000
   Behavior: behavior_1
    Accounting Enable:
      28529 (Packets)
```

12 配置数据缓冲区

12.1 数据缓冲区简介

12.1.1 数据缓冲区

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

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

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

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

12.1.2 缓冲资源的分配

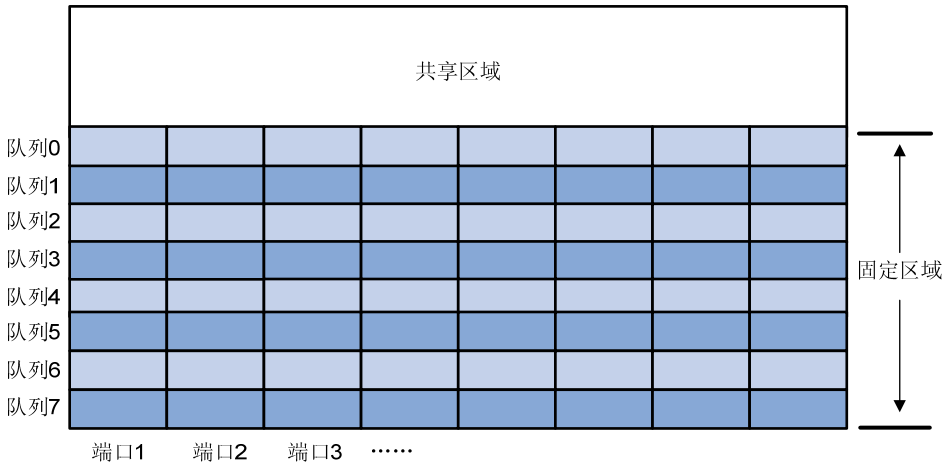
为了灵活应对网络中可能出现的突发流量，本系列交换机的 **cell** 和 **packet** 资源采用固定区域和共享区域的划分方式，资源耗尽的端口可以临时使用共享区域的资源来完成报文发送。用户可以手工设置 **cell** 资源和 **packet** 资源中共享区域所占的比例，其余部分将自动成为固定区域。


说明

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

在本系列交换机上，缓冲资源的划分方式如 图 12-1 所示：

图12-1 本系列交换机缓冲资源划分示意图



如 图 12-1 所示，固定区域的划分可以通过两个方向来进行：

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

12.1.3 共享区域的使用

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

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

1. 队列对共享区域的使用

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

2. 端口对共享区域的使用

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

说明

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

12.2 数据缓冲区配置

12.2.1 数据缓冲区的配置方式

用户可以使用以下两种方式配置本系列交换机的数据缓冲区：

- 由交换机自动配置（Burst 功能）
- 由用户手工配置

说明

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

12.2.2 通过Burst功能配置数据缓冲区

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

在下列情况下，Burst 功能可以提供更好的报文缓存功能和流量转发性能：

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

表12-1 通过 Burst 功能配置端口缓冲区

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

12.2.3 手工配置数据缓冲区

说明

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

1. 手工配置数据缓冲区配置任务简介

表12-2 手工配置数据缓冲区配置任务简介

配置任务	说明	详细配置
配置缓冲资源中共享区域的比例	请根据需要进行相应的配置	12.2.3 2.
配置队列的最小保证资源比		12.2.3 3.
配置队列的最大共享资源占用比		12.2.3 4.
配置端口的最大共享资源占用比		12.2.3 5.
应用数据缓冲区配置	必选	12.2.3 6.

2. 配置缓冲资源中共享区域的比例

表12-3 配置缓冲资源中共享区域的比例

操作	命令	说明
进入系统视图	**system-view**	-
配置**cell**资源中共享区域所占比例	**buffer egress** [**slot** *slot-number*] **cell total-shared ratio** *ratio*	至少配置其中一项 缺省情况下，**cell**资源中共享区域所占比例为64%，**packet**资源中共享区域所占比例为75%
配置**packet**资源中共享区域所占比例	**buffer egress** [**slot** *slot-number*] **packet total-shared ratio** *ratio*	

3. 配置队列的最小保证资源比

表12-4 配置队列的最小保证资源比

操作	命令	说明
进入系统视图	**system-view**	-
配置队列在**cell**缓冲区中的最小保证资源比	**buffer egress** [**slot** *slot-number*] **cell queue** *queue-id* **guaranteed ratio** *ratio*	至少配置其中一项 缺省情况下，每个队列在cell资源和packet资源的最小保证资源比均为13%
配置队列在**packet**缓冲区中的最小保证资源比	**buffer egress** [**slot** *slot-number*] **packet queue** *queue-id* **guaranteed ratio** *ratio*	

说明

- 由于端口的独享资源是由 8 个队列共同使用，因此当用户修改了某个队列的最小保证资源比之后，其它队列的最小保证资源比将随之自动变化，自动变化的原则为：除用户手工配置的最小保证资源比之外，剩余比例将平均分配给未进行手工配置的队列。例如，如果配置一个队列的最小保证资源比为 30%，则剩余 7 个队列的最小保证资源比将自动变化为 10%。
- 在配置队列的最小保证资源比时，需要注意通过手工配置的各个队列资源占用比例之和不能超过 100%。
- 队列的最小保证资源比对全局生效，即配置后每个端口上的该队列均能以相同的比例占用当前端口的独享资源。

4. 配置队列的最大共享资源占用比

表12-5 配置队列的最大共享资源占用比

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

说明

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

5. 配置端口的最大共享资源占用比

表12-6 配置端口的最大共享资源占用比

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

说明

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

6. 应用数据缓冲区的配置

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

表12-7 应用数据缓冲区的配置

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

13 附录

13.1 附录 A 缺省优先级映射表

说明

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

表13-1 dot1p-lp、dot1p-dp 缺省映射关系

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

表13-2 dscp-dp、dscp-dot1p 缺省映射关系

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

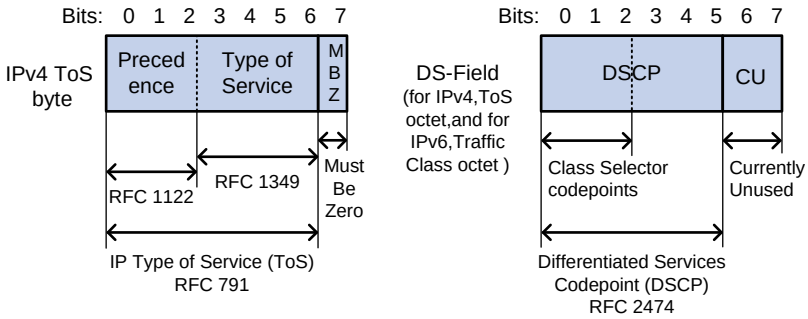
表13-3 exp-dp 缺省映射关系

映射输入索引	exp-dp 映射
exp 优先级	丢弃优先级(dp)
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

13.2 附录 B 各种优先级介绍

13.2.1 IP优先级和DSCP优先级

图13-1 ToS 和 DS 域



如 图 13-1 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13-4 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

IP 优先级（十进制）	IP 优先级（二进制）	关键字
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

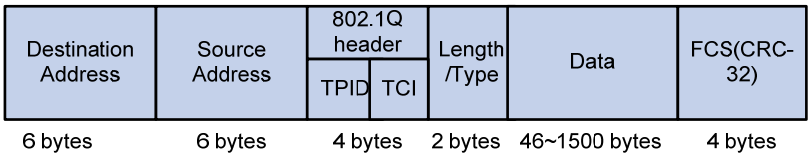
表13-5 DSCP 优先级说明

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）

13.2.2 802.1p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13-2 带有 802.1Q 标签头的以太网帧



如 图 13-2 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 13-3 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13-3 802.1Q 标签头

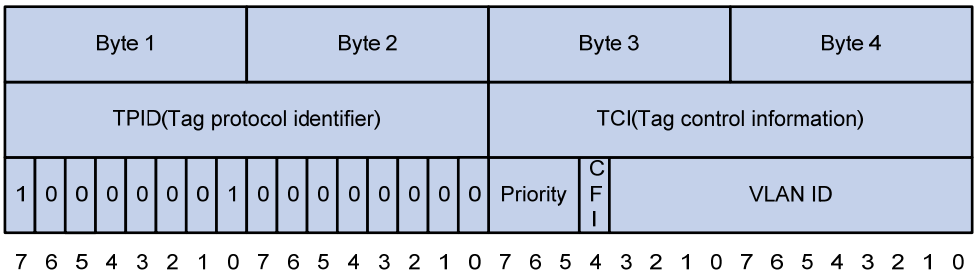


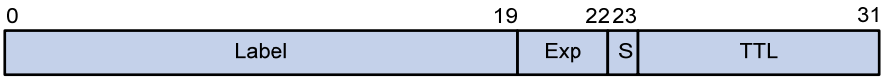
表13-6 802.1p 优先级说明

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

13.2.3 EXP优先级

EXP 优先级位于 MPLS 标签内，用于标记 MPLS QoS。

图13-4 MPLS 标签的封装结构



在 图 13-4 中，Exp字段就是EXP优先级。它由 3 个bit组成，取值范围为 0～7。

目 录

1 HQoS配置

说明

在阅读本文之前，建议您先通过“ACL 和 QoS 配置”中的“QoS”手册了解以下功能的基本介绍，以便您快速理解本文中的相关内容。

- 队列调度中的 SP、WRR 队列调度算法（“拥塞管理”章节）
- 各种优先级及优先级映射关系（“优先级映射”章节）
- 流量整形功能（“流量监管、流量整形和端口限速”章节）

1.1 HQoS简介

1.1.1 概述

目前计算机网络高速发展，语音、视频和重要数据越来越多地在网上进行传输，它们对带宽、延迟、抖动要求都比较高。为了能够保证传输质量，要求网络区分出不同的业务，进而为之提供相应的服务，QoS（Quality of Service，服务质量）技术应运而生。

随着用户规模的扩大、业务种类的增多，要求网络设备不仅能够进一步细化区分业务流量，而且还能够对多个用户、多种业务、多种流量等传输对象进行统一管理和分层调度。显然，这些应用对于传统的 QoS 技术来说是很难实现的。

HQoS（Hierarchical Quality of Service，分层 QoS）就是为解决以上问题而产生的，它采用多级调度的方式和全新的硬件设计，使设备具有内部资源的控制策略，既能够为高级用户提供质量保证，又能够从整体上节约网络构造成本。

1.1.2 HQoS的基本原理

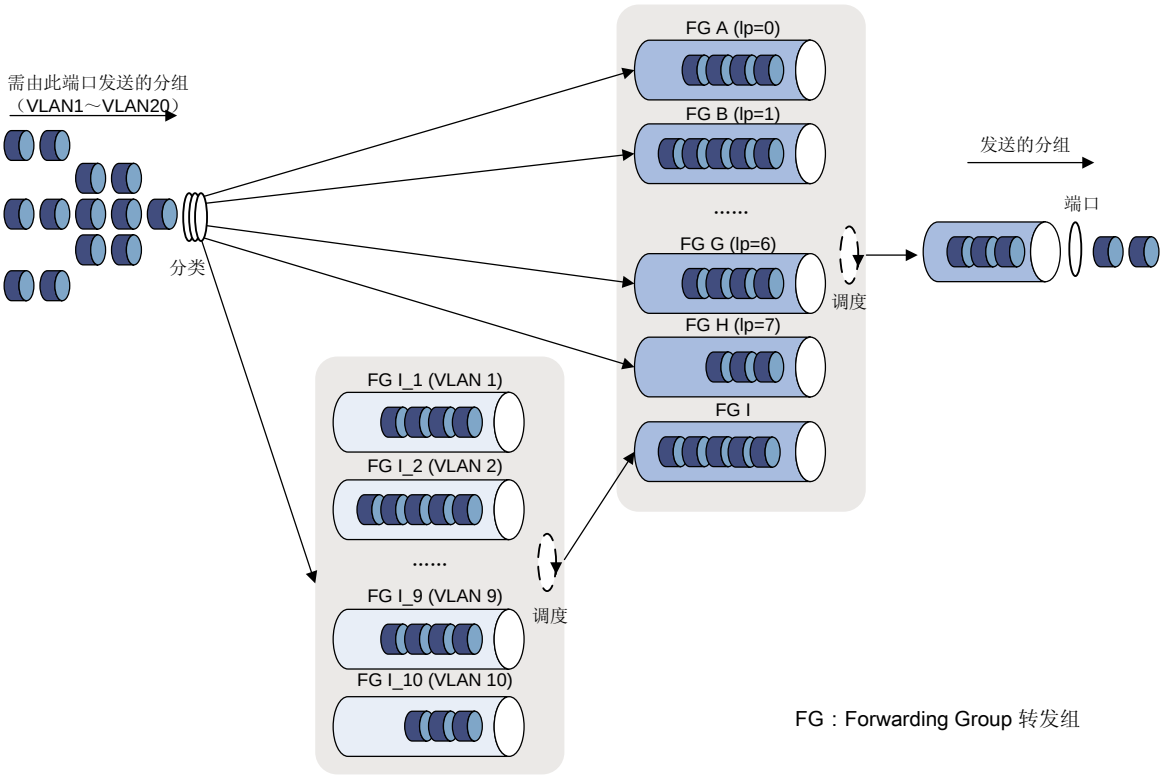
传统 QoS 的队列调度过程是根据报文的优先级字段将其映射到不同的发送队列，再通过队列间的不同调度算法实现队列调度和带宽分配。这种方式的调度依据只是业务流量的类别（优先级字段），而无法区分不同用户（通常用 VLAN 标识）的流量。

说明

关于队列调度的详细介绍，请参见“ACL 和 QoS 配置指导”中的“拥塞管理配置”。

本系列交换机支持的HQoS技术能够在传统队列调度功能的基础上增加对于不同VLAN报文的调度过程，即：在端口要发送的流量中，首先对部分VLAN的报文进行调度，调度完成后的流量再与其他流量进行再次的调度，从而实现对流量的两层调度过程，保证高优先级用户的流量传输。下面我们以 图 1-1 为例进行详细介绍。

图1-1 HQoS 实现方式示意图



在 HQoS 中，我们使用“转发组”的概念来代替传统 QoS 中的“队列”，转发组之间可以通过 SP 或 WRR 方式实现类似于队列调度的调度过程。

假设端口可以发送VLAN1～VLAN20 的报文，其中VLAN1～VLAN10 为优先级较高的用户，他们的流量希望被优先发送。我们可以首先将VLAN1～VLAN10 的流量分别划分到 10 个转发组中（图 1-1 中的FG I_1～FG I_10），并在这 10 个转发组之间进行调度，调度后的报文汇集到另一个转发组中（图 1-1 中的FG I），这个过程我们称为第二层调度。

对于端口上剩余 10 个VLAN（VLAN11～VLAN20）的流量，我们将其按本地优先级划分到 8 个转发组（图 1-1 中的FG A～FG H）。此时端口上将存在 9 个转发组，我们可以在这 9 个转发组之间再次进行调度，这个过程称为第一层调度。在第一层调度过程中，通过提高转发组FG I的调度优先等级，便可以实现对VLAN1～VLAN10 的报文进行优先发送，而其余VLAN的报文将仅根据报文优先级进行调度。

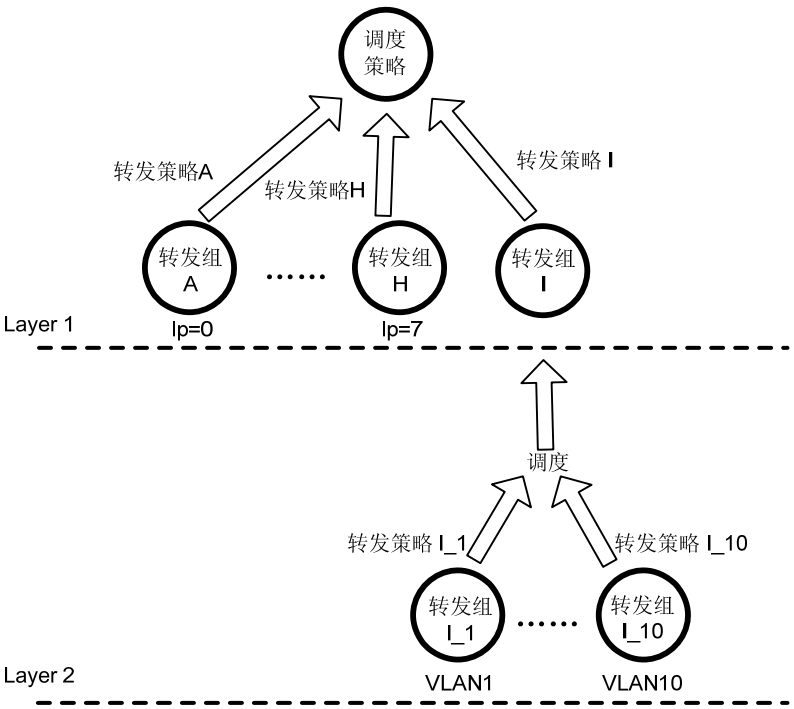
在上面的举例中，FG I 的流量是根据其他转发组经过调度汇集而来，这种转发组称为父转发组，而相应的 FG I_1～FG I_10 称为子转发组，二者之间的关系称为转发组的嵌套。

说明

- 在本系列交换机上，第一层调度最多可以调度 9 个转发组的流量。
- 在第一层调度中，最多只能存在一个父转发组，父转发组中最多可以嵌套 16 个子转发组。
- HQoS的转发组也可以和传统QoS的队列进行混合调度，具体的调度方法请参见后面章节的介绍（1.3.5 在端口上应用调度策略）。为方便您理解，建议先完成本节内容的学习后再查看混合调度的具体实现。

为便于您理解HQoS的调度机制，我们将 图 1-1 中描述的实现过程简化为如 图 1-2 的树形示意图。

图1-2 HQoS 基本原理示意图



如 图 1-2 所示，HQoS首先完成第二层的队列调度，然后将其调度的结果再参与第一层的调度过程。这样，我们可以为子转发组在第二层调度中配置一定的转发调度动作（包括调度算法、调度权重、整形参数），对流量进行第一次流量管理；当子转发组的流量汇集到父转发组后，我们再为父转发组在第一层调度中配置不同的流量控制参数，对汇聚的流量进行再一次流量管理动作。

针对不同的分类需求（如用户、流量类型等），可以为不同调度层次中的转发组配置不同的分类规则，从而实现对流量进行多层次的流量管理。

1.1.3 HQoS的基本概念

了解以下 HQoS 的基本概念，有助于您顺利的理解下面配置过程的目的和层次，使您快速掌握 HQoS 的配置技巧。

(1) 转发组

转发组（FG，Forwarding Group）：一个转发组对应一部分带有特定特征（VLAN ID 或本地优先级值）的流量，具备这种特征的流量将通过该转发组参与调度和转发。

(2) 转发策略

转发策略（FP，Forwarding Profile）：对转发组的流量采用的控制动作，包括调度算法、调度权重、流量整形等。将转发组与转发策略进行关联，即可决定该转发组可获得的调度优先级与带宽资源。

(3) 调度策略

调度策略（SP，Scheduler policy）：通过将各个转发组与不同转发策略进行关联，并将这些关联关系进行组合，形成一套转发策略集，便称为调度策略。将调度策略应用至端口，即可实现 HQoS 功能。

(4) 调度分层

调度层次（Layer）：转发组参与调度的的层次，如 图 1-2 中的Layer1 和Layer2。父转发组和未嵌套转发组的转发组位于Layer1，子转发组位于Layer2。

(5) 实例化

实例化是指将流量按匹配规则划分到不同转发组的过程，例如在 图 1-1 中将VLAN1～VLAN10 划分到不同的转发组（I_1～I_10）。通过配置一定的实例化规则（匹配规则），可以将不同的流量进行分类，对应到不同的转发组，并按照该转发组的转发策略进行调度。

1.2 HQoS配置任务简介

HQoS 的配置过程就是一个树状调度策略模型的组装过程。您需要先创建组装树的元素——转发组；然后创建转发组的嵌套关系，并为每个转发组关联转发策略；最后为各个转发组配置分类规则（实例化），从而决定转发组所对应的流量。

如 图 1-2 所示，可以将HQoS的配置过程分为如下几个阶段：

(1) 创建转发组和转发策略。

(2) 建立转发组的嵌套关系并为子转发组关联转发策略。

(3) 创建调度策略，将参与第一层调度的转发组嵌套进调度策略，并为这些转发组关联相应的转发策略。

(4) 转发组的实例化，即为转发组配置流量分类规则的过程（例如，在第一层调度中将本地优先级为 0 的流量匹配到转发组 A1，按转发策略 A1 的动作进行处理；在第二调度中层将 VLAN1 的流量匹配到转发组 B1，按转发策略 B1 的动作进行处理）。

(5) 在端口上应用调度策略，即在端口上实现 HQoS 调度功能。

下面按照以上顺序详细介绍 HQoS 的配置过程。

表1-1 HQoS 配置任务简介

配置任务		说明	详细配置
HQoS配置	配置转发策略	必选	1.3.1
	配置转发组	必选	1.3.2
	配置调度策略	必选	1.3.3
	转发组的实例化	必选	1.3.4
	在端口上应用调度策略	必选	1.3.5

配置任务		说明	详细配置
转发组和调度策略的拷贝	拷贝转发组	可选	1.4.1
	拷贝调度策略	可选	1.4.2

1.3 HQoS配置

1.3.1 配置转发策略

在一个调度策略树中，每一个转发组都需要配置相应的转发策略，转发策略的内容表示对该转发组的流量所作的一系列动作。

配置转发策略主要包括以下两方面内容：

- 创建自定义转发策略
- 修改自定义转发策略的内容

1. 创建自定义转发策略

表1-2 创建自定义转发策略

操作	命令	说明
进入系统视图	**system-view**	-
创建自定义转发策略	**qos forwarding-profile** *fp-name* [**id** *fp-id*]	必选 该命令可用来创建一个新的自定义转发策略，也可以用来进入一个已经存在的转发策略视图

2. 修改自定义转发策略的内容

您可以修改自定义转发策略的内容。转发策略的内容包括：队列调度方式、流量整形和最小带宽保证。

转发策略中支持的队列调度方式有 SP 和 WRR 两种，与转发策略关联的转发组将使用策略中配置的调度方式参与队列调度。同时，您也可以通过配置流量整形和最小带宽保证，将转发组的流量发送速率控制在一定的区间内，实现更精确的流量管理。

为简化描述，下文中将队列调度方式为 SP 的转发策略简称为 SP 转发策略，队列调度方式为 WRR 的转发策略简称为 WRR 转发策略。

表1-3 修改自定义转发策略的内容

操作		命令	说明
进入系统视图		**system-view**	-
进入自定义转发策略视图		**qos forwarding-profile** *fp-name* [**id** *fp-id*]	-
配置队列调度	配置严格优先队列调度方式（SP）	**sp**	请选择其中一种调度方式 缺省情况下，没有配置转发策略的

操作		命令	说明
方式	配置加权轮循队列调度方式及调度权重值（WRR）	**wrr** [**weight** *weight-value*]	队列调度方式
配置整形参数		**gts cir** *cir-value* [**cbs** *cbs-value*] [**ebs** *ebs-value*] [**pir** *pir-value*]	可选 缺省情况下，转发策略中不存在GTS配置，不对速率进行限制
配置最小带宽保证		**bandwidth** *bandwidth-value*	可选 缺省情况下，转发策略中不存在最小带宽保证配置 S5500-28SC-HI和S5500-52SC-HI不支持本命令

说明

- 关于 SP 和 WRR 队列调度算法的详细介绍，请参见“ACL 和 QoS 配置指导”中的“拥塞管理配置”。
- 在转发策略中配置的WRR调度算法以字节数为调度单位，其权重值与以字节数为调度单位的普通WRR队列的权重值含义相同。HQoS转发组可以与端口上以字节数为调度单位的普通WRR队列进行共同调度，HQoS转发组的权重将直接参与WRR调度的权重分配计算过程。有关转发组与普通WRR队列的共同调度，请参见 在端口上应用调度策略。有关WRR队列调度单位的内容，请参见“拥塞管理配置”。
- 转发策略在一个调度策略树中可以被不同的转发组使用，转发组对于其匹配的转发策略的内容要求是不同的。在修改转发策略的内容时，系统会根据转发策略匹配的调度实体的类型进行判断和限制。因此，可能会有依照命令行帮助信息提示输入的合法修改命令，却修改失败的情况出现。
- 修改已经应用在端口上的转发策略时，可能会有由于硬件资源不足而导致修改失败的情况出现。

1.3.2 配置转发组

转发组是调度策略中的一个基本调度实体，也是实例化的操作对象，因此，创建转发组是配置一个调度策略的必要步骤。

配置转发组主要有两方面内容：

- 创建自定义转发组
- 配置转发组的嵌套关系

1. 创建自定义转发组

表1-4 创建自定义转发组

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建自定义转发组	**qos forwarding-group** *fg-name* [**id** *fg-id*]	必选 该命令可用来创建一个新的自定义转发组，也可以用来进入一个已经存在的转发组视图

2. 配置转发组的嵌套关系

在配置转发组嵌套关系（例如在 图 1-1 中的队列 8 中嵌套转发组 9～转发组 18）时，需要您同时为嵌套的子转发组关联指定的转发策略。

您可以将一个父转发组下嵌套的所有子转发组全部关联 SP 转发策略或 WRR 转发策略，实现子转发组之间使用 SP 队列调度或 WRR 队列调度。

当多个子转发组关联到 SP 转发策略时，这些子转发组的调度优先顺序与用户配置的顺序相反，即后嵌套的子转发组在 SP 调度时被优先调度，最先嵌套的子转发组被最后调度。

您也可以将部分子转发组与 SP 转发策略关联，其余子转发组与 WRR 转发策略关联，实现 SP+WRR 调度。在使用 SP+WRR 调度时，设备将首先按与用户配置相反的顺序调度关联了 SP 转发策略的子转发组，然后再按加权轮询方式调度关联了 WRR 转发策略的子转发组。

说明

对于本系列交换机，在一个端口上只有一个转发组可以嵌套子转发组，且最多可嵌套的子转发组数量为 16 个。

表1-5 配置转发组的嵌套关系

操作	命令	说明
进入系统视图	**system-view**	-
进入自定义转发组视图	**qos forwarding-group** *fg-name* [**id** *fg-id*]	-
配置嵌套的子转发组以及子转发组与转发策略的关联	**forwarding-group** *sub-fg-name* **profile** *fp-name*	必选 重复执行该命令，可以为一个转发组嵌套多个子转发组

说明

- 系统会对转发组关联的转发策略内容进行检查，对于和转发组有冲突的转发策略，关联关系将无法创建。
- 配置转发组与转发策略的关联命令可以在转发组内嵌套一个新的转发组并关联转发策略，同时也可以为一个已经存在的转发组更换转发策略。
- 转发组不能嵌套自身。

1.3.3 配置调度策略

调度策略是一套多个转发组和转发策略关联关系的集合，通过将这些关联关系进行组装，并指定其所属的调度层次，便可以完成树形 HQoS 策略的建立。

配置调度策略主要有两方面内容：

- 创建自定义调度策略
- 配置调度策略嵌套转发组

1. 创建自定义调度策略

表1-6 创建自定义调度策略

操作	命令	说明
进入系统视图	**system-view**	-
创建自定义调度策略	**qos scheduler-policy** *sp-name* [**id** *sp-id*]	必选 该命令可用来创建一个新的自定义调度策略，也可以用来进入一个已经存在的调度策略视图

2. 配置调度策略嵌套转发组

配置调度策略嵌套转发组的过程与配置转发组嵌套关系的过程类似，既可以配置调度策略中嵌套的转发组，也可以为转发组指定关联的转发策略。如果在调度策略中需要嵌套带有嵌套关系的转发组，只需要将父转发组嵌套至调度策略，子转发组将自动完成嵌套过程。

一个调度策略可以嵌套多个转发组。同一个转发组也可以被不同的调度策略嵌套，在被不同的调度策略嵌套时可以关联不同的转发策略。

您可以将一个调度策略下嵌套的所有转发组全部关联 SP 转发策略或 WRR 转发策略，实现转发组之间使用 SP 队列调度或 WRR 队列调度；也可以将部分转发组与 SP 转发策略关联，其余转发组与 WRR 转发策略关联，实现 SP+WRR 调度。在使用 SP+WRR 调度时，将首先按严格优先顺序调度关联了 SP 转发策略的转发组，然后再按加权轮询方式调度关联了 WRR 转发策略的转发组。

当多个转发组关联到SP转发策略时，将首先调度嵌套有子转发组的父转发组，然后按照转发组实例化时匹配的本地优先级，由高到低依次调度转发组。关于实例化的内容，请参见 转发组的实例化。

表1-7 调度策略嵌套转发组

操作	命令	说明
进入系统视图	**system-view**	-
进入自定义调度策略视图	**qos scheduler-policy** *sp-name* [**id** *sp-id*]	-
配置调度策略下嵌套的转发组以及与该转发组关联的转发策略	**forwarding-group** *fg-name* **profile** *fp-name*	必选

说明

- 系统会对转发组关联的转发策略内容进行检查，对于和转发组有冲突的转发策略，关联关系将无法创建。
- 在调度策略视图下执行 **forwarding-group profile** 命令可以在调度策略内嵌套一个新的转发组并关联转发策略，同时也可以为一个已经在调度策略内存在的转发组更换转发策略。
- 一个调度策略树中最多可以关联 9 个转发组。
- 在一个调度策略中嵌套的转发组不能重复，即在一个调度策略树中，所有转发组是唯一的。

1.3.4 转发组的实例化

1. 实例化的作用

HQoS 的最大特点就是能够对流量进行多层次、多业务类型的控制和调度。实现此目的的前提是：系统能够对流量按照不同用户/业务类型进行分类。

实例化操作的作用有两个：

- 指定转发组在调度策略中所处的层次（请参考 图 1-2）；
- 以用户（VLAN）或业务类型（优先级）为分类规则来区分流量。

2. 实例化的方式

根据转发组下是否嵌套有子转发组，实例化操作有 match 和 group 两种方式：

- match 方式：需要明确指定实例化规则，用于子转发组或没有嵌套子转发组的转发组；
- group 方式：不需要明确指定实例化规则，用于父转发组。需要注意的是，父转发组下嵌套的子转发组必须使用 match 方式明确指定实例化规则。

对于本系列交换机，在使用 match 方式进行实例化操作时，位于不同调度层次上的转发组的实例化匹配条件不同：

- 对于 Layer2 的转发组，匹配规则需要配置为 **service-vlan-id**，即报文的 VLAN。
- 对于 Layer1 的转发组，匹配规则需要配置为 **local-precedence**，即报文的本地优先级。

3. 实例化的配置

由于QoS队列是以本地优先级为划分依据，因此每次在Layer1 配置一个转发组的实例化（匹配本地优先级），就相当于将一个的QoS队列转化为HQoS转发组。您可以将端口上的 8 个QoS队列全部转化为HQoS转发组，也可以仅转化部分队列。未转化的QoS队列将与HQoS转发组共同进行调度，调度方式请参见 在端口上应用调度策略。

表1-8 转发组的实例化

操作	命令	说明
进入系统视图	**system-view**	-
进入调度策略视图	**qos scheduler-policy** *sp-name* [**id** *sp-id*]	-
进入层次视图	**layer** { **1** | **2** }	-

操作			命令	说明
实例化自定义转发组	采用match方式	Layer 1	**forwarding-group** *fg-name* **match local-precedence** *local-precedence*	二者必选其一
		Layer 2	**forwarding-group** *fg-name* **match service-vlan-id** { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* } }	
	采用group方式		**forwarding-group** *fg-name* **group**	

说明

- 实例化操作是有一定顺序的，在一个调度策略树中，如果父转发组没有实例化，子转发组是不允许实例化的。当取消实例化操作时，当子转发组未完全取消实例化时，父转发组不能取消实例化。
- 在配置实例化时，各个转发组所匹配的运营商网络 VLAN 或本地优先级不能相同。
- 在使用 match 方式进行实例化时，虽然可以通过多次执行 **forwarding-group match** 命令为某个转发组指定多条匹配规则，但只有第一次配置的匹配规则生效。

1.3.5 在端口上应用调度策略

说明

在端口上应用调度策略后，该端口上将不能再配置部分 QoS 功能（包括配置流量整形、拥塞避免功能和修改队列调度方式），关于这些 QoS 功能的相关内容请参考“ACL 和 QoS 配置指导”中的“QoS”。

调度策略只有应用在端口上，并且指明应用的方向，才能对流量起控制和管理作用，实现 HQoS 功能。

如果你在实例化过程中，没有将 QoS 队列全部转化为 HQoS 转发组，则未转化的 QoS 队列将按照端口上缺省的调度方式进行调度，即 WRR 队列调度算法。此时，设备会根据转发组关联的转发策略，将 Layer1 的转发组与未匹配的流量共同进行调度：

(1) 如果存在关联了 SP 转发策略的转发组，则端口先按严格优先级顺序调度这些转发组中的流量。

(2) 对于关联了WRR转发策略的转发组，端口会根据转发策略中配置的WRR权重值（请参见 配置转发策略），将这些转发组与端口上WRR队列中的流量一起进行轮询调度。

说明

- 在本系列交换机上，只有在万兆端口上才能够应用调度策略，其余端口均不能实现 HQoS 功能。
- 目前本系列交换机仅支持在端口的出方向应用调度策略。

1. 配置准备

将调度策略应用到端口之前，请确认调度策略中嵌套的每一个转发组都已经完成实例化操作。

2. 在端口上应用调度策略

表1-9 在端口上应用调度策略

操作		命令	说明
进入系统视图		**system-view**	-
进入二层以太网端口视图或端口组视图	进入二层以太网端口视图	**interface** *interface-type interface-number*	二者必选其一 进入二层以太网端口视图后，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** *group-name*	
在端口/端口组上应用调度策略		**qos apply scheduler-policy** *sp-name* **outbound**	必选

说明

- 每个端口上只能应用一个调度策略。
- 对于应用在端口上的调度策略，在不改变调度策略树状结构（即不增删转发组）的前提下，可以修改、替换转发组关联的转发策略及其内容。如果要改变调度策略树状结构，如增删转发组、实例化等操作，需要先取消该调度策略在端口上的应用。

1.4 转发组和调度策略的拷贝

为了简化配置过程，允许对转发组和调度策略进行拷贝操作。

1.4.1 拷贝转发组

拷贝转发组的操作可以一次拷贝生成多个目的转发组，这些目的转发组的编号由系统自动生成。

拷贝生成的转发组除了名字和编号各不相同外，嵌套的内容完全相同。

由于系统允许创建的转发组数目存在上限，当由于拷贝操作使系统中的转发组总数超过上限时，则拷贝任务中止。

表1-10 拷贝转发组

操作	命令	说明
进入系统视图	**system-view**	-
拷贝转发组	**qos copy forwarding-group** *fg-source* **to** *fg-dest*&<1-8>	必选

1.4.2 拷贝调度策略

和转发组的拷贝操作不同，调度策略的一次拷贝操作只能生成一个目的调度策略，目的调度策略的编号由系统自动生成。

拷贝生成的目的调度策略除了与源调度策略名字和编号不相同外，嵌套的内容完全相同，包括实例化的内容。

表1-11 拷贝调度策略

操作	命令	说明
进入系统视图	**system-view**	-
拷贝调度策略	**qos copy scheduler-policy** *sp-source* **to** *sp-dest*	必选

1.5 HQoS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 HQoS 的运行情况，通过查看显示信息验证配置的效果。

表1-12 HQoS 显示和维护

操作	命令
显示转发组的信息	**display qos forwarding-group** [*fg-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示转发策略的信息	**display qos forwarding-profile** [*fp-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示调度策略的信息	**display qos scheduler-policy name** [*sp-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口的调度策略信息	**display qos scheduler-policy interface** [*interface-type interface-number* [**outbound**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示端口的调度策略诊断信息	**display qos scheduler-policy diagnosis interface** [*interface-type interface-number* [**outbound**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.6 HQoS典型配置举例

1.6.1 HQoS典型配置举例

Service-VLAN 方式是一种较为常见的城域网组网方式，主要特点是以运营商 VLAN 来区分不同的用户群，每个用户的多种业务都在一个 VLAN 内承载。接入广域网设备的用户基本分为两种用户类型：个人用户和企业用户。个人用户的业务类型一致，流量管理要求也基本一致。企业用户的业务类型有很大不同，并且要求能够区分不同的企业用户，并进行不同的流量管理。

1. 组网需求

组网需求如 表 1-13 所示。

说明

S5500-28SC-HI 和 S5500-52SC-HI 不支持本例中关于最小带宽保证的配置。

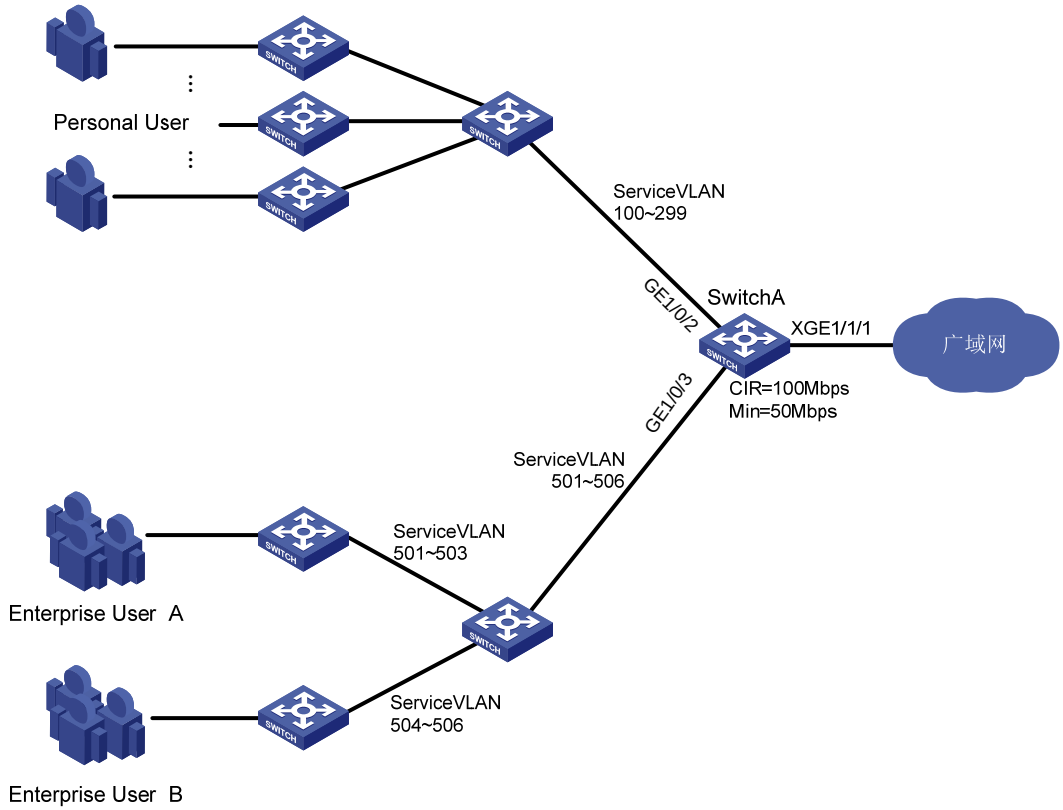
表1-13 组网需求

项目	需求内容
个人用户群的流量策略	承载个人用户群A的Service VLAN ID范围为100～299； 个人用户分四种业务类型： • VoIP（Voice over IP，在 IP 上传送语音）业务：最高优先级，802.1p 优先级 6、7，优先级为 6 的流量最小带宽保证为 20Mbps，优先级为 7 的流量最小带宽保证为 30Mbps； • VoD（Video on Demand，视频点播）业务：高优先级，802.1p 优先级 4、5； • VPN（Virtual Private Network，虚拟专用网）业务：普通优先级，802.1p 优先级 2、3； • HTTP 浏览业务：低优先级，802.1p 优先级 0、1。
企业用户群的流量策略	承载企业用户群的Service VLAN ID范围为500～506； 由于存在两组企业用户，使用两组不同的Service VLAN承载不同的企业用户。 • A 组企业用户：Service VLAN ID 为 501～503； • B 组企业用户：Service VLAN ID 为 504～506； 企业用户群总流量要求：限速为100Mbps，最小带宽保证为50Mbps

现要求 SwitchA 在调度报文时，实现以下需求：

- 首先调度企业网的数据，完成后再调度个人用户的数据。
- 在调度 A 组用户和 B 组企业用户的流量时，按照 2：1 的比例进行调度。
- 在调度个人用户的数据时，首先调度 VoIP 业务的数据，完成后再轮询调度 VoD、VPN、HTTP 的流量，调度比例为 3：2：1（调度 3 个 VoD 报文后，调度 2 个 VPN 报文，再调度 1 个 HTTP 报文）。

图1-3 HQoS 典型配置举例组网示意图



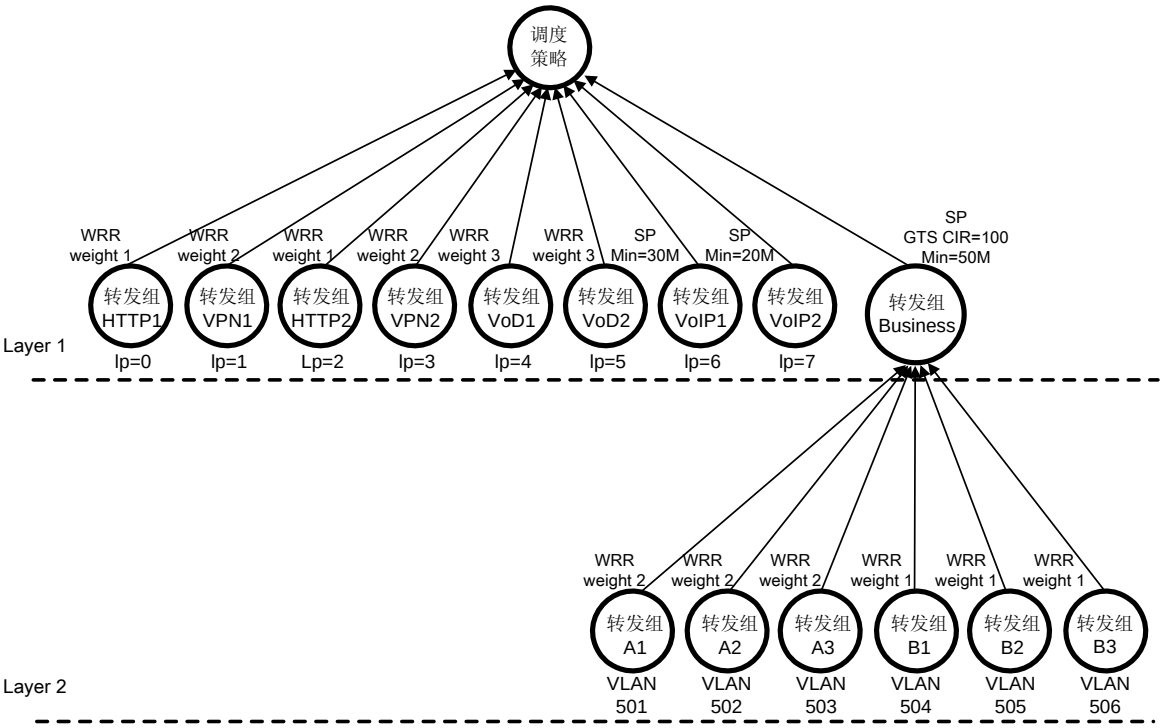
2. 配置思路

根据组网需求，对于企业网用户数据不区分数据类型，都要求优先发送；而对于个人用户数据则要根据报文优先级进行调度，因此需要采用 HQoS 功能来实现需求。

- 对于企业网用户的流量，可以将其配置为父转发组，其中嵌套 6 个子转发组，分别对应 A 组和 B 组企业用户的共 6 个 VLAN 的数据，然后为分属不同用户的转发组配置 WRR 调度权重，实现按比例进行调度的需求。最后，为父转发组关联 SP 转发策略，使企业网用户流量得到优先调度，并通过流量整形和最小带宽保证实现流量速率的控制。
- 对个人用户的各种流量，根据其 802.1p 优先级映射到不同的本地优先级，并匹配到 8 个转发组中。为 VoIP 业务的转发组关联 SP 转发策略、配置最小带宽保证，使其优先被调度。其余队列则采用 WRR 队列调度，并配置相应的权重值，实现不同的调度比例。

经过以上的配置思路分析，针对本举例的HQoS功能实现结构图可表现为 图 1-4。

图1-4 HQoS 方案实现结构图



说明

通过查找 dot1p-lp 优先级映射表，可以得知 HTTP 浏览的流量对应的本地优先级为 0 和 2，VPN 流量对应的本地优先级为 1 和 3，其余业务流量的 802.1p 优先级和本地优先级都是一一对应关系。

3. 配置步骤

(1) 创建组网中所需的 VLAN，并配置 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 端口允许相应 VLAN 通过。（此处以使用 Trunk 类型端口为例进行介绍）

```
<Sysname> system-view
[Sysname] vlan 100 to 299
 Please wait....... Done.
[Sysname] vlan 501 to 506
 Please wait....... Done.
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-type trunk
[Sysname-GigabitEthernet1/0/2] port trunk permit vlan 100 to 299
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port link-type trunk
[Sysname-GigabitEthernet1/0/3] port trunk permit vlan 501 to 506
```

(2) 创建企业用户的子转发组

```
[Sysname] qos forwarding-group A1
[Sysname-hqos-fg-A1] quit
[Sysname] qos forwarding-group A2
```

```
[Sysname-hqos-fg-A2] quit
[Sysname] qos forwarding-group A3
[Sysname-hqos-fg-A3] quit
[Sysname] qos forwarding-group B1
[Sysname-hqos-fg-B1] quit
[Sysname] qos forwarding-group B2
[Sysname-hqos-fg-B2] quit
[Sysname] qos forwarding-group B3
[Sysname-hqos-fg-B3] quit
```

(3) 创建企业用户子转发组对应的转发策略，并根据 图 1-4 配置相应的策略内容

说明

一个转发策略可以关联到多个转发组，因此这里只为A组和B组企业用户各创建一个转发策略即可。

```
[Sysname] qos forwarding-profile A
[Sysname-hqos-fp-A] wrr weight 2
[Sysname-hqos-fp-A] quit
[Sysname] qos forwarding-profile B
[Sysname-hqos-fp-B] wrr weight 1
[Sysname-hqos-fp-B] quit
```

(4) 创建企业用户的父转发组，指定其嵌套的子转发组并关联转发策略

```
[Sysname] qos forwarding-group business
[Sysname-hqos-fg-business] forwarding-group A1 profile A
[Sysname-hqos-fg-business] forwarding-group A2 profile A
[Sysname-hqos-fg-business] forwarding-group A3 profile A
[Sysname-hqos-fg-business] forwarding-group B1 profile B
[Sysname-hqos-fg-business] forwarding-group B2 profile B
[Sysname-hqos-fg-business] forwarding-group B3 profile B
[Sysname-hqos-fg-business] quit
```

(5) 创建企业用户父转发组对应的转发策略

```
[Sysname] qos forwarding-profile business
[Sysname-hqos-fp-business] sp
[Sysname-hqos-fp-business] gts cir 102400
[Sysname-hqos-fp-business] bandwidth 51200
[Sysname-hqos-fp-business] quit
```

(6) 配置个人用户流量的转发组

```
[Sysname] qos forwarding-group VoIP1
[Sysname-hqos-fg-VoIP1] quit
[Sysname] qos forwarding-group VoIP2
[Sysname-hqos-fg-VoIP2] quit
[Sysname] qos forwarding-group VoD1
[Sysname-hqos-fg-VoD1] quit
[Sysname] qos forwarding-group VoD2
[Sysname-hqos-fg-VoD2] quit
[Sysname] qos forwarding-group VPN1
[Sysname-hqos-fg-VPN1] quit
```

```
[Sysname] qos forwarding-group VPN2
[Sysname-hqos-fg-VPN2] quit
[Sysname] qos forwarding-group HTTP1
[Sysname-hqos-fg-HTTP1] quit
[Sysname] qos forwarding-group HTTP2
[Sysname-hqos-fg-HTTP2] quit
```

(7) 配置个人用户流量的转发策略，并根据并根据 图 1-4 配置相应的策略内容

说明

一个转发策略可以关联到多个转发组，因此这里除 VoIP 需要配置两个转发策略并配置不同的最小保证带宽之外，对其他业务流量只创建一个转发策略即可。

```
[Sysname] qos forwarding-profile VoIP1
[Sysname-hqos-fp-VoIP1] sp
[Sysname-hqos-fp-VoIP1] bandwidth 30720
[Sysname-hqos-fp-VoIP1] quit
[Sysname] qos forwarding-profile VoIP2
[Sysname-hqos-fp-VoIP2] sp
[Sysname-hqos-fp-VoIP2] bandwidth 20480
[Sysname-hqos-fp-VoIP2] quit
[Sysname] qos forwarding-profile VoD
[Sysname-hqos-fp-VoD] wrr weight 3
[Sysname-hqos-fp-VoD] quit
[Sysname] qos forwarding-profile VPN
[Sysname-hqos-fp-VPN] wrr weight 2
[Sysname-hqos-fp-VPN] quit
[Sysname] qos forwarding-profile HTTP
[Sysname-hqos-fp-HTTP] wrr weight 1
[Sysname-hqos-fp-HTTP] quit
```

(8) 创建调度策略，并将个人用户转发组和企业用户转发组进行嵌套

```
[Sysname] qos scheduler-policy hqos
[Sysname-hqos-sp-hqos] forwarding-group VoIP1 profile VoIP1
[Sysname-hqos-sp-hqos] forwarding-group VoIP2 profile VoIP2
[Sysname-hqos-sp-hqos] forwarding-group VoD1 profile VoD
[Sysname-hqos-sp-hqos] forwarding-group VoD2 profile VoD
[Sysname-hqos-sp-hqos] forwarding-group VPN1 profile VPN
[Sysname-hqos-sp-hqos] forwarding-group VPN2 profile VPN
[Sysname-hqos-sp-hqos] forwarding-group HTTP1 profile HTTP
[Sysname-hqos-sp-hqos] forwarding-group HTTP2 profile HTTP
[Sysname-hqos-sp-hqos] forwarding-group business profile business
```

(9) 在调度策略的 Layer1 中，为个人用户的转发组和企业用户父转发组配置实例化规则

```
[Sysname-hqos-sp-hqos] layer 1
[Sysname-hqos-sp-hqos-layer1] forwarding-group VoIP2 match local-precedence 7
[Sysname-hqos-sp-hqos-layer1] forwarding-group VoIP1 match local-precedence 6
[Sysname-hqos-sp-hqos-layer1] forwarding-group VoD2 match local-precedence 5
[Sysname-hqos-sp-hqos-layer1] forwarding-group VoD1 match local-precedence 4
```

```
[Sysname-hqos-sp-hqos-layer1] forwarding-group VPN2 match local-precedence 3
[Sysname-hqos-sp-hqos-layer1] forwarding-group VPN1 match local-precedence 1
[Sysname-hqos-sp-hqos-layer1] forwarding-group HTTP2 match local-precedence 2
[Sysname-hqos-sp-hqos-layer1] forwarding-group HTTP1 match local-precedence 0
[Sysname-hqos-sp-hqos-layer1] forwarding-group business group
[Sysname-hqos-sp-hqos-layer1] quit
[Sysname-hqos-sp-hqos] quit
```

(10) 在调度策略的 Layer2 中，为企业用户的 6 个子转发组配置匹配实例化规则

```
[Sysname-hqos-sp-hqos] layer 2
[Sysname-hqos-sp-hqos-layer2] forwarding-group A1 match service-vlan-id 501
[Sysname-hqos-sp-hqos-layer2] forwarding-group A2 match service-vlan-id 502
[Sysname-hqos-sp-hqos-layer2] forwarding-group A3 match service-vlan-id 503
[Sysname-hqos-sp-hqos-layer2] forwarding-group B1 match service-vlan-id 504
[Sysname-hqos-sp-hqos-layer2] forwarding-group B2 match service-vlan-id 505
[Sysname-hqos-sp-hqos-layer2] forwarding-group B3 match service-vlan-id 506
[Sysname-hqos-sp-hqos-layer2] quit
```

(11) 在端口 Ten-GigabitEthernet1/1/1 上应用调度策略

```
[Sysname] interface Ten-GigabitEthernet 1/1/1
[Sysname-Ten-GigabitEthernet1/1/1] qos apply scheduler-policy hqos outbound
```