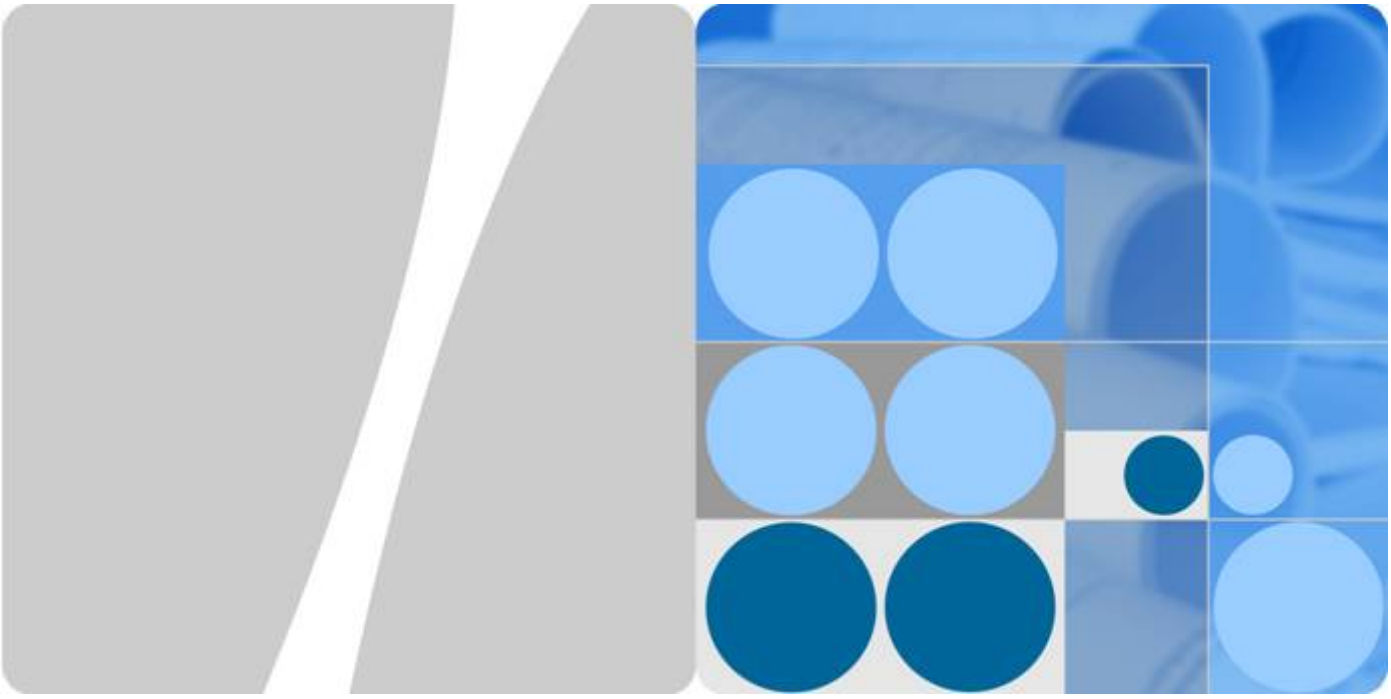


S12700, S12700E 系列敏捷交换机

V200R023C00

配置指南-QoS

文档版本　01

发布日期　2023-09-30

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

前言

读者对象

本文档适用于负责配置和管理交换机的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
须知	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其他不可预知的结果。 “须知”不涉及人身伤害。
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

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。

格式	意义
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

接口编号约定

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

安全约定

- 密码配置约定
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置明文模式的密码时，请不要以“%^%#.....%^%#”、“%#%#.....%#%#”、“%@%@.....%@%@”或者“@%@%.....@%@%”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文。
  - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
- 加密算法约定

  目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。
- 个人数据约定

  您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。
- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用，不涉及采集、处理任何个人数据或任何用户通信内容。

- 可靠性设计声明

  对于网络规划和站点设计，必须严格遵守可靠性设计原则，具备设备级和方案级保护。设备级保护包括双网双平面，双机、跨板双链路的规划原则，避免出现单点，单链路故障。方案级指FRR、VRRP等快速收敛保护机制。在应用方案级保护时，应避免保护方案的主备路径经过相同链路或者传输，以免方案级保护不生效。

参考标准和协议

请登录**华为网站**，搜索“标准协议顺从表”，获取《华为S系列交换机标准协议顺从表》。获取该信息需要访问权限，如需帮助，请联系技术支持人员。

特别声明

- 本文档仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。文档提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成文档中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本文档不再针对前述情况造成的差异一一说明。
- 本文档中提供的最大值是设备在实验室特定场景（例如，被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与文档中提供的数据不一致。
- 出于特性介绍及配置示例的需要，本文档可能会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。

目 录

1 QoS 简介

QoS 产生的背景

网络的普及和业务的多样化使得互联网流量激增，从而产生网络拥塞，增加转发时延，严重时还会产生丢包，导致业务质量下降甚至不可用。所以，要在网络上开展这些实时性业务，就必须解决网络拥塞问题。解决网络拥塞的最好的办法是增加网络的带宽，但从运营、维护的成本考虑，这是不现实的，最有效的解决方案就是应用一个“有保证”的策略对网络流量进行管理。

QoS技术就是在这种背景下发展起来的。QoS（Quality of Service）即服务质量，其目的是针对各种业务的不同需求，为其提供端到端的服务质量保证。QoS是有效利用网络资源的工具，它允许不同的流量不平等的竞争网络资源，语音、视频和重要的数据应用在网络设备中可以优先得到服务。QoS技术在当今的互联网中应用越来越多，其作用越来越重要。

QoS 服务模型

- Best-Effort服务模型

  Best-Effort是最简单的QoS服务模型，用户可以在任何时候，发出任意数量的报文，而且不需要通知网络。提供Best-Effort服务时，网络尽最大的可能来发送报文，但对时延、丢包率等性能不提供任何保证。Best-Effort服务模型适用于对时延、丢包率等性能要求不高的业务，是现在Internet的缺省服务模型，它适用于绝大多数网络应用，如FTP、E-Mail等。

- IntServ服务模型

  IntServ模型是指用户在发送报文前，需要通过信令（Signaling）向网络描述自己的流量参数，申请特定的QoS服务。网络根据流量参数，预留资源以承诺满足该请求。在收到确认信息，确定网络已经为这个应用程序的报文预留了资源后，用户才开始发送报文。用户发送的报文应该控制在流量参数描述的范围内。网络节点需要为每个流维护一个状态，并基于这个状态执行相应的QoS动作，来满足对用户的承诺。

  IntServ模型使用了RSVP（Resource Reservation Protocol）协议作为信令，在一条已知路径的网络拓扑上预留带宽、优先级等资源，路径沿途的各网元必须为每个要求服务质量保证的数据流预留想要的资源，通过RSVP信息的预留，各网元可以判断是否有足够的资源可以使用。只有所有的网元都给RSVP提供了足够的资源，“路径”方可建立。

- DiffServ服务模型

  DiffServ模型的基本原理是将网络中的流量分成多个类，每个类享受不同的处理，尤其是网络出现拥塞时不同的类会享受不同级别的处理，从而得到不同的丢包

率、时延以及时延抖动。同一类的业务在网络中会被聚合起来统一发送，保证相同的时延、抖动、丢包率等QoS指标。

Diffserv模型中，业务流的分类和汇聚工作在网络边缘由边界节点完成。边界节点可以通过多种条件（比如报文的源地址和目的地址、ToS域中的优先级、协议类型等）灵活地对报文进行分类，对不同的报文设置不同的标记字段，而其他节点只需要简单地识别报文中的这些标记，即可进行资源分配和流量控制。

与Intserv模型相比，DiffServ模型不需要信令。在DiffServ模型中，应用程序发出报文前，不需要预先向网络提出资源申请，而是通过设置报文的QoS参数信息，来告知网络节点它的QoS需求。网络不需要为每个流维护状态，而是根据每个报文流指定的QoS参数信息来提供差分服务，即对报文的服务等级划分，有差别地进行流量控制和转发，提供端到端的QoS保证。DiffServ模型充分考虑了IP网络本身灵活性、可扩展性强的特点，将复杂的服务质量保证通过报文自身携带的信息转换为单跳行为，从而大大减少了信令的工作，是当前网络中的主流服务模型。

基于 DiffServ 模型的 QoS 组成

本文介绍的QoS都是基于DiffServ服务模型的，基于Diffserv模型的QoS业务主要分为以下几大类：

- 报文分类和标记

  要实现差分服务，需要首先将数据包分为不同的类别或者设置为不同的优先级。报文分类即把数据包分为不同的类别，可以通过MQC配置中的流分类实现；报文标记即为数据包设置不同的优先级，可以通过优先级映射和重标记优先级实现。

- 流量监管、流量整形和接口限速

  流量监管和流量整形可以将业务流量限制在特定的带宽内，当业务流量超过额定带宽时，超过的流量将被丢弃或缓存。其中，将超过的流量丢弃的技术称为流量监管，将超过的流量缓存的技术称为流量整形。接口限速分为基于接口的流量监管和基于接口的流量整形。

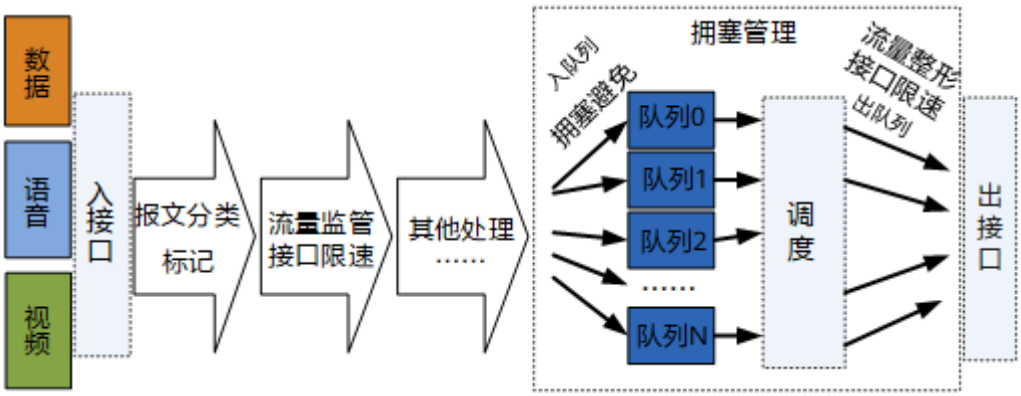
- 拥塞管理和拥塞避免

  拥塞管理在网络发生拥塞时，将报文放入队列中缓存，并采取某种调度算法安排报文的转发次序。而拥塞避免可以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，通过调整流量来解除网络的过载。

其中，报文分类和标记是实现差分服务的前提和基础；流量监管、流量整形、接口限速、拥塞管理和拥塞避免从不同方面对网络流量及其分配的资源实施控制，是提供差分服务的具体体现。

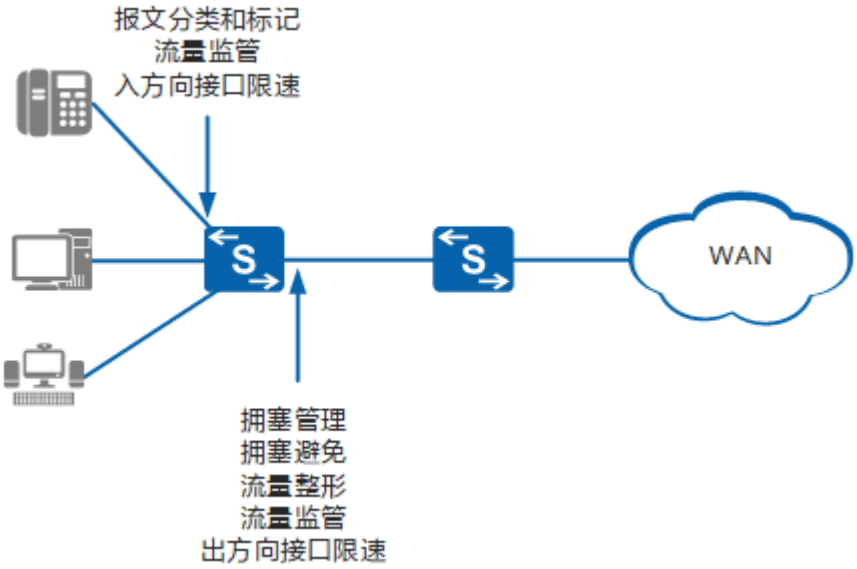
各种QoS技术在网络设备上的处理顺序如图1-1所示。

图 1-1 QoS 技术处理流程



上述QoS技术在网络中的位置如图1-2所示。

图 1-2 QoS 技术在网络中的位置



相关信息

技术论坛

QoS专题-第1期-QoS理论篇

2 MQC 配置

2.1 MQC 简介

模块化QoS命令行接口MQC（Modular QoS Command-Line Interface）将具有某类共同特征的报文划分为一类，并为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。随着网络中QoS业务的不断丰富，在网络规划时若要实现对不同流量（如不同业务或不同用户）的差分服务，会使部署比较复杂。通过配置MQC，用户可以更加便捷地按需对网络中的流量提供不同的服务。

MQC是一种配置方法，通过配置流分类、流行为、流策略和应用流策略来完成QoS业务的配置。MQC的常见应用：

- **3.7 配置重标记优先级**
- **4.6.1 配置MQC实现流量监管**
- **6.4 配置报文过滤**
- **7.4 配置重定向**
- **8.4 配置流量统计**

MQC 三要素

MQC包含三个要素：流分类（traffic classifier）、流行为（traffic behavior）和流策略（traffic policy）。

流分类

流分类用来定义一组流量匹配规则，用于对报文进行分类。配置流分类，需要确定如下三点：

- 流分类的名称。
- 流分类的分类规则。
- 当流分类中有多条分类规则时，各规则之间的关系。

流分类规则可以分为二层规则、三层规则、基本ACL6规则、高级ACL6规则和自定义ACL规则。具体的分类规则如表2-1所示：

表 2-1 流分类的分类规则

类别	分类规则
二层规则	• 目的MAC地址 • 源MAC地址 • VLAN报文外层Tag的VLAN ID • VLAN报文外层Tag的802.1p优先级 • VLAN报文内层Tag的VLAN ID • VLAN报文内层Tag的802.1p优先级 • 基于二层封装的协议字段：目前支持的二层封装协议包括ARP、IP、MPLS、RARP等。 • MPLS报文的EXP优先级 • ACL 4000～4999匹配的字段：基于二层ACL进行分类。 • 丢弃报文：匹配被丢弃的报文，可以对该类报文进行流量统计或镜像等动作，从而分析该类报文。 • 所有报文：当需要对所有的数据报文作统一的处理时，可以基于所有数据报文进行分类。 • 入接口 • 出接口
三层规则	• IP报文的DSCP优先级 • IP报文的IP优先级 • IPv6下一报文头类型 • IP协议类型（IPv4协议或IPv6协议） • TCP报文的TCP-Flag标志 • ACL 2000～3999匹配的字段 • VXLAN内层报文的VNI ID
基本ACL6规则	ACL6 2000～2999匹配的字段
高级ACL6规则	ACL6 3000～3999匹配的字段
自定义ACL规则	ACL 5000～5999匹配的字段（自定义ACL）

流分类中各规则之间的关系分为：or或and，缺省情况下的关系为or。

- or：报文只要匹配了流分类中的一个规则，设备就认为报文属于此类。
- and：当流分类中包含ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；当流分类中没有ACL规则时，报文必须匹配所有非ACL规则才属于该类。

以流分类c1为例。流分类c1包括如下规则：

- ACL规则：
  - 匹配ACL 3000
  - 匹配ACL 3001
- 非ACL规则：
  - 匹配VLAN ID为10的报文
  - 匹配入接口为GE1/0/1的报文

若流分类c1各规则之间的关系为or：只要报文的VLAN ID为10，或报文的入接口为GE1/0/1，或报文匹配ACL 3000，或报文匹配ACL 3001，报文就属于流分类c1。

若流分类c1各规则之间的关系为and：只有报文的VLAN ID为10，入接口为GE1/0/1，且报文匹配ACL 3000或ACL 3001时，报文才属于流分类c1。

流行为

流行为用来定义针对某类报文所做的动作。配置流行为，需要确定如下两点：

- 流行为的名称。
- 流行为中的动作。

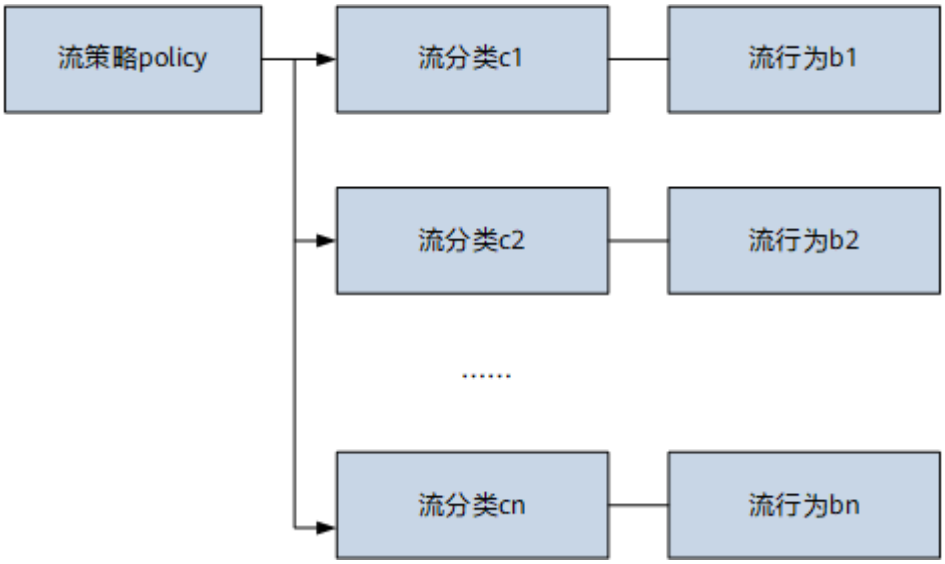
设备支持报文过滤、重标记优先级、重标记流ID、重定向、流量监管、流量统计等动作。如果在一个流行为中定义了多个动作且这些动作互不冲突，那么这些动作都能配置成功且同时生效。如果在一个流行为中定义的多个动作产生冲突，将出现以下情况之一：

- 在流行为视图定义冲突的动作时，系统提示错误，命令无法执行。
- 应用流策略时，系统提示错误，流策略应用失败。

流策略

流策略用来将指定的流分类和流行为绑定，对分类后的报文执行对应流行为中定义的动作。如**图2-1**所示，一个流策略可以绑定多个流分类和流行为。

图 2-1 流策略绑定多个流分类和流行为



配置流策略和应用流策略时，需要确定如下四点：

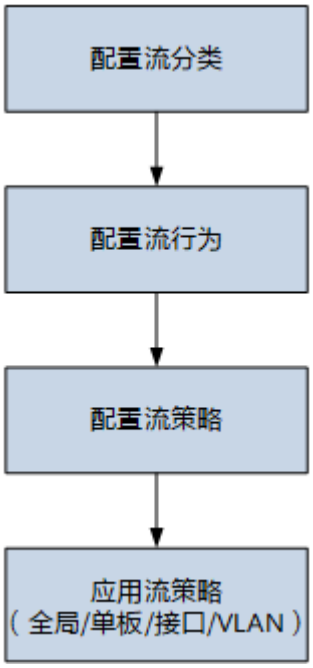
- 流策略的名称。
- 流分类和流行为的对应关系，即需要对匹配指定流分类的报文执行的动作。
- 应用流策略的视图。如接口视图、VLAN视图或系统视图。
- 应用流策略的方向。QoS业务既可以应用于设备接收的报文（即入方向报文），也可以应用于设备发送的报文（即出方向报文）。用户可以在应用流策略时，通过指定**inbound**或**outbound**参数，对入方向或出方向报文实施策略控制。

MQC 配置流程

MQC配置流程如**图2-2**所示。

1. **配置流分类**：按照一定规则对报文进行分类，是提供差分服务的基础。
2. **配置流行为**：为符合流分类规则的报文指定流量控制或资源分配动作。
3. **配置流策略**：将指定的流分类和指定的流行为绑定，形成完整的策略。
4. **应用流策略**：将流策略应用到全局、单板、接口或VLAN。

图 2-2 MQC 配置流程



相关信息

技术论坛

QoS专题-第2期-QoS实现工具之MQC

2.2 MQC 配置注意事项

涉及网元

无需其他网元配合。

License 支持

MQC是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持MQC。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

- MQC的规格如**表2-2**所示。

表 2-2 MQC 规格

项目	规格
设备支持的流分类数	512
一个流分类支持的if-match规则数	2048
设备支持的流行为数	256
设备支持的流策略数	256
一个流策略支持绑定的流分类数	256
设备支持应用流策略的VLAN数	3000

- 应用流策略需要设备有足够的ACL资源，否则会导致应用失败。以一个流策略中的**if-match**占用一条ACL为例，同一个流策略应用到M个接口时，将占用M条ACL资源；应用到L个VLAN且设备上存在N块接口板时，将占用L*N条ACL规则；应用到全局且设备上存在N块接口板时，将占用N条ACL规则。**if-match**规则占用ACL资源的情况参考**表2-3**。

表 2-3 流分类规则占用 ACL 资源介绍

流分类规则	ACL资源占用情况说明
if-match vlan-id *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*] **if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**vlan-id** *vlan-id*]	分段下发，占用多条ACL资源，分段规则可以通过命令**display acl division** *start-id* **to** *end-id*查看。
if-match acl { *acl-number* | *acl-name* } **if-match ipv6 acl** { *acl-number* | *acl-name* }	• 上行：包含**range** *port-start port-end*的rule规则，在range资源耗尽时，会分段下发，导致一条规则占用多条ACL资源。包含有**tcp-flag established**的rule规则，每条规则占用2条ACL资源。（X系列单板与下行一致） • 下行：包含**range** *port-start port-end*参数的rule规则分段下发，占用多条ACL资源，其他情况一条rule规则占用一条资源。分段规则可以通过命令**display acl division** *start-id* **to** *end-id*查看。
其他if-match规则	占用一条ACL资源。

V200R013C02及后续版本中，应用在接口入方向的流策略所占用的资源，通常可以与单板上其他在入方向应用相同流策略的接口共享，不支持ACL资源共享的情况包括：

- 流行为配置**car**或者**statistic enable**

  - 除X系列以外的单板，支持配置扩展表项空间资源模式
  - X系列中不支持配置扩展表项空间资源模式的单板，流分类配置IPv6规则（例如**if-match ipv6 dscp**、**if-match protocol ipv6**、**if-match ipv6 acl**）
  - 除X系列以外的单板，流行为配置**remark 8021p**、**mac-address learning disable**、**add-tag vlan-id**、**remark flow-id**、**remark cvlan-id**、**redirect vpn-instance**或者**remark vlan-id**

  在任意视图执行以下命令，可以查询ACL资源相关信息：

  - 执行命令**display traffic-policy applied-record** [*policy-name*]，查看应用在接口入方向的流策略是否支持ACL资源共享。
  - 执行命令**display acl resource** [**slot** *slot-id*]，查看ACL资源信息。

- 当一个流策略在多个视图下应用时：高优先级视图下的流策略生效。视图的生效优先级从高到低为：VLANIF接口视图 > WLAN-ESS接口视图/SSID模板视图 > 物理接口子接口视图/Eth-Trunk子接口视图 > 物理接口视图/Eth-Trunk接口视图/端口组视图 > VLAN视图 > 全局视图。
- 当报文同时匹配多个流策略，或同一流策略的多个流分类+流行为时，生效的流策略或流分类+流行为如**表2-4**和**表2-5**所示：

表 2-4 流分类的分类规则属于同一类

报文匹配不同视图下不同流策略	报文匹配同一视图下同方向的同一流策略的多个流分类+流行为
仅生效优先级最高的视图下的一个流策略生效。	只有该流策略的配置信息中第一个流分类+流行为生效。 在流策略视图下执行命令**display this**查看该流策略的配置信息，配置信息中的第一个流分类+流行为即为最终生效的流分类+流行为。

表 2-5 流分类的分类规则不属于同一类

单板	报文匹配不同视图下的不同流策略	报文匹配同一视图下同方向的同一流策略的多个流分类+流行为
X系列单板	仅生效优先级最高的视图下的一个流策略生效。	只有该流策略的配置信息中第一个流分类+流行为生效。 在流策略视图下执行命令**display this**查看该流策略的配置信息，配置信息中的第一个流分类+流行为即为最终生效的流分类+流行为。

单板	报文匹配不同视图下的不同流策略	报文匹配同一视图下同方向的同一流策略的多个流分类+流行为
除X系列单板以外的单板	若流动作彼此不冲突，则流策略都会生效。 若流动作产生冲突： ● 当流策略中流分类的匹配顺序为配置顺序（**config**），仅生效优先级最高的视图下的一个流策略生效。 ● 当流策略中流分类的匹配顺序为自动顺序（**auto**），流分类规则生效优先级较高的流策略生效。流分类规则的生效优先级为：二层规则+三层规则 > 高级ACL6规则 > 基本ACL6规则 > 二层规则 > 三层规则 > 自定义ACL规则。	若流动作彼此不冲突，则流分类+流行为都会生效，流动作都会执行。 若流动作产生冲突： ● 当流策略中流分类的匹配顺序为配置顺序（**config**），在流策略视图下执行命令**display this**查看该流策略的配置信息，配置信息中的第一个流分类+流行为即为最终生效的流分类+流行为。 ● 当流策略中流分类的匹配顺序为自动顺序（**auto**），流分类规则生效优先级较高的流分类+流行为生效。流分类规则的生效优先级为：二层规则+三层规则 > 高级ACL6规则 > 基本ACL6规则 > 二层规则 > 三层规则 > 自定义ACL规则。

建议用户按照从高到低的优先级顺序配置，否则可能会导致流策略不能立即生效。流分类的分类规则详见“MQC简介”。

- X系列单板（除X1E、X2H、X5H、X6H单板以外）上配置的ACL6规则应用为硬件ACL时的约束请参见《S12700, S12700E V200R023C00 配置指南-安全配置》ACL配置中的配置高级ACL6。
- 匹配同一个ACL的MQC流策略和基于ACL的简化流策略应用到同一对象时，基于ACL的简化流策略优先生效。以下情况例外：使用**traffic-secure**命令配置基于ACL的报文过滤，可以与匹配同一个ACL的MQC流策略同时生效。
- 如果ACL规则匹配了报文的VPN实例名称，则流策略下发不成功。
- 如果流策略因交换机上ACL资源不足而应用失败，建议删除应用失败的流策略配置。否则如果交换机保存配置并且重启，其他已正常运行的业务的配置会恢复失败。
- 如果需要删除的流策略已经应用到全局、接口或VLAN，则不允许直接删除该策略，需要先在相应的视图下执行**undo traffic-policy**命令取消对该策略的应用，然后再到全局执行**undo traffic policy**命令完成删除。如果没有应用，则可以直接删除。
- X系列单板（除X1E、X2H、X5H、X6H单板以外）只支持在全局、VLAN、物理接口或者Eth-Trunk接口下应用ACL6，不支持在其他逻辑接口上应用ACL6。
- V200R009C00版本之前的设备，VLANIF接口不支持应用流策略。V200R009C00及之后版本的设备，VLANIF接口支持应用流策略。
- 目的IP是本机的报文会上送CPU，另外一些协议报文对应的功能使能后也会上送CPU，比如BGP、OSPF、LACP使能后也会上送CPU处理。上送CPU的报文同时匹配流策略中的流分类规则，如果CPCAR和流策略动作冲突，CPCAR生效。

- 若对入方向流量同时配置MQC和VLAN Mapping功能：
  - 除X系列以外的单板在流行为中配置重定向报文到VPN实例，MQC匹配映射前的VLAN ID。
  - X系列单板在流行为中配置灵活QinQ、VLAN Mapping、重标记流ID、重标记VLAN报文的802.1p优先级或禁止MAC地址学习，MQC匹配映射前的VLAN ID。
  - 其他情况下，MQC匹配映射后的VLAN ID。
- 子接口下应用流策略的相关限制：
  - 流行为中不能存在修改VLAN信息的相关动作，譬如**remark 8021p**、**remark cvlan-id**、**remark vlan-id**、**add-tag vlan-id**，否则流策略会应用失败。
  - 流策略应用在子接口下，设备默认匹配报文的内层或外层VLAN（跟子接口的具体配置相关，例如子接口下配置了**qinq termination pe-vid ce-vid**，则同时匹配内层和外层VLAN），此时如果在流分类中也配置了匹配内层或外层VLAN的规则，则会存在冲突，导致流策略应用失败。

2.3 配置 MQC

2.3.1 配置流分类

背景信息

流分类各规则之间属于并列关系，只要匹配规则不冲突，都可以在同一流分类中配置。若匹配规则冲突，在流策略中绑定流行为和该流分类时系统会提示错误，应用流策略将不能生效。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，创建一个流分类并进入流分类视图，或进入已存在的流分类视图。

   and表示流分类中各规则之间关系为逻辑“与”，指定该逻辑关系后：
   - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；
   - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

   or表示流分类各规则之间是逻辑“或”，即报文只需匹配流分类中的一个或多个规则即属于该类。

   缺省情况下，流分类中各规则之间的关系为逻辑“或”。
3. 请根据实际情况定义流分类中的匹配规则。

   说明

   if-match ip-precedence和**if-match tcp**命令仅对IPv4报文生效。

   X系列单板不支持配置包含高级ACL中的**ttl-expired**字段的流分类规则。

   当流分类匹配**if-match ipv6 acl** { *acl-number* | *acl-name* }时，X系列单板不支持**add-tag vlan-id** *vlan-id*、**remark 8021p** [*8021p-value* | **inner-8021p**]、**remark cvlan-id** *cvlan-id*、**remark vlan-id** *vlan-id*、**mac-address learning disable**。

匹配规则	命令	说明
外层VLAN ID或基于QinQ报文内外两层Tag的VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]	-
QinQ报文内外层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**vlan-id** *vlan-id*]	-
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个802.1p值，报文只需匹配其中一个802.1p值就匹配该规则。
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>	-
丢弃报文	**if-match discard**	包含该流分类的报文只能与流量统计和流镜像两种动作绑定。
QinQ报文双层Tag	**if-match double-tag**	-
MPLS报文EXP优先级	**if-match mpls-exp** *exp-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个MPLS EXP值，报文只需匹配其中一个MPLS EXP值就属于该类。
目的MAC地址	**if-match destination-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
源MAC地址	**if-match source-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }	-
所有报文	**if-match any**	-

匹配规则	命令	说明
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个DSCP值，报文只需匹配其中一个DSCP值就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
IP报文的IP优先级	**if-match ip-precedence** *ip-precedence-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个IP优先级，报文只需匹配其中一个IP优先级就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }	-
IPv6下一报文头类型	**if-match ipv6 next-header** *header-number* **first-next-header**	ET1D2X12SSA0单板不支持Prefix的长度为(64,128)之间的路由。
TCP报文SYN Flag	**if-match tcp syn-flag** { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	-
入接口	**if-match inbound-interface** *interface-type interface-number*	包含该流分类的流策略不能应用在出方向。 包含该流分类的流策略不能应用在接口视图。
出接口	**if-match outbound-interface** *interface-type interface-number*	X系列单板不支持将包含该流分类的流策略应用在入方向。 包含该流分类的流策略不能应用在接口视图。

匹配规则	命令	说明
ACL规则	**if-match acl** { *acl-number* | *acl-name* }	• 使用ACL作为流分类规则，请先配置相应的ACL规则。 • 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果某ACL规则中有多个rule，报文只需匹配其中一个rule就匹配该ACL规则。 • 如果ACL的规则指定了参数**vpn-instance**，那么基于该ACL进行分类的流分类对应的流策略将不生效。
ACL6规则	**if-match ipv6 acl** { *acl-number* | *acl-name* }	使用ACL6作为流分类规则，请先配置相应的ACL6规则。 如果ACL6的规则指定了参数**vpn-instance**，那么基于该ACL6进行分类的流分类对应的流策略将不生效。
流ID	**if-match flow-id** *flow-id*	包含**if-match flow-id**匹配规则的流分类和包含**remark flow-id**动作的流行为应在不同的流策略中使用。 包含**if-match flow-id**匹配规则的流策略只能应用在接口、VLAN、VLANIF接口、单板、全局的入方向。 SA系列单板不支持配置匹配流ID。
VXLAN内层报文信息	**if-match vxlan** [**transit**] **vni** *vni-id*	包含该流分类的流策略不能应用在出方向上。 当流分类中包含此匹配规则时，流行为只支持流量监管、报文过滤和流量统计。

4. 执行命令**quit**，退出流分类视图。

2.3.2 配置流行为

操作步骤

步骤1 执行命令**traffic behavior** *behavior-name*，创建一个流行为并进入流行为视图，或进入已存在的流行为视图。

步骤2 请根据实际情况定义流行为中的动作，只要各动作不冲突，都可以在同一流行为中配置。

表 2-6 流行为中的动作

动作	命令	说明
报文过滤	**deny** | **permit**	同一流行为下，流动作**deny**和其他流动作互斥（流量统计、流镜像除外）。 有关报文过滤的详细配置过程请参见**6 报文过滤配置**。
重标记优先级	重标记VLAN报文的802.1p优先级：**remark 8021p** [*8021p-value* | **inner-8021p**] 重标记IP报文的DSCP优先级：**remark dscp** { *dscp-name* | *dscp-value* } 重标记报文的内部优先级：**remark local-precedence** { *local-precedence-name* | *local-precedence-value* } [**green** | **yellow** | **red**]	基于MQC的优先级重标记的详细配置过程请参见**3.7 配置重标记优先级**。
重标记目的MAC地址	**remark destination-mac** *mac-address*	基于MQC的目的MAC地址重标记的详细配置过程请参见《S12700, S12700E V200R023C00 配置指南-以太网交换》MAC配置 中的“配置重新标记报文的目的MAC地址”。
重标记流ID	**remark flow-id** *flow-id*	SA系列单板不支持配置重标记流ID。
重定向	重定向报文到CPU：**redirect cpu** 重定向报文到指定接口：**redirect interface** *interface-type interface-number* [**forced**] 重定向IP数据流到公网目标LSP：**redirect lsp public** *dest-address* { *nexthop-address* | **interface** *interface-type interface-number* | **secondary** } 重定向报文到多个Eth-Trunk：**redirect multi-trunk** { **eth-trunk** *trunk-id* } &<1-4> 重定向报文到VPN实例：**redirect vpn-instance** *vpn-instance-name*	包含**redirect interface**和**redirect cpu**的策略只能应用在入方向。 包含流行为**redirect multi-trunk**的策略只对IP类型的报文生效。 重定向的详细配置过程请参见**7 重定向配置**。

动作	命令	说明
流量监管	**car cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**coupling-flag** *flag-value*] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**service-class** *class* **color** *color*] } | **yellow** { **discard** | **pass** [**service-class** *class* **color** *color*] } | **red** { **discard** | **pass** [**service-class** *class* **color** *color*] }]*	包含流行为**car share**的策略只能应用在入方向。 基于MQC的流量监管详细配置过程请参见**4.6.1 配置MQC实现流量监管**。
层次化流量监管	**car** *car-name* **share**	包含**car share**的策略只能应用在入方向。
流镜像	**mirroring to observe-port** *observe-port-index*	基于MQC的流镜像的详细配置过程请参见《S12700, S12700E V200R023C00 配置指南-网络管理与监控》镜像配置 中的“配置镜像”。
禁止URPF检查	**ip urpf disable**	包含**ip urpf disable**的流策略只能应用在入方向。
策略路由	重定向报文到单个下一跳IP地址：**redirect ip-nexthop** 重定向报文到单个下一跳IPv6地址：**redirect ipv6-nexthop** 重定向报文到多个下一跳IP地址：**redirect ip-multihop** 重定向报文到多个下一跳IPv6地址：**redirect ipv6-multihop**	包含策略路由的策略只对IP类型的报文生效。 策略路由的详细配置过程请参见《S12700, S12700E V200R023C00 配置指南-IP单播路由》策略路由配置 中的“配置策略路由”。
禁止MAC地址学习	**mac-address learning disable**	-
VLAN Mapping	重标记VLAN报文的VLAN tag值：**remark vlan-id** *vlan-id* 重标记QinQ报文中的内层VLAN tag值：**remark cvlan-id** *cvlan-id*	当流分类匹配**if-match outbound-interface** *interface-type interface-number*时，设备不支持配置流行为为VLAN Mapping。 基于MQC的VLAN Mapping详细配置过程请参见《S12700, S12700E V200R023C00 配置指南-以太网交换》VLAN Mapping配置 中的“配置基于MQC的VLAN Mapping”。

动作	命令	说明
灵活QinQ	**add-tag vlan-id** *vlan-id*	当流分类匹配**if-match ipv6 acl** { *acl-number* | *acl-name* }时，X系列单板不支持**add-tag vlan-id** *vlan-id*。 基于MQC的灵活QinQ详细配置过程请参见《S12700, S12700E V200R023C00 配置指南-以太网交换》QinQ配置 中的“配置基于MQC的灵活QinQ”。
流量统计	**statistic enable**	流量统计的详细配置过程请参见8 流量统计配置。
取消ACL或ACL6中deny规则	**rule-deny skip-action**	定义该动作的流行为需要与定义ACL或ACL6规则的流分类绑定。

说明

灵活QinQ和VLAN Mapping不支持在同一流行为中配置。

当流行为中已经配置灵活QinQ、VLAN Mapping、重标记流ID、重标记VLAN报文的802.1p优先级或禁止MAC地址学习时，不支持定义以下动作：流量统计（X6E和X6S单板支持）、流镜像、重定向、策略路由、重标记IP报文的DSCP优先级、重标记报文的内部优先级、重标记目的MAC地址、流量监管、层次化流量监管和禁止URPF检查。

当流行为中已经配置重定向报文到VPN实例时，除X系列以外的单板不支持定义以下动作：流量统计、流镜像、重定向、策略路由、重标记IP报文的DSCP优先级、重标记报文的内部优先级、重标记目的MAC地址、流量监管、层次化流量监管和禁止URPF检查。

步骤3 执行命令**quit**，退出流行为视图。

步骤4 执行命令**quit**，退出系统视图。

----结束

2.3.3 配置流策略

前置任务

- 配置流分类
- 配置流行为

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**traffic policy** *policy-name* [**match-order** { **auto** | **config** }]，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。创建流策略时，如果未指定规则匹配顺序，缺省规则匹配顺序为**config**。

   应用流策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先清除该策略的应用，再重新创建并指定所需的匹配顺序。

设备支持在创建流策略时指定流策略中多个规则的匹配顺序，匹配顺序包括自动顺序（**auto**）和配置顺序（**config**）两种：

- 如果选择自动顺序，匹配顺序由系统预先指定的流分类类型的优先级决定，该优先级由高到低依次为：基于二层和IPv4三层信息流分类 > 基于高级ACL6规则流分类 > 基于基本ACL6规则流分类 > 基于二层信息流分类 > 基于IPv4三层信息流分类 > 基于用户自定义ACL规则流分类。规则优先匹配优先级高的流分类。当某一数据流量同时匹配不同流分类，且对应的流行为存在冲突时，只有流行为优先级高的规则生效。
- 如果选择配置顺序，匹配顺序由流分类规则的优先级决定，先匹配优先级较高的流分类规则。配置流分类时指定优先级，则数值越小，优先级越高；如果配置流分类时未指定precedence-value，则缺省优先级为0。关于流分类优先级的详细说明，请参见**traffic classifier**。

3. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。
4. 执行命令**quit**，退出流策略视图。
5. 执行命令**quit**，退出系统视图。

2.3.4 应用流策略

前置任务

在应用流策略之前，请完成**配置流策略**。

操作步骤

说明

请判断需要通过流策略控制的业务流量是通过物理接口、VLAN、VLANIF接口，还是全局或单板，从而选择对应的视图应用流策略。在物理接口、VLAN、全局或单板上应用流策略，可以控制通过物理接口、VLAN、全局或单板的二层流量和三层流量；在VLANIF接口上应用流策略，仅可以控制通过该VLANIF接口的三层转发流量。

- 在接口上应用流策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。

  说明

  - 仅E系列、X系列和S系列中的SC单板支持配置以太网子接口。单板详情请参见《硬件描述》中的单板分类。
  - 对于上述系列单板的二层接口，仅hybrid和trunk类型接口支持配置二层以太网子接口。
  - 对于上述系列单板的二层接口，执行命令**undo portswitch**切换为三层接口后，支持配置三层以太网子接口。
  - S系列中的SA单板不支持创建以太网子接口，也不支持转发IP流量到其它单板的以太网子接口。
  - 建议用户先将成员接口加入Eth-Trunk后，再配置Eth-Trunk子接口。只有当成员接口所在的单板系列均支持配置以太网子接口时，Eth-Trunk子接口才能配置成功。
  - VCMP的角色是Client时，不能配置VLAN终结子接口。

  c. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口或子接口视图上应用流策略。

每个接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同接口的不同方向。应用后，系统对流经该接口并匹配流分类中规则的入方向或出方向报文实施策略控制。

说明

- 子接口仅支持**inbound**参数。
- 建议不要在Untagged类型接口出方向上应用包含有**remark 8021p**、**remark cvlan-id**、**remark vlan-id**等动作的流策略，否则，可能导致报文内容出错。
- ET1D2X12SSA0、ET1D2X48SEC0、SC系列单板有2N个接口，如果1～N号中的接口与N+1～2N号中的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的2倍。
- 在X系列单板中，如果不同的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，且这些接口的ACL资源分散在N个组中进行统计（执行命令**display acl resource**查看），那么Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的N倍。
- 应用流策略需要设备有足够的ACL资源，否则会导致应用失败。以一个流策略中的if-match占用一条ACL为例，同一个流策略应用到M个接口时，将占用M条ACL资源；应用到L个VLAN且设备上存在N块接口板时，将占用L*N条ACL规则；应用到全局且设备上存在N块接口板时，将占用N条ACL规则。if-match规则占用ACL资源的情况参考“MQC配置-配置注意事项”中的表3。
- 配置Tunnel接口的隧道协议为GRE后，可在Tunnel接口入方向应用流策略。
- 在VXLAN二层子接口、Dot1q终结子接口和绑定了BGP AD方式的子接口下，应用流策略不生效，建议在主接口配置基于流ID的分类方式。

- 在VLAN上应用流策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  c. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLAN上应用流策略。

     每个VLAN的每个方向能且只能应用一个流策略。

     应用后，系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施策略控制。但是流策略对VLAN 0的报文不生效。
- 在VLANIF接口上应用流策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。
  c. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLANIF接口上应用流策略。

     每个VLANIF接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同VLANIF接口的不同方向。

     对于应用流策略的VLANIF接口，其对应的VLAN不能是Super-VLAN或MUX VLAN。

     对于X系列单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文生效。对于其它单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文及三层组播报文生效。

说明

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的入方向上应用该流策略：

- **remark vlan-id**
- **remark cvlan-id**
- **add-tag vlan-id**
- **remark 8021p**
- **remark flow-id**
- **mac-address learning disable**

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的出方向上应用该流策略：

- **add-tag vlan-id**
- **remark flow-id**
- **mac-address learning disable**

- 在全局或单板上应用流策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**traffic-policy** *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]，在全局或单板上应用流策略。

     全局或单板的每个方向上能且只能应用一个流策略，如果在全局某方向应用了流策略，则不能在单板的该方向上再次应用流策略；指定单板在某方向应用流策略后，也不能在全局的该方向上再次应用流策略。
- 在SSID模板上应用流策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**wlan**，进入WLAN视图。
  c. 执行命令**ssid-profile name** *profile-name*，创建SSID模板并进入模板视图。
  d. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在SSID模板上应用流策略。
- 在AP组上应用流策略
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**wlan**，进入WLAN视图。
  c. 执行命令**ap-group name** *group-name*，创建AP组并进入AP组视图。
  d. 执行命令**traffic-policy** *policy-name* **outbound**，在AP组上应用流策略。

2.3.5 检查 MQC 配置结果

操作步骤

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior user-defined** [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看用户定义的流策略的配置信息。

- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

  说明

  流策略可以应用到子接口上，但暂不支持通过此命令查看子接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

- 执行命令**display traffic policy** { **interface** [*interface-type interface-number*[*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]，查看已配置的流策略信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

2.4 维护 MQC

2.4.1 查看 MQC 统计信息

背景信息

MQC统计信息即流策略统计信息，用户需要了解全局或指定对象上应用指定流策略后报文通过和被丢弃的情况时，可以查看流策略统计信息。

查看流策略统计信息时，MQC配置必须存在且已经包含**statistic enable**动作。否则，将无法查看流策略统计信息，系统会提示流策略不存在或流量统计功能未使能。

操作步骤

- 执行命令**display traffic policy statistics** { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* [*.subinterface-number*] | **vlan** *vlan-id* | **ssid-profile** *ssid-profile-name* } { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]，查看全局、指定单板、指定接口、指定VLAN或指定SSID模板下应用流策略后的报文统计信息。

----结束

2.4.2 清除 MQC 统计信息

背景信息

MQC统计信息即流策略统计信息，当需要对全局或指定对象上流策略的统计信息重新进行统计时，可以执行以下命令，清除之前的流策略统计信息。

须知

清除流策略统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- 用户视图下执行命令**reset traffic policy statistics** { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* [*.subinterface-number*] | **vlan** *vlan-id* | **ssid-profile** *ssid-profile-name* } { **inbound** | **outbound** }，清除全局、指定单板、指定接口、指定VLAN或指定SSID模板下应用的流策略的统计信息。

----结束

2.5 MQC 配置示例

业务需求

丢弃接口GE1/0/1接收的VLAN ID为2的报文。

操作步骤

步骤1 配置流分类

创建流分类c1，匹配VLAN ID为2的报文。

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match vlan-id 2
[HUAWEI-classifier-c1] quit
```

步骤2 配置流行为

创建流行为b1，动作为**deny**，即丢弃匹配指定规则的报文。

```
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] deny
[HUAWEI-behavior-b1] quit
```

步骤3 配置流策略

创建流策略p1，绑定流分类c1和流行为b1。

```
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
```

步骤4 应用流策略

在接口GE1/0/1的入方向应用流策略p1。

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] quit
```

步骤5 验证配置结果

查看流分类c1的配置信息。

```
<HUAWEI> display traffic classifier user-defined c1
  User Defined Classifier Information:
   Classifier: c1
    Operator: OR
    Rule(s) : if-match vlan-id 2
```

查看流行为b1的配置信息。


```
<HUAWEI> display traffic behavior user-defined b1
 User Defined Behavior Information:
   Behavior: b1
     Deny
```

查看流策略p1的配置信息。

```
<HUAWEI> display traffic policy user-defined p1
 User Defined Traffic Policy Information:
 Policy: p1
  Classifier: c1
   Operator: OR
    Behavior: b1
     Deny
```

查看流策略p1的应用记录信息。

```
<HUAWEI> display traffic-policy applied-record p1
-------------------------------------------------
 Policy Name:   p1
 Policy Index:  0
    Classifier:c1      Behavior:b1
-------------------------------------------------
*interface GigabitEthernet1/0/1
   traffic-policy p1 inbound
     slot 1    :  success (support sharing)
-------------------------------------------------
 Policy total applied times: 1.
```

----结束

更多示例

配置MQC实现流量监管示例

配置层次化流量监管示例

配置在指定时间段进行限速示例

配置针对不同网段用户限速示例

配置报文过滤示例

配置重定向示例

配置流量统计示例

2.6 MQC FAQ

2.6.1 ACL 与 traffic policy 有什么关系

ACL与traffic policy经常组合使用。traffic policy定义符合ACL的流分类，然后再定义符合流分类的行为，即动作，例如允许通过，拒绝通过等等。

ACL里面的permit/deny与traffic policy中的behavior的permit/deny组合有如下四种情况：

ACL规则中的动作	Traffic policy中的behavior	匹配报文的最终处理结果
permit	permit	permit
permit	deny	deny
deny	permit	deny
deny	deny	deny

交换机目前默认报文都是permit的，如果只要求网段之间不能访问，只需要在ACL中配置想要deny的报文。如果ACL中最后多添加一条**rule permit**命令，此时所有报文都会命中此规则。如果在流行为behavior中配置deny，将会丢弃所有报文，导致全部业务中断。

2.6.2 为什么 ACL 规则中包含 TCP 或 UDP 端口号范围段 range 时下发流策略通常会出现错误提示：Add rule to chip failed 或者 Error: Adding rule failed

应用的包含range的规则已经达到或超过规格。S系列单板支持16个TCP或UDP端口号范围段range，E系列单板支持32个TCP或UDP端口号范围段range，当在inbound方向应用包含range规则超过规格时都会下发失败，出现上述错误提示。

3 优先级映射配置

3.1 优先级映射概述

优先级映射用来实现报文携带的QoS优先级与设备内部优先级（又称为本地优先级，是设备内部区分报文服务等级的优先级）之间的转换，从而设备根据内部优先级提供有差别的QoS服务质量。

用户可以根据网络规划在不同网络中使用不同的QoS优先级字段，例如在MPLS网络中使用EXP，VLAN网络中使用802.1p，IP网络中使用DSCP。当报文经过不同网络时，为了保持报文的优先级，需要在连接不同网络的设备上配置这些优先级字段的映射关系。当设备连接不同网络时，所有进入设备的报文，其外部优先级字段（包括MPLS EXP、802.1p和DSCP）都被映射为内部优先级；设备发出报文时，将内部优先级映射为某种外部优先级字段。

相关信息

技术论坛

QoS专题-第3期-QoS实现之报文简单分类与标记

3.2 优先级映射原理描述

优先级映射

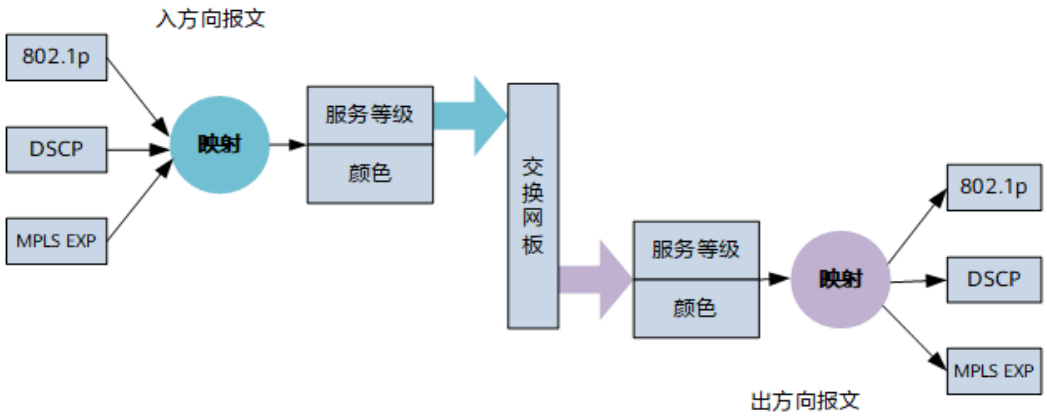
不同的报文使用不同的QoS优先级，例如VLAN报文使用802.1p，IP报文使用DSCP，MPLS报文使用EXP。当报文经过不同网络时，为了保持报文的优先级，需要在连接不同网络的网关处配置这些优先级字段的映射关系。

为了保证不同报文的服务质量，优先级映射利用DS（Differentiated Service）域来管理和记录QoS优先级与服务等级CoS（Class of Service）、颜色Color之间的映射关系，其过程如下：

1. 在报文进入设备时，报文携带的QoS优先级被映射到设备内部服务等级（也叫内部优先级或本地优先级）和颜色。
2. 设备根据报文的服务等级及颜色实现拥塞避免。
3. 在报文离开设备时，内部服务等级和颜色被映射为QoS优先级。设备根据内部服务等级与QoS优先级之间的映射关系确定报文进入的队列，从而针对队列进行流量整形、拥塞避免、队列调度等处理。设备可以修改报文发送出去时所携带的QoS优先级，以便其他设备根据报文携带的优先级提供相应的QoS服务。

将QoS优先级映射到服务等级、颜色是对入方向的报文进行，而将服务等级、颜色映射为QoS优先级则是对出方向的报文进行，如图3-1所示。

图 3-1 QoS 优先级映射



服务等级是指报文在设备内部的服务质量，它决定了报文在设备内部所属的队列类型。服务等级有8种取值，即8种PHB（Per-Hop Behavior），优先级从高到低依次为CS7、CS6、EF、AF4、AF3、AF2、AF1、BE。PHB行为的详细描述，参见PHB行为。

颜色是指报文在设备内部的丢弃优先级，用于决定同一个队列内部当队列发生拥塞时报文的丢弃顺序。颜色有3种取值，IEEE定义的优先级从低到高依次为Green、Yellow、Red。丢弃优先级的高低实际取决于对应参数的配置。

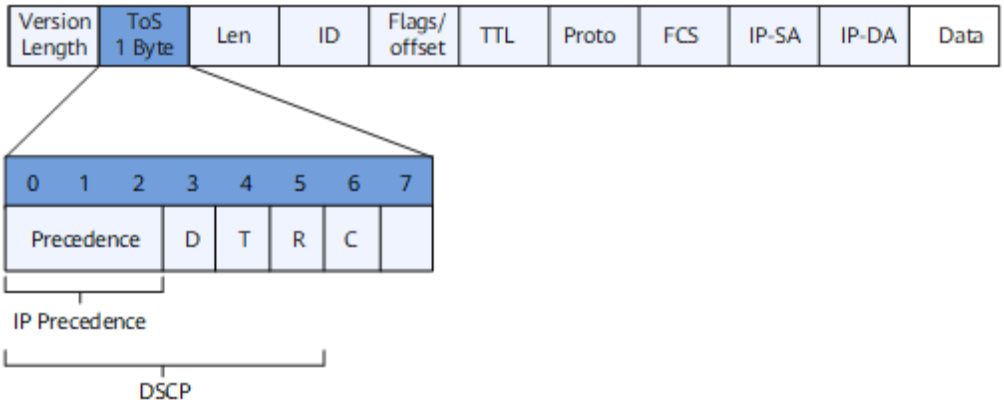
QoS 优先级字段

为了在Internet上针对不同的业务提供有差别的QoS服务质量，人们根据报文头中的某些字段记录QoS信息，从而让网络中的各设备根据此信息提供有差别的服务质量。这些和QoS相关的报文字段包括：

- Precedence字段

  根据RFC791定义，IP报文头ToS（Type of Service）域由8个比特组成，其中3个比特的Precedence字段标识了IP报文的优先级，Precedence在报文中的位置如图3-2所示。

  图 3-2 IP Precedence/DSCP 字段

  比特0～2表示Precedence字段，代表报文传输的8个优先级，按照优先级从高到低顺序取值为7、6、5、4、3、2、1和0。高优先级是7和6，经常是为路由选择或更新网络控制通信保留的，用户级应用仅能使用0～5。

  除了Precedence字段外，ToS域中还包括D、T、R三个比特：

  - D比特表示延迟要求（Delay，0代表正常延迟，1代表低延迟）。
  - T比特表示吞吐量（Throughput，0代表正常吞吐量，1代表高吞吐量）。
  - R比特表示可靠性（Reliability，0代表正常可靠性，1代表高可靠性）。

- DSCP字段

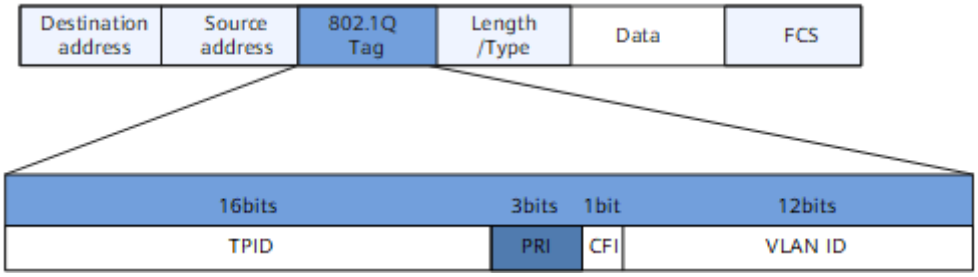
  RFC1349重新定义了IP报文中的ToS域，增加了C比特，表示传输开销（Monetary Cost）。之后，IETF DiffServ工作组在RFC2474中将IPv4报文头ToS域中的比特0～5重新定义为DSCP，并将ToS域改名为DS字节。DSCP在报文中的位置如图3-2所示。

  DS字段的前6位（0位～5位）用作区分服务代码点DSCP（DS Code Point），后2位（6位、7位）是保留位。DS字段的前3位（0位～2位）是类选择代码点CSCP（Class Selector Code Point），相同的CSCP值代表一类DSCP。DS节点根据DSCP的值选择相应的PHB。

- VLAN帧头中的802.1p优先级

  通常二层设备之间交互VLAN帧。根据IEEE 802.1Q定义，VLAN帧头中的PRI字段（即802.1p优先级），或称CoS字段，标识了服务质量需求。VLAN帧中的PRI字段位置如图3-3所示。

图 3-3 VLAN 帧中的 802.1p 优先级

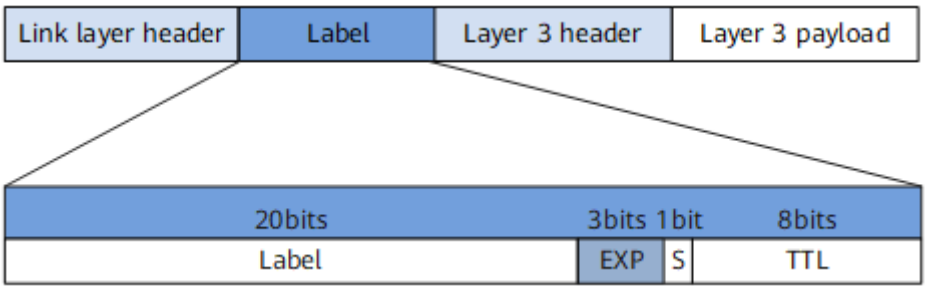


在802.1Q头部中包含3比特长的PRI字段。PRI字段定义了8种业务优先级CoS，按照优先级从高到低顺序取值为7、6、5、4、3、2、1和0。

- MPLS EXP字段

  MPLS报文与普通的IP报文相比增加了标签信息。标签的长度为4个字节，封装结构如图3-4所示。

图 3-4 MPLS 标签的封装格式



标签共有4个域：

- Label：20比特，标签值字段，用于转发的指针。
- Exp：3比特，保留字段，用于扩展，现在通常用做CoS。
- S：1比特，栈底标识。MPLS支持标签的分层结构，即多重标签，S值为1时表明为最底层标签。
- TTL：8比特，和IP分组中的TTL（Time To Live）意义相同。

对于MPLS报文，通常将标签信息中的EXP域作为MPLS报文的CoS域，与IP网络的ToS域等效，用来区分数据流量的服务等级，以支持MPLS网络的DiffServ。EXP字段表示8个传输优先级，按照优先级从高到低顺序取值为7、6、……、1和0。

- 在IP网络，由IP报文的IP优先级或DSCP标识服务等级。但是对于MPLS网络，由于报文的IP头对LSR（Label Switching Router）设备是不可见的，所以需要在MPLS网络的边缘对MPLS报文的EXP域进行标记。
- 缺省的情况下，在MPLS网络的边缘，将IP报文的IP优先级直接拷贝到MPLS报文的EXP域；但是在某些情况下，如ISP不信任用户网络、或者ISP定义的差别服务类别不同于用户网络，则可以根据一定的分类策略，依据内部的服务等级重新设置MPLS报文的EXP域，而在MPLS网络转发的过程中保持IP报文的ToS域不变。
- 在MPLS网络的中间节点，根据MPLS报文的EXP域对报文进行分类，并实现拥塞管理，流量监管或者流量整形。

PHB 行为

在每一个DS节点上对报文的处理称为PHB。PHB描述了DS节点对报文采用的外部可见的转发行为。PHB可以用优先级来定义，也可以用一些可见的服务特征如报文延迟、抖动或丢包率来定义。PHB只定义了一些外部可见的转发行为，没有指定特定的实现方式。

RFC定义了四种标准的PHB：CS（Class Selector），EF（Expedited Forwarding），AF（Assured Forwarding）和BE（Best-Effort）。其中，BE是缺省的PHB。

在RFC 2474中，CS又被划分为两个等级，即CS6和CS7；在RFC 2597中，AF又被划分为四个等级，即为AF1～AF4。至此，PHB共有8个细分级别，每个PHB在设备内部都有对应的服务等级，不同的服务等级将决定不同流的拥塞管理策略。同时每个PHB又再被划分为三个颜色（Color，也可以叫丢弃优先级），分别用Green、Yellow和Red表示，不同的颜色将决定不同流的拥塞避免策略。

- CS

  CS代表的服务等级与网络中使用的IP Precedence相同。在所有标准PHB中，CS的优先级最高。

  CS可以细分为CS7和CS6，默认用于协议报文，如企业内部各个交换机之间的STP报文、LLDP报文、LACP报文等。如果这些报文无法接收会引起协议中断。

- EF

  EF被定义为这样的一种转发处理：从任何DS节点发出的信息流速率在任何情况下必须获得等于或大于设定的速率。EF PHB在DS域内不能被重新标记，仅允许在边界节点重新标记。

  EF流要求低时延、低抖动、低丢包率，对应于实际应用中的视频、语音、会议电视等实时业务。

  EF用于承载VoIP语音的流量，或者企业内部视频会议的数据流，因为语音业务的报文要求低延迟、低抖动、低丢包率，其重要程度仅次于协议报文。

  说明

  EF PHB提供的是低时延服务，应该具有最低的抖动和丢包率，因而必须限制EF的专用带宽，以免其他服务得不到可用带宽。

- AF

  AF的推出是为了满足这样的需求：用户在与ISP订购带宽服务时，允许业务量超出所订购的规格。对不超出所订购规格的流量要求确保转发的质量；对超出规格的流量将降低服务待遇继续转发，而不只是简单地被丢弃。

  AF流要求较低的延迟、低丢包率、高可靠性，对应于数据可靠性要求高的业务如电子商务、企业VPN等。

  AF又可以细分为AF4、AF3、AF2、AF1。

  - AF4用来承载语音的信令流量，即VoIP业务的协议报文。

    说明

    语音信令是语音的呼叫控制。对用户而言，在接通的时候等待几秒钟是可以忍受的，但是在通话过程的中断是绝对不能允许的，因此语音流量必须优先于语音的信令流量。

  - AF3可以用作远端设备的Telnet、FTP等服务。这些业务对带宽要求适当，但是对网络时延、抖动都非常敏感，同时要求完全可靠的传输，不能出现丢包。

  - AF2可以用来承载企业内部IPTV的直播流量，可以保证在线视频业务的流畅性。直播业务的实时性强，需要有连续性和大吞吐量的保证，但是允许小规模的丢包。
  - AF1用作企业内部普通数据流业务，例如E-Mail。普通数据对实时性和抖动等因素要求都不高，只要保证不丢包的传达即可。
- BE

  BE对应于传统的IP报文投递服务，只关注可达性，其他方面不做任何要求。任何交换机必须支持BE PHB。

  BE用于尽力而为的服务，用作不紧急、不重要、不需要负责的业务，如员工HTTP网页浏览业务。

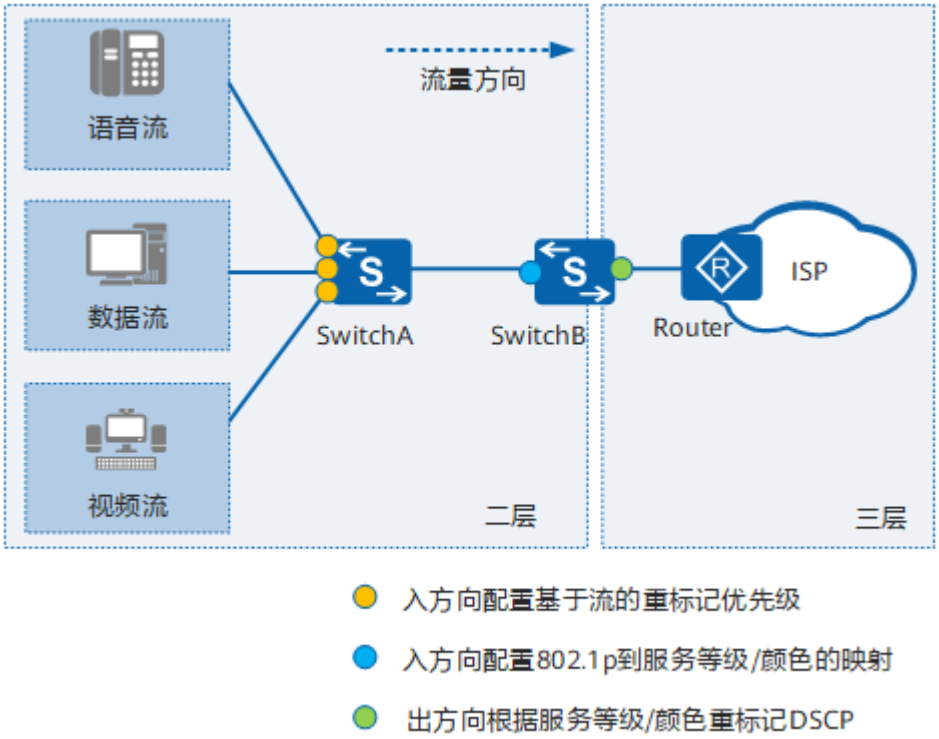
3.3 优先级映射应用场景

组网需求

如图3-5所示，网络中存在语音、数据和视频等多种业务流，当不同业务流量进入ISP网络时，需要在整个网络中对三类业务区分优先级，保证语音优先级一直最高、视频其次、数据优先级最低，这样设备可以根据优先级的高低对三类业务提供不同的QoS服务。

不同网络中的报文使用不同的优先级字段，例如二层网络中的报文使用802.1p优先级，三层网络中的报文使用DSCP优先级。报文在进入设备时，设备将报文携带的优先级映射到内部服务等级和颜色，再根据服务等级和颜色对报文进行不同的QoS服务。报文在出设备时，设备可以根据内部服务等级和颜色重标记报文优先级，以便后续网络根据报文优先级进行服务。

图 3-5 优先级映射应用组网图



业务部署

- SwitchA入方向配置流策略将语音、视频、数据三类业务重标记不同的802.1p优先级，其中语音优先级最高、视频其次、数据最低。
- SwitchB入方向将802.1p优先级映射为服务等级和颜色，SwitchB根据服务等级和颜色为报文提供不同的QoS服务。
- SwitchB出方向根据服务等级和颜色重标记DSCP优先级，以便后续三层网络根据DSCP优先级为三类业务提供不同的QoS服务。

3.4 优先级映射配置注意事项

涉及网元

无需其他网元配合。

License 支持

优先级映射是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持优先级映射。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

交换机连接ET1D2IPS0S00、ET1D2FW00S00、ET1D2FW00S01、ET1D2FW00S02、ACU2单板的XGE接口不支持配置本地优先级和队列之间的映射关系。

3.5 优先级映射缺省配置

Diffserv 域中接口入方向上优先级与服务等级（PHB 行为）/颜色的映射

缺省情况下，DiffServ域中映射关系包括：

- 802.1p优先级到PHB行为/颜色的映射关系如**表3-1**。
- DSCP优先级到PHB行为/颜色的映射关系如**表3-2**。
- MPLS报文的EXP优先级到PHB行为/颜色的映射关系如**表3-3**。

端口优先级到PHB行为/颜色的映射关系与802.1p到PHB行为/颜色的映射关系一致。颜色仅用在流量控制时识别是否丢包，对内部优先级与队列的映射关系没有影响。

表 3-1 DiffServ 域中接口入方向上 VLAN 报文的 802.1p 优先级和 PHB 行为/颜色之间的映射关系

802.1p优先级	PHB行为	Color
0	BE	green

802.1p优先级	PHB行为	Color
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

表 3-2 DiffServ 域中接口入方向上 IP 报文的 DSCP 优先级和 PHB 行为/颜色之间的映射关系

DSCP	PHB行为	Color	DSCP	PHB行为	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green

DSCP	PHB行为	Color	DSCP	PHB行为	Color
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

表 3-3 DiffServ 域中接口入方向上 MPLS 报文的 EXP 优先级和 PHB 行为/颜色之间的映射关系

EXP优先级	PHB行为	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

服务等级与端口队列索引关系

缺省情况下，内部优先级（报文的服务等级）与端口队列的对应关系是一对一。在实际部署时，有时需要调整服务等级与队列的映射关系或者将不同的服务等级放入同一队列中进行调度，从而有效地节约设备缓存。设备按照内部优先级将报文送入不同的端口队列，从而针对队列进行流量整形、拥塞避免、队列调度等处理。

设备支持的内部优先级与各队列之间的对应关系如表3-4和表3-5所示。

表 3-4 内部优先级与各队列之间的对应关系表（SC 系列单板）

内部优先级	队列索引
BE（未知单播报文、组播报文、广播报文）	0
AF1（未知单播报文、组播报文、广播报文）	1
AF2（未知单播报文、组播报文、广播报文）	1
AF3（未知单播报文、组播报文、广播报文）	1
AF4（未知单播报文、组播报文、广播报文）	2
EF（未知单播报文、组播报文、广播报文）	2
CS6（未知单播报文、组播报文、广播报文）	6
CS7（未知单播报文、组播报文、广播报文）	6
BE（已知单播报文）	0
AF1（已知单播报文）	1
AF2（已知单播报文）	2
AF3（已知单播报文）	3
AF4（已知单播报文）	4
EF（已知单播报文）	5
CS6（已知单播报文）	6
CS7（已知单播报文）	7

表 3-5 内部优先级与各队列之间的对应关系表（其他单板）

内部优先级	队列索引
BE	0
AF1	1
AF2	2
AF3	3

内部优先级	队列索引
AF4	4
EF	5
CS6	6
CS7	7

Diffserv 域中出方向上服务等级（PHB 行为）/颜色与优先级的映射

缺省情况下，DiffServ域中映射关系包括：

- PHB行为/颜色到802.1p优先级的映射关系如表3-6。
- PHB行为/颜色到DSCP优先级的映射关系如表3-7。
- PHB行为/颜色到MPLS报文的EXP优先级的映射关系如表3-8。

端口优先级到PHB行为/颜色的映射关系与802.1p到PHB行为/颜色的映射关系一致。颜色仅用在流量控制时识别是否丢包，对内部优先级与队列的映射关系没有影响。

表 3-6 DiffServ 域中接口出方向上 VLAN 报文的 PHB 行为/颜色和 802.1p 优先级之间的映射关系

PHB行为	Color	802.1p优先级
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5

PHB行为	Color	802.1p优先级
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

表 3-7 DiffServ 域中接口出方向上 IP 报文的 PHB 行为/颜色和 DSCP 优先级之间的映射关系

PHB行为	Color	DSCP
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46

PHB行为	Color	DSCP
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

表 3-8 DiffServ 域中接口出方向上 MPLS 报文的 PHB 行为/颜色和 EXP 优先级之间的映射关系

PHB行为	Color	EXP优先级
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6

PHB行为	Color	EXP优先级
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

3.6 配置优先级映射

配置优先级映射后，设备将根据报文携带的优先级信息或者端口优先级映射到相应的PHB行为/颜色，从而提供差异化的服务。

优先级映射的配置逻辑

1. 配置优先级信任模式：配置优先级信任模式可以确定设备根据哪种优先级进行映射。
2. 配置DiffServ域：配置DiffServ域可以确定报文优先级与内部优先级（服务等级）的映射关系。以便设备在根据内部优先级提供有差别的QoS服务。
3. 应用DiffServ域：将DiffServ域应用在对象上，使DiffServ域中的映射和重标记关系生效。
4. 配置内部优先级与队列索引关系：配置内部优先级与队列的索引关系可以将不同内部优先级的报文送入不同队列进行差分服务。因为设备上有缺省的内部优先级与队列索引的关系，该步骤可选。

前置任务

配置优先级映射之前，需要完成以下任务：

- 配置相关接口的物理参数
- 配置相关接口的链路层属性

3.6.1 配置优先级信任模式

背景信息

配置优先级信任模式可以确定设备根据哪种优先级进行映射。

设备提供两种优先级信任模式：

- 信任报文的802.1p优先级
  - 对于带VLAN Tag的报文，根据报文自带的802.1p优先级，查找802.1p优先级到内部优先级映射表，然后为报文标记内部优先级。
  - 对于不带VLAN Tag的报文，设备将使用端口优先级，根据此优先级查找802.1p优先级到内部优先级映射表，然后为报文标记内部优先级。
- 信任报文的DSCP优先级

  根据报文的DSCP优先级，查找DSCP优先级到内部优先级映射表，为报文标记内部优先级。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**trust** { **8021p** { **inner** | **outer** } | **dscp** }，指定对报文按照某类优先级进行映射。

缺省情况下，接口信任的报文优先级为8021p outer。

说明

- SA系列单板：
  - 在报文的入接口，如果配置为**trust 8021p inner**，实际使用的仍然是外层Tag的802.1p优先级进行映射。
  - 在报文的入接口，如果配置为**trust 8021p outer**，使用外层Tag的802.1p优先级进行映射。如果报文不带Tag，按照端口缺省802.1p优先级入队列。
- E系列单板和SC系列单板：
  - 在报文的入接口，系统按照实际配置对报文进行优先级映射。
  - 在报文的出接口，如果配置为**trust 8021p inner**，如果从接口发出的报文是双Tag的，那么根据PHB/颜色映射到的外层Tag的802.1p优先级会被写入到外层Tag的802.1p优先级字段，而不会写入到内层Tag的802.1p优先级字段。
- 当设备出方向对双层tag报文做去掉外层tag的处理时，在设备接口出方向配置优先级映射功能，只有X系列单板生效。

----结束

3.6.2 （可选）配置端口优先级

背景信息

在以下两种情况下，会使用到端口优先级：

- 接口收到了不带VLAN Tag的报文，设备根据端口优先级对报文进行后续的差分服务。
- 若在接口上使用命令**trust upstream none**取消了接口优先级映射的功能，报文只要能被转发，都根据端口优先级进行后续的差分服务。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**port priority** *priority-value*，配置端口优先级。

缺省情况下，端口优先级为0。

说明

当接口通过**undo portswitch**切换到三层模式后，不能配置端口优先级值，端口优先级值均为0。

----结束

3.6.3 配置 DiffServ 域

背景信息

当设备作为DiffServ域和其他网络的边界节点时，需要配置内部优先级和外部优先级的相互映射关系：

- 当业务流流入设备时，设备将报文携带的优先级信息映射到相应的PHB行为/颜色，在设备内部，根据报文的PHB行为进行拥塞管理，根据报文的颜色进行拥塞避免；
- 当业务流流出设备时，设备将报文的PHB行为/颜色映射为相应的优先级，对端设备根据报文的优先级提供相应的QoS服务。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**diffserv domain** { **default** | *ds-domain-name* }，创建DiffServ域并进入DiffServ域视图。

default域定义了缺省情况下报文的优先级和PHB行为/颜色之间的映射关系。用户可以修改**default**域中定义的映射关系，但不能删除**default**域。除了**default**域外，设备最多可创建7个域。

步骤3 请根据实际情况对设备的优先级映射进行定义。

操作	命令
在接口入方向，将VLAN报文的802.1p优先级映射为PHB行为，并为报文着色	**8021p-inbound** *8021p-value* **phb** *service-class* [**green** | **yellow** | **red**]
在接口出方向，将PHB行为/颜色映射为VLAN报文的802.1p优先级	**8021p-outbound** *service-class* { **green** | **yellow** | **red** } **map** *8021p-value*
在接口入方向，将IP报文的DSCP优先级映射为PHB行为，并为报文着色	**ip-dscp-inbound** *dscp-value* **phb** *service-class* [**green** | **yellow** | **red**]
在接口出方向，将PHB行为/颜色映射为IP报文的DSCP优先级	**ip-dscp-outbound** *service-class* { **green** | **yellow** | **red** } **map** *dscp-value*
在接口入方向，将MPLS报文的EXP优先级映射为PHB行为，并为报文着色	**mpls-exp-inbound** *exp-value* **phb** *service-class* [*color*]
在接口出方向，将PHB行为/颜色映射为MPLS报文的EXP优先级	**mpls-exp-outbound** *service-class color* **map** *exp-value*

缺省映射关系请参见**3.5 优先级映射缺省配置**:

- 802.1p优先级到PHB行为/颜色映射
- PHB行为/颜色到802.1p优先级映射
- DSCP到PHB行为/颜色映射
- PHB行为/颜色到DSCP映射

- MPLS EXP优先级到PHB行为/颜色映射
- PHB行为/颜色到MPLS EXP优先级映射

----结束

3.6.4 应用 DiffServ 域

背景信息

当需要根据DiffServ域中定义的映射关系，对出/入设备的报文进行优先级到PHB行为/颜色之间的映射操作时，可以将DiffServ域绑定到报文的出/入接口，系统会根据DiffServ域中的映射关系进行报文优先级与PHB行为/颜色之间的映射。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**trust upstream** { *ds-domain-name* | **default** | **none** }，在接口上绑定DiffServ域。

如果接口上配置了**trust upstream none**命令，系统对出/入该接口的报文不做优先级映射。

如果要修改接口下绑定的DiffServ域，必须先执行**undo trust upstream**命令删除已绑定的DiffServ域，再执行**trust upstream**命令重新应用新的DiffServ域。

步骤4 （可选）执行命令**undo qos phb marking enable**，取消对接口出方向的报文进行PHB映射。

缺省情况下，对接口出方向的报文进行PHB映射。

----结束

3.6.5 （可选）配置内部优先级和队列之间的映射关系

背景信息

通过配置内部优先级和队列之间的映射关系，设备依据内部优先级和队列之间的映射关系将报文送入指定队列。

说明

SC系列和X系列单板不支持配置本地优先级和队列之间的映射关系。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**qos local-precedence-queue-map** *local-precedence queue-index*，配置内部优先级和队列之间的映射关系。

内部优先级和队列之间的映射关系仅会在接口入方向上起作用，即映射关系影响报文流入队列操作。

----结束

3.6.6 检查优先级映射配置结果

操作步骤

- 执行命令**display diffserv domain** [**all** | **name** *ds-domain-name*]，查看DiffServ域的配置信息。

  说明

  设备中缺省存在一个名为default的DiffServ域。仅支持该DiffServ域，仅支持命令**display diffserv domain name default**。

- 执行命令**display qos local-precedence-queue-map**，查看本地优先级到队列的映射关系。

----结束

3.7 配置重标记优先级

背景信息

通过配置重标记优先级，设备对符合流分类规则的报文的指定优先级字段进行更改，如VLAN报文的802.1p优先级、IP报文的DSCP和内部优先级等。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，创建一个流分类并进入流分类视图，或进入已存在的流分类视图。

      and表示流分类中各规则之间关系为逻辑“与”，指定该逻辑关系后：

      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

      or表示流分类各规则之间是逻辑“或”，即报文只需匹配流分类中的一个或多个规则即属于该类。

      缺省情况下，流分类中各规则之间的关系为逻辑“或”。
   c. 请根据实际情况定义流分类中的匹配规则。

      说明

      if-match ip-precedence和**if-match tcp**命令仅对IPv4报文生效。

      X系列单板不支持配置包含高级ACL中的**ttl-expired**字段的流分类规则。

      当流分类匹配**if-match ipv6 acl** { *acl-number* | *acl-name* }时，X系列单板不支持**add-tag vlan-id** *vlan-id*、**remark 8021p** [*8021p-value* | **inner-8021p**]、**remark cvlan-id** *cvlan-id*、**remark vlan-id** *vlan-id*、**mac-address learning disable**。

匹配规则	命令	说明
外层VLAN ID或基于QinQ报文内外两层Tag的VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]	-
QinQ报文内外层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**vlan-id** *vlan-id*]	-
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个802.1p值，报文只需匹配其中一个802.1p值就匹配该规则。
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>	-
丢弃报文	**if-match discard**	包含该流分类的报文只能与流量统计和流镜像两种动作绑定。
QinQ报文双层Tag	**if-match double-tag**	-
MPLS报文EXP优先级	**if-match mpls-exp** *exp-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个MPLS EXP值，报文只需匹配其中一个MPLS EXP值就属于该类。
目的MAC地址	**if-match destination-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
源MAC地址	**if-match source-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }	-
所有报文	**if-match any**	-

匹配规则	命令	说明
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个DSCP值，报文只需匹配其中一个DSCP值就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
IP报文的IP优先级	**if-match ip-precedence** *ip-precedence-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个IP优先级，报文只需匹配其中一个IP优先级就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }	-
IPv6下一报文头类型	**if-match ipv6 next-header** *header-number* **first-next-header**	ET1D2X12SSA0单板不支持Prefix的长度为(64,128)之间的路由。
TCP报文SYN Flag	**if-match tcp syn-flag** { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	-
入接口	**if-match inbound-interface** *interface-type interface-number*	包含该流分类的流策略不能应用在出方向。 包含该流分类的流策略不能应用在接口视图。
出接口	**if-match outbound-interface** *interface-type interface-number*	X系列单板不支持将包含该流分类的流策略应用在入方向。 包含该流分类的流策略不能应用在接口视图。

匹配规则	命令	说明
ACL规则	**if-match acl** { *acl-number* | *acl-name* }	• 使用ACL作为流分类规则，请先配置相应的ACL规则。 • 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果某ACL规则中有多个rule，报文只需匹配其中一个rule就匹配该ACL规则。 • 如果ACL的规则指定了参数**vpn-instance**，那么基于该ACL进行分类的流分类对应的流策略将不生效。
ACL6规则	**if-match ipv6 acl** { *acl-number* | *acl-name* }	使用ACL6作为流分类规则，请先配置相应的ACL6规则。 如果ACL6的规则指定了参数**vpn-instance**，那么基于该ACL6进行分类的流分类对应的流策略将不生效。
流ID	**if-match flow-id** *flow-id*	包含**if-match flow-id**匹配规则的流分类和包含**remark flow-id**动作的流行为应在不同的流策略中使用。 包含**if-match flow-id**匹配规则的流策略只能应用在接口、VLAN、VLANIF接口、单板、全局的入方向。 SA系列单板不支持配置匹配流ID。
VXLAN内层报文信息	**if-match vxlan** [**transit**] **vni** *vni-id*	包含该流分类的流策略不能应用在出方向上。 当流分类中包含此匹配规则时，流行为只支持流量监管、报文过滤和流量统计。

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

a. 执行命令**traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

b. 请根据实际需要进行如下配置：

- 执行命令**remark 8021p** [*8021p-value* | **inner-8021p**]，将符合流分类的报文重新标记802.1p优先级。

说明

SA系列单板不支持从内层继承802.1p优先级。

包含**remark 8021p**动作的流策略应用在接口出方向时，出接口VLAN必须工作在tag方式。

- 执行命令**remark dscp** { *dscp-name* | *dscp-value* }，将符合流分类的报文重新标记DSCP值。
- 执行命令**remark local-precedence** { *local-precedence-name* | *local-precedence-value* } [**green** | **yellow** | **red**]，将符合流分类的重新标记内部优先级。

c. （可选）执行命令**statistic enable**，使能流量统计功能。

d. 执行命令**quit**，退出流行为视图。

e. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name* [**match-order** { **auto** | **config** }]，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。创建流策略时，如果未指定规则匹配顺序，缺省规则匹配顺序为**config**。

应用流策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先清除该策略的应用，再重新创建并指定所需的匹配顺序。

设备支持在创建流策略时指定流策略中多个规则的匹配顺序，匹配顺序包括自动顺序（**auto**）和配置顺序（**config**）两种：

- 如果选择自动顺序，匹配顺序由系统预先指定的流分类类型的优先级决定，该优先级由高到低依次为：基于二层和IPv4三层信息流分类 > 基于高级ACL6规则流分类 > 基于基本ACL6规则流分类 > 基于二层信息流分类 > 基于IPv4三层信息流分类 > 基于用户自定义ACL规则流分类。规则优先匹配优先级高的流分类。当某一数据流量同时匹配不同流分类，且对应的流行为存在冲突时，只有流行为优先级高的规则生效。
- 如果选择配置顺序，匹配顺序由流分类规则的优先级决定，先匹配优先级较高的流分类规则。配置流分类时指定优先级，则数值越小，优先级越高；如果配置流分类时未指定precedence-value，则缺省优先级为0。关于流分类优先级的详细说明，请参见**traffic classifier**。

c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

– 在接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。

说明

- 仅E系列、X系列和S系列中的SC单板支持配置以太网子接口。单板详情请参见《硬件描述》中的单板分类。
- 对于上述系列单板的二层接口，仅hybrid和trunk类型接口支持配置二层以太网子接口。
- 对于上述系列单板的二层接口，执行命令**undo portswitch**切换为三层接口后，支持配置三层以太网子接口。
- S系列中的SA单板不支持创建以太网子接口，也不支持转发IP流量到其它单板的以太网子接口。
- 建议用户先将成员接口加入Eth-Trunk后，再配置Eth-Trunk子接口。只有当成员接口所在的单板系列均支持配置以太网子接口时，Eth-Trunk子接口才能配置成功。
- VCMP的角色是Client时，不能配置VLAN终结子接口。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口或子接口视图上应用流策略。

每个接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同接口的不同方向。应用后，系统对流经该接口并匹配流分类中规则的入方向或出方向报文实施策略控制。

说明

- 子接口仅支持**inbound**参数。
- 建议不要在Untagged类型接口出方向上应用包含有**remark 8021p**、**remark cvlan-id**、**remark vlan-id**等动作的流策略，否则，可能导致报文内容出错。
- ET1D2X12SSA0、ET1D2X48SEC0、SC系列单板有2N个接口，如果1～N号中的接口与N+1～2N号中的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的2倍。
- 在X系列单板中，如果不同的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，且这些接口的ACL资源分散在N个组中进行统计（执行命令**display acl resource**查看），那么Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的N倍。
- 应用流策略需要设备有足够的ACL资源，否则会导致应用失败。以一个流策略中的if-match占用一条ACL为例，同一个流策略应用到M个接口时，将占用M条ACL资源；应用到L个VLAN且设备上存在N块接口板时，将占用L*N条ACL规则；应用到全局且设备上存在N块接口板时，将占用N条ACL规则。if-match规则占用ACL资源的情况参考“MQC配置-配置注意事项”中的表3。
- 配置Tunnel接口的隧道协议为GRE后，可在Tunnel接口入方向应用流策略。
- 在VXLAN二层子接口、Dot1q终结子接口和绑定了BGP AD方式的子接口下，应用流策略不生效，建议在主接口配置基于流ID的分类方式。

- 在VLAN上应用流策略

  i. 执行命令**system-view**，进入系统视图。

  ii. 执行命令**vlan** *vlan-id*，进入VLAN视图。

  iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLAN上应用流策略。

  每个VLAN的每个方向能且只能应用一个流策略。

  应用后，系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施策略控制。但是流策略对VLAN 0的报文不生效。

- 在VLANIF接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLANIF接口上应用流策略。

每个VLANIF接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同VLANIF接口的不同方向。

对于应用流策略的VLANIF接口，其对应的VLAN不能是Super-VLAN或MUX VLAN。

对于X系列单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文生效。对于其它单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文及三层组播报文生效。

说明

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的入方向上应用该流策略：

- **remark vlan-id**
- **remark cvlan-id**
- **add-tag vlan-id**
- **remark 8021p**
- **remark flow-id**
- **mac-address learning disable**

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的出方向上应用该流策略：

- **add-tag vlan-id**
- **remark flow-id**
- **mac-address learning disable**

– 在全局或单板上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**traffic-policy** *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]，在全局或单板上应用流策略。

全局或单板的每个方向上能且只能应用一个流策略，如果在全局某方向应用了流策略，则不能在单板的该方向上再次应用流策略；指定单板在某方向应用流策略后，也不能在全局的该方向上再次应用流策略。

– 在SSID模板上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**wlan**，进入WLAN视图。

iii. 执行命令**ssid-profile name** *profile-name*，创建SSID模板并进入模板视图。

iv. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在SSID模板上应用流策略。

– 在AP组上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**wlan**，进入WLAN视图。

iii. 执行命令**ap-group name** *group-name*，创建AP组并进入AP组视图。

iv. 执行命令**traffic-policy** *policy-name* **outbound**，在AP组上应用流策略。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior user-defined** [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看用户定义的流策略的配置信息。
- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

  说明

  流策略可以应用到子接口上，但暂不支持通过此命令查看子接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。
- 执行命令**display traffic policy** { **interface** [*interface-type interface-number*[*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]，查看已配置的流策略信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

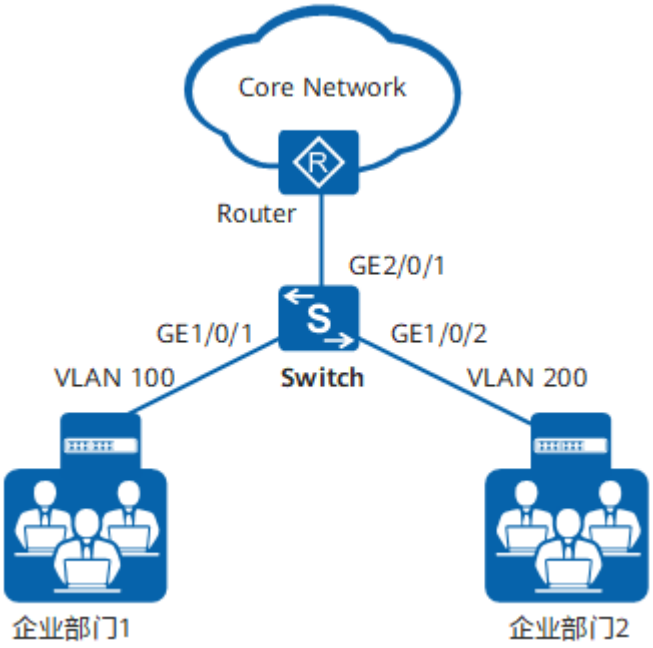
3.8 配置优先级映射示例

组网需求

如图3-6所示，Switch通过接口GE2/0/1与路由器互连，企业部门1和企业部门2可经由Switch和路由器访问网络。企业部门1和企业部门2的VLAN ID分别为100、200。

由于企业部门1的服务等级高，需要得到更好的QoS保证。来自企业部门1和2的报文802.1p值均为0，通过定义DiffServ域，将来自企业部门1的数据报文优先级映射为4，将来自企业部门2的数据报文优先级映射为2，以提供差分服务。

图 3-6 优先级映射配置组网图



配置思路

采用如下的思路配置优先级映射：

1. 创建VLAN，并配置各接口，企业部门1和企业部门2都能够通过Switch访问网络。
2. 创建DiffServ域，将802.1p优先级映射为PHB行为和颜色。
3. 在Switch入接口GE1/0/1和GE1/0/2上绑定DiffServ域。

操作步骤

步骤1 创建VLAN并配置各接口

创建VLAN 100和VLAN 200。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
```

将接口GE1/0/1、GE1/0/2、GE2/0/1的接入类型分别配置为trunk，并分别将接口GE1/0/1、GE1/0/2加入VLAN 100和VLAN 200；接口GE2/0/1加入VLAN 100和VLAN 200。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 200
[Switch-GigabitEthernet2/0/1] quit
```


步骤2 创建并配置DiffServ域

在Switch上创建DiffServ域ds1、ds2，并配置将企业部门1和企业部门2的802.1p优先级映射到服务等级。

```
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 0 phb af4 green
[Switch-dsdomain-ds1] quit
[Switch] diffserv domain ds2
[Switch-dsdomain-ds2] 8021p-inbound 0 phb af2 green
[Switch-dsdomain-ds2] quit
```

步骤3 将DiffServ域绑定到接口

将DiffServ域ds1和ds2分别绑定到接口GE1/0/1、GE1/0/2。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] trust upstream ds1
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] trust upstream ds2
[Switch-GigabitEthernet1/0/2] quit
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 200
#
diffserv domain ds1
 8021p-inbound 0 phb af4 green
diffserv domain ds2
 8021p-inbound 0 phb af2 green
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 trust upstream ds1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 trust upstream ds2
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
return
```

相关信息

技术论坛

QoS专题-第3期-QoS实现之报文简单分类与标记

3.9 优先级映射常见配置错误

3.9.1 报文未进入正确队列

常见原因

报文未进入正确队列的常见原因主要包括：

- 入接口应用的DiffServ域下的优先级映射关系与要求不一致。
- 入接口有影响报文入队列的配置。
- 报文所属VLAN下有影响报文入队列的配置。
- 全局有影响报文入队列的配置。

说明

在SC系列单板上，已知单播报文和非已知单播报文的入队列方式有所不同：对于非已知单播报文，只有0、1、2、6四个队列供使用；对于已知单播报文，有0～7队列供使用。详细内容请参见**3.5 优先级映射缺省配置**。

操作步骤

步骤1 检查优先级映射关系是否正确

进入报文入方向的接口视图，执行命令**display this**，查看入接口配置的**trust upstream**命令，然后执行命令**display diffserv domain name** *domain-name*检查DiffServ域中配置的优先级映射关系是否与业务规划符合：

- 如果配置不符合业务规划，请使用命令**ip-dscp-inbound**、**mpls-exp-inbound**或**8021p-inbound**正确配置优先级映射关系。
- 如果配置符合业务规划，请执行步骤2。

步骤2 检查入接口上是否有影响报文入队列的配置

如果入接口上配置了：

- **port vlan-stacking**、**port vlan-stacking 8021p**或**port vlan-stacking vlan 8021p**，且命令中带有**remark-8021p**参数，则报文的802.1p优先级为**remark**后的，影响802.1p优先级到本地优先级的映射，进而会影响报文入队列。
- **port vlan-mapping 8021p**、**port vlan-mapping vlan 8021p**、**port vlan-mapping vlan map-vlan**，且命令中带有**remark-8021p**参数，则报文的802.1p优先级为**remark**后的，影响802.1p优先级到本地优先级的映射，进而会影响报文入队列。
- 入方向且与报文匹配的**traffic-policy**，若流策略下配置了**remark local-precedence**动作，系统按照**remark**后的本地优先级入队列。
- 入方向且与报文匹配的**traffic-policy**，若流策略下有**remark 8021p**或**remark dscp**动作，则系统根据**remark**后的报文优先级进行报文优先级到本地优先级的映射，并根据映射后的本地优先级入队列。
- 入方向且与报文匹配的**traffic-policy**，若流策略下有**add-tag vlan-id**动作，对于进入该接口的带VLAN Tag的报文，系统给报文打上一层外层VLAN Tag后仍按照原VLAN Tag的优先级进行优先级映射；对于进入该接口的不带VLAN Tag的报文，系统给报文打上一层VLAN Tag后，系统按照端口优先级进行优先级映射，并根据映射后的本地优先级入队列。
- **trust upstream none**，则进入该接口的所有报文不进行优先级映射，报文按照端口优先级入队列。

- **port link-type dot1q-tunnel**，且该接口下没有配置**trust 8021p inner**，则进入该接口的所有报文将根据端口优先级入对应的队列。

进入接口视图，执行命令**display this**，检查入接口是否有上述影响报文入队列的配置：

- 如果有，请根据以上情况删除或修改该配置。
- 如果没有，执行步骤3。

步骤3 检查报文所属VLAN下是否有影响报文入队列的配置

如果报文所属VLAN下配置了：

- 入方向且与报文匹配的**traffic-policy**，若流策略下配置了**remark local-precedence**动作，系统按照**remark**后的PHB行为入队列。
- 入方向且与报文匹配的**traffic-policy**，若流策略下有**remark 8021p**或**remark dscp**动作，则系统根据**remark**后的报文优先级进行报文优先级到本地优先级的映射，并根据映射后的本地优先级入队列。
- 入方向的**traffic-policy**，若流策略下有**add-tag vlan-id**动作，对于进入该接口的带VLAN Tag的报文，系统给报文打上一层外层VLAN Tag后仍按照原VLAN Tag的优先级进行优先级映射；对于进入该接口的不带VLAN Tag的报文，系统给报文打上一层VLAN Tag后，系统按照端口优先级进行优先级映射，并根据映射后的本地优先级入队列。

进入报文所属VLAN，执行命令**display this**，检查报文所属VLAN下是否有上述影响报文入队列的配置：

- 如果有，请根据以上情况删除或修改该配置。
- 如果没有，执行步骤4。

步骤4 检查全局是否有影响报文入队列的配置

如果全局配置了：

- **qos local-precedence-queue-map**，则系统按照此命令指定的本地优先级与队列之间的映射关系入队列。

  说明

  SC系列和X系列单板不支持配置**qos local-precedence-queue-map**。
- 入方向且与报文匹配的**traffic-policy global**，若流策略下配置了**remark local-precedence**动作，系统按照**remark**后的本地优先级入队列。
- 入方向且与报文匹配的**traffic-policy global**，若流策略下有**remark 8021p**或**remark dscp**动作，则系统根据**remark**后的报文优先级进行报文优先级到本地优先级的映射，并根据映射后的本地优先级入队列。
- 入方向且与报文匹配的**traffic-policy global**，若流策略下有**add-tag vlan-id**动作，对于进入该接口的带VLAN Tag的报文，系统给报文打上一层外层VLAN Tag后仍按照原VLAN Tag的优先级进行优先级映射；对于进入该接口的不带VLAN Tag的报文，系统给报文打上一层VLAN Tag后，系统按照端口优先级进行优先级映射，并根据映射后的本地优先级入队列。

执行命令**display current-configuration**，检查全局是否有上述影响报文入队列的配置，如果有，请根据实际情况删除或修改该配置。

----结束

3.9.2 优先级映射结果不正确

常见原因

优先级映射结果不正确的常见原因主要包括：

- 报文在出接口未按报文优先级入队列。
- 出/入接口信任的优先级类型与要求不一致。
- 出/入接口信任的DiffServ域下配置的优先级映射关系与要求不一致。
- 出/入接口有影响优先级映射的配置。

操作步骤

步骤1 检查报文在出接口是否进入正确的队列

执行命令**display qos queue statistics interface** *interface-type interface-number*，检查报文在出接口是否按照要求进入了相应的队列。

- 如果报文在出接口没有按照要求入队列，请参见**3.9.1 报文未进入正确队列**定位错误。
- 如果报文在出接口进入了正确的队列，执行步骤2。

步骤2 检查出/入接口信任的优先级类型是否正确

进入出/入接口的接口视图，执行命令**display this**，查看接口配置的**trust**命令（如果没有配置，则系统缺省信任外层802.1p优先级），看信任的优先级类型是否与业务规划符合：

- 如果不符合，执行命令**trust**正确配置接口信任的优先级类型。
- 如果符合，执行步骤3。

步骤3 检查出/入接口信任的DiffServ域中的优先级映射关系是否正确

进入出/入接口的接口视图，执行命令**display this**，查看出/入接口配置的**trust upstream**命令（如果没有配置，系统缺省信任default域）。

然后执行命令**display diffserv domain name** *domain-name*，检查本地优先级和报文优先级之间的映射是否与业务规划符合：

说明

本地优先级即入接口优先级映射后的本地优先级。

- 如果不符合，执行命令**ip-dscp-outbound**、**mpls-exp-outbound**或**8021p-outbound**正确配置本地优先级到报文优先级的映射。
- 如果符合，执行步骤4。

步骤4 检查出/入接口是否有影响优先级映射的配置

如果接口配置了：

- **undo qos phb marking enable**，则系统对接口出方向的报文不进行PHB映射。
- **trust upstream none**，则系统对从此接口出去的报文不进行优先级映射。
- 出/入方向且与报文匹配的**traffic-policy**，若流策略下有**remark 8021p**或**remark dscp**动作，报文优先级为**remark**后的报文优先级。

进入出/入接口的接口视图，执行命令**display this**，检查接口是否有上述影响优先级映射的配置，如果有，请根据以上情况删除或修改该配置。

----结束

3.10 优先级映射 FAQ

3.10.1 入端口 remark 8021p/dscp 是否会修改本地优先级及对应报文内容

入端口remark 8021p修改本地优先级，remark dscp不修改本地优先级。

关于报文内容是否修改：

单板类型	remark 8021p	remark dscp
入端口标准板、出端口标准板	No	Yes
入端口标准板、出端口增强板	Yes	Yes
入端口增强板、出端口标准板	No	Yes
入端口增强板、出端口增强板	Yes	Yes

4 流量监管、流量整形和接口限速配置

4.1 流量监管、流量整形和接口限速简介

当报文的发送速率大于接收速率，或者下游设备的接口速率小于上游设备的接口速率时，可能会引起网络的拥塞。如果不限制用户发送的业务流量大小，大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源更有效的为用户服务，需要对用户的业务流量加以限制。

流量监管、流量整形和接口限速就是一种通过对流量规格进行监督，以限制流量及其资源使用的流控策略。

流量监管

流量监管TP（Traffic Policing）可以监督不同流量进入网络的速率，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，从而保护网络资源和用户的利益。

流量整形

流量整形TS（Traffic Shaping）是一种主动调整流量输出速率的措施。流量整形将上游不规整的流量进行削峰填谷，使流量输出比较平稳，从而解决下游设备的拥塞问题。

接口限速

接口限速LR（Limit Rate）可以对一个接口上发送或者接收全部报文的总速率进行限制。当不需要区分报文类型而要限制通过接口全部流量速率时，接口限速功能可以简化配置。

相关信息

技术论坛

QoS专题-第4期-QoS实现之限速

4.2 流量监管、流量整形和接口限速原理描述

网络中存在不同用户的多种业务流量，如果对所有用户的业务流量都不加限制，那么当大量用户产生不断突发的业务数据时，网络会更加拥挤。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，必须对用户的业务流量加以限制。

流量监管TP、流量整形TS和接口限速LR通过监督进入网络的流量速率来限制流量及其资源的使用。要监督进入网络的流量首先需要对流量进行度量，然后才能根据度量结果实施调控策略。一般采用令牌桶（Token Bucket）对流量的规格进行度量。

4.2.1 流量评估与令牌桶技术

概述

为了保证有限的网络资源能够更有效的被利用，更好的为更多的用户服务，必须对用户的流量加以限制。流量监管、流量整形和接口限速都可以通过对流量规格进行监督以限制流量及其资源的使用，但是它们必须要有一个前提条件，那就是需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。一般采用令牌桶对流量的规格进行评估。

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。在使用令牌桶对流量规格进行评估时，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，称流量遵守或符合约定值，否则称为不符合或超标。

关于令牌桶处理报文的方式，RFC中定义了以下标记算法：

- 单速率三色标记（single rate three color marker，srTCM，或称为单速双桶算法）算法，主要关注报文尺寸的突发。
- 双速率三色标记（two rate three color marker，trTCM，或称为双速双桶算法）算法，主要关注报文速率的突发。

令牌桶算法的评估结果都是为报文打上红、黄、绿三种颜色的标记，所以称为“三色标记”。QoS会根据报文的颜色做相应的处理，两种算法都可以工作于色盲模式和色敏模式下。以下以色盲模式为例对标记算法进行详细介绍。

单速双桶

单速双桶采用RFC2697定义的单速三色标记器srTCM（Single Rate Three Color Marker）算法对流量进行测评，根据评估结果为报文打颜色标记，即绿色、黄色和红色。

如图4-1所示，为方便描述将两个令牌桶称为C桶和E桶，用Tc和Te表示桶中的令牌数量。单速双桶有3个参数：

- CIR（Committed Information Rate）：承诺信息速率，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（Committed Burst Size）：承诺突发尺寸，表示C桶的容量，即C桶瞬间能够通过的承诺突发流量；
- EBS（Excess Burst Size）：超额突发尺寸，表示E桶的容量，即E桶瞬间能够通过的超出突发流量。

系统按照CIR速率向桶中投放令牌：

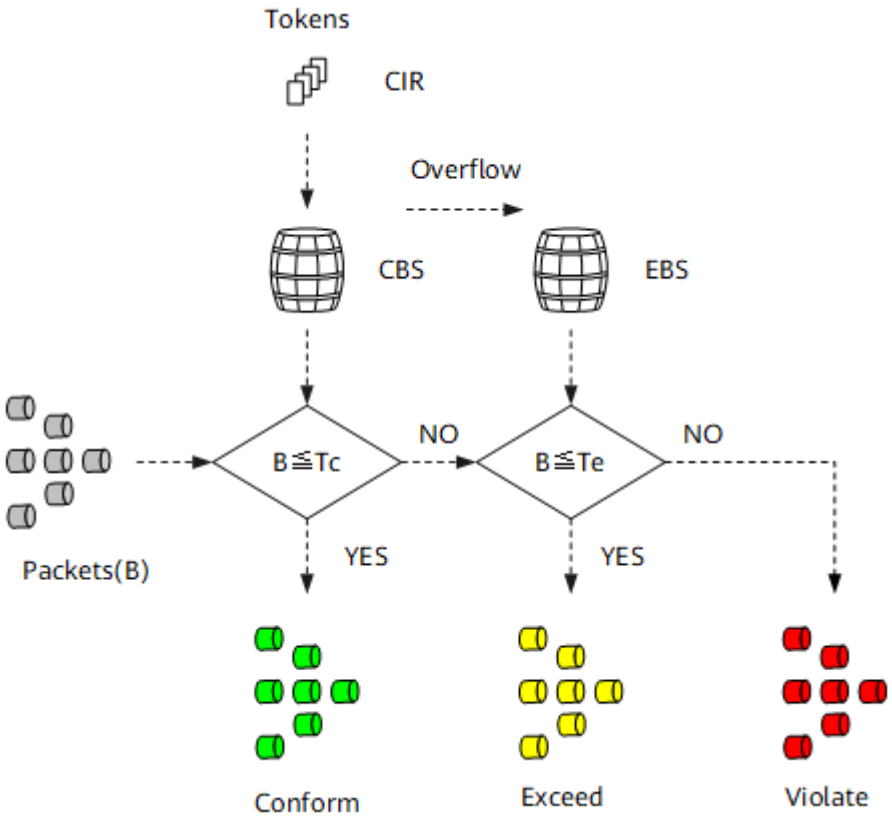
- 若Tc<CBS，Tc增加；
- 若Tc=CBS，Te<EBS，Te增加；
- 若Tc=CBS，Te=EBS，则都不增加。

对于到达的报文，用B表示报文的大小：

- 若B≤Tc，报文被标记为绿色，且Tc减少B；
- 若Tc<B≤Te，报文被标记为黄色，且Te减少B；
- 若Te<B，报文被标记为红色，且Tc和Te都不减少。

单速双桶模式允许流量突发，当用户的流量速率小于配置的CIR时，报文被标记为绿色；当用户的突发流量大于配置的CBS而小于EBS时，报文被标记为黄色；当用户的突发流量大于配置的EBS时，报文被标记为红色。

图 4-1 单速双桶示意图



假设设备接口的CIR设置为1Mbit/s，CBS为2000bytes，EBS为2000bytes，初始状态时C桶和E桶满。单速双桶模式下，令牌桶对报文的处理过程如下：

说明

为方便计算，此处1Mbit/s按1×10^6bit/s计算。

- 假设第1个到达的报文是1500bytes。检查C桶发现令牌数大于数据包的长度，所以数据包被标为绿色，C桶减少令牌1500bytes，还剩500bytes，E桶令牌数量保持不变。
- 假设1ms之后到达第2个报文1500bytes。在此间隔内，C桶新增令牌 = CIR × 1ms = 1000bits = 125bytes，加上C桶原来剩余的令牌500bytes，此时C桶共有625bytes，检查发现C桶内令牌数量不够。检查E桶发现有足够令牌，因此报文标记为黄色，E桶减少令牌1500bytes，剩余500bytes，C桶剩余625bytes保持不变。
- 假设又过1ms后到达第3个报文1000bytes。在此间隔内，C桶新增令牌125bytes，加上C桶原来剩余的令牌625bytes，此时C桶共有750bytes，检查发现C桶内令牌数量不够。检查E桶发现令牌数量也不够，因此报文被标记为红色，C桶、E桶令牌数不变。
- 假设又过20ms后到达第4个报文1500bytes。在此间隔内，C桶新增令牌 = CIR × 20ms = 20000bits = 2500bytes，加上C桶原来剩余的令牌750bytes，C桶此时令牌数为3250bytes。而CBS = 2000bytes，因此溢出的1250bytes添加到E桶，此时E桶有1750bytes。由于C桶中令牌数大于报文长度，报文标记为绿色，C桶减少令牌1500bytes，剩余500bytes，E桶令牌数量保持不变。

报文处理过程汇总见表4-1。

表 4-1 单速双桶模式下报文处理过程

包序号	时刻(ms)	报文长度(bytes)	与上次添加令牌的间隔(ms)	本轮增加令牌(bytes)	令牌增加后各桶令牌(bytes)		报文处理后各桶剩余令牌(bytes)		报文标记结果
					C桶	E桶	C桶	E桶	
-	-	-	-	-	2000	2000	2000	2000	-
1	0	1500	0	0	2000	2000	500	2000	绿色
2	1	1500	1	125	625	2000	625	500	黄色
3	2	1000	1	125	750	500	750	500	红色
4	22	1500	20	2500	2000	1750	500	1750	绿色

单速单桶

如果不允许突发流量，上面单速双桶算法中的EBS则设置为0，此时E桶的令牌数始终为0，相当于只使用了一个令牌桶，这种情况称为单速单桶。

如图4-2所示，为方便描述将此令牌桶称为C桶，用Tc表示桶中的令牌数量。单速单桶有2个参数：

- CIR：承诺信息速率，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：承诺突发尺寸，表示C桶的容量，即C桶瞬间能够通过的承诺突发流量。

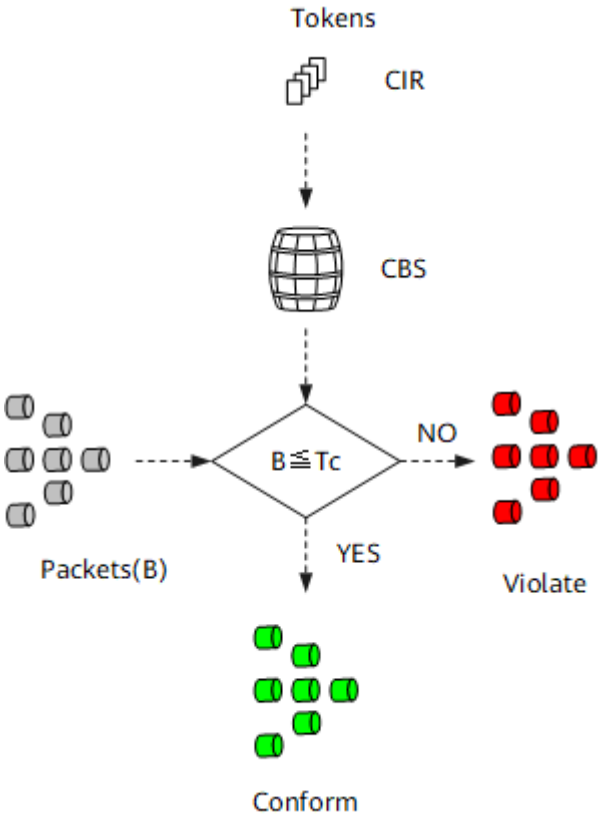
系统按照CIR速率向C桶中投放令牌，当Tc<CBS时，令牌数增加，否则不增加。

对于到达的报文，用B表示报文的大小：

- 若B≤Tc，报文被标记为绿色，且Tc减少B；
- 若B>Tc，报文被标记为红色，Tc不减少。

单速单桶模式不允许流量突发，当用户的流量速率小于配置的CIR时，报文被标记为绿色；当用户的流量大于CIR时直接被标记为红色。

图 4-2 单速单桶示意图



假设设备端口的CIR设置为1Mbit/s，CBS为2000bytes，初始状态时C桶满。单速单桶模式下，令牌桶对报文的处理过程如下：

说明

为方便计算，此处1Mbit/s按1×10^6bit/s计算。

- 假设第1个到达的报文是1500bytes时，检查C桶发现令牌数大于数据包的长度，所以数据包被标为绿色，C桶减少令牌1500bytes，还剩500bytes。
- 假设1ms之后到达第2个报文1500bytes。在此间隔内，C桶新增令牌 = CIR × 1ms = 1000bits = 125bytes，加上C桶原来剩余的令牌500bytes，此时C桶共有625bytes。令牌数量不够，报文标记为红色。
- 假设又过1ms后到达第3个报文1000bytes。在此间隔内，C桶新增令牌125bytes，加上C桶原来剩余的令牌625bytes，此时C桶共有750bytes。令牌数量不够，因此报文被标记为红色。
- 假设又过20ms后到达第4个报文1500bytes。在此间隔内，C桶新增令牌 = CIR × 20ms = 20000bits = 2500bytes，加上C桶原来剩余的令牌750bytes，C桶此时令牌数为3250bytes。而CBS = 2000bytes，因此溢出1250bytes令牌被丢弃。此时C桶令牌数大于报文长度，报文标记为绿色，C桶减少令牌1500bytes，剩500bytes。

报文处理过程汇总见表4-2。

表 4-2 单速单桶模式下报文处理过程

包序号	时刻(ms)	报文长度(bytes)	与上次添加令牌的间隔(ms)	本轮增加令牌(bytes)	令牌增加后C桶令牌(bytes)	报文处理后C桶剩余令牌(bytes)	报文标记结果
-	-	-	-	-	2000	2000	-
1	0	1500	0	0	2000	500	绿色
2	1	1500	1	125	625	625	红色
3	2	1000	1	125	750	750	红色
4	22	1500	20	2500	2000	500	绿色

双速双桶

双速双桶采用RFC2698定义的双速三色标记器trTCM（A Two Rate Three Color Marker）算法对流量进行测评，根据评估结果为报文打颜色标记，即绿色、黄色和红色。

如图4-3所示，为方便描述将两个令牌桶称为P桶和C桶，用Tp和Tc表示桶中的令牌数量。双速双桶有4个参数：

- PIR（Peak information rate）：峰值信息速率，表示向P桶中投放令牌的速率，即P桶允许传输或转发报文的峰值速率，PIR大于CIR；
- CIR：承诺信息速率，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；
- PBS（Peak Burst Size）：峰值突发尺寸，表示P桶的容量，即P桶瞬间能够通过的峰值突发流量；
- CBS：承诺突发尺寸，表示C桶的容量，即C桶瞬间能够通过的承诺突发流量。

系统按照PIR速率向P桶中投放令牌，按照CIR速率向C桶中投放令牌：

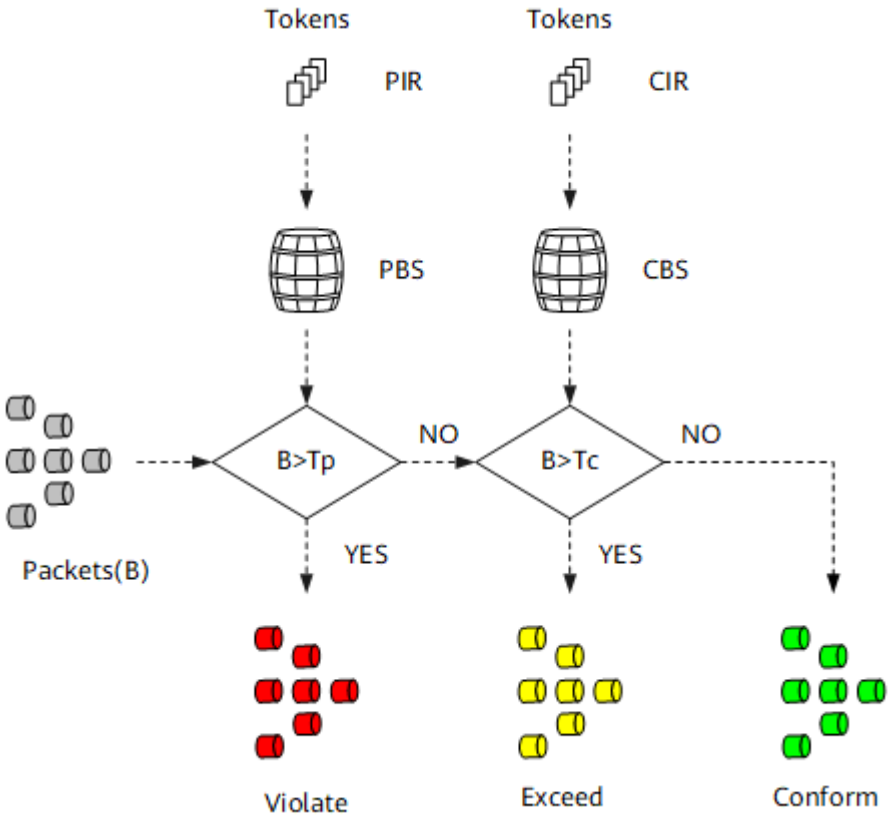
- 当Tp<PBS时，P桶中令牌数增加，否则不增加。
- 当Tc<CBS时，C桶中令牌数增加，否则不增加。

对于到达的报文，用B表示报文的大小：

- 若Tp<B，报文被标记为红色；
- 若Tc<B≤Tp，报文被标记为黄色，且Tp减少B；
- 若B≤Tc，报文被标记为绿色，且Tp和Tc都减少B。

双速双桶模式允许流量速率突发，当用户的流量速率小于配置的CIR时，报文被标记为绿色；当用户的流量大于CIR而小于PIR时，报文被标记为黄色；当用户的流量大于PIR时，报文被标记为红色。

图 4-3 双速双桶示意图



假设设备端口的CIR设置为1Mbit/s，PIR设置为2Mbit/s，CBS为2000 bytes，PBS为3000 bytes，初始状态时C桶和P桶满。双速双桶模式下，令牌桶对报文的处理过程如下：

说明

为方便计算，此处1Mbit/s按1×10^6bit/s计算。

- 第1个到达的报文假设是1500bytes。检查发现报文长度不超过P桶也不超过C桶，所以数据包被标为绿色，C桶和P桶都减少令牌1500bytes，C桶还剩500bytes，P桶还剩1500bytes。
- 假设1ms后到达第2个报文1800bytes。在此间隔内，P桶新增令牌 = PIR × 1ms = 2000bit = 250bytes，加上P桶原来剩余的令牌1500bytes，此时P桶共有1750bytes，小于报文长度。C桶新增令牌 = CIR × 1ms = 1000bits = 125bytes，加上C桶原来剩余的令牌500bytes，此时C桶共有625bytes。报文标记为红色，P桶、C桶令牌数不变。
- 假设又过1ms后到达第3个报文1000bytes。在此间隔内，P桶新增令牌250byte，加上P桶原来剩余的令牌1750bytes，此时P桶共有令牌2000bytes，大于报文长度。再检查C桶，C桶新增令牌125bytes，加上C桶原来剩余的令牌625bytes，此时C桶共有750bytes，仍然小于报文长度。因此报文被标记为黄色，P桶减少令牌1000bytes，剩余1000bytes，C桶令牌不变。
- 假设又过20ms之后到达报文1500bytes。在此间隔内，P桶新增令牌 = PIR × 20ms = 40000bits = 5000bytes，超过P桶容量PBS，因此P桶令牌数 = PBS = 3000bytes，溢出的令牌丢弃。这样P桶有3000bytes，大于报文长度。此时C桶增加令牌 = CIR × 20ms = 20000bits = 2500bytes，超过C桶容量CBS，因此C桶令牌

数 = CBS = 2000bytes，溢出的令牌丢弃。C桶此时令牌数2000bytes，大于报文长度。报文被标记为绿色，P桶减少令牌1500bytes，剩余1500bytes；C桶减少令牌1500bytes，剩余500bytes。

报文处理过程汇总见表4-3。

表 4-3 双速双桶模式下报文处理过程

包序号	时刻(ms)	报文长度(bytes)	与上次添加令牌的间隔(ms)	本轮增加令牌(bytes)		令牌增加后各桶令牌(bytes)		报文处理后各桶剩余令牌(bytes)		报文标记结果
				C桶	P桶	C桶	P桶	C桶	P桶	
-	-	-	-	-	-	2000	3000	2000	3000	-
1	0	1500	0	0	0	2000	3000	500	1500	绿色
2	1	1800	1	125	250	625	1750	625	1750	红色
3	2	1000	1	125	250	750	2000	750	1000	黄色
4	22	1500	20	2500	5000	2000	3000	500	1500	绿色

三种令牌桶模式的区别和应用

三种令牌桶模式之间的区别和相互关系如表4-4所示。

表 4-4 三种令牌桶模式之间的区别和相互关系

区别	单速单桶	单速双桶	双速双桶
参数	CIR和CBS	CIR、CBS和EBS	CIR、CBS、PIR和PBS
令牌投放方式	以CIR速率向C桶投放令牌。C桶满时令牌溢出。	C桶满时令牌投放到E桶。C桶和E桶都不满时，只向C桶投放令牌。	以CIR速率向C桶投放令牌，以PIR速率向P桶中投放令牌。两个桶相对独立。桶中令牌满时令牌溢出。
是否允许流量突发	不允许流量突发。报文的处理以C桶中是否有足够令牌为依据。	允许报文尺寸的突发。先使用C桶中的令牌，C桶中令牌数量不够时，使用E桶中的令牌。	允许报文速率的突发。C桶和P桶中的令牌足够时，两个桶中的令牌都使用。C桶中令牌不够时，只使用P桶中的令牌。
报文颜色标记结果	绿色或红色	绿色、黄色或红色	绿色、黄色或红色

区别	单速单桶	单速双桶	双速双桶
相互关系	单速双桶模式中，如果EBS等于0，其效果和单速单桶是一样的。 双速双桶模式中，如果PIR等于CIR，其效果和单速单桶是一样的。		

基于上述三种令牌桶模式之间的区别，其功能和选用场景也有所不同，见表4-5。

表 4-5 三种令牌桶模式的功能及选用场景

令牌桶模式	功能	选用场景
单速单桶	限制带宽	优先级较低的业务（如企业外网HTTP流量），对于超过额度的流量直接丢弃保证其他业务，不考虑突发。
单速双桶	限制带宽，还可以容许一部分流量突发，并且可以区分突发业务和正常业务	较为重要的业务，容许有突发的业务（如企业邮件数据），对于突发流量有宽容。
双速双桶	限制带宽，可以进行流量带宽划分，可以区别带宽小于CIR还是在CIR与PIR之间	重要业务，可以更好的监控流量的突发程度，对流量分析起到指导作用。

色敏模式

色敏模式下，如果到达的报文本身已经被标记为红、黄或者绿等颜色，令牌桶对流量的评估会参考报文已标记颜色，即报文本身已携带颜色会影响令牌桶的评估结果，评估机制简单的来说遵循以下原则：

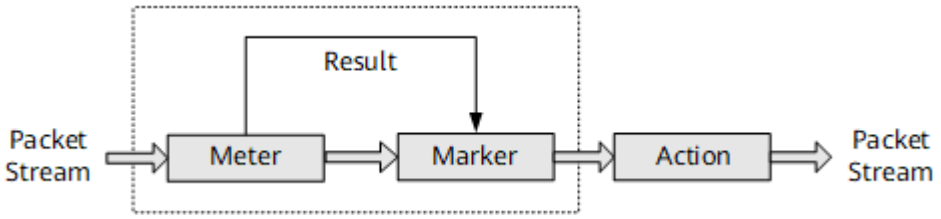
- 如果报文已被标记为绿色，则令牌桶的评估机制与色盲模式保持一致。
- 如果报文已被标记为黄色，则令牌桶根据报文长度和令牌数的大小，为符合流量规定的报文标记为黄色，为不符合的报文标记为红色，单速单桶模式下则直接标记为红色。
- 如果报文已被标记为红色，则令牌桶直接将到达报文标记为红色。

4.2.2 流量监管

流量监管可以对不同流量进行监督，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，从而保护网络资源和用户的利益。

流量监管的原理

图 4-4 流量监管组件



如图4-4所示，流量监管由三部分组成：

- Meter：通过令牌桶机制对网络流量进行度量，向Marker输出度量结果。
- Marker：根据Meter的度量结果对报文进行染色，报文会被染成green、yellow、red三种颜色。
- Action：根据Marker对报文的染色结果，对报文进行一些动作，动作包括：
  - pass：对测量结果为“符合”的报文继续转发。
  - remark + pass：对测量结果为“不符合”的报文修改其内部优先级后再转发。
  - discard：对测量结果为“不符合”的报文进行丢弃。

经过流量监管，如果某流量速率超过标准，超出标准部分的报文其测量结果为“不符合”，此时设备可以选择降低报文优先级再进行转发或者直接丢弃。缺省情况下，green、yellow进行转发，red报文丢弃。

4.2.3 流量整形

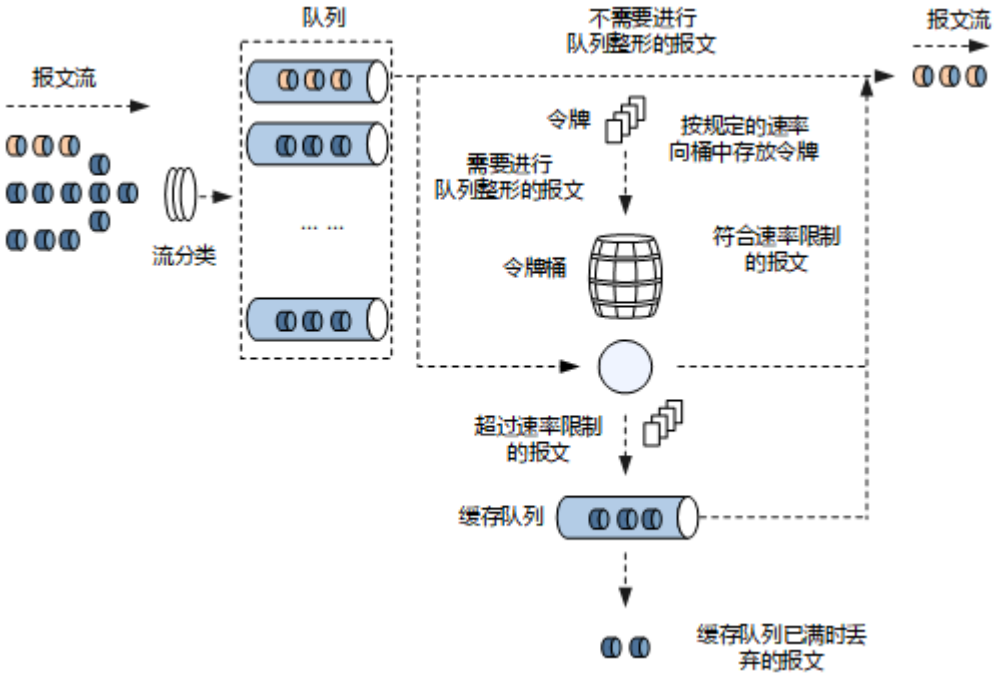
流量整形是一种主动调整流量输出速率的措施，其作用是限制流量与突发，使这类报文以比较均匀的速率向外发送。流量整形通常使用缓冲区和令牌桶来完成，当报文的发送速度过快时，首先在缓冲区进行缓存，在令牌桶的控制下，再均匀地发送这些被缓冲的报文。

处理流程

流量整形是一种队列的流量控制技术，可以对从接口上经过的某类报文进行速率限制。

下面以采用单速单桶技术的基于流的队列整形为例介绍流量整形的处理流程，其处理流程如图4-5所示。

图 4-5 流量整形处理流程图



具体处理流程如下：

1. 当报文到来的时候，首先对报文进行分类，使报文进入不同的队列。
2. 若报文进入的队列没有配置队列整形功能，则直接发送该队列的报文；否则，进入下一步处理。
3. 按用户设定的队列整形速率向令牌桶中放置令牌：
   - 如果令牌桶中有足够的令牌可以用来发送报文，则报文直接被发送，在报文被发送的同时，令牌做相应的减少。
   - 如果令牌桶中没有足够的令牌，则将报文放入缓存队列，如果报文放入缓存队列时，缓存队列已满，则丢弃报文。
4. 缓存队列中有报文的时候，会与令牌桶中的令牌数作比较，如果令牌数足够发送报文则转发报文，直到缓存队列中的报文全部发送完毕为止。

4.2.4 接口限速

接口限速可以限制一个接口上发送或者接收报文的总速率。

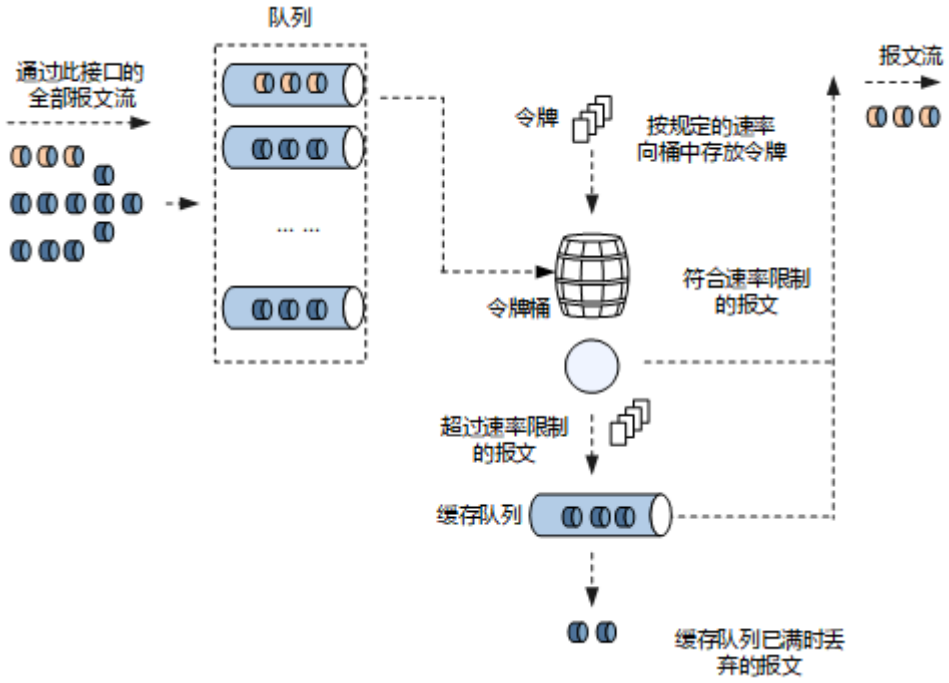
接口限速也是采用令牌桶进行流量控制。如果在设备的某个接口配置了接口限速，所有经由该接口发送的报文首先要经过接口限速的令牌桶进行处理。如果令牌桶中有足够的令牌，则报文可以发送；否则，报文将被丢弃或者被缓存。这样，就可以对通过该接口的报文流量进行控制。

接口限速支持出/入两个方向，下面以出方向为例介绍接口限速的处理过程。

处理流程

下面以接口下采用单速单桶技术为例介绍出方向接口限速的处理流程，其处理流程如图4-6所示。

图 4-6 接口限速处理流程图



具体处理流程如下：

1. 如果令牌桶中有足够的令牌可以用来发送报文，则报文直接被发送，在报文被发送的同时，令牌做相应的减少。
2. 如果令牌桶中没有足够的令牌，则将报文放入缓存队列，如果报文放入缓存队列时，缓存队列已满，则丢弃报文。
3. 缓存队列中有报文的时候，会与令牌桶中的令牌数作比较，如果令牌数足够发送报文则转发报文，直到缓存队列中的报文全部发送完毕为止。

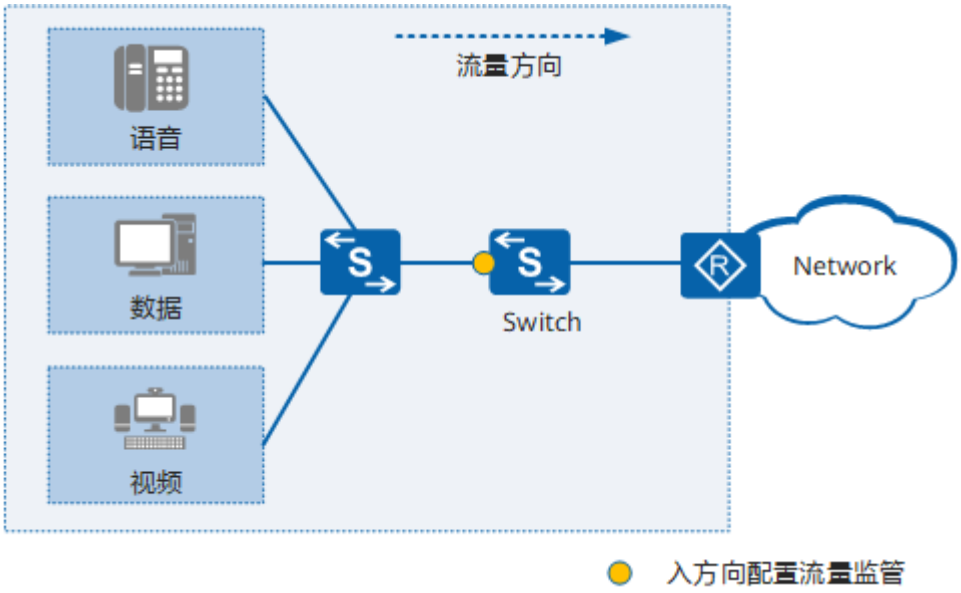
4.3 流量监管、流量整形和接口限速应用场景

流量监管的应用

组网需求

网络中存在语音、视频和数据等多种不同的业务，当大量的业务流量进入网络侧时，可能会因为带宽不足产生拥塞，需要对三种业务提供不同的带宽，优先保证语音业务报文的转发，其次是视频业务，最后是数据业务。因此可以对不同业务进行不同的流量监督，为语音报文提供最大带宽，视频报文次之，数据报文带宽最小，从而在网络产生拥塞时，可以保证语音报文优先通过。如图4-7所示。

图 4-7 流量监管应用组网图



业务部署

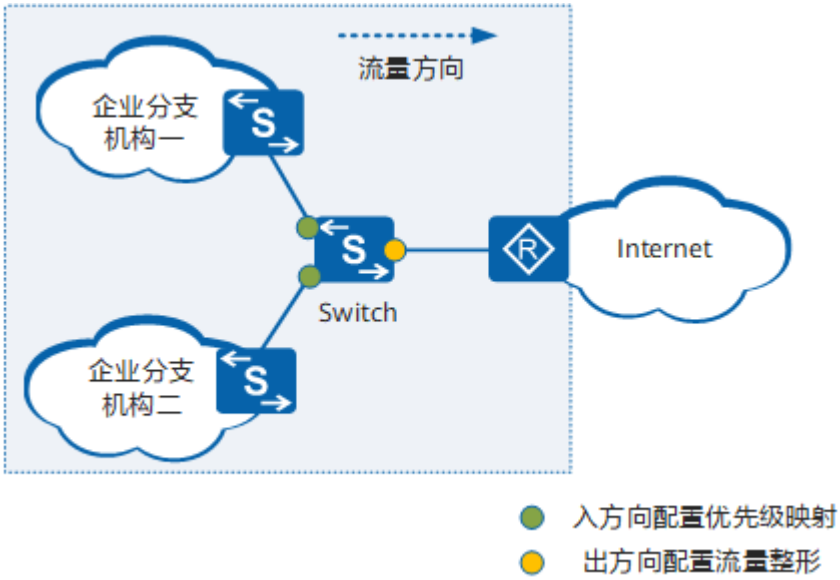
- 配置流分类将语音，视频和数据报文进行分类。
- 为语音，视频和数据报文分别配置流行为，实现不同速率的流量监管。
- 将对应的流分类和流行为进行绑定，并应用在Switch的入方向。

流量整形的应用

组网需求

网络中受带宽限制，访问网络的流量会因为被限制而丢弃，为了防止流量被丢弃可以在上游设备的出方向进行流量整形，缓存超出限制的流量，不同的企业分支可以配置不同速率的流量整形，如图4-8所示。

图 4-8 流量整形应用组网图



业务部署

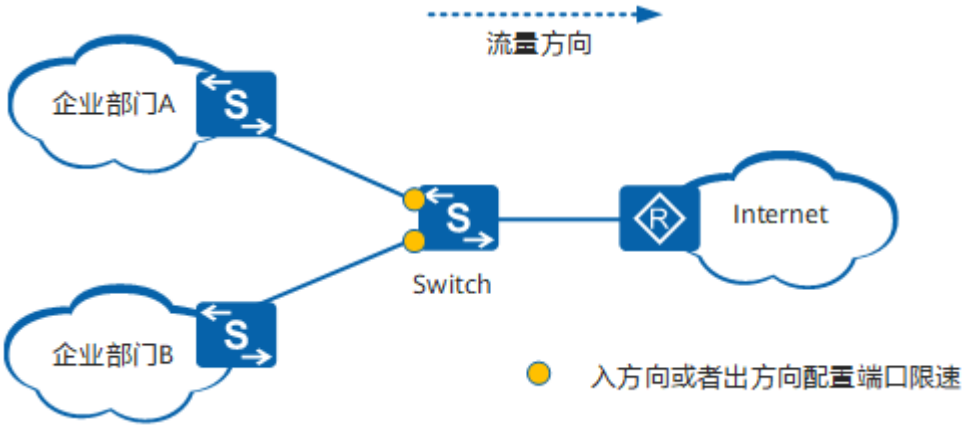
- Switch与企业分支相连的接口入方向配置优先级映射，将来自不同企业分支的流量映射到不同的本地优先级，从而进入不同的队列。
- Switch与出口网关相连的接口出方向配置流量整形，对不同企业分支的流量按照不同的速率实现流量整形。

接口限速的应用

组网需求

某交换机接入了两个不同的部门，要求每个部门的流量不能超过规定速率，因此可以在接入交换机的入接口上配置接口限速，将部门用户的流量均限制在规定范围内，超出的流量将被丢弃。如图4-9所示。

图 4-9 接口限速应用组网图



业务部署

Switch与接入交换机相连的接口分别配置接口限速，保证流量在规定速率内。

4.4 流量监管、流量整形和接口限速配置注意事项

涉及网元

无需其他网元配合。

License 支持

流量监管、流量整形和接口限速是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持流量监管、流量整形和接口限速。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

- 针对不同VLAN进行限速主要通过匹配不同的VLAN ID来实现，而当在VLAN下应用某个流策略时，则会对加入该VLAN的所有接口均生效。
- 对设备配置限速之后，可能会导致下游设备上网速率慢或者丢包等问题，因此要合理设置当前设备的限速流量值。
- 流量监管、流量整形和接口限速对数据报文和本机发送的协议报文生效，对上送到本机CPU处理的协议报文不生效。
- VLAN下的流量抑制功能、入方向的接口限速功能、基于MQC的流量监管功能和基于ACL的traffic-limit功能共用设备的CAR资源，当CAR资源不足时可能会导致上述某功能配置失败。CAR资源的使用情况可以通过命令**display acl resource** [**slot** *slot-id*]查看。
- 入方向的流量统计功能在接口限速功能之前生效，即通过流量统计无法判断接口限速是否已经生效。可以通过执行命令**display qos car statistics interface** *interface-type interface-number* **inbound**查看限速后的统计信息。
- 当设备在同一个流策略的不同流行为中分别配置了流量监管和其他流动作，且分别匹配的流分类优先级不一致，当报文同时匹配多个流分类规则时只有优先级高的流分类所对应的动作生效，则此时可能会导致流量监管限速失败。
- 使用流策略进行限速并将流策略应用在VLAN视图下时：
  - 如果加入VLAN的接口在同一单板上，则该单板上的接口共享限速值。
  - 如果加入VLAN的接口在不同单板上，则各单板上的接口独享限速值。
- 交换机支持在Eth-Trunk下配置接口限速功能（使用命令**qos car**），配置后：
  - 如果各成员接口在不同的单板，则各单板独享限速值。
  - 如果各成员接口在同一单板上，则各接口共享限速值，共享的带宽的分担方式是随机的。

- 如果在物理接口下配置流量监管、流量整形或者接口限速，那么该物理接口的子接口的流量速率将受到影响，与物理接口共享限速值。

4.5 流量监管、流量整形和接口限速缺省配置

流量监管的缺省配值如表4-6所示，流量整形的缺省配值如表4-7所示，接口限速的缺省配置如表4-8所示。

表 4-6 流量监管的缺省配值

参数	缺省值
流量监管	未进行流量监管

表 4-7 流量整形的缺省配值

参数	缺省值
流量整形	未进行流量整形

表 4-8 接口限速的缺省配值

参数	缺省值
业务接口的流量限速	未对接口进行流量限速
管理网口的流量限速	1000

4.6 配置流量监管

前置任务

配置MQC实现流量监管可以对匹配规则的报文分别进行限速。如果不仅需要对匹配规则的报文分别限速还需要对整体的流量进行限制，可以在配置MQC实现流量监管的基础上再配置层次化流量监管。

在配置流量监管之前，需要完成以下任务：

- 配置相关接口的链路层属性，保证接口的正常工作。

4.6.1 配置 MQC 实现流量监管

背景信息

若需要对接口出方向或入方向某类流量进行控制时，可以配置MQC实现流量监管。基于MQC的流量监管，可以通过流分类为不同业务提供更细致的差分服务。当匹配流分类规则的报文的接收或发送速率超过限制速率时，直接被丢弃。

操作步骤

1. 配置流分类

   a. 执行命令**system-view**，进入系统视图。

   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，创建一个流分类并进入流分类视图，或进入已存在的流分类视图。

   and表示流分类中各规则之间关系为逻辑“与”，指定该逻辑关系后：

   - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；
   - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

   or表示流分类各规则之间是逻辑“或”，即报文只需匹配流分类中的一个或多个规则即属于该类。

   缺省情况下，流分类中各规则之间的关系为逻辑“或”。

   c. 请根据实际情况定义流分类中的匹配规则。

   说明

   if-match ip-precedence和**if-match tcp**命令仅对IPv4报文生效。

   X系列单板不支持配置包含高级ACL中的**ttl-expired**字段的流分类规则。

   当流分类匹配**if-match ipv6 acl** { *acl-number* | *acl-name* }时，X系列单板不支持**add-tag vlan-id** *vlan-id*、**remark 8021p** [*8021p-value* | **inner-8021p**]、**remark cvlan-id** *cvlan-id*、**remark vlan-id** *vlan-id*、**mac-address learning disable**。

匹配规则	命令	说明
外层VLAN ID或基于QinQ报文内外两层Tag的VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]	-
QinQ报文内外层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**vlan-id** *vlan-id*]	-
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个802.1p值，报文只需匹配其中一个802.1p值就匹配该规则。
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>	-
丢弃报文	**if-match discard**	包含该流分类的报文只能与流量统计和流镜像两种动作绑定。

匹配规则	命令	说明
QinQ报文双层Tag	**if-match double-tag**	-
MPLS报文EXP优先级	**if-match mpls-exp** *exp-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个MPLS EXP值，报文只需匹配其中一个MPLS EXP值就属于该类。
目的MAC地址	**if-match destination-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
源MAC地址	**if-match source-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }	-
所有报文	**if-match any**	-
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个DSCP值，报文只需匹配其中一个DSCP值就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
IP报文的IP优先级	**if-match ip-precedence** *ip-precedence-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个IP优先级，报文只需匹配其中一个IP优先级就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }	-

匹配规则	命令	说明
IPv6下一报文头类型	**if-match ipv6 next-header** *header-number* **first-next-header**	ET1D2X12SSA0单板不支持Prefix的长度为(64,128)之间的路由。
TCP报文SYN Flag	**if-match tcp syn-flag** { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	-
入接口	**if-match inbound-interface** *interface-type interface-number*	包含该流分类的流策略不能应用在出方向。 包含该流分类的流策略不能应用在接口视图。
出接口	**if-match outbound-interface** *interface-type interface-number*	X系列单板不支持将包含该流分类的流策略应用在入方向。 包含该流分类的流策略不能应用在接口视图。
ACL规则	**if-match acl** { *acl-number* | *acl-name* }	• 使用ACL作为流分类规则，请先配置相应的ACL规则。 • 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果某ACL规则中有多个rule，报文只需匹配其中一个rule就匹配该ACL规则。 • 如果ACL的规则指定了参数**vpn-instance**，那么基于该ACL进行分类的流分类对应的流策略将不生效。
ACL6规则	**if-match ipv6 acl** { *acl-number* | *acl-name* }	使用ACL6作为流分类规则，请先配置相应的ACL6规则。 如果ACL6的规则指定了参数**vpn-instance**，那么基于该ACL6进行分类的流分类对应的流策略将不生效。
流ID	**if-match flow-id** *flow-id*	包含**if-match flow-id**匹配规则的流分类和包含**remark flow-id**动作的流行为应在不同的流策略中使用。 包含**if-match flow-id**匹配规则的流策略只能应用在接口、VLAN、VLANIF接口、单板、全局的入方向。 SA系列单板不支持配置匹配流ID。

匹配规则	命令	说明
VXLAN内层报文信息	**if-match vxlan** [**transit**] **vni** *vni-id*	包含该流分类的流策略不能应用在出方向上。 当流分类中包含此匹配规则时，流行为只支持流量监管、报文过滤和流量统计。

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

a. 执行命令**traffic behavior** *behavior-name*，创建一个流行为并进入流行为视图，或进入已存在的流行为视图。

b. 执行命令**car cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**coupling-flag** *flag-value*] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**service-class** *class* **color** *color*] } | **yellow** { **discard** | **pass** [**service-class** *class* **color** *color*] } | **red** { **discard** | **pass** [**service-class** *class* **color** *color*] }]*，配置CAR动作。

c. （可选）执行命令**statistic enable**，使能流量统计功能。

d. 执行命令**quit**，退出流行为视图。

e. （可选）执行命令**qos-car exclude-interframe**，全局使能计算流量监管的速率时不包括报文的帧间隙和前导码字段功能。

说明

使能此功能后，设备在计算流量监管和入方向接口限速的速率时均不包括报文的帧间隙和前导码字段。

f. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name* [**match-order** { **auto** | **config** }]，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。创建流策略时，如果未指定规则匹配顺序，缺省规则匹配顺序为**config**。

应用流策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先清除该策略的应用，再重新创建并指定所需的匹配顺序。

设备支持在创建流策略时指定流策略中多个规则的匹配顺序，匹配顺序包括自动顺序（**auto**）和配置顺序（**config**）两种：

- 如果选择自动顺序，匹配顺序由系统预先指定的流分类类型的优先级决定，该优先级由高到低依次为：基于二层和IPv4三层信息流分类 > 基于高级ACL6规则流分类 > 基于基本ACL6规则流分类 > 基于二层信息流分类 > 基于IPv4三层信息流分类 > 基于用户自定义ACL规则流分类。规则优先匹配优先级高的流分类。当某一数据流量同时匹配不同流分类，且对应的流行为存在冲突时，只有流行为优先级高的规则生效。

- 如果选择配置顺序，匹配顺序由流分类规则的优先级决定，先匹配优先级较高的流分类规则。配置流分类时指定优先级，则数值越小，优先级越高；如果配置流分类时未指定precedence-value，则缺省优先级为0。关于流分类优先级的详细说明，请参见**traffic classifier**。

c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

- 在接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface** *interface-type interface-number*[.*subinterface-number*]，进入接口视图或子接口视图。

说明

- 仅E系列、X系列和S系列中的SC单板支持配置以太网子接口。单板详情请参见《硬件描述》中的单板分类。
- 对于上述系列单板的二层接口，仅hybrid和trunk类型接口支持配置二层以太网子接口。
- 对于上述系列单板的二层接口，执行命令**undo portswitch**切换为三层接口后，支持配置三层以太网子接口。
- S系列中的SA单板不支持创建以太网子接口，也不支持转发IP流量到其它单板的以太网子接口。
- 建议用户先将成员接口加入Eth-Trunk后，再配置Eth-Trunk子接口。只有当成员接口所在的单板系列均支持配置以太网子接口时，Eth-Trunk子接口才能配置成功。
- VCMP的角色是Client时，不能配置VLAN终结子接口。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口或子接口视图上应用流策略。

每个接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同接口的不同方向。应用后，系统对流经该接口并匹配流分类中规则的入方向或出方向报文实施策略控制。

说明

- 子接口仅支持**inbound**参数。
- 建议不要在Untagged类型接口出方向上应用包含有**remark 8021p**、**remark cvlan-id**、**remark vlan-id**等动作的流策略，否则，可能导致报文内容出错。
- ET1D2X12SSA0、ET1D2X48SEC0、SC系列单板有2N个接口，如果1～N号中的接口与N+1～2N号中的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的2倍。
- 在X系列单板中，如果不同的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，且这些接口的ACL资源分散在N个组中进行统计（执行命令**display acl resource**查看），那么Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的N倍。
- 应用流策略需要设备有足够的ACL资源，否则会导致应用失败。以一个流策略中的if-match占用一条ACL为例，同一个流策略应用到M个接口时，将占用M条ACL资源；应用到L个VLAN且设备上存在N块接口板时，将占用L*N条ACL规则；应用到全局且设备上存在N块接口板时，将占用N条ACL规则。if-match规则占用ACL资源的情况参考“MQC配置-配置注意事项”中的表3。
- 配置Tunnel接口的隧道协议为GRE后，可在Tunnel接口入方向应用流策略。
- 在VXLAN二层子接口、Dot1q终结子接口和绑定了BGP AD方式的子接口下，应用流策略不生效，建议在主接口配置基于流ID的分类方式。

- 在VLAN上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**vlan** *vlan-id*，进入VLAN视图。
  iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLAN上应用流策略。

  每个VLAN的每个方向能且只能应用一个流策略。

  应用后，系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施策略控制。但是流策略对VLAN 0的报文不生效。
- 在VLANIF接口上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。
  iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLANIF接口上应用流策略。

  每个VLANIF接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同VLANIF接口的不同方向。

  对于应用流策略的VLANIF接口，其对应的VLAN不能是Super-VLAN或MUX VLAN。

  对于X系列单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文生效。对于其它单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文及三层组播报文生效。

  说明

  如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的入方向上应用该流策略：
  - **remark vlan-id**
  - **remark cvlan-id**
  - **add-tag vlan-id**
  - **remark 8021p**
  - **remark flow-id**
  - **mac-address learning disable**

  如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的出方向上应用该流策略：
  - **add-tag vlan-id**
  - **remark flow-id**
  - **mac-address learning disable**
- 在全局或单板上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**traffic-policy** *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]，在全局或单板上应用流策略。

  全局或单板的每个方向上能且只能应用一个流策略，如果在全局某方向应用了流策略，则不能在单板的该方向上再次应用流策略；指定单板在某方向应用流策略后，也不能在全局的该方向上再次应用流策略。
- 在SSID模板上应用流策略
  i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**wlan**，进入WLAN视图。

iii. 执行命令**ssid-profile name** *profile-name*，创建SSID模板并进入模板视图。

iv. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在SSID模板上应用流策略。

- 在AP组上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**wlan**，进入WLAN视图。

iii. 执行命令**ap-group name** *group-name*，创建AP组并进入AP组视图。

iv. 执行命令**traffic-policy** *policy-name* **outbound**，在AP组上应用流策略。

检查配置结果

说明

在配置**car**命令的同一流行为中配置流量统计后，通过**display traffic policy statistics**命令可以查看限速效果，从而确认流量监管是否生效。

需要注意的是，接口入方向的报文统计（可通过命令**display interface**或**display this interface**查看统计计数）在应用在接口入方向的流量监管前执行。因此，接口入方向的报文统计计数是否大于限速值不能作为衡量配置是否生效的标准。

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior user-defined** [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看用户定义的流策略的配置信息。
- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

  说明

  流策略可以应用到子接口上，但暂不支持通过此命令查看子接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

- 执行命令**display traffic policy** { **interface** [*interface-type interface-number*[*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]，查看已配置的流策略信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

4.6.2 配置层次化流量监管

前提条件

对需要配置层次化流量监管的业务流配置MQC实现流量监管。配置MQC实现流量监管的具体步骤，请参见**4.6.1 配置MQC实现流量监管**。

背景信息

设备支持层次化流量监管，即系统对满足流分类规则的业务流通过MQC实现流量监管（一级CAR）后，可以将同一流策略中满足一级CAR的流分类的所有业务流聚合在一起再做一次流量监管（二级CAR）。层次化流量监管可以实现用户流量的统计复用和精细业务的控制。

操作步骤

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**qos car** *car-name* **cir** *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]，创建并配置CAR模板。
3. 执行命令**traffic behavior** *behavior-name*，进入流行为视图。
4. 执行命令**car** *car-name* **share**，配置共享CAR动作。

   配置共享CAR动作前，需要在该流行为视图中配置CAR动作。由于已经**配置MQC实现流量监管**，所以该流行为中已经配置CAR动作，此处不再介绍相关配置。

   说明

   - ET1D2X48SEC0、SA系列、SC系列单板不支持配置共享CAR。
   - 包含共享CAR动作的流策略只能应用在inbound方向，不能应用在outbound方向。
   - 配置共享CAR后，绑定同一流行为的分类器的规则共用一个CAR索引，系统将这些流聚合在一起做CAR。如果这些流分类中既有基于二层信息的流分类又有基于三层信息的流分类，那么car share配置将不会生效。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior user-defined** [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看用户定义的流策略的配置信息。
- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

  说明

  流策略可以应用到子接口上，但暂不支持通过此命令查看子接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。
- 执行命令**display traffic policy** { **interface** [*interface-type interface-number*[*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]，查看已配置的流策略信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

4.7 配置流量整形

前置任务

与流量监管直接将超出承诺速率的报文丢弃不同，流量整形可以对超出速率的报文进行缓存以达到均匀向外发送报文流量的目的。

在配置流量整形之前，需要完成以下任务：

- 配置相关接口的链路层属性，保证接口的正常工作。

4.7.1 配置队列流量整形

背景信息

接口收到的报文根据优先级映射进入不同的队列，针对不同的优先级队列设置不同的流量整形参数，可以实现对不同业务的差分服务。

配置端口队列整形前，需要配置优先级映射，将报文的优先级映射为PHB行为，从而使不同业务进入不同的端口队列。优先级映射的配置请参见**配置优先级映射**。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**qos-shaping exclude-interframe**，配置计算流量整形的速率时不包括报文的帧间隙和前导码。

缺省情况下，计算流量整形的速率时，包括帧间隙和前导码。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**qos queue** *queue-index* **shaping cir** *cir-value* **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]，配置队列流量整形速率。建议配置CBS的值为CIR的120倍。

缺省情况下，队列的整形速率是接口的最大带宽。

如果同一接口下既配置队列流量整形，又配置出方向接口限速（使用命令**qos lr**），则出方向接口限速的CIR必须大于等于队列整形的CIR之和；否则，流量整形会出现异常现象，如低优先级队列抢占高优先级队列的带宽等。

----结束

4.7.2 （可选）配置数据缓冲区

背景信息

数据缓冲区可以用来缓存从接口发送的报文，防止出现由于突发流量导致拥塞而产生的丢包现象。当设备的缓冲区资源被耗尽时，接口将不能再缓存报文，未进入缓冲区的报文将直接被丢弃，因此配置数据缓冲区可以调整端口队列的缓存能力，提高设备性能。

说明

配置缓存管理的突发模式为增强模式时，**qos burst-mode（接口视图）**命令与**qos burst-mode（系统视图）**命令不能同时配置；且上述两条命令均不能与**qos queue length**命令同时配置。

操作步骤

- 配置指定接口缓存管理的突发模式。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**qos burst-mode** { **enhanced** | **extreme** }，配置接口缓存管理的突发模式。配置突发模式为极限模式，可能会影响到其它接口的正常转发功能，因此建议配置接口管理的突发模式为增强模式。

     说明

     X1E系列单板、X5E系列单板、X5EK系列单板、X5H系列单板、X5S系列单板、X6H系列单板不支持此命令。

     在业务口集群模式下，集群端口仅支持指定参数**enhanced**。
- 配置单板缓存管理的突发模式。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**qos burst-mode** { **enhanced** | **extreme** } **slot** *slot-id*，配置单板缓存管理的突发模式。配置突发模式为极限模式，可能会影响到其它接口的正常转发功能，因此建议配置接口管理的突发模式为增强模式。

     说明

     X1E系列单板、X5E系列单板、X5EK系列单板、X5H系列单板、X5S系列单板、X6H系列单板不支持此命令。
- 配置端口队列的缓存大小。
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**shutdown**，关闭接口。
  d. 执行命令**qos queue** *queue-index* **length** *length-value*，配置端口队列的缓存大小。

     说明

     ET1D2L02QSC0、ET1D2L08QSC0、ET1D2X48SEC0、ET1D2C02FEE0、SC系列和X系列单板不支持此命令。
  e. 执行命令**undo shutdown**，重启接口。

----结束

4.7.3 检查流量整形配置结果

操作步骤

- 执行命令**display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]，查看端口队列的统计信息。

说明

SA系列单板不支持**display qos queue statistics**命令。

----结束

4.8 配置接口限速

前置任务

流量限速实现对通过整个端口的全部报文流量速率的限制，以保证接口的带宽不超过规定大小。入方向与出方向的接口限速属于并列关系，用户可以根据需要同时配置，也可以单独配置。

在配置接口限速之前，需要完成以下任务：

- 配置相关接口的链路层属性，保证接口的正常工作。

4.8.1 配置入方向的接口限速

背景信息

如果不限制用户发送的流量，大量用户不断突发的数据会使网络更拥挤。通过配置入方向的接口限速，可以将通过某个接口进入网络的流量限制在一个合理的范围内。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**qos-car exclude-interframe**，全局使能计算入方向接口限速的速率时不包括报文的帧间隙和前导码字段功能。

缺省情况下，计算入方向接口限速的速率时，包括报文的帧间隙和前导码字段。

步骤3 执行命令**qos car** *car-name* **cir** *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]，创建并配置CAR模板。

步骤4 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤5 执行命令**qos car inbound** *car-name*，在接口应用CAR模板。

接口上应用CAR模板后，设备对流入该接口的所有业务流量实施限速。

如果在某VLAN上应用了QoS CAR模板（请参见**broadcast-suppression（VLAN视图）**、**multicast-suppression（VLAN视图）**和**unicast-suppression（VLAN视图）**命令），以监管入方向上的广播流量、组播流量或未知单播流量，同时又在允许该VLAN帧进入的接口上应用了QoS CAR模板，流量抑制和端口限速按照先后顺序在X系列单板依次生效，而其他单板则仅接口上配置的QoS CAR参数生效。

----结束

配置小窍门

删除入方向接口限速配置

取消名称为qoscar1的CAR模板在接口GE1/0/1下的应用，并将该模板删除。

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo qos car inbound
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] undo qos car qoscar1
```

确认入方向接口限速是否生效

通过**display qos car statistics**可以查看限速效果，从而确认入方向接口限速是否生效。

需要注意的是，接口入方向的报文统计（可通过命令**display interface**或**display this interface**查看统计计数）在入方向接口限速前执行。因此，接口入方向的报文统计计数是否大于限速值不能作为衡量配置是否生效的标准。

4.8.2 配置出方向的接口限速

背景信息

若需要对接口出方向所有流量进行控制时，可以配置出方向的接口限速。当报文的发送速率超过限制速率时，超出的那部分报文先进入缓存队列；当令牌桶有足够的令牌时，再均匀向外发送这些被缓存的报文；当缓存队列已满时，新到达的报文将被丢弃。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 （可选）执行命令**qos-shaping exclude-interframe**，全局使能计算出方向接口限速的速率时不包括报文的帧间隙和前导码字段功能。

缺省情况下，计算出方向接口限速的速率时，包括报文的帧间隙和前导码字段功能。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**qos lr cir** *cir-value* [**cbs** *cbs-value*] [**outbound**]，配置出方向的接口限速。

缺省情况下，接口限速速率为接口的最大带宽。

说明

- 在MPLS TE隧道中，如果已经配置了MPLS TE最大链路带宽和最大可预留带宽，则要求**qos lr**配置的接口限速速率必须大于已经配置的MPLS TE最大可预留带宽。
- 如果该接口上同时配置队列流量整形，则接口限速的CIR必须大于等于队列流量整形的CIR之和；否则，流量整形会出现异常现象，如低优先级队列抢占高优先级队列的带宽。
- X1E系列单板不支持**cbs** *cbs-value*。

----结束

配置小窍门

删除出方向接口限速配置

在接口视图下执行命令**undo qos lr** [**outbound**]，删除该接口的限速配置。

4.8.3 配置管理网口的流量限速

背景信息

当设备的管理网口由于恶意攻击、网络异常等原因导致流量过大时，会导致CPU占用率过高，进而影响系统正常运行，因此需要对管理网口的流量进行限制。通过在管理网口上配置流量监管，限制由管理网口进入设备的流量速率，以保证系统正常运行。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface ethernet 0/0/0**，进入管理网口视图。

步骤3 执行命令**qos lr pps** *packets*，配置管理网口的流量限速。

说明

管理网口的流量限速值不宜设置过小，否则可能会影响正常的FTP、Telnet、SFTP、STelnet和SSH等功能。

----结束

4.8.4 检查接口限速配置结果

操作步骤

- 执行命令**display qos car** { **all** | **name** *car-name* }，查看CAR模板的配置信息。
- 执行命令**display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]，查看端口队列的统计信息。

说明

SA系列单板不支持**display qos queue statistics**命令。

----结束

4.9 维护流量监管、流量整形和接口限速

4.9.1 查看流量统计信息

背景信息

查看基于MQC配置的流量统计信息时，策略必须存在且已经包含流量统计动作。

操作步骤

- 执行命令**display traffic policy statistics** { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]，查看基于MQC配置的流量统计信息。
- 执行命令**display qos car statistics interface** *interface-type interface-number* **inbound**，查看配置入方向接口限速后指定接口上通过和丢弃的报文统计信息。
- 执行命令**display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]，查看接口上基于队列的流量统计信息。

说明

SA系列单板不支持**display qos queue statistics**命令。

----结束

4.9.2 清除流量统计信息

背景信息

须知

清除基于流的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- 执行命令**reset qos queue statistics interface** *interface-type interface-number*，清除接口上基于队列的流量统计信息。

  说明

  SA系列单板不支持**reset qos queue statistics**命令。
- 执行命令**reset qos car statistics interface** *interface-type interface-number* **inbound**，清除配置入方向接口限速后指定接口上通过和丢弃的报文统计信息。

----结束

4.10 流量监管、流量整形和接口限速配置举例

4.10.1 配置 MQC 实现流量监管示例

组网需求

Switch通过接口GE2/0/1与路由器互连，企业可经由Switch和路由器访问网络，如图4-10所示。

语音业务对应的VLAN ID为120，视频业务对应的VLAN ID为110，数据业务对应的VLAN ID为100。

在Switch上需要对不同业务的报文分别进行流量监管，以将流量限制在一个合理的范围之内，并保证各业务的带宽需求。

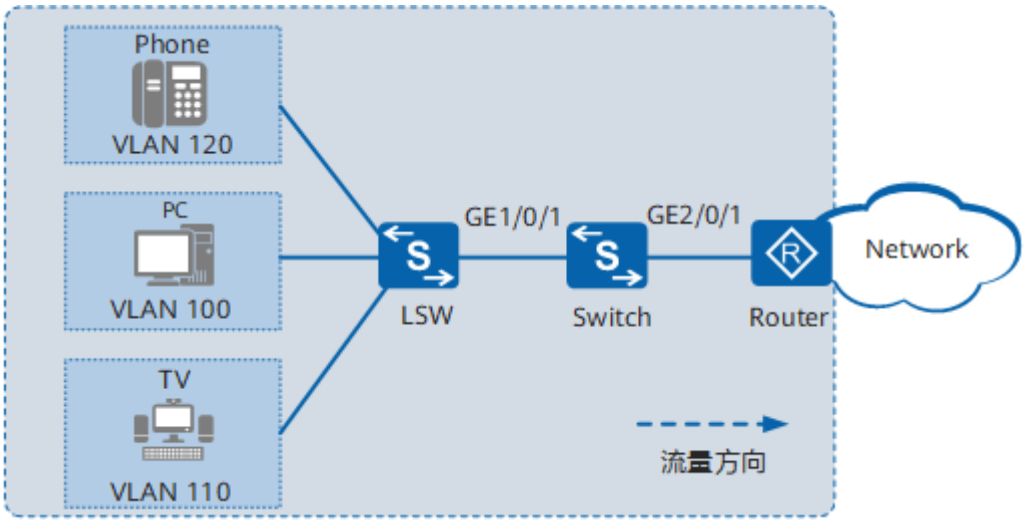
不同业务对于服务质量的需求不同，语音业务对服务质量要求最高，视频业务次之，数据业务要求最低，所以在Switch中还需要重标记不同业务报文的DSCP优先级，以便于路由器按照报文的不同优先级分别进行处理，保证各种业务的服务质量。

具体配置需求如表4-9所示。

表 4-9 Switch 为上行流量提供的 QoS 保障

流量类型	CIR(kbps)	PIR(kbps)	DSCP优先级
语音	2000	10000	46
视频	4000	10000	30
数据	4000	10000	14

图 4-10 流量监管配置组网图



配置思路

采用如下的思路配置MQC实现流量监管：

1. 创建VLAN，并配置各接口，使企业能够通过Switch访问网络。
2. 在Switch上配置基于VLAN ID进行流分类的匹配规则。
3. 在Switch上配置流行为，对报文进行流量监管并且重标记报文的DSCP优先级。
4. 在Switch上配置流量监管策略，绑定已配置的流行为和流分类，并应用到Switch与LSW连接的接口上。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN 100、110、120。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 110 120
```

将接口GE1/0/1、GE2/0/1的接入类型分别配置为trunk，并分别将接口GE1/0/1和GE2/0/1加入VLAN 100、VLAN 110、VLAN 120。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet2/0/1] quit
```

步骤2 配置流分类

在Switch上创建流分类c1～c3，对不同业务流按照其VLAN ID进行分类。

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match vlan-id 120
[Switch-classifier-c1] quit
[Switch] traffic classifier c2 operator and
[Switch-classifier-c2] if-match vlan-id 110
[Switch-classifier-c2] quit
[Switch] traffic classifier c3 operator and
[Switch-classifier-c3] if-match vlan-id 100
[Switch-classifier-c3] quit
```

步骤3 配置流量监管行为

在Switch上创建流行为b1～b3，对不同业务流进行流量监管以及重标记优先级。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] car cir 2000 pir 10000 green pass
[Switch-behavior-b1] remark dscp 46
[Switch-behavior-b1] statistic enable
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] car cir 4000 pir 10000 green pass
[Switch-behavior-b2] remark dscp 30
[Switch-behavior-b2] statistic enable
[Switch-behavior-b2] quit
[Switch] traffic behavior b3
[Switch-behavior-b3] car cir 4000 pir 10000 green pass
[Switch-behavior-b3] remark dscp 14
[Switch-behavior-b3] statistic enable
[Switch-behavior-b3] quit
```

步骤4 配置流量监管策略并应用到接口上

在Switch上创建流策略p1，将流分类和对应的流行为进行绑定并将流策略应用到接口GE1/0/1入方向上，对报文进行流量监管和重标记。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] classifier c3 behavior b3
[Switch-trafficpolicy-p1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet1/0/1] quit
```

步骤5 验证配置结果

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
 User Defined Classifier Information:
  Classifier: c2
   Precedence: 10
   Operator: AND
   Rule(s) : if-match vlan-id 110

  Classifier: c3
   Precedence: 15
   Operator: AND
```



```
  Rule(s) : if-match vlan-id 100

 Classifier: c1
  Precedence: 5
  Operator: AND
  Rule(s) : if-match vlan-id 120

Total classifier number is 3
```

查看流策略的配置信息，以流策略p1为例。

```
[Switch] display traffic policy user-defined p1
 User Defined Traffic Policy Information:
 Policy: p1
  Classifier: c1
   Operator: AND
    Behavior: b1
     Permit
     Committed Access Rate:
       CIR 2000 (Kbps), PIR 10000 (Kbps), CBS 250000 (byte), PBS 1250000 (byte)
       Color Mode: color Blind
       Conform Action: pass
       Yellow  Action: pass
       Exceed  Action: discard
     Remark:
       Remark DSCP ef
     Statistic: enable
  Classifier: c2
   Operator: AND
    Behavior: b2
     Permit
     Committed Access Rate:
       CIR 4000 (Kbps), PIR 10000 (Kbps), CBS 500000 (byte), PBS 1250000 (byte)
       Color Mode: color Blind
       Conform Action: pass
       Yellow  Action: pass
       Exceed  Action: discard
      Remark:
       Remark DSCP af33
     Statistic: enable
  Classifier: c3
   Operator: AND
    Behavior: b3
     Permit
     Committed Access Rate:
       CIR 4000 (Kbps), PIR 10000 (Kbps), CBS 500000 (byte), PBS 1250000 (byte)
       Color Mode: color Blind
       Conform Action: pass
       Yellow  Action: pass
       Exceed  Action: discard
     Remark:
       Remark DSCP af13
     Statistic: enable
```

查看在接口上应用的流策略信息，以接口GE1/0/1为例。

```
[Switch] display traffic policy statistics interface gigabitethernet 1/0/1 inbound

 Interface:  GigabitEthernet1/0/1
 Traffic policy inbound: p1
 Rule number: 3
 Current status: success
 Statistics interval: 300
-------------------------------------------------------------------------
 Board : 1
-------------------------------------------------------------------------
 Matched         |     Packets:                      0
                 |     Bytes:                      -
                 |     Rate(pps):                  0
                 |     Rate(bps):                  -
```

```
-----------------------------------------------------------------------
  Passed          |      Packets:                          0
                  |      Bytes:                          -
                  |      Rate(pps):                        0
                  |      Rate(bps):                        -
-----------------------------------------------------------------------
  Dropped         |      Packets:                          0
                  |      Bytes:                          -
                  |      Rate(pps):                        0
                  |      Rate(bps):                        -
-----------------------------------------------------------------------
    Filter        |      Packets:                          0
                  |      Bytes:                          -
-----------------------------------------------------------------------
    Car           |      Packets:                          0
                  |      Bytes:                          -
-----------------------------------------------------------------------
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 110 120
#
traffic classifier c1 operator and precedence 5
 if-match vlan-id 120
traffic classifier c2 operator and precedence 10
 if-match vlan-id 110
traffic classifier c3 operator and precedence 15
 if-match vlan-id 100
#
traffic behavior b1
 permit
 car cir 2000 pir 10000 cbs 250000 pbs 1250000 mode color-blind green pass yellow pass red discard
 remark dscp ef
 statistic enable
traffic behavior b2
 permit
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 mode color-blind green pass yellow pass red discard
 remark dscp af33
 statistic enable
traffic behavior b3
 permit
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 mode color-blind green pass yellow pass red discard
 remark dscp af13
 statistic enable
#
traffic policy p1 match-order config
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 traffic-policy p1 inbound
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
#
return
```


相关信息

技术论坛

QoS专题-第2期-QoS实现工具之MQC

4.10.2 配置层次化流量监管示例

组网需求

Switch通过接口GE2/0/1与Router互连，企业可经由Switch和Router访问网络，如图4-11所示。

在该网络中，由于网络侧带宽小于企业局域网带宽，在网络侧链路入口处会造成网络拥塞，数据丢失，因此需要对出口带宽进行限制，总带宽限制在12000kbps，另外还需要对语音、视频和数据业务分别进行流量监管将流量限制在一个合理的范围内。

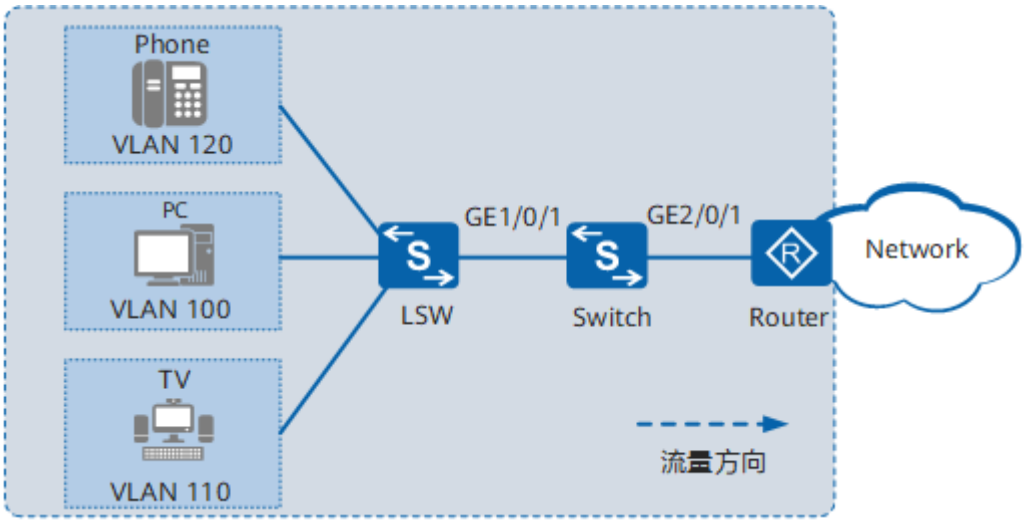
语音业务对应的VLAN ID为120，视频业务对应的VLAN ID分别为110，数据业务对应的VLAN ID为100，不同业务对于服务质量的需求不同，语音业务对服务质量要求最高，视频业务次之，数据业务要求最低，所以在Switch中还需要重标记不同业务报文的DSCP优先级，以便于下游Router按照报文的不同优先级分别进行处理，保证各种业务的服务质量。

具体配置需求如表4-10所示。

表 4-10 Switch 为上行流量提供的 QoS 保障

流量类型	CIR(kbps)	PIR(kbps)	DSCP优先级
语音	2000	10000	46
视频	4000	10000	30
数据	4000	10000	14

图 4-11 层次化流量监管配置组网图



配置思路

采用如下的思路配置层次化流量监管：

1. 创建VLAN，并配置各接口，使企业能够通过Switch访问网络。
2. 配置CAR模板，限制语音、数据、视频三种业务的总带宽。
3. 在Switch上配置基于VLAN ID进行流分类的匹配规则，区分语音、视频和数据报文。
4. 在Switch上配置流行为，对报文进行流量监管并且重标记报文的DSCP优先级。
5. 在Switch上配置流量监管策略，绑定已配置的流行为和流分类，并应用到Switch与LSW连接的接口上。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN 100、110、120。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 110 120
```

将接口GE1/0/1、GE2/0/1的接入类型分别配置为trunk，并分别将接口GE1/0/1和GE2/0/1加入VLAN 100、VLAN 110、VLAN 120。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet2/0/1] quit
```

步骤2 配置CAR模板

```
[Switch] qos car car1 cir 12000
```

步骤3 配置流分类

在Switch上创建流分类c1～c3，对不同业务流按照其VLAN ID进行分类。

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match vlan-id 120
[Switch-classifier-c1] quit
[Switch] traffic classifier c2 operator and
[Switch-classifier-c2] if-match vlan-id 110
[Switch-classifier-c2] quit
[Switch] traffic classifier c3 operator and
[Switch-classifier-c3] if-match vlan-id 100
[Switch-classifier-c3] quit
```

步骤4 配置流量监管行为

在Switch上创建流行为b1～b3，对不同业务流进行流量监管以及重标记优先级。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] car cir 2000 pir 10000 green pass
[Switch-behavior-b1] car car1 share
[Switch-behavior-b1] remark dscp 46
[Switch-behavior-b1] statistic enable
```



```
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] car cir 4000 pir 10000 green pass
[Switch-behavior-b2] car car1 share
[Switch-behavior-b2] remark dscp 30
[Switch-behavior-b2] statistic enable
[Switch-behavior-b2] quit
[Switch] traffic behavior b3
[Switch-behavior-b3] car cir 4000 pir 10000 green pass
[Switch-behavior-b3] car car1 share
[Switch-behavior-b3] remark dscp 14
[Switch-behavior-b3] statistic enable
[Switch-behavior-b3] quit
```

步骤5 配置流量监管策略并应用到接口上

在Switch上创建流策略p1，将流分类和对应的流行为进行绑定并将流策略应用到接口GE1/0/1入方向上，对报文进行流量监管和重标记。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] classifier c3 behavior b3
[Switch-trafficpolicy-p1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet1/0/1] quit
```

步骤6 验证配置结果

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Precedence: 10
    Operator: AND
    Rule(s) : if-match vlan-id 110

   Classifier: c3
    Precedence: 15
    Operator: AND
    Rule(s) : if-match vlan-id 100

   Classifier: c1
    Precedence: 5
    Operator: AND
    Rule(s) : if-match vlan-id 120

Total classifier number is 3
```

查看流策略的配置信息，以流策略p1为例。

```
[Switch] display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Permit
      Committed Access Rate:
        CIR 2000 (Kbps), PIR 10000 (Kbps), CBS 250000 (byte), PBS 1250000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      Share car:
        Car car1 share
      Remark:
```



```
    Remark DSCP ef
   Statistic: enable
 Classifier: c2
  Operator: AND
   Behavior: b2
    Permit
    Committed Access Rate:
     CIR 4000 (Kbps), PIR 10000 (Kbps), CBS 500000 (byte), PBS 1250000 (byte)
     Color Mode: color Blind
     Conform Action: pass
     Yellow  Action: pass
     Exceed  Action: discard
    Share car:
     Car car1 share
    Remark:
     Remark DSCP af33
   Statistic: enable
 Classifier: c3
  Operator: AND
   Behavior: b3
    Permit
    Committed Access Rate:
     CIR 4000 (Kbps), PIR 10000 (Kbps), CBS 500000 (byte), PBS 1250000 (byte)
     Color Mode: color Blind
     Conform Action: pass
     Yellow  Action: pass
     Exceed  Action: discard
    Share car:
     Car car1 share
    Remark:
     Remark DSCP af13
    Statistic: enable
```

查看在接口上应用的流策略信息，以接口GE1/0/1为例。

```
[Switch] display traffic policy statistics interface gigabitethernet 1/0/1 inbound

 Interface: GigabitEthernet1/0/1
 Traffic policy inbound: p1
 Rule number: 3
 Current status: success
 Statistics interval: 300
-----------------------------------------------------------------------
 Board : 1
-----------------------------------------------------------------------
 Matched          |     Packets:                      0
                  |     Bytes:                    0
                  |     Rate(pps):                  0
                  |     Rate(bps):                  0
-----------------------------------------------------------------------
  Passed          |     Packets:                      0
                  |     Bytes:                    0
                  |     Rate(pps):                  0
                  |     Rate(bps):                  0
-----------------------------------------------------------------------
  Dropped         |     Packets:                      0
                  |     Bytes:                    0
                  |     Rate(pps):                  0
                  |     Rate(bps):                  0
-----------------------------------------------------------------------
    Filter        |     Packets:                      0
                  |     Bytes:                    0
-----------------------------------------------------------------------
    Car           |     Packets:                      0
                  |     Bytes:                    0
-----------------------------------------------------------------------
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 110 120
#
qos car car1 cir 12000 cbs 2256000
#
traffic classifier c1 operator and precedence 5
 if-match vlan-id 120
traffic classifier c2 operator and precedence 10
 if-match vlan-id 110
traffic classifier c3 operator and precedence 15
 if-match vlan-id 100
#
traffic behavior b1
 permit
 car cir 2000 pir 10000 cbs 250000 pbs 1250000 mode color-blind green pass yellow pass red discard
 car car1 share
 remark dscp ef
 statistic enable
traffic behavior b2
 permit
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 mode color-blind green pass yellow pass red discard
 car car1 share
 remark dscp af33
 statistic enable
traffic behavior b3
 permit
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 mode color-blind green pass yellow pass red discard
 car car1 share
 remark dscp af13
 statistic enable
#
traffic policy p1 match-order config
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 traffic-policy p1 inbound
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
#
return
```

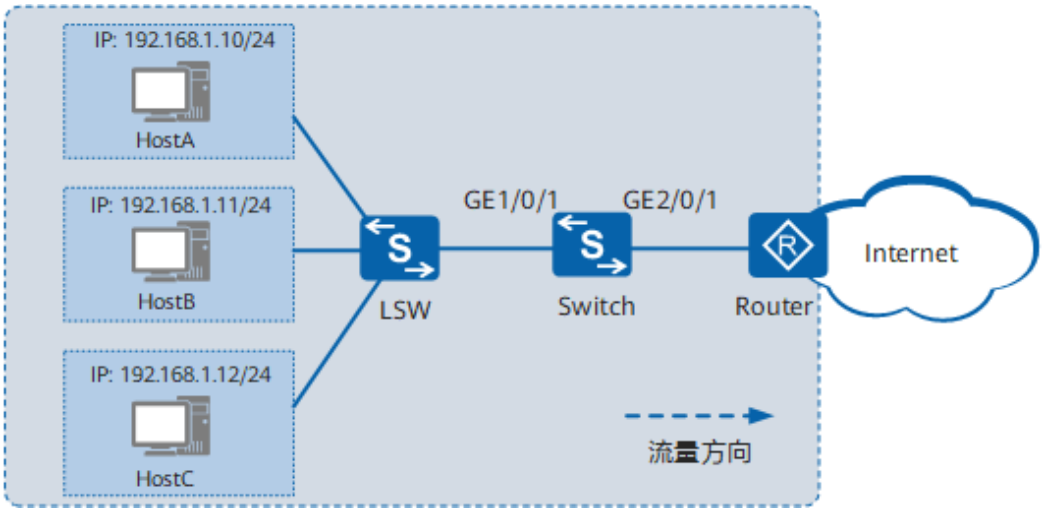
4.10.3 配置在指定时间段进行限速示例

组网需求

如图4-12所示，用户通过Switch的接口GE2/0/1连接到外部网络设备。

每天8:30～18:00的时间段为工作时间，对员工访问外网的速率进行限制，要求工作时间访问外网的速率不超过4Mbit/s。

图 4-12 配置在指定时间段进行限速组网图



配置思路

采用匹配时间段的流策略方式实现限速，具体配置思路如下：

1. 配置各接口，实现用户能通过Switch访问外部网络。
2. 配置时间范围，用于在ACL中引用。
3. 配置ACL，匹配指定时间段通过设备的流量。
4. 配置ACL，匹配指定时间段访问Internet的HTTP流量。
5. 配置流策略，对于符合ACL规则的报文进行限速。
6. 在接口GE1/0/1的入方向应用流策略。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN10。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
```

配置Switch上接口GE1/0/1和GE2/0/1为Trunk类型接口，并加入VLAN10。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet2/0/1] quit
```

说明

请配置LSW与Switch对接的接口为Trunk类型，并加入VLAN10。

创建VLANIF10，并为VLANIF10配置IP地址192.168.1.1/24。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
```

说明

请配置Router与Switch对接的接口IP地址为192.168.1.2/24。

步骤2 创建周期时间段working_time，时间范围为工作日的8:30～18:00。

```
[Switch] time-range working_time 08:30 to 18:00 working-day
```

步骤3 配置ACL 2001，配置两条规则，分别限制源IP地址为192.168.1.11、192.168.1.12的报文在工作时间的带宽。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 192.168.1.11 0 time-range working_time
[Switch-acl-basic-2001] rule permit source 192.168.1.12 0 time-range working_time
[Switch-acl-basic-2001] quit
```

步骤4 配置ACL 3000，配置一条规则，限制源IP地址为192.168.1.10的设备在工作时间访问Internet的HTTP（端口号为80）流量。

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit tcp destination-port eq 80 source 192.168.1.10 0 time-range working_time
[Switch-acl-adv-3000] quit
```

步骤5 配置匹配ACL 2001的流分类规则，实现对报文的分类。

```
[Switch] traffic classifier c1 operator or
[Switch-classifier-c1] if-match acl 2001
[Switch-classifier-c1] if-match acl 3000
[Switch-classifier-c1] quit
```

步骤6 配置流行为，限制访问外网速率不超过4Mbit/s。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] car cir 4096
[Switch-behavior-b1] quit
```

步骤7 配置流策略，并在接口GE1/0/1的入方向应用该策略。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet1/0/1] quit
```

步骤8 验证配置结果

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined c1
 User Defined Classifier Information:
  Classifier: c1
   Precedence: 5
   Operator: OR
   Rule(s) : if-match acl 2001
             if-match acl 3000
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined p1
  User Defined Traffic Policy Information:
 Policy: p1
  Classifier: c1
   Operator: OR
    Behavior: b1
     Permit
     Committed Access Rate:
```



```
  CIR 4096 (Kbps), PIR 4096 (Kbps), CBS 770048 (byte), PBS 1282048 (byte)
  Color Mode: color Blind
  Conform Action: pass
  Yellow  Action: pass
  Exceed  Action: discard
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
time-range working_time 08:30 to 18:00 working-day
#
acl number 2001
 rule 5 permit source 192.168.1.11 0 time-range working_time
 rule 10 permit source 192.168.1.12 0 time-range working_time
#
acl number 3000
 rule 5 permit tcp source 192.168.1.10 0 destination-port eq www time-range
working_time
#
traffic classifier c1 operator or precedence 5
 if-match acl 2001
 if-match acl 3000
#
traffic behavior b1
 permit
 car cir 4096 pir 4096 cbs 770048 pbs 1282048 mode color-blind green pass yellow pass red discard
#
traffic policy p1 match-order config
 classifier c1 behavior b1
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy p1 inbound
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

4.10.4 配置针对不同网段用户限速示例

组网需求

Switch通过接口GE3/0/1与路由器互连，用户可经由Switch和路由器访问网络，如图4-13所示。

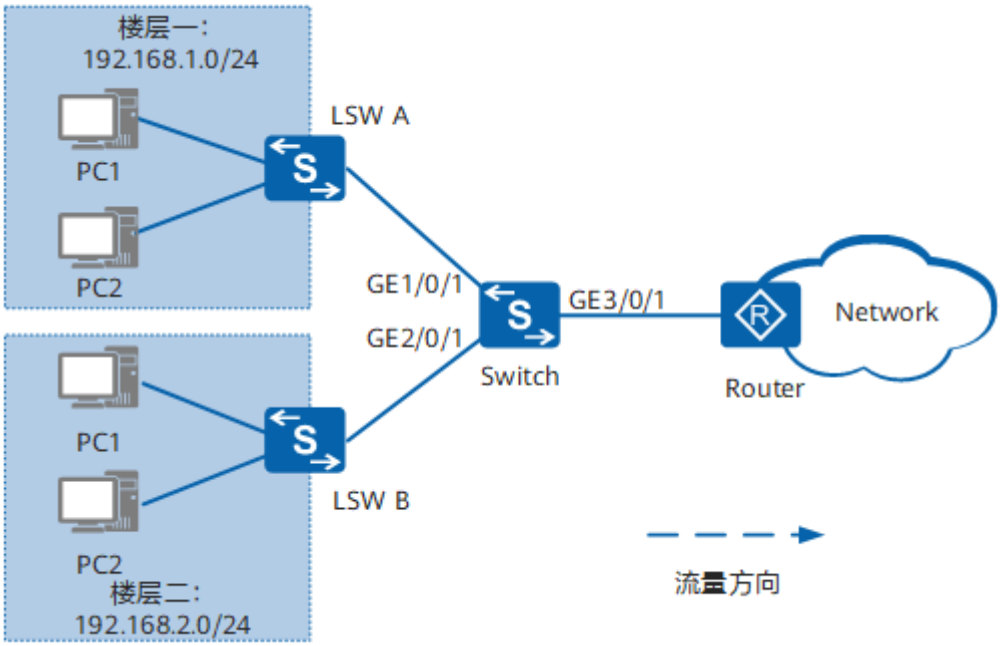
不同楼层的用户通过不同的接入交换机连接网络，且分别属于不同的网段，针对不同网段的用户提供不同的带宽。同一网段的所有用户共享带宽。

具体配置需求如表4-11所示。

表 4-11 Switch 为上行流量提供的 QoS 保障

用户	CIR(kbps)	PIR(kbps)
楼层一所有用户	4000	10000
楼层二所有用户	6000	10000

图 4-13 配置针对不同网段用户限速组网图



配置思路

采用如下的思路配置针对不同网段用户限速：

1. 创建VLAN，并配置各接口，使用户能够通过Switch访问网络。
2. 在Switch上配置ACL分别匹配不同的网段。
3. 在Switch上配置流分类匹配ACL规则。
4. 在Switch上配置流行为，对来自不同楼层的用户报文进行限速。
5. 在Switch上配置限速策略，绑定已配置的流行为和流分类，并应用到Switch与路由器连接的接口上。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN 100、200。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
```


将接口GE1/0/1、GE2/0/1的接入类型分别配置为Trunk，并分别将接口GE1/0/1和GE2/0/1加入VLAN 100、VLAN 200。将接口GE3/0/1的接入类型配置为Trunk，并加入VLAN100和VLAN200。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 200
[Switch-GigabitEthernet2/0/1] quit
[Switch] interface gigabitethernet 3/0/1
[Switch-GigabitEthernet3/0/1] port link-type trunk
[Switch-GigabitEthernet3/0/1] port trunk allow-pass vlan 100 200
[Switch-GigabitEthernet3/0/1] quit
```

步骤2 配置ACL

配置ACL规则匹配不同的网段。

```
[Switch] acl 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Switch-acl-basic-2000] quit
[Switch] acl 2001
[Switch-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[Switch-acl-basic-2001] quit
```

步骤3 配置流分类

在Switch上创建流分类c1、c2，对来自不同楼层的用户进行分类。

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match acl 2000
[Switch-classifier-c1] quit
[Switch] traffic classifier c2 operator and
[Switch-classifier-c2] if-match acl 2001
[Switch-classifier-c2] quit
```

步骤4 配置流量监管行为

在Switch上创建流行为b1、b2，对不同业务流进行流量监管。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] car cir 4000 pir 10000 green pass
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] car cir 6000 pir 10000 green pass
[Switch-behavior-b2] quit
```

步骤5 配置流量监管策略并应用到接口上

在Switch上创建流策略p1，将流分类和对应的流行为进行绑定，并将流策略应用到接口GE3/0/1出方向上，对报文进行流量监管。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] quit
[Switch] interface gigabitethernet 3/0/1
[Switch-GigabitEthernet3/0/1] traffic-policy p1 outbound
[Switch-GigabitEthernet3/0/1] quit
```

步骤6 验证配置结果

查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
```



```
  Classifier: c2
   Precedence: 10
   Operator: AND
   Rule(s) : if-match acl 2001

  Classifier: c1
   Precedence: 5
   Operator: AND
   Rule(s) : if-match acl 2000

Total classifier number is 2
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Permit
      Committed Access Rate:
        CIR 4000 (Kbps), PIR 10000 (Kbps), CBS 500000 (byte), PBS 1250000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
   Classifier: c2
    Operator: AND
     Behavior: b2
      Permit
      Committed Access Rate:
        CIR 6000 (Kbps), PIR 10000 (Kbps), CBS 750000 (byte), PBS 1250000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 200
#
acl number 2000
 rule 5 permit source 192.168.1.0 0.0.0.255
acl number 2001
 rule 5 permit source 192.168.2.0 0.0.0.255
#
traffic classifier c1 operator and precedence 5
 if-match acl 2000
traffic classifier c2 operator and precedence 10
 if-match acl 2001
#
traffic behavior b1
 permit
 car cir 4000 pir 10000 cbs 500000 pbs 1250000 mode color-blind green pass yellow pass red discard
traffic behavior b2
 permit
 car cir 6000 pir 10000 cbs 750000 pbs 1250000 mode color-blind green pass yellow pass red discard
#
traffic policy p1 match-order config
 classifier c1 behavior b1
 classifier c2 behavior b2
```

```
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface GigabitEthernet3/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
 traffic-policy p1 outbound
#
return
```

相关信息

视频

QoS限速配置之“基于IP网段的限速”

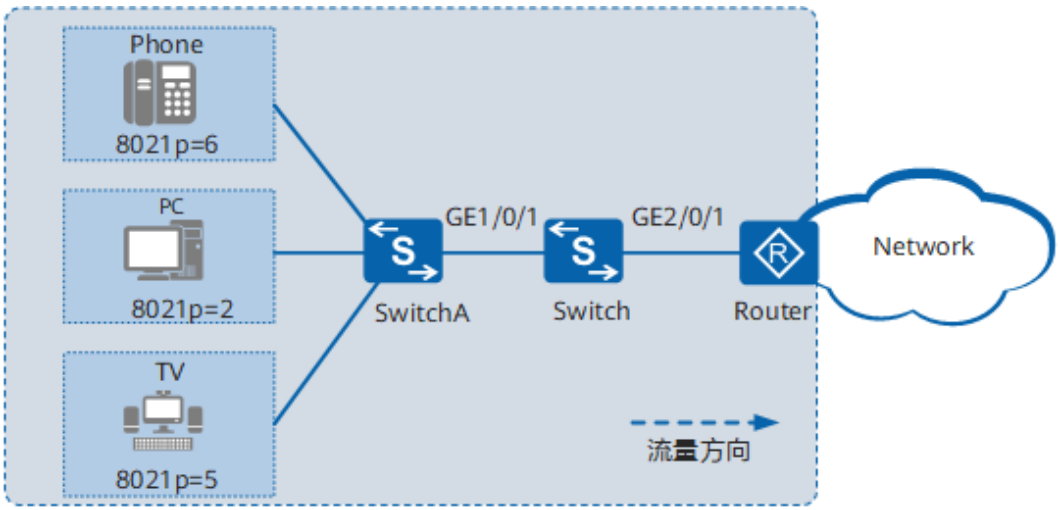
4.10.5 配置流量整形示例

组网需求

Switch通过接口GE2/0/1与路由器互连，来自网络侧的业务有语音、视频、数据，携带的802.1p优先级分别为6、5、2，这些业务可经由路由器和Switch到达用户，如图4-14所示。由于来自用户局域网的流量速率大于Router接口的速率，出接口GE2/0/1处可能会发生带宽抖动。为减少带宽抖动，同时保证各类业务带宽要求，现要求如下：

- 接口带宽限制为10000kbit/s。
- 语音带宽限制为3000kbit/s，最大不超过5000kbit/s。
- 视频带宽限制为5000kbit/s，最大不超过8000kbit/s。
- 数据带宽限制为2000kbit/s，最大不超过3000kbit/s。

图 4-14 流量整形配置组网图



配置思路

采用如下的思路配置流量整形：

1. 创建VLAN，并配置各接口，使用户能够通过Switch访问网络。
2. 配置优先级映射，将802.1p优先级映射为PHB行为。
3. 配置接口整形功能，限制接口的总带宽。
4. 配置端口队列整形功能，限制语音、视频、数据三类业务的带宽。

操作步骤

步骤1 创建VLAN并配置各接口

创建VLAN 10。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10
```

将接口GE1/0/1、GE2/0/1的接入类型分别配置为trunk，并分别将接口GE1/0/1、GE2/0/1加入VLAN 10。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet2/0/1] quit
```

创建VLANIF10，并配置网段地址10.10.10.2/24。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.10.10.2 255.255.255.0
[Switch-Vlanif10] quit
```

说明

请在Router上的与Switch对接的接口上配置IP地址10.10.10.1/24。

步骤2 配置优先级映射

创建DiffServ域ds1，将802.1p优先级6、5、2分别映射为PHB行为CS7、EF、AF2。

```
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 6 phb cs7
[Switch-dsdomain-ds1] 8021p-inbound 5 phb ef
[Switch-dsdomain-ds1] 8021p-inbound 2 phb af2
[Switch-dsdomain-ds1] quit
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] trust upstream ds1
[Switch-GigabitEthernet1/0/1] quit
```

步骤3 配置接口整形

在Switch上配置接口整形，将接口速率限制在10000kbit/s。

```
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] qos lr cir 10000 outbound
```

步骤4 配置端口队列整形

在Switch上配置端口队列整形，使语音、视频、数据业务的带宽分别限制为3000kbit/s、5000kbit/s、2000kbit/s，最大分别不超过5000kbit/s、8000kbit/s、3000kbit/s。

```
[Switch-GigabitEthernet2/0/1] qos queue 7 shaping cir 3000 pir 5000
[Switch-GigabitEthernet2/0/1] qos queue 5 shaping cir 5000 pir 8000
[Switch-GigabitEthernet2/0/1] qos queue 2 shaping cir 2000 pir 3000
[Switch-GigabitEthernet2/0/1] quit
[Switch] quit
```

步骤5 验证配置结果

查看DiffServ域ds1的配置信息。

```
<Switch> display diffserv domain name ds1
diffserv domain name:ds1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 green
 8021p-inbound 2 phb af2 green
 8021p-inbound 3 phb af3 green
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb ef green
 8021p-inbound 6 phb cs7 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 ......
```

配置成功后，从接口GE2/0/1发出的报文带宽限制为10000kbit/s；语音业务带宽限制为3000kbit/s，不超过5000kbit/s；视频业务带宽限制为5000kbit/s，不超过8000kbit/s；数据业务带宽限制为2000kbit/s，不超过3000kbit/s。

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
diffserv domain ds1
 8021p-inbound 6 phb cs7 green
#
interface Vlanif10
 ip address 10.10.10.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 trust upstream ds1
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 qos lr cir 10000 cbs 1250000 outbound
 qos queue 2 shaping cir 2000 pir 3000
 qos queue 5 shaping cir 5000 pir 8000
 qos queue 7 shaping cir 3000 pir 5000
#
return
```

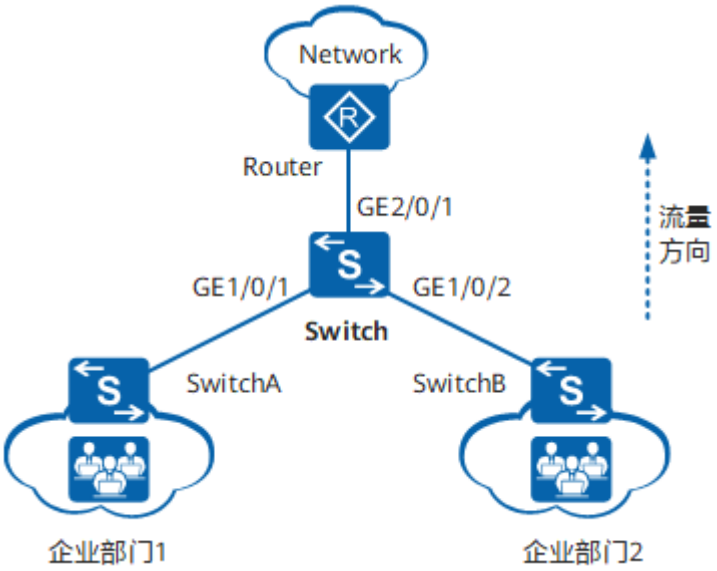
4.10.6 配置接口限速示例

组网需求

如图4-15所示，Switch通过接口GE2/0/1与路由器互连，企业部门1和企业部门2通过接口GE1/0/1和GE1/0/2接入Switch，经由Switch和路由器访问网络。

由于该网络只有数据业务流量，不需要对业务进行区分，但是网络带宽有限，因此需要对企业部门1和企业部门2的接入带宽进行整体限制。要求企业部门1带宽限制为8Mbit/s，最高不超过10Mbit/s；企业部门2带宽限制为5Mbit/s，最高不超过8Mbit/s。

图 4-15 接口限速配置组网图



配置思路

采用如下的思路配置接口限速：

1. 创建VLAN，并配置各接口，使用户能够通过Switch访问网络。
2. 创建不同的CAR模板并配置其中的CIR、PIR，在Switch接口GE1/0/1和GE1/0/2的入方向上分别应用CAR模板，实现对不同企业部门的限速功能。

操作步骤

步骤1 创建VLAN并配置Switch各接口

创建VLAN 100、200。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
```

配置接口GE1/0/1、GE1/0/2和GE2/0/1的接口类型为Trunk，并将GE1/0/1加入VLAN100，GE1/0/2加入VLAN200，GE2/0/1加入VLAN100和VLAN200。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 200
[Switch-GigabitEthernet2/0/1] quit
```

步骤2 配置CAR模板

在Switch上创建CAR模板car1、car2，分别对企业部门1和企业部门2的流量进行限速。

```
[Switch] qos car car1 cir 8192 pir 10240
[Switch] qos car car2 cir 5120 pir 8192
```

步骤3 应用CAR模板

在Switch的接口GE1/0/1、GE1/0/2上的上行方向分别应用car1、car2，对企业部门1和企业部门2的流量进行限速。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos car inbound car1
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos car inbound car2
[Switch-GigabitEthernet1/0/2] quit
[Switch] quit
```

步骤4 验证配置结果

查看CAR模板的配置信息。

```
<Switch> display qos car all
 ------------------------------------------------------------------
  CAR Name     : car1
  CAR Index    : 0
   car cir 8192 (Kbps) pir 10240 (Kbps) cbs 1024000 (byte) pbs 1280000 (byte)
 ------------------------------------------------------------------
  CAR Name     : car2
  CAR Index    : 1
   car cir 5120 (Kbps) pir 8192 (Kbps) cbs 640000 (byte) pbs 1024000 (byte)
```

分别使用6000kbps、9000kbps和11000kbps的速率向接口GE1/0/1和GE1/0/2输入报文流，然后使用命令**display qos car statistics**查看流量统计信息。如果配置成功：使用6000kbps向接口GE1/0/1和GE1/0/2输入报文流时，报文全部转发，无丢弃报文；使用9000kbps向接口GE1/0/1和GE1/0/2输入报文流时，接口GE1/0/1上的报文全部转发，接口GE1/0/2上的报文有部分丢弃；使用11000kbps向接口GE1/0/1和GE1/0/2输入报文流时，接口GE1/0/1上和GE1/0/2上的报文均有部分丢弃。

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 200
#
qos car car1 cir 8192 pir 10240 cbs 1024000 pbs 1280000
```



```
qos car car2 cir 5120 pir 8192 cbs 640000 pbs 1024000
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 qos car inbound car1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 qos car inbound car2
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
return
```

相关信息

视频

QoS限速配置之“接口限速”

4.11 流量监管、流量整形和接口限速 FAQ

4.11.1 配置限速时，如何设置 CIR 和 CBS 等参数

配置限速时，需要配置**cir** *cir-value*和**cbs** *cbs-value*等参数，其中**cir** *cir-value*指承诺信息速率，即保证能够通过的平均速率；**cbs** *cbs-value*指承诺突发尺寸，即瞬间能够通过的承诺突发流量。例如，用户想要配置限速4Mbit/s，则配置*cir-value*=4*1024 kbit/s=4096 kbit/s。*cbs-value*建议配置为*cir-value*的100–200倍，如果用户没有配置*cbs-value*，则设备会自动指定其为缺省值。单令牌桶时，*cbs-value*缺省为*cir-value*的188倍；双令牌桶时，*cbs-value*缺省为*cir-value*的125倍。

4.11.2 为什么交换机配置限速之后限速效果不准确

交换机配置限速时，可以在出方向或者入方向分开配置，也可以同时配置。流量统计时出入方向的流量分开计算，互不影响。限速受到帧间隙及前导码等报文开销影响，可能会与预期的限速效果存在一定的差异。

帧间隙和前导码：设备在计算流量监管、流量整形和接口限速的速率时，缺省情况下是包括帧间隙和前导码的，即统计出来的流量速率并不是只包括数据报文流量。设备支持通过命令**qos-car exclude-interframe**和**qos-shaping exclude-interframe**配置计算流量监管、流量整形和接口限速的速率时不包括报文的帧间隙和前导码，从而提高限速功能的准确性。

4.11.3 在接口上配置 CAR 限速和在全局配置 CAR 限速的区别是什么

在接口上做CAR限速只对本接口进行限速，而在全局做CAR限速时指定slot参数时相当于指定单板的所有端口共享此CAR，不指定slot参数时相当于设备各个单板的所有端口共享此CAR。

例如：CAR 5000kbit/s如果应用在接口下，则只对此接口进行限速，此接口发送或接收报文速率最多只能达到5000kbit/s；如果应用在全局下且未指定slot参数，则相当于设备每个单板的所有接口转发报文的速率加起来的和最多都只能达到5000kbit/s。

5 拥塞避免和拥塞管理配置

5.1 拥塞避免和拥塞管理概述

拥塞避免通过指定报文丢弃策略来解除网络过载，拥塞管理通过指定报文调度次序来确保高优先级业务优先被处理。

传统网络所面临的服务质量问题主要由拥塞引起，拥塞是指由于网络资源不足而造成速率下降、引入额外延时的一种现象。拥塞会造成报文的传输时延、吞吐率低及资源的大量耗费。而在IP分组交换及多业务并存的复杂环境下，拥塞又极为常见。

拥塞避免和拥塞管理就是解决网络拥塞的两种流控方式。

拥塞避免

拥塞避免是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞发生或有加剧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的一种流量控制机制。

设备支持以下拥塞避免功能：

- 尾部丢弃

  传统的丢弃策略采用尾部丢弃的方法，同等对待所有报文，不对报文进行服务等级的区分。在拥塞发生时，队列尾部的数据报文将被丢弃，直到拥塞解除。

  这种丢弃策略会引起TCP全局同步现象。所谓TCP全局同步现象，是指当多个队列同时丢弃多个TCP连接报文时，将造成一些TCP连接同时进入拥塞避免和慢启动状态，降低流量以解除拥塞；而后这些TCP连接又会在某个时刻同时出现流量高峰。如此反复，使网络流量忽大忽小，影响链路利用率。

  缺省情况下，接口采用尾部丢弃的丢弃策略。

- WRED

  加权随机先期检测WRED（Weighted Random Early Detection）基于丢弃参数随机丢弃报文。考虑到高优先级报文的利益并使其被丢弃的概率相对较小，WRED可以为不同业务的报文指定不同的丢弃策略。此外，通过随机丢弃报文，让多个TCP连接不同时降低发送速度，避免了TCP全局同步现象。

  WRED技术为每个队列的长度都设定了阈值上下限，并规定：

  - 当队列的长度小于阈值下限时，不丢弃报文。
  - 当队列的长度大于阈值上限时，丢弃所有新收到的报文。
  - 当队列的长度在阈值下限和阈值上限之间时，开始随机丢弃新收到的报文。方法是为每个新收到的报文赋予一个随机数，并用该随机数与当前队列的丢弃概率比较，如果小于丢弃概率则报文被丢弃。队列越长，报文被丢弃的概率越高。

拥塞管理

拥塞管理是指在网络间歇性出现拥塞，时延敏感业务要求得到比其它业务更高质量的QoS服务时，通过调整报文的调度次序来满足时延敏感业务高QoS服务的一种流量控制机制。

设备支持以下拥塞管理功能：

- PQ调度

  优先队列PQ（Priority Queuing）调度，就是严格按照队列优先级的高低顺序进行调度。只有高优先级队列中的报文全部调度完毕后，低优先级队列才有调度机会。

  采用PQ调度方式，将时延敏感业务放入高优先级队列，将其它业务放入低优先级队列，从而确保时延敏感业务被优先调度。

  PQ调度的缺点是：拥塞发生时，如果高优先级队列中长时间有报文存在，那么低优先级队列中的报文就会得不到调度机会。

- WRR调度

  WRR（Weighted Round Robin）调度即加权轮询调度。WRR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。

  以接口有8个输出队列为例，WRR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。举个更具体的例子，一个100M的接口，配置它的WRR算法的加权值为50、50、30、30、10、10、10、10（依次对应w7、w6、w5、w4、w3、w2、w1、w0），这样可以保证最低优先级队列至少获得5M带宽，避免了采用PQ调度时发生拥塞的情况下低优先级队列中的报文长时间得不到服务的缺点。

  WRR还有一个优点：虽然多个队列的调度是轮流进行的，但对每个队列不是固定地分配服务时间片，也就是说如果某个队列为空，马上换到下一个队列进行调度，这样带宽资源可以得到充分的利用。

WRR调度有两个缺点：

- WRR调度按照报文个数进行调度，而用户一般关心的是带宽。当每个队列的平均报文长度相等或已知时，通过配置WRR权重，用户能够获得想要的带宽；但是，当队列的平均报文长度变化时，用户就不能通过配置WRR权重获取想要的带宽。
- 时延敏感业务（如语音）得不到及时调度。

- WDRR调度

  加权赤字轮询调度WDRR（Weighted Deficit Round Robin）调度实现原理与WRR调度基本相同。

  WDRR调度与WRR调度的区别是：WRR调度是按照报文个数进行调度，而WDRR是按照报文长度进行调度。如果报文长度超过了队列的调度能力，WDRR调度允许出现负权重，以保证长报文也能够得到调度。但下次轮询调度时该队列将不会被调度，直到权重为正，该队列才会参与WDRR调度。

  WDRR调度避免了采用PQ调度时发生拥塞的情况下低优先级队列中的报文长时间得不到服务的缺点，也避免了各队列报文长度不等或变化较大时，WRR调度不能按配置比例分配带宽资源的缺点。

  但是，WDRR调度也具有时延敏感业务（如语音）得不到及时调度的缺点。

  当所有参与WDRR调度的队列的权重相同时，WDRR调度与DRR调度效果相同。

- WFQ调度

  公平队列FQ（Fair Queue）的目的是尽可能公平地分享网络资源，使所有流的延迟和抖动达到最优，让不同队列获得公平的调度机会。WFQ（Weighted Fair Queue）调度即加权公平队列调度，在FQ的基础上增加了优先权方面的考虑，使高优先权的报文获得优先调度的机会多于低优先权的报文。

  WFQ能够按流的“会话”信息（协议类型、源和目的TCP或UDP端口号、源和目的IP地址、ToS域中的优先级位等）自动进行流分类，并且尽可能多地提供队列，以将每个流均匀地放入不同队列中，从而在总体上均衡各个流的延迟。在出队的时候，WFQ按流的优先级（precedence）来分配每个流应占有出口的带宽。优先级的数值越小，所得的带宽越少。优先级的数值越大，所得的带宽越多。

- PQ+WRR/PQ+WDRR/PQ+WFQ调度

  PQ调度和WRR/WDRR/WFQ调度各有优缺点。单纯采用PQ调度时，低优先级队列中的报文长期得不到带宽，而单纯采用WRR/WDRR/WFQ调度时低延时需求业务得不到优先调度，PQ+WRR/PQ+WDRR/PQ+WFQ调度方式则将前两种调度方式结合起来，不仅能发挥两种调度的优势，而且能克服两种调度各自的缺点。

  用户可以借助PQ+WRR/PQ+WDRR/PQ+WFQ调度方式，将重要的协议报文和时延敏感业务报文放入采用PQ调度的队列中，并为该队列分配指定带宽；而将其他报文按各自的优先级放入采用WRR/WDRR/WFQ调度的各队列中，按照权值对各队列进行循环调度。

相关信息

技术论坛

QoS专题-第5期-QoS实现之队列调度与报文丢弃

5.2 拥塞管理和拥塞避免原理描述

5.2.1 拥塞避免

拥塞避免（Congestion Avoidance）是指通过监视网络资源（如队列或内存缓冲区）的使用情况，在拥塞发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的一种流控机制。

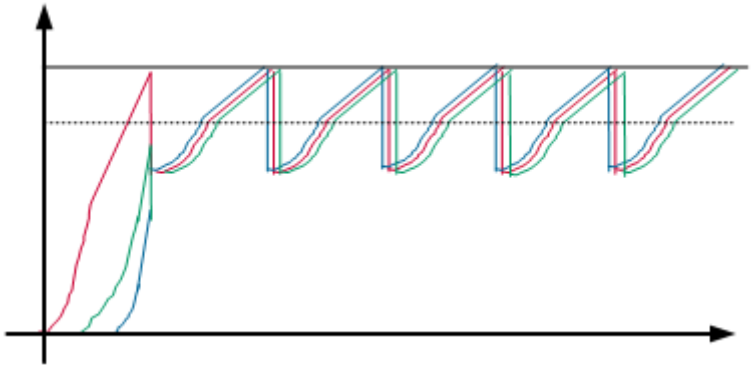
拥塞避免常用的两种丢弃报文方式为：尾部丢包策略和WRED。

- 传统的尾部丢包策略

  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，所有新入队列的报文（缓存在队列尾部）都将被丢弃。

  这种丢弃策略会引发TCP全局同步现象，导致TCP连接始终无法建立。所谓TCP全局同步现象如图，三种颜色表示三条TCP连接，当同时丢弃多个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而导致流量降低，之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。

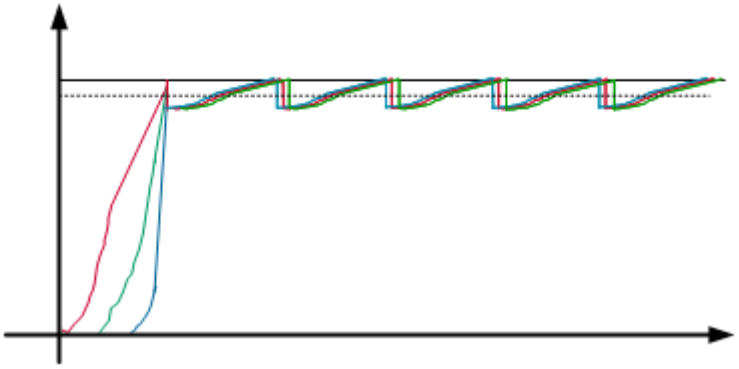
  图 5-1 尾部丢包示意图

- WRED

  为避免TCP全局同步现象，出现了RED（Random Early Detection）技术。RED通过随机地丢弃数据报文，让多个TCP连接不同时降低发送速度，从而避免了TCP的全局同步现象。使TCP速率及网络流量都趋于稳定。

  图 5-2 RED 算法示意图

  基于RED技术，设备实现了WRED（Weighted Random Early Detection）。

流队列支持基于DSCP或IP优先级进行WRED丢弃。每一种优先级都可以独立设置报文丢包的上下门限及丢包率。当队列中报文的总长度达到丢弃的下限时，开始丢包。随着队列中报文总长度的增加，丢包率不断增加，最高丢包率不超过设置的丢包率。直至队列中报文的总长度达到丢弃的上限，报文全部丢弃。这样按照一定的丢弃概率主动丢弃队列中的报文，从而在一定程度上避免拥塞问题。

5.2.2 拥塞管理

随着生活质量的提高，网络业务种类繁多，人们对网络质量的要求也越来越高，有限的带宽与超负荷的网络需求产生冲突，造成网络中时常会出现延迟、信号丢失等情况，这些都是由于拥塞产生的。当网络间歇性的出现拥塞，且时延敏感业务要求得到比非时延敏感业务更高质量的QoS服务时，需要进行拥塞管理；如果配置拥塞管理后仍然出现拥塞，则需要增加带宽。拥塞管理一般采用队列技术，使用不同的调度算法来发送队列中的报文流。

根据排队和调度策略的不同，设备上的拥塞管理技术分为PQ、WDRR、WRR、WFQ、PQ+WDRR、PQ+WRR和PQ+WFQ。每种调度算法都是为了解决特定网络流量的问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

设备上，每个接口出方向都拥有8个队列，以队列索引号进行标识，队列索引号分别为0、1、2、3、4、5、6、7。设备根据本地优先级和队列之间的映射关系，自动将分类后的报文流送入各队列，然后按照各种队列调度机制进行调度。

- PQ调度

  PQ调度，针对于关键业务类型应用设计，PQ调度算法维护一个优先级递减的队列系列并且只有当更高优先级的所有队列为空时才服务低优先级的队列。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（如E-Mail）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。

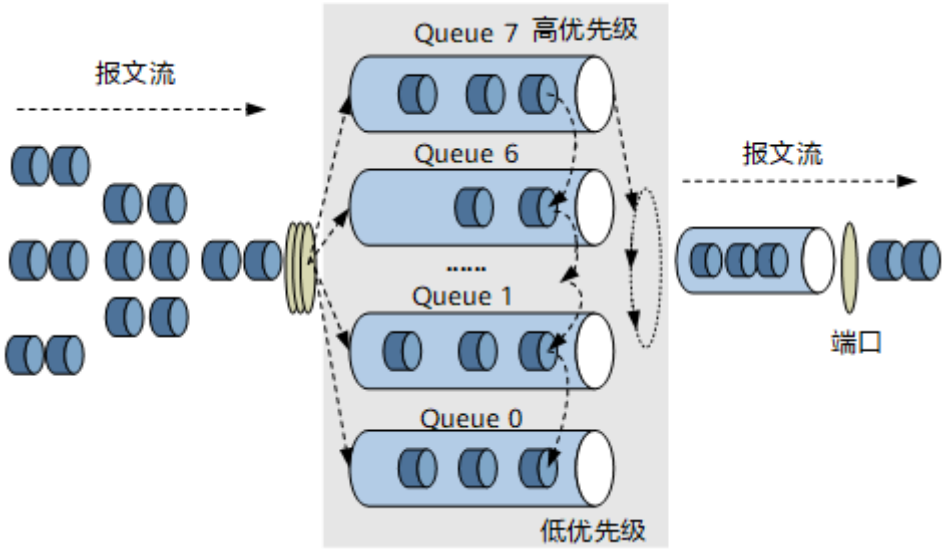
  如图5-3所示，Queue7比Queue6具有更高的优先权，Queue6比Queue5具有更高的优先权，依次类推。只要链路能够传输分组，Queue7尽可能快地被服务。只有当Queue7为空，调度器才考虑Queue6。当Queue6有分组等待传输且Queue7为空时，Queue6以链路速率接受类似地服务。当Queue7和Queue6为空时，Queue5以链路速率接收服务，以此类推。

  PQ调度算法对低时延业务非常有用。假定数据流X在每一个节点都被映射到最高优先级队列，那么当数据流X的分组到达时，则分组将得到优先服务。

  然而PQ调度机制会使低优先级队列中的报文得不到调度机会。例如，如果映射到Queue7的数据流在一段时间内以100%的输出链路速率到达，调度器将从不为Queue6及以下的队列服务。

  为了避免队列饥饿，上游设备需要精心规定数据流的业务特性，以确保映射到Queue7的业务流不超出输出链路容量的一定比例，这样Queue7会经常为空，低优先级队列中的报文才能得到调度机会。

图 5-3 PQ 调度示意图

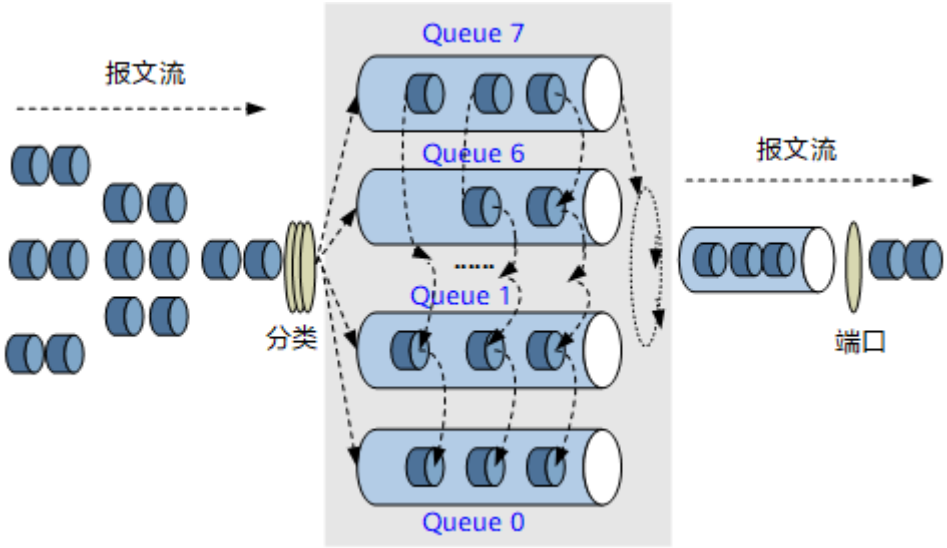


- WRR调度

  加权循环调度WRR（Weight Round Robin）在循环调度RR（Round Robin）的基础上演变而来，在队列之间进行轮流调度，根据每个队列的权重来调度各队列中的报文流。实际上，RR调度相当于权值为1的WRR调度。

  WRR调度示意图如图5-4所示。

  图 5-4 WRR 调度示意图

  在进行WRR调度时，设备根据每个队列的权值进行轮循调度。调度一轮权值减一，权值减到零的队列不参加调度，当所有队列的权限减到0时，开始下一轮的调度。例如，用户根据需要为接口上8个队列指定的权值分别为4、2、5、3、6、4、2和1，按照WRR方式进行调度的结果请参见表5-1所示。

表 5-1 WRR 调度的结果

队列索引	Q7	Q6	Q5	Q4	Q3	Q2	Q1	Q0
队列权值	4	2	5	3	6	4	2	1
参加第1轮调度的队列	Q7	Q6	Q5	Q4	Q3	Q2	Q1	Q0
参加第2轮调度的队列	Q7	Q6	Q5	Q4	Q3	Q2	Q1	-
参加第3轮调度的队列	Q7	-	Q5	Q4	Q3	Q2	-	-
参加第4轮调度的队列	Q7	-	Q5	-	Q3	Q2	-	-
参加第5轮调度的队列	-	-	Q5	-	Q3	-	-	-
参加第6轮调度的队列	-	-	-	-	Q3	-	-	-
参加第7轮调度的队列	Q7	Q6	Q5	Q4	Q3	Q2	Q1	Q0
参加第8轮调度的队列	Q7	Q6	Q5	Q4	Q3	Q2	Q1	-

队列索引	Q7	Q6	Q5	Q4	Q3	Q2	Q1	Q0
参加第9轮调度的队列	Q7	-	Q5	Q4	Q3	Q2	-	-
参加第10轮调度的队列	Q7	-	Q5	-	Q3	Q2	-	-
参加第11轮调度的队列	-	-	Q5	-	Q3	-	-	-
参加第12轮调度的队列	-	-	-	-	Q3	-	-	-

从统计上看，各队列中的报文流被调度的次数与该队列的权值成正比，权值越大被调度的次数相对越多。由于WRR调度的以报文为单位，因此每个队列没有固定的带宽，同等调度机会下大尺寸报文获得的实际带宽要大于小尺寸报文获得的带宽。

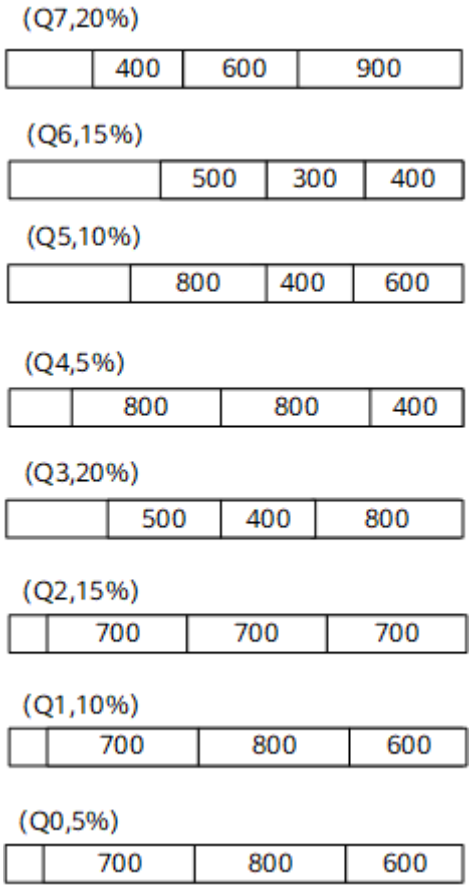
WRR调度避免了采用PQ调度时发生拥塞的情况下低优先级队列中的报文长时间得不到服务的缺点。WRR调度还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。但WRR调度无法使低延时需求业务得到及时调度。

- WDRR调度

  WDRR（Weighted Deficit Round Robin）调度同样也是RR的扩展，相对于WRR来言，解决了WRR只关心报文，同等调度机会下大尺寸报文获得的实际带宽要大于小尺寸报文获得的带宽的问题，在调度过程中考虑包长的因素以达到调度的速率公平性。

  WDRR调度中，Deficit表示队列的带宽赤字，初始值为0。每次调度前，系统按权重为各队列分配带宽，计算Deficit值，如果队列的Deficit值大于0，则参与此轮调度，发送一个报文，并根据所发送报文的长度计算调度后Deficit值，作为下一轮调度的依据；如果队列的Deficit值小于0，则不参与此轮调度，当前Deficit值作为下一轮调度的依据。

图 5-5 队列权重示意图



如图5-5所示，假设用户配置各队列权重为40、30、20、10、40、30、20、10（依次对应Q7、Q6、Q5、Q4、Q3、Q2、Q1、Q0），调度时，队列Q7、Q6、Q5、Q4、Q3、Q2、Q1、Q0依次能够获取20%、15%、10%、5%、20%、15%、10%、5%的带宽。下面以Q7、Q6为例，简要描述WDRR队列调度的实现过程（假设Q7队列获取400byte/s的带宽，Q6队列获取300byte/s的带宽）。

- 第1轮调度

  Deficit[7][1] = 0+400 = 400，Deficit[6][1] = 0+300 = 300，从Q7队列取出一个900byte的报文发送，从Q6队列取出一个400byte的报文发送；发送后，Deficit[7][1] = 400–900 =–500，Deficit[6][1] = 300–400 =–100。

- 第2轮调度

  Deficit[7][2] = -500+400 = -100，Deficit[6][2] = -100+300 = 200，Q7队列Deficit值小于0，此轮不参与调度，从Q6队列取出一个300byte的报文发送；发送后，Deficit[6][2] = 200–300 =–100。

- 第3轮调度

  Deficit[7][3] = -100+400 = 300，Deficit[6][3] = -100+300 = 200，从Q7队列取出一个600byte的报文发送，从Q6队列取出一个500byte的报文发送；发送后，Deficit[7][3] = 300–600 =–300，Deficit[6][3] = 200–500 =–300。

  如此循环调度，最终Q7、Q6队列获取的带宽将分别占总带宽的20%、15%，因此，用户能够通过设置权重获取想要的带宽。

但WDRR调度仍然没有解决WRR调度中低延时需求业务得不到及时调度的问题。

- WFQ调度

  公平队列FQ（Fair Queuing）的目的是尽可能公平地分享网络资源，使所有流的延迟和抖动达到最优：

  - 不同的队列获得公平的调度机会，从总体上均衡各个流的延迟。
  - 短报文和长报文获得公平的调度：如果不同队列间同时存在多个长报文和短报文等待发送，让短报文优先获得调度，从而在总体上减少各个流的报文间的抖动。

  与FQ相比，WFQ（Weighted Fair Queue）在计算报文调度次序时增加了优先权方面的考虑。从统计上，WFQ使高优先权的报文获得优先调度的机会多于低优先权的报文。

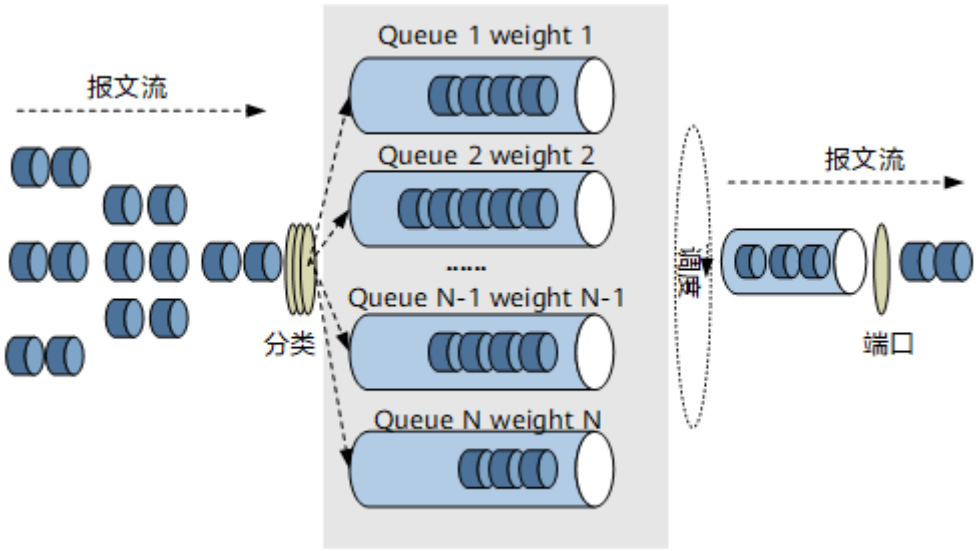
  WFQ调度在报文入队列之前，先对流量进行分类，有两种分类方式：

  - 按流的“会话”信息分类：

    根据报文的协议类型、源和目的TCP或UDP端口号、源和目的IP地址、ToS域中的优先级位等自动进行流分类，并且尽可能多地提供队列，以将每个流均匀地放入不同队列中，从而在总体上均衡各个流的延迟。在出队的时候，WFQ按流的优先级（precedence）来分配每个流应占有带宽。优先级的数值越小，所得的带宽越少。优先级的数值越大，所得的带宽越多。这种方式只有CBQ的default-class支持。
  - 按优先级分类：

    通过优先级映射把流量标记为本地优先级，每个本地优先级对应一个队列号。每个接口预分配8个队列，报文根据队列号进入队列。默认情况，队列的WFQ权重相同，流量平均分配接口带宽。用户可以通过配置修改权重，高优先权和低优先权按权重比例分配带宽。

  图 5-6 WFQ 调度示意图

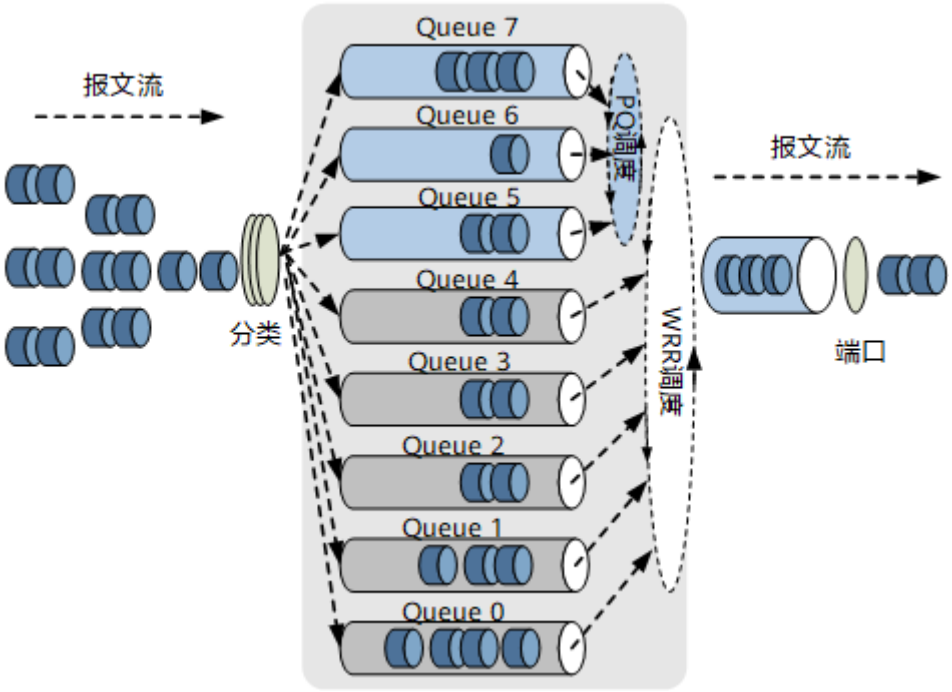
  

- PQ+WRR调度

  PQ调度和WRR调度各有优缺点，为了克服单纯采用PQ调度或WRR调度时的缺点，PQ+WRR调度以发挥两种调度的各自优势，不仅可以通过WRR调度可以让低优先级队列中的报文也能及时获得带宽，而且可以通过PQ调度可以保证了低延时需求的业务能优先得到调度。

在设备上，用户可以配置队列的WRR参数，根据配置将接口上的8个队列分为两组，一组（例如Queue7、Queue6、Queue5）采用PQ调度，另一组（例如Queue4、Queue3、Queue2、Queue1和Queue0队列）采用WRR调度。设备上只有LAN侧接口支持PQ+WRR调度。PQ+WRR调度示意图如图5-7所示。

图 5-7 PQ+WRR 混合调度示意图



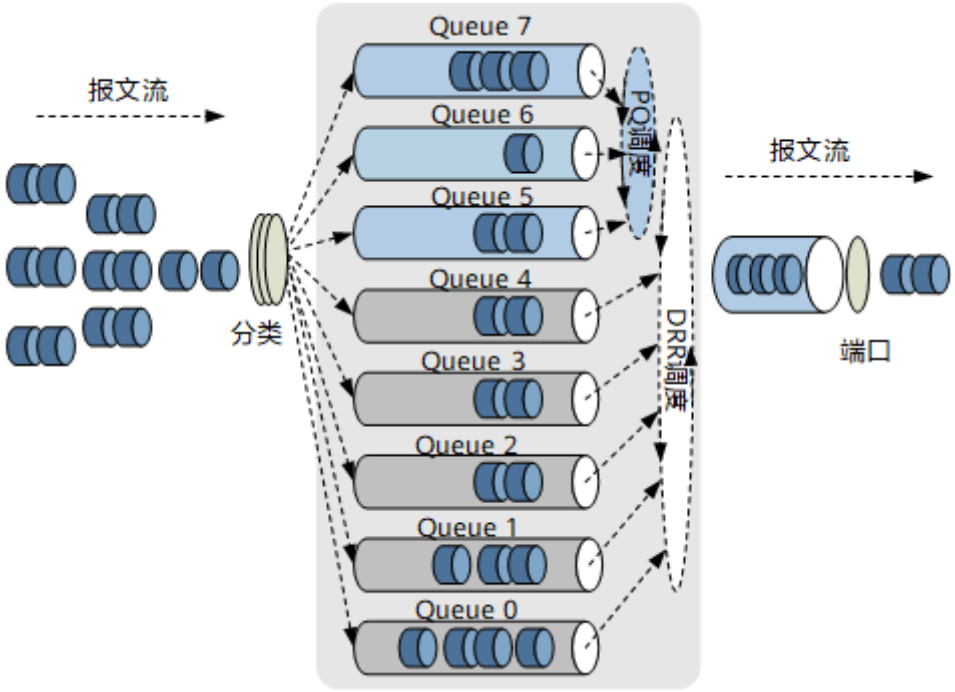
在调度时，设备首先按照PQ方式调度Queue7、Queue6、Queue5队列中的报文流，只有这些队列中的报文流全部调度完毕后，才开始以WRR方式循环调度其他队列中的报文流。Queue4、Queue3、Queue2、Queue1和Queue0队列包含自己的权值。重要的协议报文和有低延时需求的业务报文应放入采用PQ调度的队列中，得到优先调度的机会，其余报文放入以WRR方式调度的各队列中。

- PQ+WDRR调度

  与PQ+WRR相似，其集合了PQ调度和WDRR调度各有优缺点。单纯采用PQ调度时，低优先级队列中的报文流长期得不到带宽，而单纯采用WDRR调度时低延时需求业务（如语音）得不到优先调度，如果将两种调度方式结合起来形成PQ+WDRR调度，不仅能发挥两种调度的优势，而且能克服两种调度各自的缺点。

  设备接口上的8个队列被分为两组，用户可以指定其中的某几组队列进行PQ调度，其他队列进行WDRR调度。

图 5-8 PQ+WDRR 调度示意图



如图5-8所示，在调度时，设备首先按照PQ方式优先调度Queue7、Queue6和Queue5队列中的报文流，只有这些队列中的报文流全部调度完毕后，才开始以WDRR方式调度Queue4、Queue3、Queue2、Queue1和Queue0队列中的报文流。其中，Queue4、Queue3、Queue2、Queue1和Queue0队列包含自己的权值。

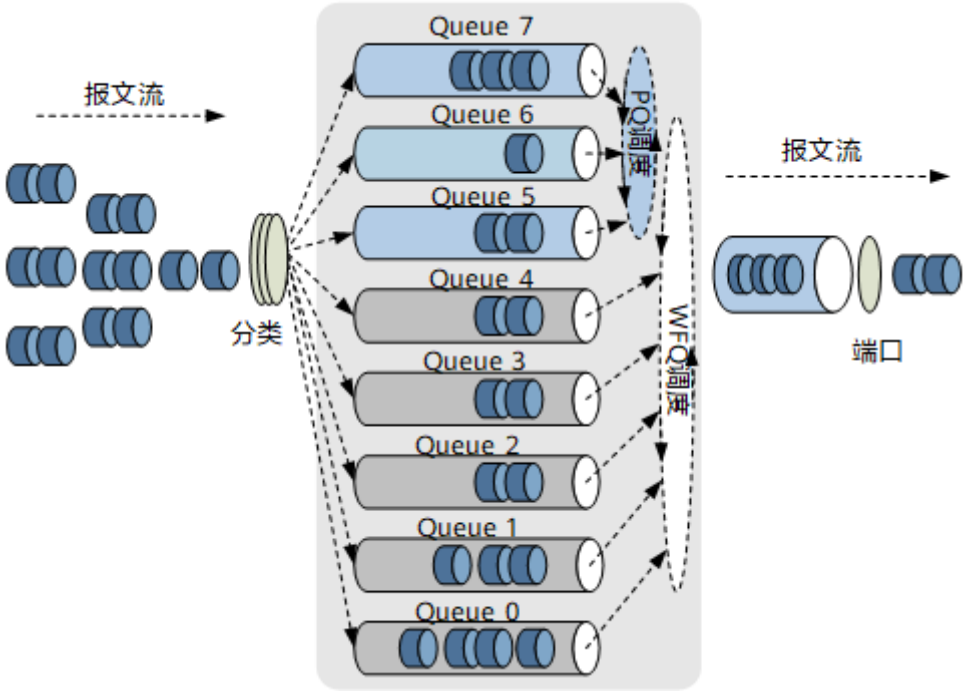
重要的协议报文以及有低延时需求的业务报文应放入需要进行PQ调度的队列中，得到优先调度的机会，其他报文放入以WDRR方式调度的各队列中。

- PQ+WFQ调度

  与PQ+WRR相似，其集合了PQ调度和WFQ调度各有优缺点。单纯采用PQ调度时，低优先级队列中的报文流长期得不到带宽，而单纯采用WFQ调度时低延时需求业务（如语音）得不到优先调度，如果将两种调度方式结合起来形成PQ+WFQ调度，不仅能发挥两种调度的优势，而且能克服两种调度各自的缺点。

  设备接口上的8个队列被分为两组，用户可以指定其中的某几组队列进行PQ调度，其他队列进行WFQ调度。

图 5-9 PQ+WFQ 调度示意图



如图5-9所示，在调度时，设备首先按照PQ方式优先调度Queue7、Queue6和Queue5队列中的报文流，只有这些队列中的报文流全部调度完毕后，才开始以WFQ方式调度Queue4、Queue3、Queue2、Queue1和Queue0队列中的报文流。其中，Queue4、Queue3、Queue2、Queue1和Queue0队列包含自己的权值。

重要的协议报文以及有低延时需求的业务报文应放入需要进行PQ调度的队列中，得到优先调度的机会，其他报文放入以WFQ方式调度的各队列中。

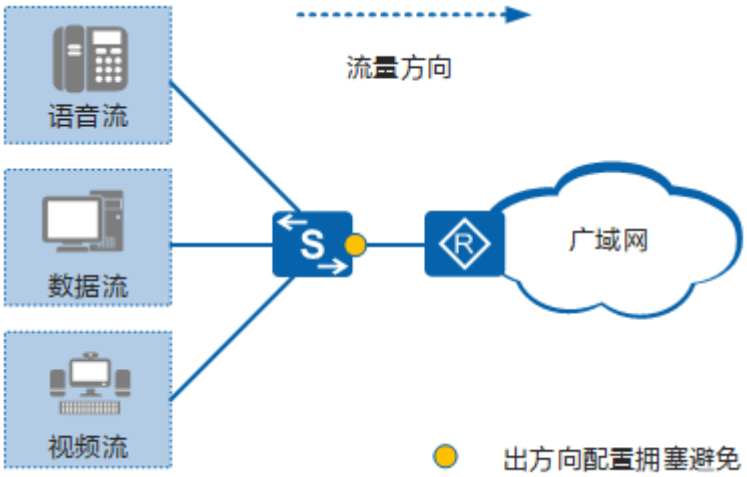
5.3 拥塞避免和拥塞管理应用场景

拥塞避免的应用

拥塞避免可以在网络产生拥塞或者拥塞加剧时，主动丢弃优先级较低的报文，调整网络流量，缓解网络压力，以保证高优先级报文正常通过。

当两个局域网用户需要通过广域网进行通信时，由于广域网带宽小于局域网的带宽，位于广域网和局域网之间的边缘交换机将发生拥塞，此时可以通过配置拥塞避免，主动丢弃优先级较低的报文（比如数据报文等），减少网络的拥塞，保证高优先级业务正常运行，如图5-10所示。

图 5-10 拥塞避免应用组网图

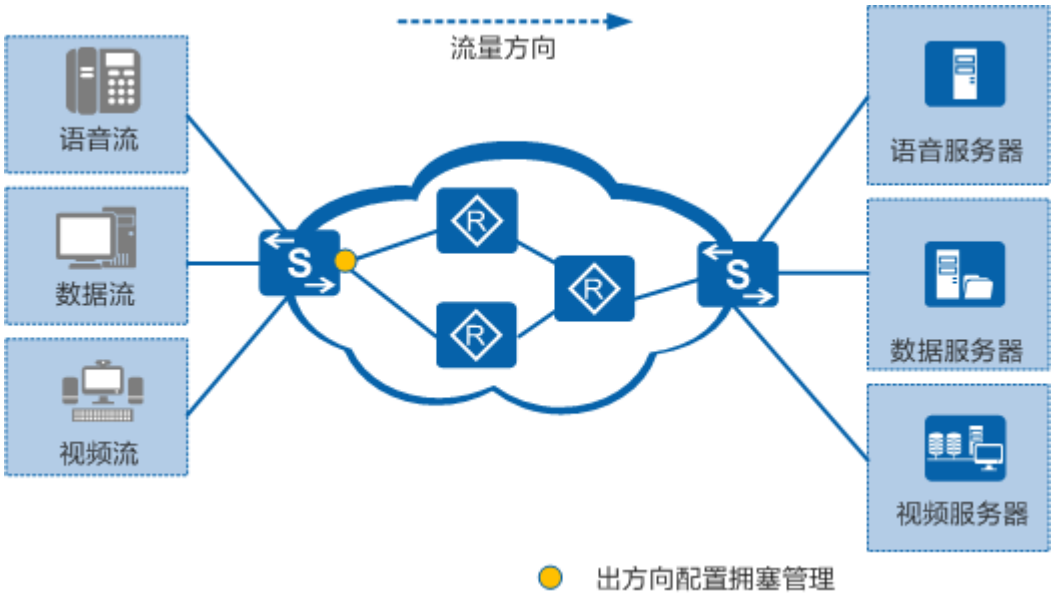


拥塞管理的应用

拥塞管理可以实现对不同的业务按照不同的优先级进行调度，在QoS方案部署中比较常用。

在网络中，当共享同一网络的多种业务竞争相同的资源（带宽，缓冲区等）时可能会产生拥塞，高优先级业务无法得到保证，此时客户可以为语音、视频和数据等多种不同业务标记不同的优先级，报文会根据不同优先级进入不同的队列，因此通过不同的队列调度算法可以实现对业务的差分服务。如图5-11所示。

图 5-11 拥塞管理应用组网图



5.4 拥塞避免和拥塞管理配置注意事项

涉及网元

无需其他网元配合。

License 支持

拥塞管理和拥塞避免是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持拥塞避免和拥塞管理。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

- 设备最多可以配置64个WRED丢弃模板。X系列单板上最多可以应用最先配置的16个WRED丢弃模板。其他单板上最多可以应用64个WRED丢弃模板。
- 交换机连接ET1D2IPS0S00、ET1D2FW00S00、ET1D2FW00S01、ET1D2FW00S02、ACU2单板的XGE接口不支持配置端口队列长度。
- 对于X1E系列单板，出现拥塞场景时报文转发会出现一定的时延。对于报文时延有较高要求的场景，请提前做好单板选型。

5.5 配置拥塞避免（WRED 丢弃模板模式）

前置任务

当网络中发生拥塞造成了报文丢弃时，可以配置基于WRED丢弃模板的拥塞避免，设备将根据配置信息对不同业务的报文（以服务等级/颜色区分）进行不同的处理，保证重要业务的利益，使之丢弃较少。

在配置拥塞避免之前，需在报文的入接口上完成以下任务：

- 将报文的优先级映射为服务等级/颜色。

5.5.1 （可选）配置端口队列长度

背景信息

通过配置端口队列的缓存大小，确保该队列有足够可用的缓冲区，可以避免报文因为不能得到缓存而丢失流量。

须知

在接口上配置端口队列缓存前需要时使用**shutdown**命令关闭接口，配置完成后，再使用**undo shutdown**命令打开接口，此操作过程可能会引起网络的短暂中断。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**shutdown**，关闭接口。

步骤4 执行命令**qos queue** *queue-index* **length** *length-value*，配置接口优先级队列的长度。

说明

ET1D2L02QSC0、ET1D2L08QSC0、ET1D2X48SEC0、ET1D2C02FEE0、SC系列和X系列单板不支持此命令。

步骤5 执行命令**undo shutdown**，重启接口。

----结束

5.5.2 （可选）配置 CFI 作为内部丢弃优先级

背景信息

VLAN Tag中的CFI（Canonical Format Indicator）字段又称为DEI（Drop Eligible Indicator），可以用来标识报文的丢弃优先级。设备在配置CFI作为内部丢弃优先级后，对超出CIR（承诺信息速率）报文的DEI位置1，标识该报文的丢弃优先级为高，后续设备在拥塞时优先丢弃DEI位为1的报文。

如果用户希望在后续处理时丢弃之前超出CIR的报文，可以使用该配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 执行命令**dei enable**，配置CFI作为内部丢弃优先级。

缺省情况下，CFI字段不作为内部丢弃优先级。

----结束

5.5.3 配置 WRED 丢弃模板

背景信息

WRED技术基于丢弃参数随机丢弃报文以避免TCP全局同步现象，它通过报文的不同颜色来指定不同的丢弃策略，考虑了高优先级报文的利益并使其被丢弃的概率相对较小。通过配置WRED丢弃模板可以配置不同颜色报文的丢弃门限百分比和最大丢弃概率。为报文区分颜色请参见**配置优先级映射**。

说明

拥塞避免只对已知单播流量生效。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**drop-profile** *drop-profile-name*，创建WRED丢弃模板，并进入WRED丢弃模板视图。

缺省情况下，系统存在一个名为**default**的WRED丢弃模板，只能修改其参数，不能删除。

步骤3 执行命令**color** { **green** | **non-tcp** | **red** | **yellow** } **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*，配置WRED参数。

缺省情况下，WRED丢弃模板的高低门限百分比以及最大丢弃概率的取值均为100。

说明

ET1D2X48SEC0、SC系列、SA系列、EE系列和X系列单板不支持针对非TCP报文的WRED算法。

步骤4 （可选）执行命令**queue-depth** *queue-depth-value*，配置端口队列的长度。

说明

仅X1E系列单板和X6H系列单板支持此命令。

----结束

5.5.4 应用 WRED 丢弃模板

背景信息

配置WRED丢弃模板后，需要在接口或端口队列上应用，WRED丢弃模板才会生效。

用户可以根据需要在接口和端口队列上同时应用WRED丢弃模板。如果同时在接口和端口队列应用了WRED丢弃模板，系统按照先端口队列后接口的顺序依次匹配报文流，然后依次对匹配WRED丢弃模板的报文流进行拥塞避免控制。

操作步骤

- 在接口上应用WRED丢弃模板
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 执行命令**qos wred** *drop-profile-name*，将WRED丢弃模板应用于接口。

  说明

  *drop-profile-name*为WRED丢弃模板名，必须与**配置WRED丢弃模板**中配置的WRED丢弃模板名相同。
- 在端口队列上应用WRED丢弃模板
  a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 执行命令**qos queue** *queue-index* **wred** *drop-profile-name*，将WRED丢弃模板应用于端口队列。

说明

*drop-profile-name*为WRED丢弃模板名，必须与**配置WRED丢弃模板**中配置的WRED丢弃模板名相同。

ET1D2X48SX2S单板上编号36～47的接口不支持该命令。

----结束

5.5.5 检查拥塞避免配置结果

操作步骤

- 执行命令**display drop-profile** [**all** | **name** *drop-profile-name*]，查看WRED丢弃模板的配置结果。
- 执行命令**display qos configuration interface** *interface-type interface-number*，查看指定接口上所有的QoS配置信息。

----结束

5.6 配置拥塞避免（WRED 队列模式）

背景信息

加权随机先期检测WRED（Weighted Random Early Detection）是一种基于丢弃参数随机丢弃报文的技术。报文进入设备时会根据DiffServ域中定义的映射关系，被着上相应的颜色，系统将根据WRED的配置信息对不同颜色的报文进行相应的处理。

若希望利用WRED对所有端口队列的不同颜色报文配置相同的门限值来避免拥塞时，可配置该功能，以便减少重复配置工作。

说明

仅ET1D2G48TX5S、ET1D2G48TX5E、ET1D2G48TX5H、ET1D2G48SX5S、ET1D2G48SX5E、ET1D2G48SX5H、ET1D2G24SX5E、ET1D2S04SX5E、ET1D2X08SX5E和ET1D2X08SX5H单板支持该功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**qos wred slot** *slot-id* **high-limit** *high-limit-percentage*，在所有端口队列上配置WRED丢弃的门限值。

说明

如果设备在配置了该功能的同时在端口队列也应用了WRED丢弃模板，则端口队列中应用的WRED丢弃模板生效。

----结束

检查配置结果

- 执行命令**display qos configuration interface** *interface-type interface-number*，查看接口上所有的QoS配置信息。
- 执行命令**display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]，查看接口上基于队列的流量统计信息。

5.7 配置拥塞管理

前置任务

在配置拥塞管理之前，需在报文的入接口上完成以下任务：

- 将报文的优先级映射为服务等级。

背景信息

当网络中发生间歇性拥塞时，可以配置拥塞管理，设备将按照指定的调度策略决定报文转发时的处理次序，以达到高优先级报文优先被调度的目的。

设备上每个接口有8个端口队列，不同的队列可以采用不同的队列调度方式，但一个队列只能使用一种队列调度方式。设备上支持的队列调度方式包括PQ、WRR和WDRR，以及PQ+WRR、PQ+WDRR混合调度。当采用混合调度时，先进行PQ调度，多个队列使用PQ调度时，按优先级高低顺序进行调度，队列索引越大，优先级越高。PQ调度完成后，再对队列进行WRR或WDRR调度。

WRR和WDRR调度都涉及权重，差别在于：WRR是按照报文个数进行调度，WDRR是按照报文字节大小进行调度。

说明

对于X5E、X5EK、X5S、X5H系列单板的GE接口，以及ET1D2X08SX5E、ET1D2X08SX5H单板的XGE接口，设备拥塞严重时会引起端口队列调度不准，甚至部分低优先级队列断流。建议配置拥塞避免，从而规避该问题。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 配置端口队列的调度方式。

1. 执行命令**qos** { **pq** | **wrr** | **drr** }，配置端口队列调度方式为PQ、WRR或WDRR。

   或执行命令**qos** { **pq** { *start-queue-index* [**to** *end-queue-index*] } &<1-8> | { **wrr** | **drr** } { *start-queue-index* [**to** *end-queue-index*] } &<1-8> } *，配置端口队列调度方式为PQ+WRR或PQ+WDRR。

   缺省情况下，端口队列采用PQ调度方式。

   说明

   X系列单板不支持WRR调度和PQ+WRR调度。

2. （可选）执行命令**qos queue** *queue-index* **wrr weight** *weight*，指定端口队列WRR调度的权值。

   缺省情况下，WRR调度方式的队列权值均为1。

只有端口队列调度方式为WRR或PQ+WRR时，才需要使用此步骤配置。

3. （可选）执行命令**qos queue** *queue-index* **drr weight** *weight*，指定端口队列WDRR调度的权值。

   缺省情况下，WDRR调度方式的队列权值均为1。

   只有端口队列调度方式为WDRR或PQ+WDRR时，才需要使用此步骤配置。

----结束

检查配置结果

- 执行命令**display qos configuration interface** [*interface-type interface-number*]，查看指定接口上所有的QoS配置信息。
- 执行命令**display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]，查看接口上基于队列的流量统计信息。

5.8 配置集群口拥塞管理

前置任务

在集群口配置拥塞管理后，设备将按照制定的调度策略决定报文转发时的处理次序，以达到高优先级报文优先被调度的目的。

在配置集群口拥塞管理之前，需要完成以下任务：

- 完成集群的配置。
- 在报文入方向接口上配置优先级映射。

背景信息

设备配置集群之后，设备的集群口之间会有集群协议报文、跨框转发报文的交互，大量的报文交互可能会导致集群口发生拥塞，导致关键业务（如视频业务、语音业务）报文不能得到及时处理，可以通过配置集群口调度模式，保证相同优先级业务得到公平处理，不同优先级业务按照各自权值处理。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**css-port qos** { **pq** | **drr** }，配置集群口队列调度模式为PQ或WDRR。

缺省情况下，端口队列的调度模式为PQ调度模式。

说明

S12700E不支持WRR调度模式。

步骤3 执行命令**css-port qos queue** *queue-index* **drr weight** *weight*，配置集群口队列的WDRR调度的权值。

当集群口队列的调度模式配置为WDRR时，用户可为每个队列配置权重，设备根据权重轮询调度各队列。如果设置某队列权值为0，说明该队列以PQ方式调度，此时整体调度模式为PQ+WDRR方式。

----结束

检查配置结果

- 执行命令**display qos configuration interface** [*interface-type interface-number*]，查看指定接口上所有的QoS配置信息。
- 执行命令**display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]，查看接口上基于队列的流量统计信息。

5.9 维护拥塞避免和拥塞管理

5.9.1 查看队列统计信息

操作步骤

- 执行命令**display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]，查看接口上基于队列的流量统计信息。

----结束

5.9.2 清除队列统计信息

背景信息

当需要对接口上基于队列的流量信息重新进行统计时，可以在用户视图下执行以下命令，清除之前的统计信息。

须知

清除接口上基于队列的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- 执行命令**reset qos queue statistics interface** *interface-type interface-number*，清除接口上基于队列的流量统计信息。

----结束

5.9.3 检测微突发流量

背景信息

微突发检测功能用于检测在极短时间内（毫秒级别）接口出方向的突发流量。通过该功能，用户可以查看微突发流量关键指标的统计信息，统计丢包情况，从而识别网络中潜在的拥塞风险。

微突发是指接口在极短时间（毫秒级别）内收到大量突发流量，以至于瞬时速率达到平均速率的数十倍、数百倍，甚至超过接口带宽的现象。当微突发流量的瞬时速率超过交换机的转发能力时，交换机会将突发的数据进行缓存以便稍后发送。如果交换机没有足够的缓存，那么超出的数据只能丢弃，这就产生了拥塞丢包。在发生接口出方向拥塞丢包后，传统的问题定位方法较为困难和繁琐，通常是抓取出方向报文，提取

流量趋势，从而找到突发流量的特征。为此，维护人员可以使用微突发检测功能，确认是否是微突发引起丢包。通过检测微突发流量，既可以在拥塞发生前识别潜在的拥塞风险，也可以在拥塞发生后快速定位异常流量。

微突发检测支持两种模式：

- 默认模式：报文的采样周期为5毫秒，支持多个接口同时使能微突发检测功能。
- 增强模式：报文的采样周期为1毫秒，仅支持一个接口使能微突发检测功能。

微突发检测的统计周期为5分钟，每5分钟统计一次接口的关键性能指标，并生成相关表项。设备最多支持保存使能微突发检测功能后最近300分钟内的统计数据。微突发检测的关键性能指标包括：

- 从设备的其他接口转发到本接口的突发流量平均速率。
- 从设备的其他接口转发到本接口的突发流量峰值速率。
- 接口丢弃报文的数量。
- 接口平均缓存占用量。
- 接口缓存占用峰值。
- 接口缓存达到检查周期内的峰值时，接口队列的缓存占用情况。

说明

仅X系列单板支持微突发流量检测功能。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**qos micro-burst detection** [**enhanced**] **enable slot** *slot-id*，使能全局的微突发检测功能。

缺省情况下，单板未使能微突发检测功能。

步骤3 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤4 执行命令**qos micro-burst detection enable**，使能接口的微突发检测功能。

缺省情况下，接口未使能微突发检测功能。

步骤5 执行命令**quit**，返回系统视图。

----结束

后续处理

执行以下命令，查看微突发检测的统计数据：

- 执行命令**display qos micro-burst peak-buffer verbose interface** *interface-type interface-number*，查看接口的缓存峰值和接口队列的缓存占用情况。
- 执行命令**display qos micro-burst statistics interface** *interface-type interface-number*，查看接口的微突发检测关键统计数据，包括接口的突发流量平均速率、突发流量最大速率、丢包计数、平均缓存占用、最大缓存占用和表项的记录时间。
- 执行命令**display qos micro-burst status all** [**slot** *slot-id*]，查看所有使能微突发检测的接口及接口的丢包情况。

可以通过如下几种方法，来降低微突发的发生，缓解微突发的影响：

- 针对传统TCP拥塞控制机制中存在的突发严重、过度消耗网络交换机缓存、有损线路上性能不佳、延时抖动大等问题，采用业界常用的改进技术，确保服务器不会过度、过快、突发过强地发包，从根源上减少微突发。
- 在网络业务流量规划时，尽量避免多打一场景，避免收敛比过高的场景，及时扩容突发严重的出端口，消除突发瓶颈。
- 在转发设备发生拥塞时，可以在发生拥塞的接口下执行**qos burst-mode** { **enhanced** | **extreme** }命令配置接口下缓存管理的突发模式为增强模式，以尝试缓解网络拥塞。
- 在延时可控和缓存充足的情况下，在发生拥塞的转发设备的上游交换机下行接口通过**qos queue** *queue-index* **shaping cir** *cir-value* **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]命令开启流量整形功能，削弱流量的瞬时波峰，可以控制突发的程度。需要注意的是，此方案会导致报文转发时延加大。

5.10 配置拥塞避免和拥塞管理综合示例

组网需求

Switch通过接口GE2/0/1与Router互连，来自Internet的业务有语音、视频、数据，携带的802.1p优先级分别为6、5、2，这些业务可经由Router和Switch到达用户，如图5-12所示。由于Switch入接口GE2/0/1的速率大于出接口GE1/0/1、GE1/0/2的速率，在这两个出接口处可能会发生拥塞。

为了减轻网络拥塞造成的影响，保证用户对于高优先级、低延迟业务的服务要求，配置需求如表5-2和表5-3所述。

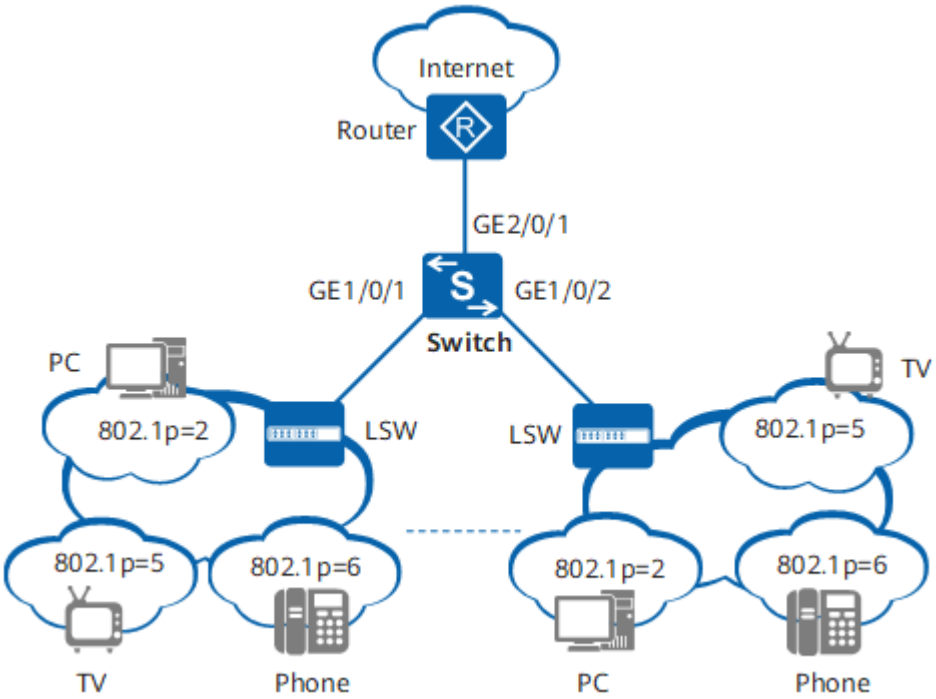
表 5-2 拥塞避免配置参数

业务类型	颜色	阈值下限（%）	阈值上限（%）	丢弃概率
语音	绿	80	100	10
视频	黄	60	80	20
数据	红	40	60	40

表 5-3 拥塞管理配置参数

业务类型	服务等级
语音	EF
视频	AF3
数据	AF1

图 5-12 拥塞避免和拥塞管理配置组网图



配置思路

采用如下的思路配置：

1. 配置各接口所属的VLAN，实现各设备间链路互通。
2. 在Switch上创建并配置DiffServ域，将802.1p优先级映射为PHB行为并着色，并在Switch入接口上绑定DiffServ域。
3. 在Switch上配置WRED模板，并在出接口应用WRED模板。
4. 在Switch出接口上配置各服务等级队列的调度参数。

操作步骤

步骤1 配置各接口所属的VLAN，使各设备间链路互通。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 2 5 6
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 2 5 6
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 2 5 6
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 2 5 6
[Switch-GigabitEthernet2/0/1] quit
```

步骤2 配置基于简单流分类的优先级映射

创建DiffServ域ds1，将802.1p优先级6、5、2分别映射为PHB行为EF、AF3、AF1，并分别将颜色标记为绿色、黄色、红色。

```
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 6 phb ef green
[Switch-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow
[Switch-dsdomain-ds1] 8021p-inbound 2 phb af1 red
[Switch-dsdomain-ds1] quit
```

在Switch入接口GE2/0/1上绑定DiffServ域。

```
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] trust upstream ds1
[Switch-GigabitEthernet2/0/1] trust 8021p inner
[Switch-GigabitEthernet2/0/1] quit
```

步骤3 配置拥塞避免

在Switch上创建WRED模板wred1，并配置wred1的三色报文参数。

```
[Switch] drop-profile wred1
[Switch-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[Switch-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[Switch-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[Switch-drop-wred1] quit
```

在Switch出接口GE1/0/1、GE1/0/2上应用WRED模板wred1。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos wred wred1
[Switch-GigabitEthernet1/0/1] qos queue 5 wred wred1
[Switch-GigabitEthernet1/0/1] qos queue 3 wred wred1
[Switch-GigabitEthernet1/0/1] qos queue 1 wred wred1
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos wred wred1
[Switch-GigabitEthernet1/0/2] qos queue 5 wred wred1
[Switch-GigabitEthernet1/0/2] qos queue 3 wred wred1
[Switch-GigabitEthernet1/0/2] qos queue 1 wred wred1
[Switch-GigabitEthernet1/0/2] quit
```

步骤4 配置拥塞管理

在Switch的报文出接口GE1/0/1、GE1/0/2上配置各服务等级队列的调度参数。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos pq 5
[Switch-GigabitEthernet1/0/1] qos drr 0 to 4
[Switch-GigabitEthernet1/0/1] qos queue 3 drr weight 100
[Switch-GigabitEthernet1/0/1] qos queue 1 drr weight 50
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos pq 5
[Switch-GigabitEthernet1/0/2] qos drr 0 to 4
[Switch-GigabitEthernet1/0/2] qos queue 3 drr weight 100
[Switch-GigabitEthernet1/0/2] qos queue 1 drr weight 50
[Switch-GigabitEthernet1/0/2] quit
```

步骤5 验证配置结果

查看DiffServ域ds1的配置信息。

```
[Switch] display diffserv domain name ds1
diffserv domain name:ds1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 green
 8021p-inbound 2 phb af1 red
 8021p-inbound 3 phb af3 green
 8021p-inbound 4 phb af4 green
```



```
 8021p-inbound 5 phb af3 yellow
 8021p-inbound 6 phb ef green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
......
```

查看WRED模板配置信息。

```
[Switch] display drop-profile name wred1
Drop-profile[1]: wred1
Queue depth    : default
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
Non-tcp   100         100         100
------------------------------------------------------------------
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 2 5 to 6
#
diffserv domain ds1
 8021p-inbound 2 phb af1 red
 8021p-inbound 5 phb af3 yellow
 8021p-inbound 6 phb ef green
#
drop-profile wred1
 color green low-limit 80 high-limit 100 discard-percentage 10
 color yellow low-limit 60 high-limit 80 discard-percentage 20
 color red low-limit 40 high-limit 60 discard-percentage 40
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 5 to 6
 qos wred wred1
 qos pq 5 to 7 drr 0 to 4
 qos queue 1 drr weight 50
 qos queue 3 drr weight 100
 qos queue 1 wred wred1
 qos queue 3 wred wred1
 qos queue 5 wred wred1
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 5 to 6
 qos wred wred1
 qos pq 5 to 7 drr 0 to 4
 qos queue 1 drr weight 50
 qos queue 3 drr weight 100
 qos queue 1 wred wred1
 qos queue 3 wred wred1
 qos queue 5 wred wred1
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 5 to 6
 trust upstream ds1
 trust 8021p inner
#
return
```


5.11 拥塞避免和拥塞管理 FAQ

5.11.1 为什么在接口上配置了 PQ+WDRR 调度后不生效

配置队列调度之前，首先要保证不同的业务进入不同的队列，只有在业务进入要求的队列后才能实现期望的调度。

业务报文进入不同队列的方法有两种： 一是在上行设备上修改报文的8021p；二是在交换机入端口配置流策略，并使用**remark local-precedence**命令配置报文优先级队列。

6 报文过滤配置

6.1 报文过滤简介

网络中存在大量不信任报文，所谓的不信任报文是指对用户来说存在安全隐患或者不愿意接收的报文，部署报文过滤可以将这类报文直接丢弃，以提高用户在网络中的安全性。

当用户认为某类报文不可信时，可以通过MQC将这类报文与其他报文区别出来并进行丢弃；同样的，当用户认为某类报文可信时，也可以通过MQC将这类报文与其他报文区别出来并允许通过。

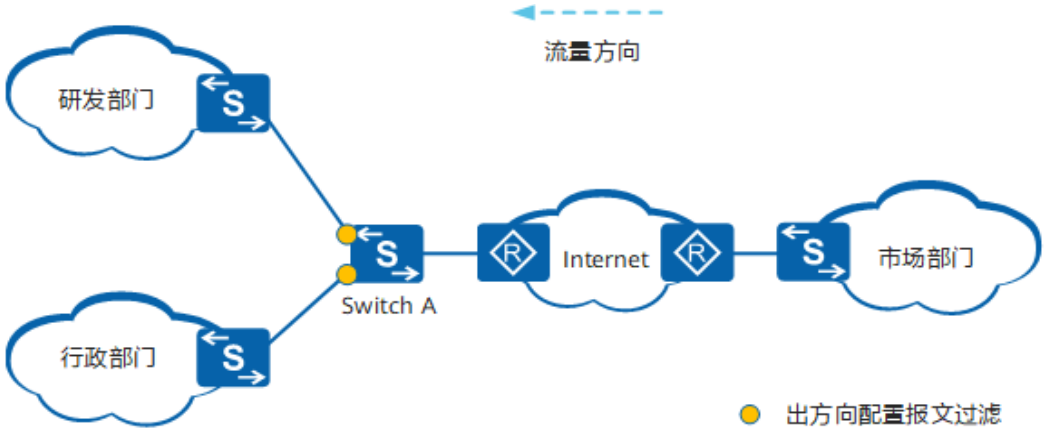
与黑名单相比，通过MQC实现报文过滤可以对报文进行更精细的划分，在网络部署时更加灵活。

6.2 报文过滤应用场景

部署报文过滤可以丢弃用户的不信任报文并允许信任的报文通过，以提高网络安全性并使网络规划更加灵活。

如**图6-1**所示，为了保证企业研发部门、行政部门以及市场部门之间信息的安全性，公司规定研发部门、行政部门不能与市场部门互访。

图 6-1 报文过滤应用组网图



6.3 报文过滤配置注意事项

涉及网元

无需其他网元配合。

License 支持

报文过滤是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持报文过滤。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

- 流行为中，**permit**动作和其他流动作一起配置时，将依次执行这些动作；**deny**动作和其他流动作互斥，即使配置其它动作也不会生效（流量统计和流镜像除外）。
- 为匹配ACL规则的报文指定报文过滤动作时，如果此ACL中的rule规则配置为**permit**，则设备对此报文采取的动作由流行为中配置的**deny**或**permit**决定；如果此ACL中的rule规则配置为**deny**，则无论流行为中配置了**deny**或**permit**，此报文都被丢弃。为匹配ACL规则的报文指定其他非报文过滤动作时，如果此ACL中的rule规则配置为**deny**，则报文被丢弃且流行为动作不生效（MAC地址不学习、流量统计和流镜像除外）。

6.4 配置报文过滤

背景信息

配置报文过滤后，设备将对符合流分类规则的报文进行过滤，从而实现对网络流量的控制。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，创建一个流分类并进入流分类视图，或进入已存在的流分类视图。

      and表示流分类中各规则之间关系为逻辑“与”，指定该逻辑关系后：

      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

      or表示流分类各规则之间是逻辑“或”，即报文只需匹配流分类中的一个或多个规则即属于该类。

      缺省情况下，流分类中各规则之间的关系为逻辑“或”。
   c. 请根据实际情况定义流分类中的匹配规则。

      说明

      if-match ip-precedence和**if-match tcp**命令仅对IPv4报文生效。

      X系列单板不支持配置包含高级ACL中的**ttl-expired**字段的流分类规则。

      当流分类匹配**if-match ipv6 acl** { *acl-number* | *acl-name* }时，X系列单板不支持**add-tag vlan-id** *vlan-id*、**remark 8021p** [*8021p-value* | **inner-8021p**]、**remark cvlan-id** *cvlan-id*、**remark vlan-id** *vlan-id*、**mac-address learning disable**。

匹配规则	命令	说明
外层VLAN ID或基于QinQ报文内外两层Tag的VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]	-
QinQ报文内外层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**vlan-id** *vlan-id*]	-

匹配规则	命令	说明
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个802.1p值，报文只需匹配其中一个802.1p值就匹配该规则。
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>	-
丢弃报文	**if-match discard**	包含该流分类的报文只能与流量统计和流镜像两种动作绑定。
QinQ报文双层Tag	**if-match double-tag**	-
MPLS报文EXP优先级	**if-match mpls-exp** *exp-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个MPLS EXP值，报文只需匹配其中一个MPLS EXP值就属于该类。
目的MAC地址	**if-match destination-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
源MAC地址	**if-match source-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }	-
所有报文	**if-match any**	-
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个DSCP值，报文只需匹配其中一个DSCP值就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。

匹配规则	命令	说明
IP报文的IP优先级	**if-match ip-precedence** *ip-precedence-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个IP优先级，报文只需匹配其中一个IP优先级就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }	-
IPv6下一报文头类型	**if-match ipv6 next-header** *header-number* **first-next-header**	ET1D2X12SSA0单板不支持Prefix的长度为(64,128)之间的路由。
TCP报文SYN Flag	**if-match tcp syn-flag** { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	-
入接口	**if-match inbound-interface** *interface-type interface-number*	包含该流分类的流策略不能应用在出方向。 包含该流分类的流策略不能应用在接口视图。
出接口	**if-match outbound-interface** *interface-type interface-number*	X系列单板不支持将包含该流分类的流策略应用在入方向。 包含该流分类的流策略不能应用在接口视图。
ACL规则	**if-match acl** { *acl-number* | *acl-name* }	• 使用ACL作为流分类规则，请先配置相应的ACL规则。 • 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果某ACL规则中有多个rule，报文只需匹配其中一个rule就匹配该ACL规则。 • 如果ACL的规则指定了参数**vpn-instance**，那么基于该ACL进行分类的流分类对应的流策略将不生效。

匹配规则	命令	说明
ACL6规则	**if-match ipv6 acl** { *acl-number* | *acl-name* }	使用ACL6作为流分类规则，请先配置相应的ACL6规则。 如果ACL6的规则指定了参数**vpn-instance**，那么基于该ACL6进行分类的流分类对应的流策略将不生效。
流ID	**if-match flow-id** *flow-id*	包含**if-match flow-id**匹配规则的流分类和包含**remark flow-id**动作的流行为应在不同的流策略中使用。 包含**if-match flow-id**匹配规则的流策略只能应用在接口、VLAN、VLANIF接口、单板、全局的入方向。 SA系列单板不支持配置匹配流ID。
VXLAN内层报文信息	**if-match vxlan** [**transit**] **vni** *vni-id*	包含该流分类的流策略不能应用在出方向上。 当流分类中包含此匹配规则时，流行为只支持流量监管、报文过滤和流量统计。

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

a. 执行命令**traffic behavior** *behavior-name*，创建一个流行为并进入流行为视图，或进入已存在的流行为视图。

b. 请根据实际需要进行如下配置：

- 执行命令**permit**，对符合流分类的报文不做任何动作，按原来的策略转发。
- 执行命令**deny**，禁止符合流分类规则的报文通过。

说明

- 流行为中，**permit**动作和其他流动作一起配置时，将依次执行这些动作；**deny**动作和其他流动作互斥，即使配置其它动作也不会生效（流量统计和流镜像除外）。
- 为匹配ACL规则的报文指定报文过滤动作时，如果此ACL中的rule规则配置为**permit**，则设备对此报文采取的动作由流行为中配置的**deny**或**permit**决定；如果此ACL中的rule规则配置为**deny**，则无论流行为中配置了**deny**或**permit**，此报文都被丢弃。
- 如果包含**deny**动作的流策略应用到出方向，则会导致由CPU发送的ICMP、OSPF、BGP、RIP、SNMP、Telnet等协议控制报文被丢弃，相关协议的功能会受到影响。

c. （可选）执行命令**statistic enable**，使能流量统计功能。

d. 执行命令**quit**，退出流行为视图。

e. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name* [**match-order** { **auto** | **config** }] [**atomic**]，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。创建流策略时，如果未指定规则匹配顺序，缺省规则匹配顺序为**config**。

应用流策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先清除该策略的应用，再重新创建并指定所需的匹配顺序。

设备支持在创建流策略时指定流策略中多个规则的匹配顺序，匹配顺序包括自动顺序（**auto**）和配置顺序（**config**）两种：

- 如果选择自动顺序，匹配顺序由系统预先指定的流分类类型的优先级决定，该优先级由高到低依次为：基于二层和IPv4三层信息流分类 > 基于高级ACL6规则流分类 > 基于基本ACL6规则流分类 > 基于二层信息流分类 > 基于IPv4三层信息流分类 > 基于用户自定义ACL规则流分类。规则优先匹配优先级高的流分类。当某一数据流量同时匹配不同流分类，且对应的流行为存在冲突时，只有流行为优先级高的规则生效。
- 如果选择配置顺序，匹配顺序由流分类规则的优先级决定，先匹配优先级较高的流分类规则。配置流分类时指定优先级，则数值越小，优先级越高；如果配置流分类时未指定precedence-value，则缺省优先级为0。关于流分类优先级的详细说明，请参见**traffic classifier**。

c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

– 在接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。

说明

- 仅E系列、X系列和S系列中的SC单板支持配置以太网子接口。单板详情请参见《硬件描述》中的单板分类。
- 对于上述系列单板的二层接口，仅hybrid和trunk类型接口支持配置二层以太网子接口。
- 对于上述系列单板的二层接口，执行命令**undo portswitch**切换为三层接口后，支持配置三层以太网子接口。
- S系列中的SA单板不支持创建以太网子接口，也不支持转发IP流量到其它单板的以太网子接口。
- 建议用户先将成员接口加入Eth-Trunk后，再配置Eth-Trunk子接口。只有当成员接口所在的单板系列均支持配置以太网子接口时，Eth-Trunk子接口才能配置成功。
- VCMP的角色是Client时，不能配置VLAN终结子接口。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口或子接口视图上应用流策略。

每个接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同接口的不同方向。应用后，系统对流经该接口并匹配流分类中规则的入方向或出方向报文实施策略控制。

说明

- 子接口仅支持**inbound**参数。
- 建议不要在Untagged类型接口出方向上应用包含有**remark 8021p**、**remark cvlan-id**、**remark vlan-id**等动作的流策略，否则，可能导致报文内容出错。
- ET1D2X12SSA0、ET1D2X48SEC0、SC系列单板有2N个接口，如果1～N号中的接口与N+1～2N号中的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的2倍。
- 在X系列单板中，如果不同的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，且这些接口的ACL资源分散在N个组中进行统计（执行命令**display acl resource**查看），那么Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的N倍。
- 应用流策略需要设备有足够的ACL资源，否则会导致应用失败。以一个流策略中的if-match占用一条ACL为例，同一个流策略应用到M个接口时，将占用M条ACL资源；应用到L个VLAN且设备上存在N块接口板时，将占用L*N条ACL规则；应用到全局且设备上存在N块接口板时，将占用N条ACL规则。if-match规则占用ACL资源的情况参考“MQC配置-配置注意事项”中的表3。
- 配置Tunnel接口的隧道协议为GRE后，可在Tunnel接口入方向应用流策略。
- 在VXLAN二层子接口、Dot1q终结子接口和绑定了BGP AD方式的子接口下，应用流策略不生效，建议在主接口配置基于流ID的分类方式。

– 在VLAN上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**vlan** *vlan-id*，进入VLAN视图。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLAN上应用流策略。

每个VLAN的每个方向能且只能应用一个流策略。

应用后，系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施策略控制。但是流策略对VLAN 0的报文不生效。

– 在VLANIF接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLANIF接口上应用流策略。

每个VLANIF接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同VLANIF接口的不同方向。

对于应用流策略的VLANIF接口，其对应的VLAN不能是Super-VLAN或MUX VLAN。

对于X系列单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文生效。对于其它单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文及三层组播报文生效。

说明

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的入方向上应用该流策略：

- **remark vlan-id**
- **remark cvlan-id**
- **add-tag vlan-id**
- **remark 8021p**
- **remark flow-id**
- **mac-address learning disable**

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的出方向上应用该流策略：

- **add-tag vlan-id**
- **remark flow-id**
- **mac-address learning disable**

– 在全局或单板上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**traffic-policy** *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]，在全局或单板上应用流策略。

全局或单板的每个方向上能且只能应用一个流策略，如果在全局某方向应用了流策略，则不能在单板的该方向上再次应用流策略；指定单板在某方向应用流策略后，也不能在全局的该方向上再次应用流策略。

– 在SSID模板上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**wlan**，进入WLAN视图。

iii. 执行命令**ssid-profile name** *profile-name*，创建SSID模板并进入模板视图。

iv. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在SSID模板上应用流策略。

– 在AP组上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**wlan**，进入WLAN视图。

iii. 执行命令**ap-group name** *group-name*，创建AP组并进入AP组视图。

iv. 执行命令**traffic-policy** *policy-name* **outbound**，在AP组上应用流策略。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior user-defined** [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看用户定义的流策略的配置信息。

- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

  说明

  流策略可以应用到子接口上，但暂不支持通过此命令查看子接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

- 执行命令**display traffic policy** { **interface** [*interface-type interface-number*[*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]，查看已配置的流策略信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

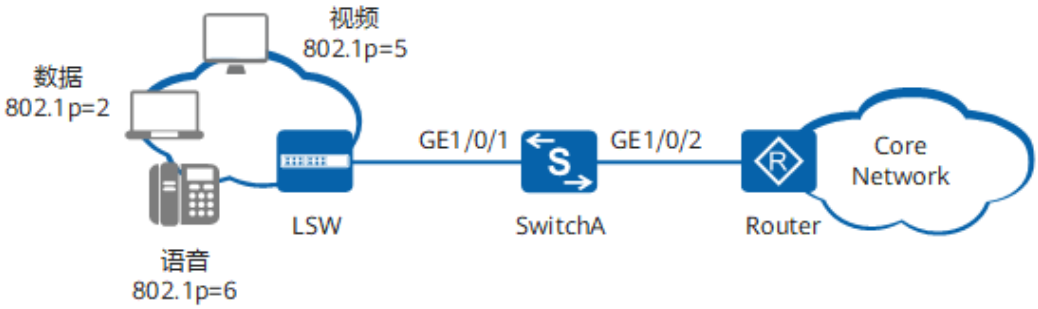
6.5 配置报文过滤示例

组网需求

如图6-2所示，用户通过SwitchA的接口GE1/0/2连接到外部网络设备。

不同业务的报文在LSW侧使用802.1p优先级进行标识，当报文从接口GE1/0/2到达外部网络时，用户希望能够对数据业务报文进行过滤，优先保证语音和视频业务的业务体验。

图 6-2 配置报文过滤组网图



配置思路

采用包含禁止动作的流策略方式实现报文过滤，具体配置思路如下：

1. 配置各接口，实现用户能通过SwitchA访问外部网络。
2. 配置流分类，实现基于802.1p优先级对报文进行分类。
3. 配置流行为，实现对满足规则的报文进行禁止或允许动作。
4. 配置流策略，绑定上述流分类和流行为，并应用到接口GE1/0/1的入方向，实现报文过滤。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN10。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

配置SwitchA上接口GE1/0/1和GE1/0/2为Trunk类型接口，并加入VLAN10。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet1/0/2] quit
```

说明

请配置LSW与SwitchA对接的接口为Trunk类型，并加入VLAN10。

创建VLANIF10，并为VLANIF10配置IP地址192.168.2.1/24。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 192.168.2.1 24
[SwitchA-Vlanif10] quit
```

说明

请配置Router与SwitchA对接的接口IP地址为192.168.2.2/24。

步骤2 配置流分类

在SwitchA上创建并配置流分类c1、c2、c3，对报文按照802.1p优先级进行分类。

```
[SwitchA] traffic classifier c1
[SwitchA-classifier-c1] if-match 8021p 2
[SwitchA-classifier-c1] quit
[SwitchA] traffic classifier c2
[SwitchA-classifier-c2] if-match 8021p 5
[SwitchA-classifier-c2] quit
[SwitchA] traffic classifier c3
[SwitchA-classifier-c3] if-match 8021p 6
[SwitchA-classifier-c3] quit
```

步骤3 配置流行为

在SwitchA上创建流行为b1，并配置禁止动作。

```
[SwitchA] traffic behavior b1
[SwitchA-behavior-b1] deny
[SwitchA-behavior-b1] quit
```

在SwitchA上创建流行为b2和b3，并配置允许动作。

```
[SwitchA] traffic behavior b2
[SwitchA-behavior-b2] permit
[SwitchA-behavior-b2] quit
[SwitchA] traffic behavior b3
[SwitchA-behavior-b3] permit
[SwitchA-behavior-b3] quit
```

步骤4 配置流策略并应用到接口上

在SwitchA上创建流策略p1，将流分类和对应的流行为进行绑定并将流策略应用到接口GE1/0/1的入方向上，对报文进行过滤。

```
[SwitchA] traffic policy p1
[SwitchA-trafficpolicy-p1] classifier c1 behavior b1
[SwitchA-trafficpolicy-p1] classifier c2 behavior b2
[SwitchA-trafficpolicy-p1] classifier c3 behavior b3
[SwitchA-trafficpolicy-p1] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] traffic-policy p1 inbound
[SwitchA-GigabitEthernet1/0/1] quit
```

步骤5 验证配置结果

查看流分类的配置信息。

```
[SwitchA] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Precedence: 10
    Operator: OR
    Rule(s) : if-match 8021p 5

   Classifier: c3
    Precedence: 15
    Operator: OR
    Rule(s) : if-match 8021p 6

   Classifier: c1
    Precedence: 5
    Operator: OR
    Rule(s) : if-match 8021p 2

Total classifier number is 3
```

查看流策略的应用信息。

```
[SwitchA] display traffic-policy applied-record p1
----------------------------------------------------
  Policy Name:   p1
  Policy Index:  0
     Classifier:c1     Behavior:b1
     Classifier:c2     Behavior:b2
     Classifier:c3     Behavior:b3
----------------------------------------------------
 *interface GigabitEthernet1/0/1
    traffic-policy p1 inbound
      slot 1    :  success
----------------------------------------------------
  Policy total applied times: 1.
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
traffic classifier c1 operator or precedence 5
 if-match 8021p 2
traffic classifier c2 operator or precedence 10
 if-match 8021p 5
traffic classifier c3 operator or precedence 15
 if-match 8021p 6
#
```



```
traffic behavior b1
 deny
traffic behavior b2
 permit
traffic behavior b3
 permit
#
traffic policy p1 match-order config
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface Vlanif10
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy p1 inbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```


7 重定向配置

7.1 重定向简介

重定向就是将符合流分类的报文流重定向到其他地方进行处理。

目前支持的重定向包括以下几种：

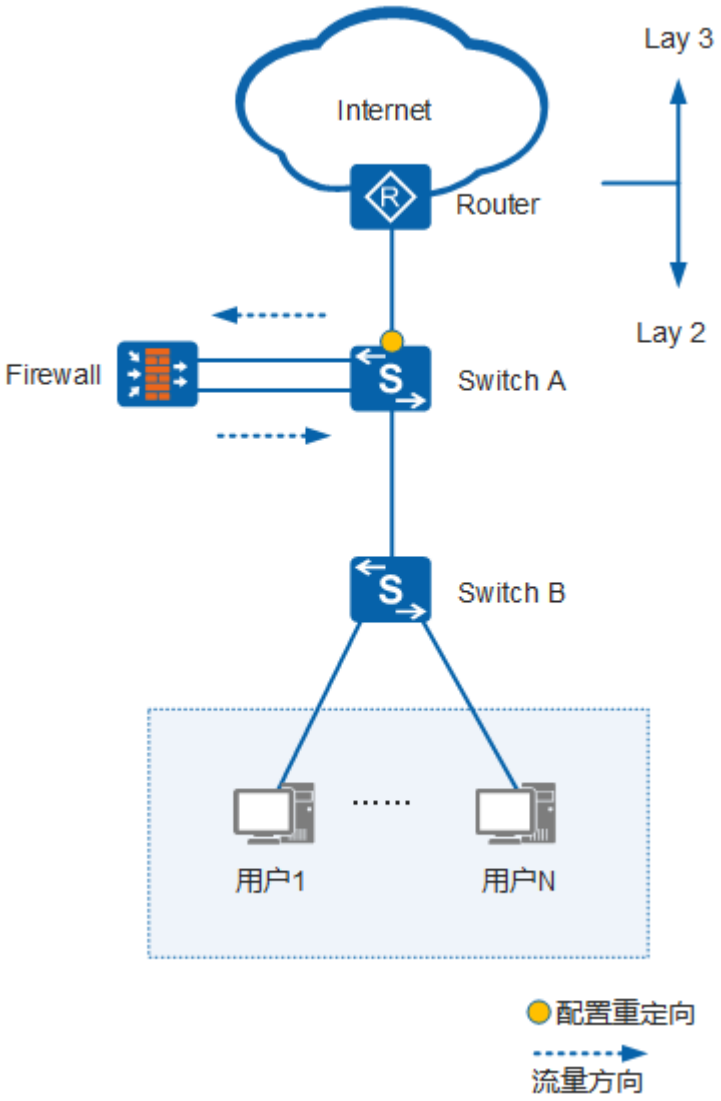
- 重定向到CPU：对于需要CPU处理的报文，可以通过此配置上送给CPU。
- 重定向到接口：对于收到需要由某个端口处理的报文，或者需要将报文通过某接口发送到指定设备处理时，可以配置重定向到此接口。
- 重定向到下一跳：对于收到需要某台下游设备处理的报文时，可以通过配置重定向到该下游设备，针对三层报文转发。该方式可以用于实现策略路由，有关策略路由的介绍，请参见《 S12700, S12700E V200R023C00 配置指南-IP单播路由 》策略路由配置。

7.2 重定向应用场景

组网需求

如**图7-1**所示，用户的业务流量经过SwitchA、SwitchB访问互联网，防火墙旁挂于SwitchA。出于网络安全考虑，用户希望对来自网络侧的流量进行验证。

图 7-1 重定向应用组网图



业务部署

- 配置流分类，匹配规则为所有报文。
- 配置流行为，将匹配的流量重定向到防火墙进行验证。
- 配置流策略，绑定以上流分类和流行为，并应用在SwitchA的入方向，实现将所有来自Internet的流量重定向到防火墙进行验证。

7.3 重定向配置注意事项

涉及网元

无需其他网元配合。

License 支持

重定向是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持重定向。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

- 包含重定向动作的流策略只能在入方向上应用。
- 对于V200R006及之前版本的设备，将流量重定向到接口之后，如果此接口Down了，就在此接口丢包，流量不会切换到原转发路径。
- 对于V200R007及后续版本的设备，将流量重定向到接口之后，如果此接口Down了，若配置了**forced**参数，则在此接口丢包，流量不会切换到原转发路径；若没有配置**forced**参数，则流量切换到原转发路径。
- 二层协议报文的透传也可以通过流策略的重定向到指定接口或者重定向到一个或多个Eth-Trunk来实现。但X系列单板不支持通过流策略重定向BPDU报文，因此，这些单板上只能通过BPDU隧道实现BPDU报文的透传。
- 交换机连接ET1D2IPS0S00、ET1D2FW00S00、ET1D2FW00S01、ET1D2FW00S02、ACU2单板的XGE接口不支持配置重定向到多个Eth-Trunk。

7.4 配置重定向

背景信息

通过配置重定向，设备将符合流分类规则的报文重定向到CPU、LSP、指定接口或VPN实例。

包含重定向动作的流策略只能在全局、单板、接口或VLAN的入方向上应用。

说明

如果流行为配置**redirect interface**时，建议只对二层数据流量应用包含此行为的流策略。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，创建一个流分类并进入流分类视图，或进入已存在的流分类视图。

      and表示流分类中各规则之间关系为逻辑“与”，指定该逻辑关系后：

      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

      or表示流分类各规则之间是逻辑“或”，即报文只需匹配流分类中的一个或多个规则即属于该类。

缺省情况下，流分类中各规则之间的关系为逻辑“或”。

c. 请根据实际情况定义流分类中的匹配规则。

说明

if-match ip-precedence和**if-match tcp**命令仅对IPv4报文生效。

X系列单板不支持配置包含高级ACL中的**ttl-expired**字段的流分类规则。

当流分类匹配**if-match ipv6 acl** { *acl-number* | *acl-name* }时，X系列单板不支持**add-tag vlan-id** *vlan-id*、**remark 8021p** [*8021p-value* | **inner-8021p**]、**remark cvlan-id** *cvlan-id*、**remark vlan-id** *vlan-id*、**mac-address learning disable**。

匹配规则	命令	说明
外层VLAN ID或基于QinQ报文内外两层Tag的VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]	-
QinQ报文内外层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**vlan-id** *vlan-id*]	-
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个802.1p值，报文只需匹配其中一个802.1p值就匹配该规则。
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>	-
丢弃报文	**if-match discard**	包含该流分类的报文只能与流量统计和流镜像两种动作绑定。
QinQ报文双层Tag	**if-match double-tag**	-
MPLS报文EXP优先级	**if-match mpls-exp** *exp-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个MPLS EXP值，报文只需匹配其中一个MPLS EXP值就属于该类。
目的MAC地址	**if-match destination-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
源MAC地址	**if-match source-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-

匹配规则	命令	说明
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }	-
所有报文	**if-match any**	-
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个DSCP值，报文只需匹配其中一个DSCP值就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
IP报文的IP优先级	**if-match ip-precedence** *ip-precedence-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个IP优先级，报文只需匹配其中一个IP优先级就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }	-
IPv6下一报文头类型	**if-match ipv6 next-header** *header-number* **first-next-header**	ET1D2X12SSA0单板不支持Prefix的长度为(64,128)之间的路由。
TCP报文SYN Flag	**if-match tcp syn-flag** { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	-
入接口	**if-match inbound-interface** *interface-type interface-number*	包含该流分类的流策略不能应用在出方向。 包含该流分类的流策略不能应用在接口视图。
出接口	**if-match outbound-interface** *interface-type interface-number*	X系列单板不支持将包含该流分类的流策略应用在入方向。 包含该流分类的流策略不能应用在接口视图。

匹配规则	命令	说明
ACL规则	**if-match acl** { *acl-number* | *acl-name* }	• 使用ACL作为流分类规则，请先配置相应的ACL规则。 • 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果某ACL规则中有多个rule，报文只需匹配其中一个rule就匹配该ACL规则。 • 如果ACL的规则指定了参数**vpn-instance**，那么基于该ACL进行分类的流分类对应的流策略将不生效。
ACL6规则	**if-match ipv6 acl** { *acl-number* | *acl-name* }	使用ACL6作为流分类规则，请先配置相应的ACL6规则。 如果ACL6的规则指定了参数**vpn-instance**，那么基于该ACL6进行分类的流分类对应的流策略将不生效。
流ID	**if-match flow-id** *flow-id*	包含**if-match flow-id**匹配规则的流分类和包含**remark flow-id**动作的流行为应在不同的流策略中使用。 包含**if-match flow-id**匹配规则的流策略只能应用在接口、VLAN、VLANIF接口、单板、全局的入方向。 SA系列单板不支持配置匹配流ID。
VXLAN内层报文信息	**if-match vxlan** [**transit**] **vni** *vni-id*	包含该流分类的流策略不能应用在出方向上。 当流分类中包含此匹配规则时，流行为只支持流量监管、报文过滤和流量统计。

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为

a. 执行命令**traffic behavior** *behavior-name*，创建一个流行为并进入流行为视图，或进入已存在的流行为视图。

b. 请根据实际需要进行如下配置：

- 执行命令**redirect interface** *interface-type interface-number* [**forced**]，将符合流分类的报文重定向到指定接口。

说明

将流量重定向到接口之后，如果此接口Down了，若配置了**forced**参数，则在此接口丢包，流量不会切换到原转发路径；若没有配置**forced**参数，则流量切换到原转发路径。

将报文重定向到指定接口，如果接口上没有配置允许报文对应的VLAN通过，则报文在该接口上将被丢弃。

- 执行命令**redirect multi-trunk** { **eth-trunk** *trunk-id* } &<1-4>，将符合流分类的报文重定向到一个或多个Eth-Trunk。

  如果入端口为高速率接口（比如XGE接口），而重定向的出接口为低速率接口（比如GE接口），需要将报文重定向到多个Eth-Trunk下的物理接口，以保证流量较均匀地分配出去，避免丢包。此时，可通过将符合流分类的报文重定向到一个或多个Eth-Trunk来实现负载分担。

  说明

  包含流行为redirect multi-trunk的策略只对IP类型的报文生效。

- 执行命令**redirect cpu**，将符合流分类的报文重定向到CPU。

  须知

  应用包含**redirect cpu**的流策略后，会将符合流分类规则的报文重定向到CPU，可能对系统性能造成影响。请谨慎使用此命令。

- 执行命令**redirect lsp public** *dest-address* { *nexthop-address* | **interface** *interface-type interface-number* | **secondary** }，将符合流分类的报文重定向到目标LSP上。

  说明

  二层协议报文的透传也可以通过流策略的重定向到指定接口或者重定向到一个或多个Eth-Trunk来实现。但X系列单板不支持通过流策略重定向BPDU报文，因此，这些单板上只能通过BPDU隧道实现BPDU报文的透传。

- 执行命令**redirect vpn-instance** *vpn-instance-name*，将符合流分类的报文重定向到VPN实例。

c. 执行命令**quit**，退出流行为视图。

d. 执行命令**quit**，退出系统视图。

3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name* [**match-order** { **auto** | **config** }]，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。创建流策略时，如果未指定规则匹配顺序，缺省规则匹配顺序为**config**。

应用流策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先清除该策略的应用，再重新创建并指定所需的匹配顺序。

设备支持在创建流策略时指定流策略中多个规则的匹配顺序，匹配顺序包括自动顺序（**auto**）和配置顺序（**config**）两种：

- 如果选择自动顺序，匹配顺序由系统预先指定的流分类类型的优先级决定，该优先级由高到低依次为：基于二层和IPv4三层信息流分类 > 基于

高级ACL6规则流分类 > 基于基本ACL6规则流分类 > 基于二层信息流分类 > 基于IPv4三层信息流分类 > 基于用户自定义ACL规则流分类。规则优先匹配优先级高的流分类。当某一数据流量同时匹配不同流分类，且对应的流行为存在冲突时，只有流行为优先级高的规则生效。

- 如果选择配置顺序，匹配顺序由流分类规则的优先级决定，先匹配优先级较高的流分类规则。配置流分类时指定优先级，则数值越小，优先级越高；如果配置流分类时未指定precedence-value，则缺省优先级为0。关于流分类优先级的详细说明，请参见**traffic classifier**。

c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

说明

包含重定向的流策略不能应用在出方向。

应用流策略需要设备有足够的ACL资源，否则会导致应用失败。以一个流策略中的if-match占用一条ACL为例，同一个流策略应用到M个接口时，将占用M条ACL资源；应用到L个VLAN且设备上存在N块接口板时，将占用L*N条ACL规则；应用到全局且设备上存在N块接口板时，将占用N条ACL规则。if-match规则占用ACL资源的情况参考“MQC配置-配置注意事项”中的表3。

– 在接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。

说明

- 仅E系列、X系列和S系列中的SC单板支持配置以太网子接口。单板详情请参见《硬件描述》中的单板分类。
- 对于上述系列单板的二层接口，仅hybrid和trunk类型接口支持配置二层以太网子接口。
- 对于上述系列单板的二层接口，执行命令**undo portswitch**切换为三层接口后，支持配置三层以太网子接口。
- S系列中的SA单板不支持创建以太网子接口，也不支持转发IP流量到其它单板的以太网子接口。
- 建议用户先将成员接口加入Eth-Trunk后，再配置Eth-Trunk子接口。只有当成员接口所在的单板系列均支持配置以太网子接口时，Eth-Trunk子接口才能配置成功。
- VCMP的角色是Client时，不能配置VLAN终结子接口。

iii. 执行命令**traffic-policy** *policy-name* **inbound**，在接口或子接口视图上应用流策略。

– 在VLAN上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**vlan** *vlan-id*，进入VLAN视图。

iii. 执行命令**traffic-policy** *policy-name* **inbound**，在VLAN上应用流策略。

流策略对VLAN 0的报文不生效。

- 在VLANIF接口上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。
  iii. 执行命令**traffic-policy** *policy-name* **inbound**，在VLANIF接口上应用流策略。

  每个VLANIF接口的入方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同VLANIF接口的入方向。

  对于应用流策略的VLANIF接口，其对应的VLAN不能是Super-VLAN或MUX VLAN。

  应用在VLANIF接口上的流策略，只对相应VLANIF下的单播报文及三层组播报文生效。

  说明

  如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的入方向上应用该流策略：

  - **remark vlan-id**
  - **remark cvlan-id**
  - **add-tag vlan-id**
  - **remark 8021p**
  - **remark flow-id**
  - **mac-address learning disable**

  如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的出方向上应用该流策略：

  - **add-tag vlan-id**
  - **remark flow-id**
  - **mac-address learning disable**
- 在全局或单板上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**traffic-policy** *policy-name* **global inbound** [**slot** *slot-id*]，在全局或单板上应用流策略。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior user-defined** [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看用户定义的流策略的配置信息。
- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

  说明

  流策略可以应用到子接口上，但暂不支持通过此命令查看子接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

- 执行命令**display traffic policy** { **interface** [*interface-type interface-number*[*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]，查看已配置的流策略信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

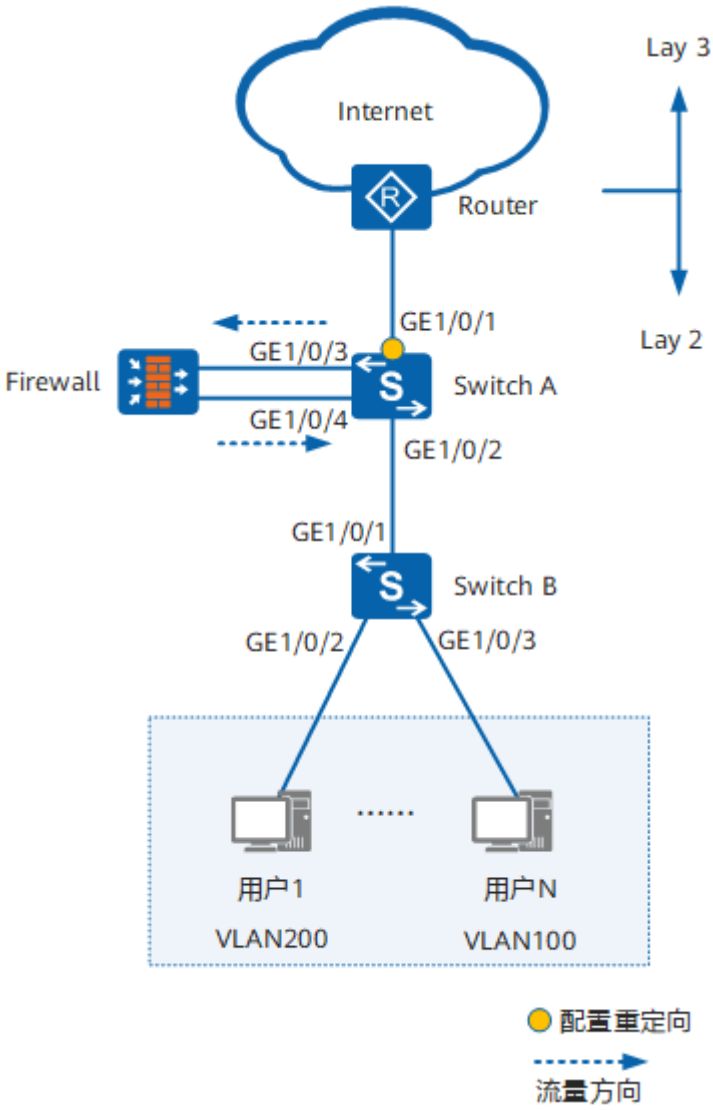
7.5 配置重定向示例

组网需求

如图7-2所示，由于业务需要，用户有访问Internet的需求。用户通过接入层交换机SwitchB和核心层交换机SwitchA以及接入网关Router与Internet进行通信。

为了保证数据和网络的安全性，用户希望保证Internet到服务器全部流量的安全性。

图 7-2 配置重定向的组网图



配置思路

- 出于安全性考虑，在SwitchA上旁挂一台核心防火墙Firewall，对流量进行安全过滤。
- 由于进入防火墙的流量是二层流量，因此通过重定向到接口将来自Internet的所有流量重定向到防火墙进行安全过滤。
- 为了防止出现环路，在SwitchA与防火墙相连的接口上配置端口隔离，并配置禁止MAC地址学习防止MAC漂移。

操作步骤

步骤1 创建VLAN并配置各接口，保证二层互通

在SwitchB上创建VLAN100和VLAN200。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] vlan batch 100 200
```

配置SwitchB上接口GE1/0/2和GE1/0/3的接口类型为Access，并将GE1/0/2加入VLAN200，将GE1/0/3加入VLAN100，配置GE1/0/1的接口类型为Trunk，并将GE1/0/1加入VLAN100和VLAN200。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type access
[SwitchB-GigabitEthernet1/0/2] port default vlan 200
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type access
[SwitchB-GigabitEthernet1/0/3] port default vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 200
[SwitchB-GigabitEthernet1/0/1] quit
```

在SwitchA上创建VLAN100和VLAN200。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200
```

配置SwitchA上接口GE1/0/1、GE1/0/2、GE1/0/3和GE1/0/4接口类型为Trunk，并将它们都加入VLAN100和VLAN200。将接口GE1/0/3和GE1/0/4加入同一个端口隔离组，配置接口GE1/0/4禁止MAC地址学习防止MAC漂移。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/3] port-isolate enable
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/4] port-isolate enable
[SwitchA-GigabitEthernet1/0/4] mac-address learning disable
[SwitchA-GigabitEthernet1/0/4] quit
```


步骤2 配置MQC实现重定向到接口

配置流分类。

```
[SwitchA] traffic classifier c1
[SwitchA-classifier-c1] if-match any
[SwitchA-classifier-c1] quit
```

配置流行为。

```
[SwitchA] traffic behavior b1
[SwitchA-behavior-b1] redirect interface gigabitethernet 1/0/3
[SwitchA-behavior-b1] quit
```

配置流策略。

```
[SwitchA] traffic policy p1
[SwitchA-trafficpolicy-p1] classifier c1 behavior b1
[SwitchA-trafficpolicy-p1] quit
```

在SwitchA的GigabitEthernet1/0/1入方向应用流策略。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] traffic-policy p1 inbound
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] quit
```

步骤3 验证配置结果

查看流分类的配置信息。

```
<SwitchA> display traffic classifier user-defined c1
 User Defined Classifier Information:
  Classifier: c1
   Precedence: 5
   Operator: OR
   Rule(s) : if-match any
```

查看流行为的配置信息。

```
<SwitchA> display traffic behavior user-defined b1
  User Defined Behavior Information:
    Behavior: b1
      Permit
      Redirect: no forced
        Redirect interface GigabitEthernet1/0/3
```

查看流策略的配置信息。

```
<SwitchA> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: OR
     Behavior: b1
      Permit
      Redirect: no forced
        Redirect interface GigabitEthernet1/0/3
```

查看流策略的应用信息。

```
<SwitchA> display traffic-policy applied-record
#
----------------------------------------------------
  Policy Name:   p1
  Policy Index:  0
     Classifier:c1      Behavior:b1
----------------------------------------------------
 *interface GigabitEthernet1/0/1
    traffic-policy p1 inbound
      slot 1    :  success
----------------------------------------------------
```



```
  Policy total applied times: 1.
#
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 100 200
#
traffic classifier c1 operator or precedence 5
 if-match any
#
traffic behavior b1
 permit
 redirect interface GigabitEthernet1/0/3
#
traffic policy p1 match-order config
 classifier c1 behavior b1
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
 traffic-policy p1 inbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
 port-isolate enable group 1
#
interface GigabitEthernet1/0/4
 port link-type trunk
 mac-address learning disable
 port trunk allow-pass vlan 100 200
 port-isolate enable group 1
#
return
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 100 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 200
#
interface GigabitEthernet1/0/3
 port link-type access
 port default vlan 100
#
return
```


8 流量统计配置

8.1 流量统计简介

配置MQC实现流量统计后，设备将对符合流分类规则的报文进行报文数和字节数的统计，可以帮助用户了解应用流策略后流量通过和被丢弃的情况，由此分析和判断流策略的应用是否合理，也有助于进行相关的故障诊断与排查。

只有配置MQC实现流量统计后，才可以通过**display traffic policy statistics**命令查看应用流策略后流量通过和被丢弃的情况。

流量统计与接口统计的区别如**表8-1**所示。

表 8-1 流量统计与接口统计的区别

统计方式	查询命令	统计范围	说明
流量统计	**display traffic policy statistics**	流策略应用后符合流分类规则的报文	不包括上送CPU报文
接口统计	• **display interface** • **display this interface**	接口上所有报文	包括上送CPU报文

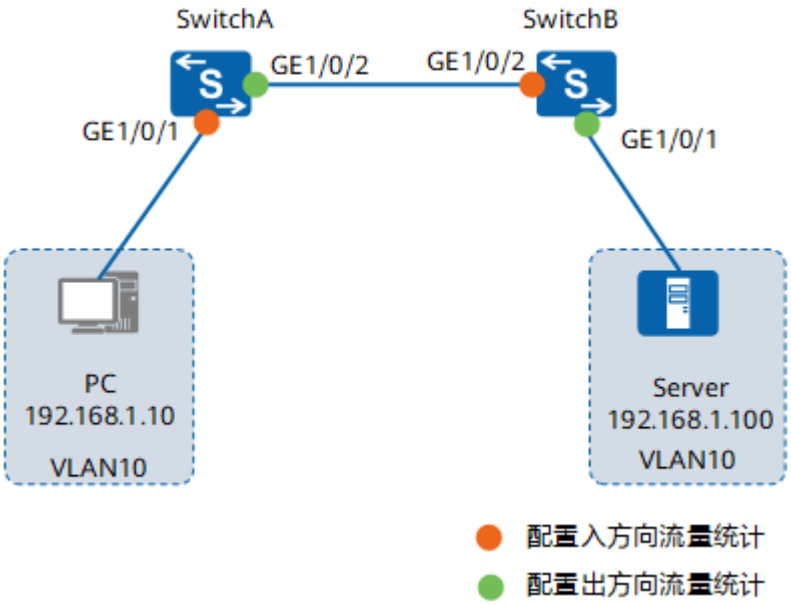
8.2 流量统计应用场景

组网需求

流量统计主要用来对网络故障进行定位，协助判断设备是否正确转发报文，是否正确接收报文，是否正确发送报文等。进而逐步缩小故障范围，最终确定故障点。

如图8-1所示，如果PC访问服务器慢，或者Ping丢包，则说明网络中可能存在故障，可以通过流量统计功能对故障点进行定位。

图 8-1 流量统计应用组网图



业务部署

- 在SwitchA的GE1/0/1接口入方向和GE1/0/2接口出方向配置流量统计，如果出入方向报文数量相同，则说明SwitchA能正确转发报文。反之，如果出方向报文比入方向报文少，则说明在SwitchA丢包，故障点在SwitchA上。检查SwitchB是否存在故障的方法与此类似。
- 同样，可以在SwitchA的GE1/0/2出方向和SwitchB的GE1/0/2入方向配置流量统计，如果报文数量相同，则说明SwitchA到SwitchB之间的链路没有故障，反之则说明存在故障。

8.3 流量统计配置注意事项

涉及网元

无需其他网元配合。

License 支持

流量统计是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持流量统计。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

SA系列单板只支持基于包的流量统计，其它单板支持基于字节和基于包的流量统计。

8.4 配置流量统计

背景信息

配置流量统计后，设备将对符合流分类规则的报文进行流量统计，可以帮助用户了解应用流策略后报文通过和被丢弃的情况，由此分析和判断流策略的应用是否合理，也有助于进行相关的故障诊断与排查。

操作步骤

1. 配置流分类
   a. 执行命令**system-view**，进入系统视图。
   b. 执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，创建一个流分类并进入流分类视图，或进入已存在的流分类视图。

      and表示流分类中各规则之间关系为逻辑“与”，指定该逻辑关系后：

      - 当流分类中有ACL规则时，报文必须匹配其中一条ACL规则以及所有非ACL规则才属于该类；
      - 当流分类中没有ACL规则时，则报文必须匹配所有非ACL规则才属于该类。

      or表示流分类各规则之间是逻辑“或”，即报文只需匹配流分类中的一个或多个规则即属于该类。

      缺省情况下，流分类中各规则之间的关系为逻辑“或”。
   c. 请根据实际情况定义流分类中的匹配规则。

      说明

      if-match ip-precedence和**if-match tcp**命令仅对IPv4报文生效。

      X系列单板不支持配置包含高级ACL中的**ttl-expired**字段的流分类规则。

      当流分类匹配**if-match ipv6 acl** { *acl-number* | *acl-name* }时，X系列单板不支持**add-tag vlan-id** *vlan-id*、**remark 8021p** [*8021p-value* | **inner-8021p**]、**remark cvlan-id** *cvlan-id*、**remark vlan-id** *vlan-id*、**mac-address learning disable**。

匹配规则	命令	说明
外层VLAN ID或基于QinQ报文内外两层Tag的VLAN ID	**if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]	-

匹配规则	命令	说明
QinQ报文内外层VLAN ID	**if-match cvlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**vlan-id** *vlan-id*]	-
VLAN报文802.1p优先级	**if-match 8021p** *8021p-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个802.1p值，报文只需匹配其中一个802.1p值就匹配该规则。
QinQ报文内层VLAN的802.1p优先级	**if-match cvlan-8021p** *8021p-value* &<1-8>	-
丢弃报文	**if-match discard**	包含该流分类的报文只能与流量统计和流镜像两种动作绑定。
QinQ报文双层Tag	**if-match double-tag**	-
MPLS报文EXP优先级	**if-match mpls-exp** *exp-value* &<1-8>	无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个MPLS EXP值，报文只需匹配其中一个MPLS EXP值就属于该类。
目的MAC地址	**if-match destination-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
源MAC地址	**if-match source-mac** *mac-address* [[**mac-address-mask**] *mac-address-mask*]	-
以太网帧头中协议类型字段	**if-match l2-protocol** { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }	-
所有报文	**if-match any**	-

匹配规则	命令	说明
IP报文的DSCP优先级	**if-match** [**ipv6**] **dscp** *dscp-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个DSCP值，报文只需匹配其中一个DSCP值就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
IP报文的IP优先级	**if-match ip-precedence** *ip-precedence-value* &<1-8>	• 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果输入多个IP优先级，报文只需匹配其中一个IP优先级就匹配该规则。 • 不能在一个逻辑关系为“与”的流分类中同时配置**if-match** [**ipv6**] **dscp**和**if-match ip-precedence**。
报文三层协议类型	**if-match protocol** { **ip** | **ipv6** }	-
IPv6下一报文头类型	**if-match ipv6 next-header** *header-number* **first-next-header**	ET1D2X12SSA0单板不支持Prefix的长度为(64,128)之间的路由。
TCP报文SYN Flag	**if-match tcp syn-flag** { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	-
入接口	**if-match inbound-interface** *interface-type interface-number*	包含该流分类的流策略不能应用在出方向。 包含该流分类的流策略不能应用在接口视图。
出接口	**if-match outbound-interface** *interface-type interface-number*	X系列单板不支持将包含该流分类的流策略应用在入方向。 包含该流分类的流策略不能应用在接口视图。

匹配规则	命令	说明
ACL规则	**if-match acl** { *acl-number* | *acl-name* }	• 使用ACL作为流分类规则，请先配置相应的ACL规则。 • 无论流分类中各规则间关系是“或”还是“与”，执行一次命令，如果某ACL规则中有多个rule，报文只需匹配其中一个rule就匹配该ACL规则。 • 如果ACL的规则指定了参数**vpn-instance**，那么基于该ACL进行分类的流分类对应的流策略将不生效。
ACL6规则	**if-match ipv6 acl** { *acl-number* | *acl-name* }	使用ACL6作为流分类规则，请先配置相应的ACL6规则。 如果ACL6的规则指定了参数**vpn-instance**，那么基于该ACL6进行分类的流分类对应的流策略将不生效。
流ID	**if-match flow-id** *flow-id*	包含**if-match flow-id**匹配规则的流分类和包含**remark flow-id**动作的流行为应在不同的流策略中使用。 包含**if-match flow-id**匹配规则的流策略只能应用在接口、VLAN、VLANIF接口、单板、全局的入方向。 SA系列单板不支持配置匹配流ID。
VXLAN内层报文信息	**if-match vxlan** [**transit**] **vni** *vni-id*	包含该流分类的流策略不能应用在出方向上。 当流分类中包含此匹配规则时，流行为只支持流量监管、报文过滤和流量统计。

d. 执行命令**quit**，退出流分类视图。

2. 配置流行为
   a. 执行命令**traffic behavior** *behavior-name*，创建一个流行为并进入流行为视图，或进入已存在的流行为视图。
   b. 执行命令**statistic enable**，使能流量统计功能。
      缺省情况下，流行为中未使能流量统计功能。
   c. 执行命令**quit**，退出流行为视图。
   d. 执行命令**quit**，退出系统视图。
3. 配置流策略

a. 执行命令**system-view**，进入系统视图。

b. 执行命令**traffic policy** *policy-name* [**match-order** { **auto** | **config** }]，创建一个流策略并进入流策略视图，或进入已存在的流策略视图。创建流策略时，如果未指定规则匹配顺序，缺省规则匹配顺序为**config**。

应用流策略后，不能再使用该命令来修改策略中流分类的匹配顺序。必须先清除该策略的应用，再重新创建并指定所需的匹配顺序。

设备支持在创建流策略时指定流策略中多个规则的匹配顺序，匹配顺序包括自动顺序（**auto**）和配置顺序（**config**）两种：

- 如果选择自动顺序，匹配顺序由系统预先指定的流分类类型的优先级决定，该优先级由高到低依次为：基于二层和IPv4三层信息流分类 > 基于高级ACL6规则流分类 > 基于基本ACL6规则流分类 > 基于二层信息流分类 > 基于IPv4三层信息流分类 > 基于用户自定义ACL规则流分类。规则优先匹配优先级高的流分类。当某一数据流量同时匹配不同流分类，且对应的流行为存在冲突时，只有流行为优先级高的规则生效。
- 如果选择配置顺序，匹配顺序由流分类规则的优先级决定，先匹配优先级较高的流分类规则。配置流分类时指定优先级，则数值越小，优先级越高；如果配置流分类时未指定precedence-value，则缺省优先级为0。关于流分类优先级的详细说明，请参见**traffic classifier**。

c. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

d. 执行命令**quit**，退出流策略视图。

e. 执行命令**quit**，退出系统视图。

4. 应用流策略

- 在接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。

说明

- 仅E系列、X系列和S系列中的SC单板支持配置以太网子接口。单板详情请参见《硬件描述》中的单板分类。
- 对于上述系列单板的二层接口，仅hybrid和trunk类型接口支持配置二层以太网子接口。
- 对于上述系列单板的二层接口，执行命令**undo portswitch**切换为三层接口后，支持配置三层以太网子接口。
- S系列中的SA单板不支持创建以太网子接口，也不支持转发IP流量到其它单板的以太网子接口。
- 建议用户先将成员接口加入Eth-Trunk后，再配置Eth-Trunk子接口。只有当成员接口所在的单板系列均支持配置以太网子接口时，Eth-Trunk子接口才能配置成功。
- VCMP的角色是Client时，不能配置VLAN终结子接口。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口或子接口视图上应用流策略。

每个接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同接口的不同方向。应用后，系统对流经该接口并匹配流分类中规则的入方向或出方向报文实施策略控制。

说明

- 子接口仅支持**inbound**参数。
- 建议不要在Untagged类型接口出方向上应用包含有**remark 8021p**、**remark cvlan-id**、**remark vlan-id**等动作的流策略，否则，可能导致报文内容出错。
- ET1D2X12SSA0、ET1D2X48SEC0、SC系列单板有2N个接口，如果1～N号中的接口与N+1～2N号中的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的2倍。
- 在X系列单板中，如果不同的接口加入同一Eth-Trunk或VLAN，Eth-Trunk或VLAN出方向使用**car**动作进行限速，且这些接口的ACL资源分散在N个组中进行统计（执行命令**display acl resource**查看），那么Eth-Trunk或VLAN的下行实际通过流量是配置CAR值的限速的N倍。
- 应用流策略需要设备有足够的ACL资源，否则会导致应用失败。以一个流策略中的if-match占用一条ACL为例，同一个流策略应用到M个接口时，将占用M条ACL资源；应用到L个VLAN且设备上存在N块接口板时，将占用L*N条ACL规则；应用到全局且设备上存在N块接口板时，将占用N条ACL规则。if-match规则占用ACL资源的情况参考“MQC配置-配置注意事项”中的表3。
- 配置Tunnel接口的隧道协议为GRE后，可在Tunnel接口入方向应用流策略。
- 在VXLAN二层子接口、Dot1q终结子接口和绑定了BGP AD方式的子接口下，应用流策略不生效，建议在主接口配置基于流ID的分类方式。

– 在VLAN上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**vlan** *vlan-id*，进入VLAN视图。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLAN上应用流策略。

每个VLAN的每个方向能且只能应用一个流策略。

应用后，系统对属于该VLAN并匹配流分类中规则的入方向或出方向报文实施策略控制。但是流策略对VLAN 0的报文不生效。

– 在VLANIF接口上应用流策略

i. 执行命令**system-view**，进入系统视图。

ii. 执行命令**interface vlanif** *vlan-id*，进入VLANIF接口视图。

iii. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在VLANIF接口上应用流策略。

每个VLANIF接口的每个方向上能且只能应用一个流策略，但同一个流策略可以同时应用在不同VLANIF接口的不同方向。

对于应用流策略的VLANIF接口，其对应的VLAN不能是Super-VLAN或MUX VLAN。

对于X系列单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文生效。对于其它单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文及三层组播报文生效。

说明

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的入方向上应用该流策略：

- **remark vlan-id**
- **remark cvlan-id**
- **add-tag vlan-id**
- **remark 8021p**
- **remark flow-id**
- **mac-address learning disable**

如果流策略包含的流行为配置了如下动作，则不能在VLANIF接口的出方向上应用该流策略：

- **add-tag vlan-id**
- **remark flow-id**
- **mac-address learning disable**

- 在全局或单板上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**traffic-policy** *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]，在全局或单板上应用流策略。

  全局或单板的每个方向上能且只能应用一个流策略，如果在全局某方向应用了流策略，则不能在单板的该方向上再次应用流策略；指定单板在某方向应用流策略后，也不能在全局的该方向上再次应用流策略。
- 在SSID模板上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**wlan**，进入WLAN视图。
  iii. 执行命令**ssid-profile name** *profile-name*，创建SSID模板并进入模板视图。
  iv. 执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，在SSID模板上应用流策略。
- 在AP组上应用流策略
  i. 执行命令**system-view**，进入系统视图。
  ii. 执行命令**wlan**，进入WLAN视图。
  iii. 执行命令**ap-group name** *group-name*，创建AP组并进入AP组视图。
  iv. 执行命令**traffic-policy** *policy-name* **outbound**，在AP组上应用流策略。

检查配置结果

- 执行命令**display traffic classifier user-defined** [*classifier-name*]，查看已配置的流分类信息。
- 执行命令**display traffic behavior user-defined** [*behavior-name*]，查看已配置的流行为信息。
- 执行命令**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看用户定义的流策略的配置信息。

- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

  说明

  流策略可以应用到子接口上，但暂不支持通过此命令查看子接口上应用的基于ACL的简化流策略和基于MQC的流策略配置信息。

- 执行命令**display traffic policy** { **interface** [*interface-type interface-number*[*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]，查看已配置的流策略信息。
- 执行命令**display traffic-policy applied-record** [*policy-name*]，查看指定流策略的应用记录。

8.5 配置流量统计示例

组网需求

如图8-2所示，PC1的MAC地址为xxxx-xxxx-xxxx，它连接在Switch的GE1/0/1端口上，实现与其他设备的互连互通。现希望Switch对源MAC为xxxx-xxxx-xxxx的报文进行流量统计。

图 8-2 配置流量统计组网图

配置思路

采用包含流量统计动作的流策略方式实现流量统计，具体配置思路如下：

1. 配置各接口，实现Switch与Router、PC1互通。
2. 配置ACL规则，匹配源MAC为xxxx-xxxx-xxxx的报文。
3. 配置流分类，实现基于上述ACL规则对报文进行分类。
4. 配置流行为，实现对满足规则的报文进行流量统计。
5. 配置流策略，绑定上述流分类和流行为，并应用到接口GE1/0/1的入方向，实现对该接口收到的源MAC为xxxx-xxxx-xxxx的报文进行流量统计。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 20
[Switch-vlan20] quit
```


配置接口GE1/0/1为Access类型接口，接口GE1/0/2为Trunk类型接口，并将GE1/0/1和GE1/0/2加入VLAN20。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type access
[Switch-GigabitEthernet1/0/1] port default vlan 20
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 20
[Switch-GigabitEthernet1/0/2] quit
```

创建VLANIF20，并配置IP地址10.10.10.2/24。

```
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 10.10.10.2 24
[Switch-Vlanif20] quit
```

说明

请配置Router与Switch对接的接口IP地址为10.10.10.1/24。

步骤2 配置ACL规则

在Switch上创建编码为4000的二层ACL，匹配源MAC为xxxx-xxxx-xxxx的报文。

```
[Switch] acl 4000
[Switch-acl-L2-4000] rule permit source-mac xxxx-xxxx-xxxx ffff-ffff-ffff
[Switch-acl-L2-4000] quit
```

步骤3 配置流分类

在Switch上创建流分类c1，匹配规则为ACL 4000。

```
[Switch] traffic classifier c1 operator and
[Switch-classifier-c1] if-match acl 4000
[Switch-classifier-c1] quit
```

步骤4 配置流行为

在Switch上创建流行为b1，并配置流量统计动作。

```
[Switch] traffic behavior b1
[Switch-behavior-b1] statistic enable
[Switch-behavior-b1] quit
```

步骤5 配置流策略并应用到接口上

在Switch上创建流策略p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
```

将流策略p1应用到接口GE1/0/1。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet1/0/1] quit
```

步骤6 验证配置结果

查看ACL规则的配置信息。

```
[Switch] display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 permit source-mac xxxx-xxxx-xxxx
```


查看流分类的配置信息。

```
[Switch] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Precedence: 5
    Operator: AND
    Rule(s) : if-match acl 4000

Total classifier number is 1
```

查看流策略的配置信息。

```
[Switch] display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Permit
      Statistic: enable
```

查看流量统计信息。

```
[Switch] display traffic policy statistics interface gigabitethernet 1/0/1 inbound

 Interface: GigabitEthernet1/0/1
 Traffic policy inbound: p1
 Rule number: 1
 Current status: success
 Statistics interval: 300
-----------------------------------------------------------------------------
 Board : 1
-----------------------------------------------------------------------------
 Matched          |      Packets:                      0
                  |      Bytes:                    0
                  |      Rate(pps):                  0
                  |      Rate(bps):                  0
-----------------------------------------------------------------------------
  Passed          |      Packets:                      0
                  |      Bytes:                    0
                  |      Rate(pps):                  0
                  |      Rate(bps):                  0
-----------------------------------------------------------------------------
  Dropped         |      Packets:                      0
                  |      Bytes:                    0
                  |      Rate(pps):                  0
                  |      Rate(bps):                  0
-----------------------------------------------------------------------------
    Filter        |      Packets:                      0
                  |      Bytes:                    0
-----------------------------------------------------------------------------
    Car           |      Packets:                      0
                  |      Bytes:                    0
-----------------------------------------------------------------------------
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 20
#
acl number 4000
 rule 5 permit source-mac xxxx-xxxx-xxxx
```



```
#
traffic classifier c1 operator and precedence 5
 if-match acl 4000
#
traffic behavior b1
 permit
 statistic enable
#
traffic policy p1 match-order config
 classifier c1 behavior b1
#
interface Vlanif20
 ip address 10.10.10.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 20
 traffic-policy p1 inbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```


9 基于 ACL 的简化流策略配置

9.1 基于 ACL 的简化流策略概述

基于ACL的简化流策略是指通过将报文信息与ACL规则进行匹配，为符合相同ACL规则的报文提供相同的QoS服务，实现对不同类型业务的差分服务。

当用户希望对进入网络的流量进行控制时，可以配置ACL规则根据报文的源IP地址、分片标记、目的IP地址、源端口号、源MAC地址等信息对报文进行匹配，进而配置基于ACL的简化流策略实现对匹配ACL规则的报文过滤、流量监管、流镜像、重定向、重标记或流量统计。

与流策略相比，基于ACL的简化流策略不需要单独创建流分类、流行为或流策略，配置更为简洁；但是由于仅基于ACL规则对报文进行匹配，因此匹配规则没有流策略丰富。

9.2 基于 ACL 的简化流策略配置注意事项

涉及网元

无需其他网元配合。

License 支持

基于ACL的简化流策略是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

S12700, S12700E系列交换机中所有款型均支持基于ACL的简化流策略。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

在VLANIF接口配置时的限制：

- V200R012C00及后续版本的设备支持在VLANIF接口上配置基于ACL的简化流策略。
  - 在V200R019C10之前版本，只能在VLANIF接口的入方向配置基于ACL的简化流策略；从V200R019C10版本开始，支持在VLANIF接口的入方向和出方向配置基于ACL的简化流策略。
  - VLANIF接口对应的VLAN不能是Super-VLAN或MUX VLAN。
  - 对于X系列单板，应用在VLANIF接口上的基于ACL的简化流策略只对相应VLANIF下的单播报文生效。对于其它单板，应用在VLANIF接口上的流策略只对相应VLANIF下的单播报文及三层组播报文生效。
- 对于X系列单板中不支持配置扩展表项空间资源模式的单板，仅支持匹配ACL6规则中的协议号、源端口号、目的端口号、源IPv6地址和目的IPv6地址，且不支持将匹配这些内容的基于ACL6的简化流策略应用在VLANIF接口上。

配置时可能导致冲突或功能不生效的限制：

- V200R013C00及之前版本同一接口、VLAN或全局下配置多条基于ACL的简化流策略，如果其中一条基于ACL的流策略引用的ACL规则发生变化，会导致此视图所有已配置的基于ACL的简化流策略短暂失效。
- 如果ACL规则匹配了报文的VPN实例名称，则基于ACL的简化流策略下发不成功。
- 对于ET1D2L16QX2H和ET1D2C08HX2H单板，如果同一接口、VLAN或全局下已经配置基于ACL的简化流策略，当在此视图中再配置新的基于ACL的简化流策略时，会导致此视图所有已配置的基于ACL的简化流策略短暂失效。
- 配置基于ACL的简化流策略时，
  - 当命令中指定**name** *acl-name*时，需要通过**acl name**或者**acl ipv6 name**命令创建对应的ACL，否则命令配置不成功。
  - 当命令中指定**rule** *rule-id*时，需要先创建ACL并且配置对应的rule，否则命令配置不成功。
- 若对入方向报文同时配置VLAN Mapping功能和基于ACL的重标记，且指定重标记报文的802.1p优先级或者VLAN编号，那么基于ACL的重标记匹配映射前VLAN ID。其他情况下，若对报文同时配置VLAN Mapping功能和基于ACL的简化流策略，那么基于ACL的简化流策略匹配映射后的VLAN ID。

与其他功能同时配置时的优先级关系：

- 匹配同一个ACL的MQC流策略和基于ACL的简化流策略应用到同一对象时，基于ACL的简化流策略优先生效。以下情况例外：使用**traffic-secure**命令配置基于ACL的报文过滤，可以与匹配同一个ACL的MQC流策略同时生效。

- 目的IP是本机的报文会上送CPU，另外一些协议报文对应的功能使能后也会上送CPU，比如BGP、OSPF、LACP使能后也会上送CPU处理。上送CPU的报文同时匹配简化流策略所基于的ACL，如果CPCAR和基于ACL的简化流策略动作冲突，CPCAR生效。

其他限制：

- X系列单板（除X1E、X2H、X5H、X6H单板以外）只支持在全局、VLAN、物理接口或者Eth-Trunk接口下应用ACL6，不支持在其他逻辑接口上应用ACL6。
- X系列单板（除X1E、X2H、X5H、X6H单板以外）上配置的ACL6规则应用为硬件ACL时的约束请参见《S12700, S12700E V200R023C00 配置指南-安全配置》ACL配置中的配置高级ACL6。
- 配置**traffic-limit** 、**traffic-redirect** 、**traffic-remark**、**traffic-statistic**或**traffic-mirror**时，无论报文命中ACL的是permit规则还是deny规则，设备都会按照配置的简化流策略对报文执行相应动作。如果希望设备能过滤掉命中deny规则的报文，则必须同时配置**traffic-filter**或**traffic-secure**。
- 如果配置**traffic-redirect（接口视图）**或**traffic-redirect（系统视图）**命令将流量重定向到接口时，建议ACL规则匹配二层流量。
- V200R011C10及后续版本的X系列单板支持基于用户自定义ACL的简化流策略。

9.3 配置基于 ACL 的报文过滤

背景信息

通过配置基于ACL的报文过滤，对匹配ACL规则报文进行禁止/允许动作，进而实现对网络流量的控制。

traffic-filter和**traffic-secure**命令都是用来配置报文过滤功能，不建议在设备上同时配置。可以根据以下原则选用**traffic-filter**或**traffic-secure**命令配置报文过滤：

- 如果**traffic-filter**或**traffic-secure**关联的ACL没有同时被其他基于ACL的简化流策略所关联，且报文不会同时匹配报文过滤和其他简化流策略关联的ACL规则时，**traffic-filter**和**traffic-secure**可以任选其一。
- 如果**traffic-filter**或**traffic-secure**关联的ACL同时被其他基于ACL的简化流策略所关联，或者报文同时匹配了报文过滤和其他简化流策略关联的ACL时，**traffic-filter**和**traffic-secure**的区别如下：
  - 当**traffic-secure**和其他基于ACL的简化流策略同时配置，且ACL规则中的动作为deny时，仅**traffic-secure**、**traffic-mirror**和**traffic-statistics**命令生效，且报文被过滤。
  - 当**traffic-secure**和其他基于ACL的简化流策略同时配置，且ACL规则中的动作为permit时，**traffic-secure**命令和其他基于ACL的简化流策略均生效。
  - 当**traffic-filter**和其他基于ACL的简化流策略同时配置，且ACL规则中的动作为deny时，仅**traffic-filter**、**traffic-mirror**和**traffic-statistics**命令生效，且报文被过滤。
  - 当**traffic-filter**和其他基于ACL的简化流策略同时配置，且ACL规则中的动作为permit时，先配置的简化流策略生效。如果同一个ACL下同时配置了**traffic-filter**和**traffic-statistic**，则两个配置同时生效。如果不是同一个ACL，则不会同时生效的。

如果ACL中rule规则配置为**deny**且基于该ACL的**traffic-filter**配置在出方向，当报文匹配该ACL规则时，会导致由CPU发送的ICMP、OSPF、BGP、RIP、SNMP、Telnet等协议控制报文被丢弃，相关协议的功能会受到影响。

说明

在全局或VLAN上实现的基于ACL的报文过滤，ACL范围为2000～5999。在NAC网络中用于对用户访问控制的基于ACL的报文过滤，ACL范围为6000～9999，参考**traffic-filter acl**。

操作步骤

- 在全局或VLAN上配置报文过滤
  a. 执行命令**system-view**，进入系统视图。
  b. 请根据实际需要选择进行如下配置：
     - 执行命令**traffic-filter** [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]，对匹配单个ACL规则的入方向的报文进行过滤。

       说明

       如果用于报文过滤的ACL引用了UCL组，该UCL组的ID值不能超过48。

     - 执行命令**traffic-secure** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | *l2–acl* | **name** *acl-name* } [**rule** *rule-id*]，对匹配单个ACL规则的入方向的报文进行过滤。
     - 执行命令**traffic-filter** [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] {*bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]，对匹配单个ACL规则的出方向的报文进行过滤。
     - 执行命令**traffic-filter** [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]或**traffic-filter** [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的报文进行过滤。
     - 执行命令**traffic-secure** [**vlan** *vlan-id*] **inbound acl** { *l2–acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行过滤。
- 在接口上配置报文过滤
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 请根据实际需要选择进行如下配置：
     - 执行命令**traffic-filter inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]，对匹配单个ACL规则的入方向的报文进行过滤。

       说明

       如果用于报文过滤的ACL引用了UCL组，该UCL组的ID值不能超过48。

     - 执行命令**traffic-secure inbound acl** { *bas-acl* | *adv-acl* | *l2–acl* | **name** *acl-name* } [**rule** *rule-id*]，对匹配单个ACL规则的入方向的报文进行过滤。

- 执行命令**traffic-filter outbound acl** { [**ipv6**] {*bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]，对匹配单个ACL规则的出方向的报文进行过滤。
- 执行命令**traffic-filter** { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]或**traffic-filter** { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的报文进行过滤。
- 执行命令**traffic-secure inbound acl** { *l2–acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行过滤。

----结束

9.4 配置基于 ACL 的流量监管

背景信息

通过配置基于ACL的流量监管，对匹配ACL规则的报文进行限速。

操作步骤

- 在全局或VLAN上配置流量监管
  a. 执行命令**system-view**，进入系统视图。
  b. 请根据实际需要选择进行如下配置：
     - 执行命令**traffic-limit** [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]]，对匹配单个ACL规则的入方向的报文进行流量监管。
     - 执行命令**traffic-limit** [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]，对匹配单个ACL规则的出方向的报文进行流量监管。
     - 执行命令**traffic-limit** [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]，对同时匹配二层和三层ACL的入方向的报文进行流量监管。

- 执行命令**traffic-limit** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]，对同时匹配二层和三层ACL的入方向的报文进行流量监管。
- 执行命令**traffic-limit** [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]，对同时匹配二层和三层ACL的入方向的报文进行流量监管。
- 执行命令**traffic-limit** [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]，对同时匹配二层和三层ACL的出方向的报文进行流量监管。
- 执行命令**traffic-limit** [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]，对同时匹配二层和三层ACL的出方向的报文进行流量监管。
- 执行命令**traffic-limit** [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]，对同时匹配二层和三层ACL的出方向的报文进行流量监管。

  说明

  报文的颜色可以在流量监管中定义：
  - 报文的突发尺寸 < *cbs-value*时，报文被标记为绿色；
  - *cbs-value* ≤ 报文的突发尺寸 < *pbs-value*时，报文被标记为黄色；
  - 报文的突发尺寸 ≥ *pbs-value*时，报文被标记为红色。

  缺省情况下，绿色、黄色报文被允许通过，红色报文被丢弃。

- 在接口上配置流量监管
  a. 执行命令**system-view**，进入系统视图。

b. 执行命令**interface** *interface-type interface-number*，进入接口视图。

c. 请根据实际需要选择进行如下配置：

- 执行命令**traffic-limit inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]]，对匹配单个ACL规则的入方向的报文进行流量监管。
- 执行命令**traffic-limit outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]]，对匹配单个ACL规则的出方向的报文进行流量监管。
- 执行命令**traffic-limit inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量监管。
- 执行命令**traffic-limit inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量监管。
- 执行命令**traffic-limit inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量监管。
- 执行命令**traffic-limit outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量监管。
- 执行命令**traffic-limit outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-*

value] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量监管。

- 执行命令**traffic-limit outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量监管。

说明

报文的颜色可以在流量监管中定义：

- 报文的突发尺寸 < *cbs-value*时，报文被标记为绿色；
- *cbs-value* ≤ 报文的突发尺寸 < *pbs-value*时，报文被标记为黄色；
- 报文的突发尺寸 ≥ *pbs-value*时，报文被标记为红色。

缺省情况下，绿色、黄色报文被允许通过，红色报文被丢弃。

----结束

9.5 配置基于 ACL 的重定向

背景信息

通过配置基于ACL的重定向，将匹配ACL规则的报文重定向到CPU、指定接口或指定下一跳地址。

说明

在全局或VLAN上实现的基于ACL的重定向，ACL范围为2000～5999。在NAC网络中用于对用户访问控制的基于ACL的重定向，ACL范围为6000～9999，参考**traffic-redirect acl**。

操作步骤

- 在全局或VLAN上配置重定向
  a. 执行命令**system-view**，进入系统视图。
  b. 请根据实际需要选择进行如下配置：

  - 执行命令**traffic-redirect** [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect** [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对匹配单个ACL规则的入方向的报文进行重定向。

  - 执行命令**traffic-redirect** [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

{ **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect** [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对同时匹配二层ACL和三层ACL的入方向的报文进行重定向。

- 执行命令**traffic-redirect** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对同时匹配二层ACL和三层ACL的入方向的报文进行重定向。

- 执行命令**traffic-redirect** [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect** [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对同时匹配二层ACL和三层ACL的入方向的报文进行重定向。

- 在接口上配置重定向
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 请根据实际需要选择进行如下配置：

  - 执行命令**traffic-redirect inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对匹配单个ACL规则的入方向的报文进行重定向。

  - 执行命令**traffic-redirect inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对同时匹配二层ACL和三层ACL的入方向的报文进行重定向。

  - 执行命令**traffic-redirect inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-*

instance-name] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对同时匹配二层ACL和三层ACL的入方向的报文进行重定向。

- 执行命令**traffic-redirect inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }或**traffic-redirect inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*，对同时匹配二层ACL和三层ACL的入方向的报文进行重定向。

----结束

9.6 配置基于 ACL 的重标记

背景信息

通过配置基于ACL的重标记，对匹配指定ACL规则的报文进行重标记，如802.1p优先级、QinQ报文中的内层VLAN Tag、目的MAC地址、DSCP服务类型、本地优先级、IP优先级、VLAN编号。

操作步骤

- 在全局或VLAN上配置重标记
  a. 执行命令**system-view**，进入系统视图。
  b. 请根据实际需要选择进行如下配置：
     - 执行命令**traffic-remark** [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }，对匹配单个ACL规则的入方向的报文进行重标记。
     - 执行命令**traffic-remark** [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对匹配单个ACL规则的出方向的报文进行重标记。
     - 执行命令**traffic-remark** [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的入方向的报文进行重标记。

- 执行命令**traffic-remark** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的入方向的报文进行重标记。
- 执行命令**traffic-remark** [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的入方向的报文进行重标记。
- 执行命令**traffic-remark** [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的出方向的报文进行重标记。
- 执行命令**traffic-remark** [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的出方向的报文进行重标记。
- 执行命令**traffic-remark** [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的出方向的报文进行重标记。

说明

X系列单板不支持**destination-mac** *mac-address*。

- 在接口上配置重标记
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 请根据实际需要选择进行如下配置：
     - 执行命令**traffic-remark inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }，对匹配单个ACL规则的入方向的报文进行重标记。
     - 执行命令**traffic-remark outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对匹配单个ACL规则的出方向的报文进行重标记。
     - 执行命令**traffic-remark inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } |

local-precedence *local-precedence-value* | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的入方向的报文进行重标记。

- 执行命令**traffic-remark inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的入方向的报文进行重标记。
- 执行命令**traffic-remark inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的入方向的报文进行重标记。
- 执行命令**traffic-remark outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的出方向的报文进行重标记。
- 执行命令**traffic-remark outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的出方向的报文进行重标记。
- 执行命令**traffic-remark outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }，对同时匹配二层ACL和三层ACL规则的出方向的报文进行重标记。

说明

X系列单板不支持**destination-mac** *mac-address*。

----结束

9.7 配置基于 ACL 的流量统计

背景信息

通过配置基于ACL的流量统计，对匹配指定ACL规则的报文进行流量统计。

操作步骤

- 在全局或VLAN上配置流量统计
  a. 执行命令**system-view**，进入系统视图。
  b. 请根据实际需要选择进行如下配置：

- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* | *l2-acl* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对匹配单个ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **inbound acl** { **ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* } | *user-acl* } [**rule** *rule-id*] [**by-bytes**]，对匹配单个ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]，对匹配单个ACL规则的出方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量统计。
- 执行命令**traffic-statistic** [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量统计。

- 在接口上配置流量统计
  a. 执行命令**system-view**，进入系统视图。
  b. 执行命令**interface** *interface-type interface-number*，进入接口视图。
  c. 请根据实际需要选择进行如下配置：
     - 执行命令**traffic-statistic inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* | *l2-acl* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对匹配单个ACL规则的入方向的报文进行流量统计。
     - 执行命令**traffic-statistic inbound acl** { **ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* } | *user-acl* } [**rule** *rule-id*] [**by-bytes**]，对匹配单个ACL规则的入方向的报文进行流量统计。

- 执行命令**traffic-statistic outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]，对匹配单个ACL规则的出方向的报文进行流量统计。
- 执行命令**traffic-statistic inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]，对同时匹配二层ACL和三层ACL规则的入方向的报文进行流量统计。
- 执行命令**traffic-statistic outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量统计。
- 执行命令**traffic-statistic outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量统计。
- 执行命令**traffic-statistic outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]，对同时匹配二层ACL和三层ACL规则的出方向的报文进行流量统计。

----结束

9.8 配置基于 ACL 的流镜像

通过配置基于ACL的流镜像，将匹配ACL规则的报文镜像到指定接口，以便于对报文进行分析。

有关基于ACL的流镜像的配置，请参见《 S12700, S12700E V200R023C00 配置指南-网络管理与监控 》镜像配置 中的“配置镜像”。

9.9 检查基于 ACL 的简化流策略配置结果

操作步骤

- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看全局、VLAN或接口上应用的基于ACL的简化流策略的配置信息。
- 执行命令**display traffic-applied brief**，查看设备上应用的基于ACL的简化流策略的概要配置信息。

- 执行命令**display traffic-applied record**，查看设备上所有应用的基于ACL的简化流策略的配置信息。

----结束

9.10 维护基于 ACL 的简化流策略

9.10.1 查看基于 ACL 的报文过滤的流量统计信息

背景信息

设备上配置基于ACL进行报文过滤后，用户需要了解报文通过和被丢弃的情况时，可以查看其流量统计信息。

操作步骤

- 执行以下命令查看设备上基于ACL的报文过滤的流量统计信息。
  - **display traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*]] [**secure**]
  - **display traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound acl** *user-acl* [**rule** *rule-id*]
  - **display traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *bas-acl* | *adv-acl* | *user-acl* } [**rule** *rule-id*]]
  - **display traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]] [**secure**]
  - **display traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]]
  - **display traffic-statistics interface inbound** [**secure**]
  - **display traffic-statistics interface outbound**
  - **display traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl ipv6** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]

----结束

9.10.2 清除基于 ACL 的报文过滤的流量统计信息

背景信息

当需要对基于ACL的报文过滤的流量统计信息重新进行统计时，可以执行以下命令，清除之前的统计信息。

须知

清除基于ACL的报文过滤的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

- 执行以下命令清除设备上基于ACL的报文过滤的流量统计信息。
  - **reset traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*]] [**secure**]
  - **reset traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound acl** *user-acl* [**rule** *rule-id*]
  - **reset traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *bas-acl* | *adv-acl* | *user-acl* } [**rule** *rule-id*]]
  - **reset traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]] [**secure**]
  - **reset traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]]
  - **reset traffic-statistics** { **interface** | **vlan** } **inbound** [**secure**]
  - **reset traffic-statistics** { **interface** | **vlan** } **outbound**
  - **reset traffic-statistics** [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl ipv6** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]

----结束

9.11 基于 ACL 的简化流策略配置举例

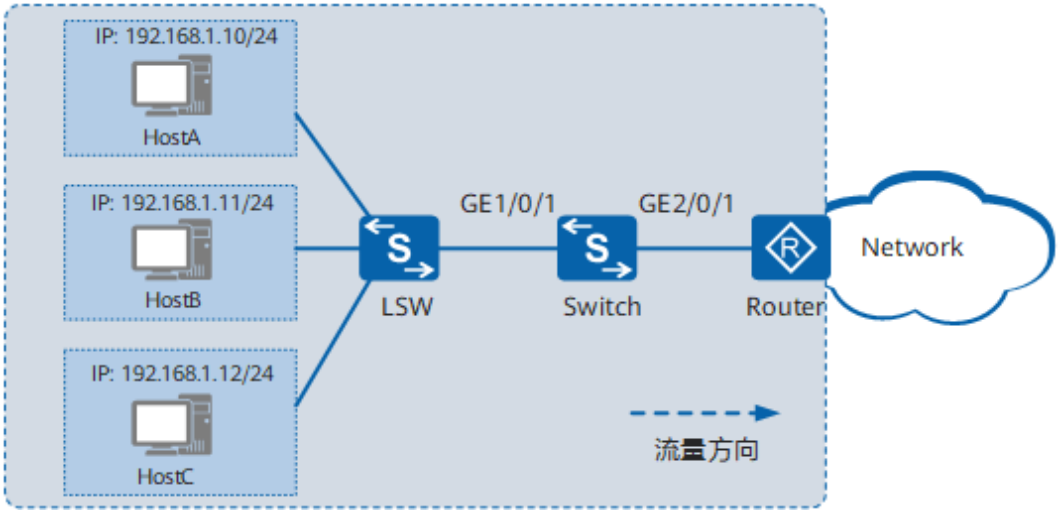
9.11.1 配置禁止指定主机访问网络示例

组网需求

如图9-1所示，用户通过Switch的接口GE2/0/1连接到外部网络设备。

每天8:30～18:00的时间段为工作时间，通过GE1/0/1接口对报文进行过滤，禁止访问外网。

图 9-1 配置禁止指定主机访问网络组网图



配置思路

采用包含禁止动作的流策略方式实现报文过滤，具体配置思路如下：

1. 配置各接口，实现用户能通过Switch访问外部网络。
2. 配置时间范围，用于在ACL中引用。
3. 配置ACL，在工作时间段禁止报文通过。
4. 在接口GE1/0/1的入方向配置报文过滤。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN10。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 10
[Switch-vlan10] quit
```

配置Switch上接口GE1/0/1和GE2/0/1为Trunk类型接口，并加入VLAN10。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet2/0/1] quit
```

说明

请配置LSW与Switch对接的接口为Trunk类型，并加入VLAN10。

创建VLANIF10，并为VLANIF10配置IP地址192.168.1.1/24。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
```

说明

请配置Router与Switch对接的接口IP地址为192.168.1.2/24。

步骤2 创建周期时间段working_time，时间范围为每天的8:30～18:00。

```
[Switch] time-range working_time 08:30 to 18:00 working-day
```

步骤3 配置ACL 3001，配置三条规则，分别为禁止源IP地址为192.168.1.10、192.168.1.11、192.168.1.12的报文在工作时间通过。

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule deny ip source 192.168.1.10 0 time-range working_time
[Switch-acl-adv-3001] rule deny ip source 192.168.1.11 0 time-range working_time
[Switch-acl-adv-3001] rule deny ip source 192.168.1.12 0 time-range working_time
[Switch-acl-adv-3001] quit
```

步骤4 在接口GE1/0/1的入方向配置报文过滤。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-filter inbound acl 3001
[Switch-GigabitEthernet1/0/1] quit
```

步骤5 验证配置结果

看设备接口入方向上应用的ACL规则和流动作信息。

```
[Switch] display traffic-applied interface gigabitethernet 1/0/1 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet1/0/1

ACL 3001
 rule 5 deny ip source 192.168.1.10 0 time-range working_time (match-counter 0)
ACTIONS:
 filter
-------------------------------------------------------------

ACL 3001
 rule 10 deny ip source 192.168.1.11 0 time-range working_time (match-counter 0)
ACTIONS:
 filter
-------------------------------------------------------------

ACL 3001
 rule 15 deny ip source 192.168.1.12 0 time-range working_time (match-counter 0)
ACTIONS:
 filter
-------------------------------------------------------------
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 10
#
time-range working_time 08:30 to 18:00 working-day
#
acl number 3001
 rule 5 deny ip source 192.168.1.10 0 time-range working_time
 rule 10 deny ip source 192.168.1.11 0 time-range working_time
 rule 15 deny ip source 192.168.1.12 0 time-range working_time
```



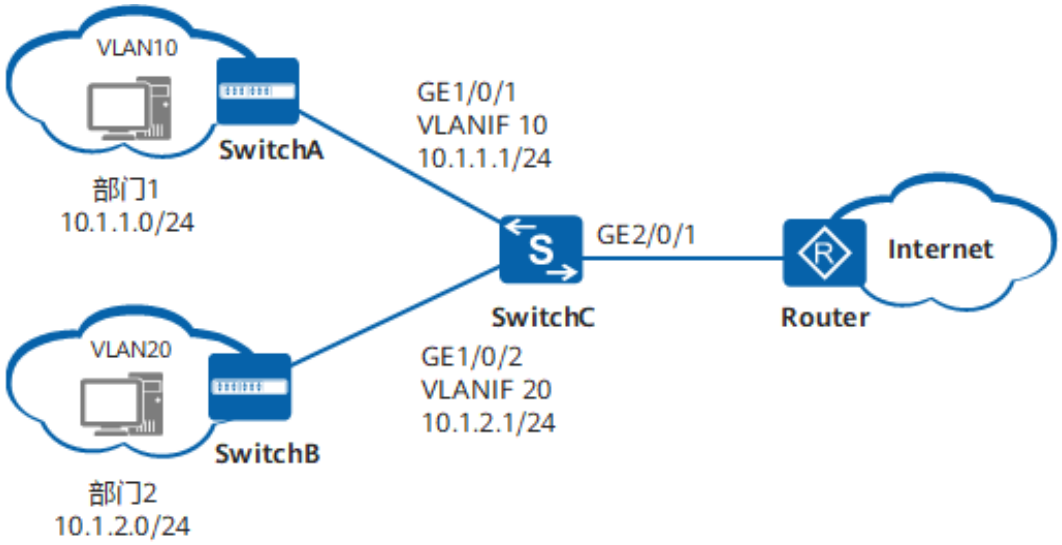
```
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-filter inbound acl 3001
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

9.11.2 配置限制不同网段的用户互访示例

组网需求

如图9-2所示，部门1和部门2可经由SwitchC和路由器访问网络。为方便管理网络，管理员将部门1和部门2划分在不同VLAN之中，规划了两个网段的IP地址。现要求SwitchC能够限制两个网段之间互访。

图 9-2 限制不同网段的用户互访组网图



配置思路

采用如下的思路在SwitchC上进行配置：

1. 配置接口所属的VLAN以及接口的IP地址。
2. 配置ACL，用于匹配两个部门互访的报文。
3. 在接口GE1/0/1和GE1/0/2的入方向配置报文过滤，使SwitchC丢弃匹配ACL规则的报文。

操作步骤

步骤1 配置接口所属的VLAN以及接口的IP地址

创建VLAN10和VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] vlan batch 10 20
```

配置SwitchC的接口GE1/0/1和GE1/0/2为Trunk类型接口，并分别加入VLAN10和VLAN20。

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk allow-pass vlan 20
[SwitchC-GigabitEthernet1/0/2] quit
```

创建VLANIF10和VLANIF20，并配置各VLANIF接口的IP地址。

```
[SwitchC] interface vlanif 10
[SwitchC-Vlanif10] ip address 10.1.1.1 24
[SwitchC-Vlanif10] quit
[SwitchC] interface vlanif 20
[SwitchC-Vlanif20] ip address 10.1.2.1 24
[SwitchC-Vlanif20] quit
```

步骤2 配置ACL

创建高级ACL 3001并配置ACL规则，拒绝两个网段之间互访的报文通过。

```
[SwitchC] acl 3001
[SwitchC-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[SwitchC-acl-adv-3001] rule deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[SwitchC-acl-adv-3001] quit
```

步骤3 配置基于ACL的报文过滤

在接口GE1/0/1和GE1/0/2的入方向配置基于ACL 3001的报文过滤。

```
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] traffic-filter inbound acl 3001
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] traffic-filter inbound acl 3001
[SwitchC-GigabitEthernet1/0/2] quit
```

步骤4 验证配置结果

查看ACL规则的配置信息。

```
[SwitchC] display acl 3001
Advanced ACL 3001, 2 rules
Acl's step is 5
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
 rule 10 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

查看基于ACL的简化流策略的应用记录。

```
[SwitchC] display traffic-applied record
-------------------------------------------------------------------------
*interface GigabitEthernet1/0/1
 traffic-filter inbound acl 3001
  slot 1: success

-------------------------------------------------------------------------
*interface GigabitEthernet1/0/2
 traffic-filter inbound acl 3001
```



```
 slot 1: success

------------------------------------------------------------------------------
```

部门1和部门2所在的两个网段之间不能互访。

----结束

配置文件

SwitchC的配置文件

```
#
sysname SwitchC
#
vlan batch 10 20
#
acl number 3001
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 10 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-filter inbound acl 3001
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-filter inbound acl 3001
#
return
```

9.11.3 配置对不同 VLAN 业务分别限速示例

组网需求

网络中的语音业务对应的VLAN ID为120，视频业务对应的VLAN ID为110，数据业务对应的VLAN ID为100。

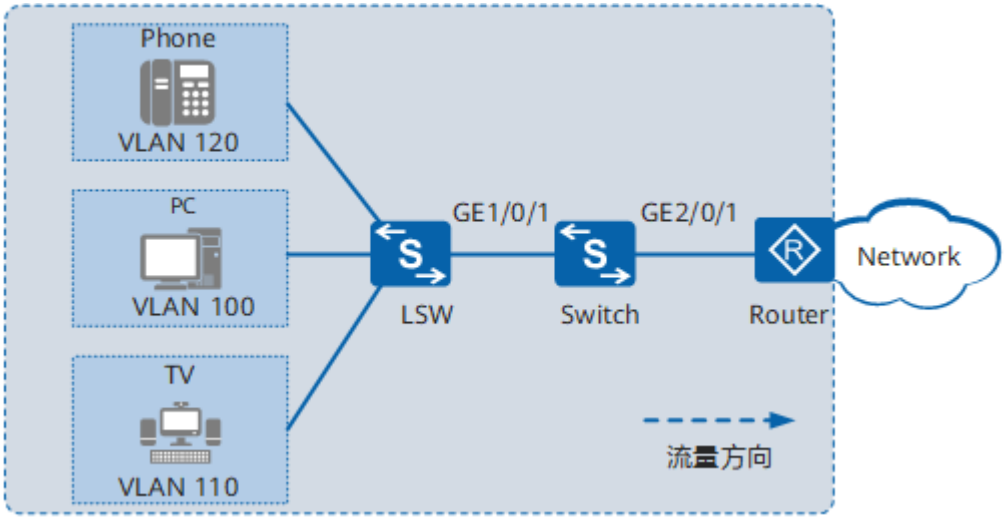
在Switch上需要对不同业务的报文分别进行流量监管，以将流量限制在一个合理的范围之内，并保证各业务的带宽需求。

具体配置需求如表9-1所示。

表 9-1 Switch 为上行流量提供的 QoS 保障

流量类型	CIR(kbps)	PIR(kbps)
语音	2000	10000
视频	4000	10000
数据	4000	10000

图 9-3 流量监管配置组网图



配置思路

采用如下的思路配置基于ACL的简化流策略实现流量监管：

1. 创建VLAN，并配置各接口，使用户能够通过Switch访问网络。
2. 在Switch上配置ACL匹配不同的VLAN ID以区分不同的业务。
3. 在Switch上配置基于ACL的流量监管，对报文分别限速。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN 100、110、120。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 110 120
```

将接口GE1/0/1、GE2/0/1的接入类型分别配置为trunk，并分别将接口GE1/0/1和GE2/0/1加入VLAN 100、VLAN 110、VLAN 120。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 110 120
[Switch-GigabitEthernet2/0/1] quit
```

步骤2 配置ACL

在Switch上创建二层ACL，对不同业务流按照其VLAN ID进行分类。

```
[Switch] acl 4001
[Switch-acl-L2-4001] rule 1 permit vlan-id 120
[Switch-acl-L2-4001] quit
[Switch] acl 4002
[Switch-acl-L2-4002] rule 1 permit vlan-id 110
```



```
[Switch-acl-L2-4002] quit
[Switch] acl 4003
[Switch-acl-L2-4003] rule 1 permit vlan-id 100
[Switch-acl-L2-4003] quit
```

步骤3 配置流量监管

在Switch的接口GE1/0/1入方向上配置流量监管，对报文进行限速。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-limit inbound acl 4001 cir 2000 pir 10000
[Switch-GigabitEthernet1/0/1] traffic-limit inbound acl 4002 cir 4000 pir 10000
[Switch-GigabitEthernet1/0/1] traffic-limit inbound acl 4003 cir 4000 pir 10000
[Switch-GigabitEthernet1/0/1] quit
```

步骤4 验证配置结果

查看设备接口入方向上应用的ACL规则和流动作信息。

```
[Switch] display traffic-applied interface gigabitethernet 1/0/1 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet1/0/1

ACL 4001
 rule 1 permit vlan-id 120
ACTIONS:
 limit cir 2000 ,cbs 250000
       pir 10000 ,pbs 1250000
       green : pass
       yellow : pass
       red : drop
-------------------------------------------------------------

ACL 4002
 rule 1 permit vlan-id 110
ACTIONS:
 limit cir 4000 ,cbs 500000
       pir 10000 ,pbs 1250000
       green : pass
       yellow : pass
       red : drop
-------------------------------------------------------------

ACL 4003
 rule 1 permit vlan-id 100
ACTIONS:
 limit cir 4000 ,cbs 500000
       pir 10000 ,pbs 1250000
       green : pass
       yellow : pass
       red : drop
-------------------------------------------------------------
```

----结束

配置文件

Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 110 120
#
acl number 4001
 rule 1 permit vlan-id 120
acl number 4002
 rule 1 permit vlan-id 110
```



```
acl number 4003
 rule 1 permit vlan-id 100
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
 traffic-limit inbound acl 4001 cir 2000 pir 10000 cbs 250000 pbs 1250000
 traffic-limit inbound acl 4002 cir 4000 pir 10000 cbs 500000 pbs 1250000
 traffic-limit inbound acl 4003 cir 4000 pir 10000 cbs 500000 pbs 1250000
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 110 120
#
return
```

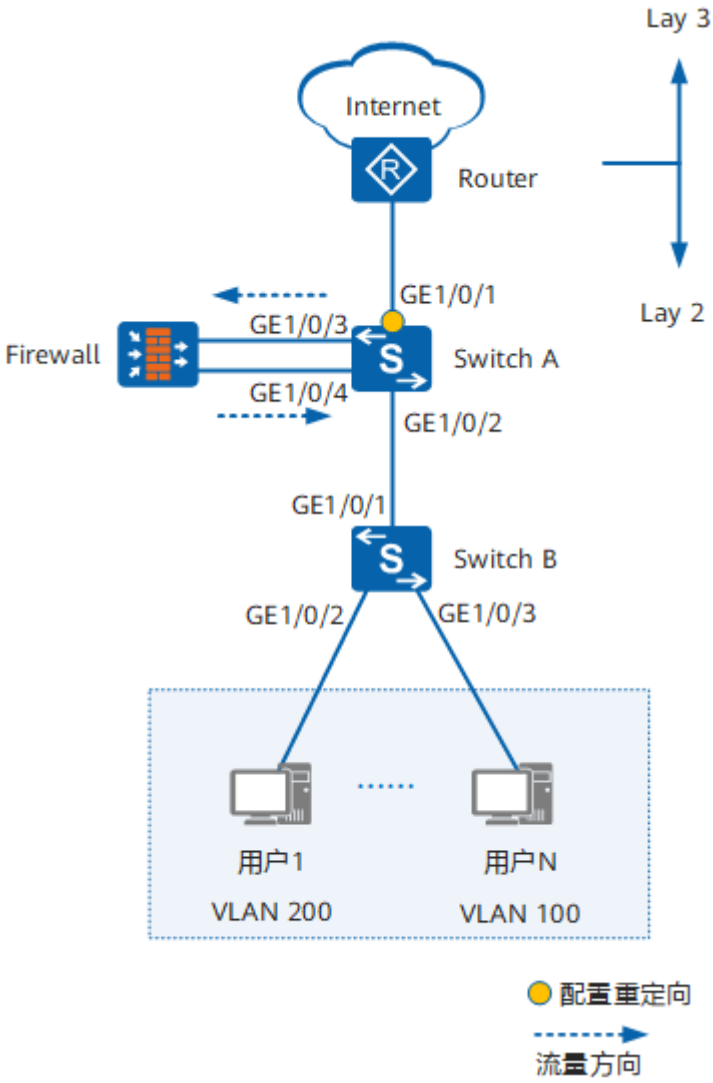
9.11.4 配置基于 ACL 的重定向示例

组网需求

如图9-4所示，由于业务需要，用户有访问Internet的需求。用户通过接入层交换机SwitchB和核心层交换机SwitchA以及接入网关Router与Internet进行通信。

为了保证数据和网络的安全性，用户希望保证Internet到服务器全部流量的安全性，配置重定向将外网到内网的全部流量送至防火墙进行安全过滤。

图 9-4 配置重定向的组网图



配置思路

- 出于安全性考虑，在SwitchA上旁挂一台核心防火墙Firewall，对流量进行安全过滤。
- 由于进入防火墙的流量是二层流量，因此通过重定向到接口将来自Internet的所有流量重定向到防火墙进行安全过滤。
- 为了防止出现环路，在SwitchA与防火墙相连的接口上配置端口隔离，并配置禁止MAC地址学习防止MAC漂移。

操作步骤

步骤1 创建VLAN并配置各接口，保证二层互通

在SwitchB上创建VLAN100和VLAN200。


```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] vlan batch 100 200
```

配置SwitchB上接口GE1/0/2和GE1/0/3的接口类型为Access，并将GE1/0/2加入VLAN200，将GE1/0/3加入VLAN100，配置GE1/0/1的接口类型为Trunk，并将GE1/0/1加入VLAN100和VLAN200。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type access
[SwitchB-GigabitEthernet1/0/2] port default vlan 200
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type access
[SwitchB-GigabitEthernet1/0/3] port default vlan 100
[SwitchB-GigabitEthernet1/0/3] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 200
[SwitchB-GigabitEthernet1/0/1] quit
```

在SwitchA上创建VLAN100和VLAN200。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200
```

配置SwitchA上接口GE1/0/1、GE1/0/2、GE1/0/3和GE1/0/4接口类型为Trunk，并将它们都加入VLAN100和VLAN200。将接口GE1/0/3和GE1/0/4加入同一个端口隔离组，配置接口GE1/0/4禁止MAC地址学习防止MAC漂移。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-GigabitEthernet1/0/1] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/3] port-isolate enable
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-type trunk
[SwitchA-GigabitEthernet1/0/4] port trunk allow-pass vlan 100 200
[SwitchA-GigabitEthernet1/0/4] port-isolate enable
[SwitchA-GigabitEthernet1/0/4] mac-address learning disable
[SwitchA-GigabitEthernet1/0/4] quit
```

步骤2 配置基于ACL的重定向实现防火墙流量过滤

配置基本ACL匹配所有允许通过的报文。

```
[SwitchA] acl 4001
[SwitchA-acl-L2-4001] rule permit vlan-id 100
[SwitchA-acl-L2-4001] rule permit vlan-id 200
[SwitchA-acl-L2-4001] quit
```

在SwitchA的GigabitEthernet1/0/1入方向配置重定向报文到指定接口。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] traffic-redirect inbound acl 4001 interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/1] quit
```

步骤3 验证配置结果

查看设备接口入方向上应用的ACL规则和流动作信息。


```
[SwitchA] display traffic-applied interface gigabitethernet 1/0/1 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet1/0/1

ACL 4001
 rule 5 permit vlan-id 100
ACTIONS:
 redirect interface GigabitEthernet1/0/3
-------------------------------------------------------------

ACL 4001
 rule 10 permit vlan-id 200
ACTIONS:
 redirect interface GigabitEthernet1/0/3
-------------------------------------------------------------
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 100 200
#
acl number 4001
 rule 5 permit vlan-id 100
 rule 10 permit vlan-id 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
 traffic-redirect inbound acl 4001 interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
 port-isolate enable group 1
#
interface GigabitEthernet1/0/4
 port link-type trunk
 mac-address learning disable
 port trunk allow-pass vlan 100 200
 port-isolate enable group 1
#
return
```

- SwitchB的配置文件

```
#
sysname SwitchB
#
vlan batch 100 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 200
#
interface GigabitEthernet1/0/3
 port link-type access
```



```
 port default vlan 100
#
return
```

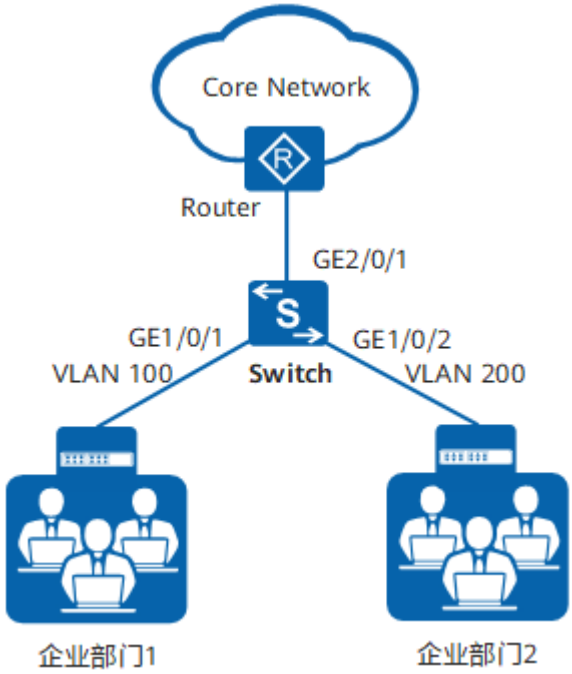
9.11.5 配置基于 ACL 的简化流策略进行优先级映射示例

组网需求

如图9-5所示，Switch通过接口GE2/0/1与路由器互连，企业部门1和企业部门2可经由Switch和路由器访问网络。企业部门1和企业部门2的VLAN ID分别为100、200。

由于企业部门1的服务等级高，需要得到更好的QoS保证。来自企业部门1和企业部门2的报文802.1p值均为0，通过定义优先级映射，将来自企业部门1的数据报文优先级映射为4，将来自企业部门2的数据报文优先级映射为2，以提供差分服务。

图 9-5 优先级映射配置组网图



配置思路

采用如下的思路配置优先级映射：

1. 创建VLAN，并配置各接口，保证用户能够通过Switch访问网络。
2. 配置ACL，根据不同的VLAN区分不同的部门。
3. 在Switch入接口GE1/0/1和GE1/0/2配置优先级映射。

操作步骤

步骤1 创建VLAN并配置各接口

创建VLAN 100和VLAN200。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
```

将接口GE1/0/1、GE1/0/2、GE2/0/1的接入类型分别配置为trunk，并分别将接口GE1/0/1、GE1/0/2加入VLAN 100、VLAN 200；接口GE2/0/1加入VLAN 100和VLAN 200。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 200
[Switch-GigabitEthernet2/0/1] quit
```

步骤2 配置优先级映射

在Switch上配置ACL 4001和ACL 4002，根据VLAN ID区分不同的部门。

```
[Switch] acl 4001
[Switch-acl-L2-4001] rule permit vlan-id 100
[Switch-acl-L2-4001] quit
[Switch] acl 4002
[Switch-acl-L2-4002] rule permit vlan-id 200
[Switch-acl-L2-4002] quit
```

步骤3 Switch入接口GE1/0/1和GE1/0/2配置优先级映射

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-remark inbound acl 4001 8021p 4
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] traffic-remark inbound acl 4002 8021p 2
[Switch-GigabitEthernet1/0/2] quit
```

步骤4 验证配置结果

看设备接口入方向上应用的ACL规则和流动作信息。

```
[Switch] display traffic-applied interface gigabitethernet 1/0/1 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet1/0/1

ACL 4001
 rule 5 permit vlan-id 100
ACTIONS:
 remark 8021p 4
-------------------------------------------------------------
[Switch] display traffic-applied interface gigabitethernet 1/0/2 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet1/0/2

ACL 4002
 rule 5 permit vlan-id 200
ACTIONS:
 remark 8021p 2
-------------------------------------------------------------
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 100 200
#
acl number 4001
 rule 5 permit vlan-id 100
acl number 4002
 rule 5 permit vlan-id 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
 traffic-remark inbound acl 4001 8021p 4
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 traffic-remark inbound acl 4002 8021p 2
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
return
```

9.11.6 配置基于 ACL 的流量统计示例

组网需求

如图9-6所示，PC1的MAC地址为00e0-fc12-3456，它连接在Switch的GE1/0/1端口上，实现与其他设备的互连互通。现希望Switch对源MAC为00e0-fc12-3456的报文进行流量统计。

图 9-6 配置流量统计组网图

配置思路

通过ACL匹配指定源MAC主机的报文实现对其进行流量统计，具体配置思路如下：

1. 配置各接口，实现Switch与Router、PC1互通。
2. 配置ACL规则，匹配源MAC为00e0-fc12-3456的报文。
3. 在接口GE1/0/1入方向配置流量统计，对该接口收到的源MAC为00e0-fc12-3456的报文进行统计。

操作步骤

步骤1 创建VLAN并配置各接口

在Switch上创建VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 20
[Switch-vlan20] quit
```

配置接口GE1/0/1为Access类型接口，接口GE1/0/2为Trunk类型接口，并将GE1/0/1和GE1/0/2加入VLAN20。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type access
[Switch-GigabitEthernet1/0/1] port default vlan 20
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 20
[Switch-GigabitEthernet1/0/2] quit
```

创建VLANIF20，并配置IP地址10.10.10.2/24。

```
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 10.10.10.2 24
[Switch-Vlanif20] quit
```

说明

请配置Router与Switch对接的接口IP地址为10.10.10.1/24。

步骤2 配置ACL规则

在Switch上创建编码为4000的二层ACL，匹配源MAC为00e0-fc12-3456的报文。

```
[Switch] acl 4000
[Switch-acl-L2-4000] rule permit source-mac 00e0-fc12-3456 ffff-ffff-ffff
[Switch-acl-L2-4000] quit
```

步骤3 配置流量统计

在接口GE1/0/1入方向配置基于ACL的流量统计。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] traffic-statistic inbound acl 4000 by-bytes
[Switch-GigabitEthernet1/0/1] quit
```

步骤4 验证配置结果

查看设备接口入方向上应用的ACL规则和流动作信息。

```
[Switch] display traffic-applied interface gigabitethernet 1/0/1 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet1/0/1

ACL 4000
 rule 5 permit source-mac 00e0-fc12-3456
ACTIONS:
 statistic by bytes
-------------------------------------------------------------
```

查看流量统计信息。

```
[Switch] display traffic-statistics interface gigabitethernet 1/0/1 inbound acl 4000
-------------------------------------------------------------------------------
Interface GigabitEthernet1/0/1
 ACL:4000 Rule:5
    matched:681.575M Bytes, passed:681.575M Bytes, dropped:0 Bytes
```

----结束

配置文件

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 20
#
acl number 4000
 rule 5 permit source-mac 00e0-fc12-3456
#
interface Vlanif20
 ip address 10.10.10.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 20
 traffic-statistic inbound acl 4000 by-bytes
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

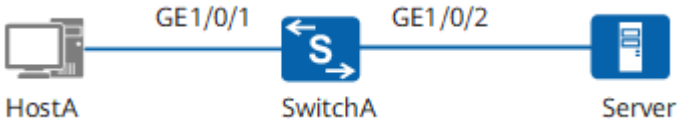
9.11.7 配置基于 ACL 的本地流镜像示例

组网需求

如图9-7所示，HostA通过接口GigabitEthernet1/0/1接入SwitchA。Server直连在SwitchA的GigabitEthernet1/0/2接口上。

用户希望通过监控设备Server对HostA发出的802.1p优先级为6的报文进行监控。

图 9-7 配置本地流镜像组网图



配置思路

采用如下的思路配置：

1. 配置接口GigabitEthernet1/0/2为本地观察端口，使直连的监控设备Server能够接收到镜像报文。
2. 配置二层ACL，匹配802.1p优先级为6的报文。
3. 在接口GigabitEthernet1/0/1上配置基于ACL的流策略，对匹配802.1p优先级为6的报文进行镜像。

操作步骤

步骤1 配置观察端口

在SwitchA上配置GigabitEthernet1/0/2为观察端口。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] observe-port 1 interface gigabitethernet 1/0/2
```

步骤2 配置二层ACL，匹配802.1p优先级为6的报文。

在SwitchA上创建编号为4001的ACL，并配置规则是匹配802.1p优先级为6的报文。

```
[SwitchA] acl 4001
[SwitchA-acl-L2-4001] rule permit 8021p 6
[SwitchA-acl-L2-4001] quit
```

步骤3 配置基于ACL的流策略

在SwitchA的接口GigabitEthernet1/0/1上配置基于ACL的流策略，对匹配802.1p优先级为6的报文进行镜像。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] traffic-mirror inbound acl 4001 to observe-port 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] quit
```

步骤4 验证配置结果

查看接口GigabitEthernet1/0/1入方向上应用的ACL规则和流行为信息。

```
<SwitchA> display traffic-applied interface gigabitethernet 1/0/1 inbound
-------------------------------------------------------------
ACL applied inbound interface GigabitEthernet1/0/1

ACL 4001
 rule 5 permit 8021p 6
ACTIONS:
 mirror to observe-port 1
-------------------------------------------------------------
```

从显示信息可以看出，接口GigabitEthernet1/0/1上应用的ACL规则和流行为是对匹配802.1p优先级为6的报文进行镜像。

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
observe-port 1 interface GigabitEthernet1/0/2
#
acl number 4001
 rule 5 permit 8021p 6
#
interface GigabitEthernet1/0/1
 traffic-mirror inbound acl 4001 to observe-port 1
#
return
```


10 HQoS 配置

10.1 HQoS 简介

HQoS（Hierarchical Quality of Service）采用多级队列调度的方式为多用户多业务提供精细化的QoS服务。

传统QoS技术可以满足语音、视频以及数据等业务的不同服务需求，可以针对不同的业务提供不同的服务。但是随着网络设备的高速发展，接入用户数量和每个用户的业务量不断增多，传统的QoS在应用中遇到了新问题：

- 传统QoS是基于端口带宽进行调度的，因此流量管理可以基于服务等级进行业务区分，却很难基于用户进行区分，比较适合部署在网络核心侧，但不适合部署在业务接入侧。
- 传统QoS无法做到同时对多个用户的多个业务进行流量管理和调度。

为了解决上述问题，人们需要一种既能区分用户流量又能根据用户业务的优先级进行调度的技术，HQoS应运而生。HQoS通过多级队列进一步细化区分业务流量，对多个用户、多种业务等传输对象进行统一管理和分层调度，在现有的硬件环境下使设备具备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建设成本。

相关信息

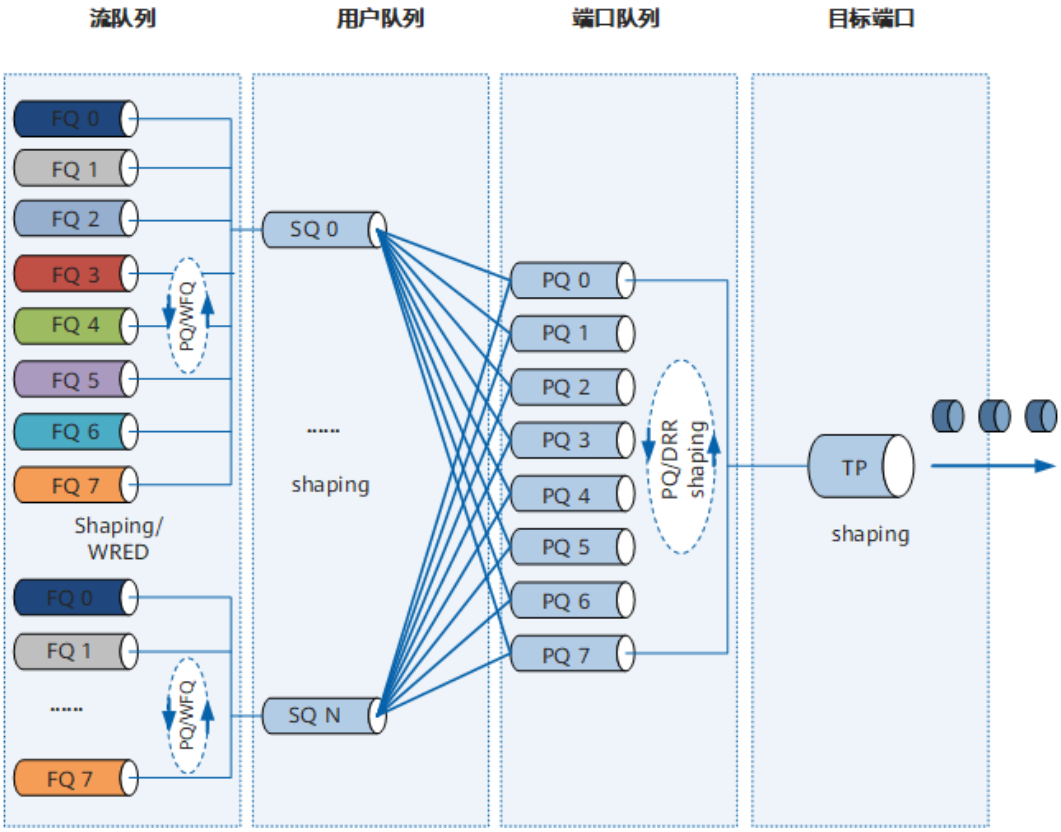
视频

S系列交换机HQoS特性介绍

10.2 HQoS 原理描述

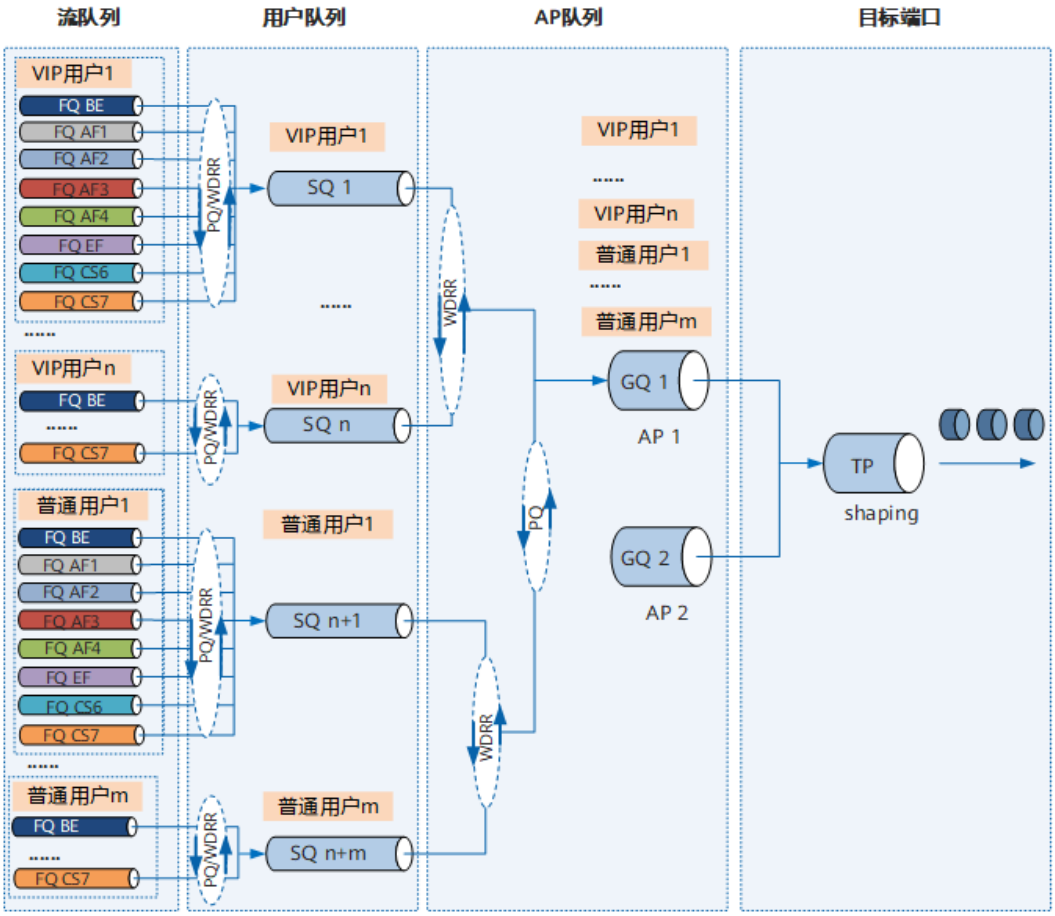
HQoS基于队列实现层次化调度，目前设备支持流队列（Flow Queue）和用户队列（Subscriber Queue）。队列以树状结构汇聚，流队列为叶子节点，用户队列为根节点。报文做层次化调度时，首先进入叶子节点，经过调度后，从根结点发送出去，同时可以进行下一步操作比如端口队列调度等。同时设备还支持从流队列到端口队列的映射功能，实现对不同用户的同一种业务的流量调度。如图10-1所示。

图 10-1 HQoS 队列调度示意图



有线无线用户认证授权场景下，在AC上进行HQoS时，设备会另外划分队列缓存，用于缓存需要层次化调度的业务流队列，并对这些流队列先进行一轮多层次化调度。目前设备支持流队列FQ（Flow Queue）、用户队列SQ（Subscriber Queue）和AP队列GQ（Subscriber Group Queue）。整个流程如图10-2所示。

图 10-2 HQoS 队列调度示意图（AC）



流队列

HQoS以DiffServ解决方案为基础，报文根据映射后的内部优先级进入对应的流队列，从而实现对业务的区分。每个用户都有8个流队列，分别对应8个业务优先级（BE、AF1、AF2、AF3、AF4、EF 、CS6、CS7），8个流队列可以配置PQ（优先级队列）或WFQ（加权公平队列）调度；每个流队列支持WRED（加权随机早期检测）以及流量整形，保证高优先级的业务能够得到优先调度和更高的带宽。

用户队列

用户队列主要用来区分不同的用户。

如图10-1所示，这里的用户通常是指一个VLAN（虚拟局域网）、VPN（虚拟私人网络）等，用户的划分主要通过ACL进行。每个用户有一个用户队列，它由8个流队列聚合而来。用户队列可以配置流量整形，限制每个用户的总带宽。

如图10-2所示，每个经过RADIUS授权HQoS属性的用户上线时都会被分配一个SQ，而其他用户会被分配到同一个SQ，即相应AP队列的默认SQ。VIP用户的SQ之间为WDRR调度，普通用户的SQ之间为WDRR调度，而VIP用户的SQ与普通用户的SQ之间为PQ调度。因此，当发生网络拥塞时，VIP用户的业务流量绝对优先。这里的“绝对优先”是指，即使是VIP用户的最低优先级报文，也会比普通用户的最高优先级报文优先得到调度。

端口队列

端口队列与流队列类似，8个端口队列对应8种业务类型。8个队列可以配置PQ或WDRR队列调度；每个队列支持配置WRED以及流量整形。具体配置可以参考**5.7 配置拥塞管理**、**5.5 配置拥塞避免（WRED丢弃模板模式）**和**4.7 配置流量整形**。设备支持配置流队列到端口队列的映射，队列映射是流队列的8个优先级队列（BE、AF1、AF2、AF3、AF4、EF、CS6、CS7）在入8个端口队列（BE、AF1、AF2、AF3、AF4、EF、CS6、CS7）时的一个入队列映射功能，通过建立流队列->端口队列的映射，可以灵活的控制流队列某一服务等级队列中的业务流量进入端口队列的某一服务等级队列。

AP 队列

每台AP对应一个GQ，即同一个AP下的所有用户就被归为一个GQ。一个GQ可以绑定多个SQ，但是一个SQ只能绑定到一个GQ内。AP队列之间为WDRR调度。

目标端口

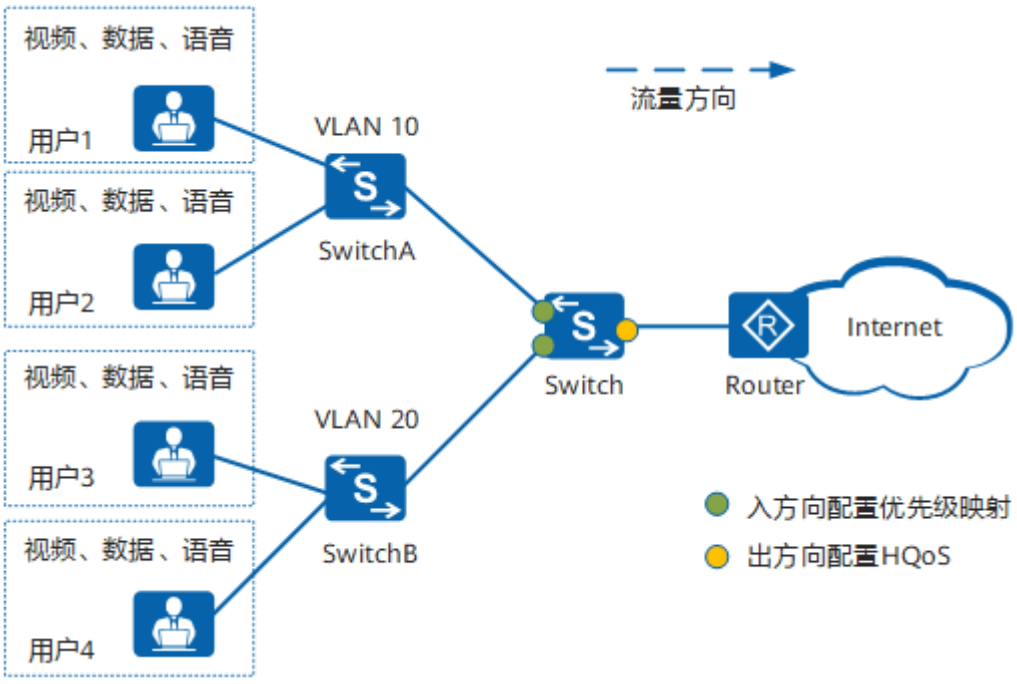
目标端口即设备的物理接口，数据最终通过目标端口转发出去，设备支持在完成上面的队列调度后还可以为每个目标端口配置流量整形。具体配置可以参考**4.8.2 配置出方向的接口限速**。

10.3 HQoS 应用场景

组网需求

网络中多个用户都有数据，语音和视频等多种不同的业务。受带宽限制，分别为接入VLAN10的用户和接入VLAN20的用户提供不同的带宽，同时为每个用户的三种业务提供不同的调度优先级，首先是语音业务，其次是视频业务，最后是数据业务，通过在园区网中部署HQoS可以实现上述需求，如**图10-3**所示。

图 10-3 HQoS 应用组网图



业务部署

- 部署优先级映射实现将不同业务的报文优先级映射为本地优先级并给报文标记颜色。
- 部署ACL区分不同的用户。
- 部署HQoS实现为不同用户的不同业务提供差分服务。

10.4 HQoS 配置注意事项

涉及网元

无需其他网元配合。

License 支持

HQoS是交换机的基本特性，无需获得License许可即可应用此功能。

V200R023C00 版本特性支持情况

对于S12700系列交换机，仅X1E系列单板支持HQoS。对于S12700E系列交换机，仅X6H单板支持HQoS。

说明

如需了解交换机软件配套详细信息，请点击**硬件中心**，并选择产品型号进行查询。

特性依赖和限制

- HQoS的规格如**表10-1**所示。

  表 10-1 HQoS 规格

项目	规格
设备支持的流队列个数	65528
设备支持的用户队列个数	V200R011C10之前版本：8191 V200R011C10及后续版本：8190
设备支持的能够进行流量统计的最大流队列个数	16376
设备支持的端口队列数	8
流队列WRED模板个数	128
流队列模板个数	128
流映射模板个数	8

- 设备目前只支持出方向的HQoS功能。

- 当不同用户的各个业务流优先级相同时，无法对不同的用户进行拥塞管理配置。
- 对于由支持HQoS的单板与不支持HQoS的单板组成的Eth-Trunk接口，不支持配置有线无线用户授权HQoS。因为用户流量会从不支持HQoS的单板转发，从而导致HQoS不生效。

10.5 HQoS 缺省配置

流队列WRED模板的缺省配值如表10-2所示；流队列模板的缺省配置如表10-3所示；流映射模板的缺省配置如表10-4所示；内部优先级与各流队列之间的映射关系如表10-5所示，映射关系不能修改。

表 10-2 流队列 WRED 模板的缺省配值

参数	缺省值
流队列WRED模板名称	default
WRED丢弃的下限百分比（红、黄、绿三色报文）	100
WRED丢弃的上限百分比（红、黄、绿三色报文）	100
WRED丢弃的最大丢弃概率（红、黄、绿三色报文）	100

表 10-3 流队列模板的缺省配置

参数	缺省值
流队列模板名称	default
流队列调度方式	PQ调度
流量整形速率	用户队列的峰值信息速率（PIR）
流队列WRED模板	default

表 10-4 流映射模板的缺省配置

参数	缺省值
流映射模板名称	default
队列映射关系	0～7号流队列分别对应0～7号端口队列

表 10-5 内部优先级与各流队列之间的映射关系表

内部优先级	流队列索引
BE	0
AF1	1
AF2	2
AF3	3
AF4	4
EF	5
CS6	6
CS7	7

10.6 配置 HQoS

配置HQoS之后，设备可以对不同用户的多种业务进行区分，提供不同的调度方式，实现精细化的差分服务。

说明

仅X1E系列单板和X6H系列单板支持HQoS功能。

前置任务

在配置HQoS之前，需要完成以下任务：

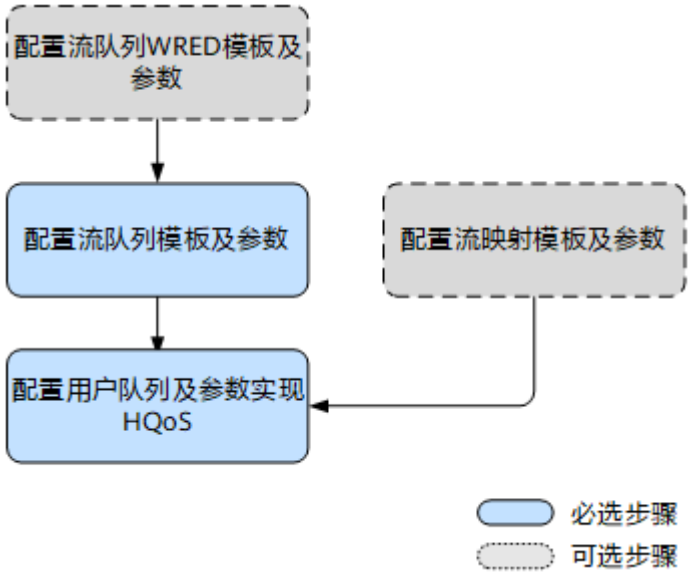
- 配置优先级映射，将报文的优先级映射为服务等级/颜色。

HQoS 配置流程

HQoS的配置流程如图10-4所示。

1. 用户希望对进入不同业务报文配置不同的丢弃优先级时，需要配置流队列WRED模板及参数。
2. 配置流队列模板以及调度方式和流量整形参数，如果上面的步骤配置了流队列WRED模板，需要在流队列模板中引用已配置的流队列WRED模板。
3. 当不同优先级的用户之间存在相同业务流量，且需要对这些来自不同用户的同一业务流量进行调度或者流量整形时，比如用户A的数据业务优先级高于用户B的数据业务优先级，需要配置流映射模板及参数调整流队列和端口队列之间的映射关系。
4. 配置用户队列及流量整形参数并引用流队列模板，如果上面的步骤中配置了流映射模板，需要在用户队列中引用已配置的流映射模板。

图 10-4 HQoS 配置流程图



说明

设备目前只支持出方向的HQoS功能。

10.6.1 配置流队列

背景信息

设备通过优先级映射将报文的优先级（802.1p优先级、MPLS-EXP优先级和DSCP优先级）映射为本地优先级，并为报文标记颜色。报文根据映射之后的本地优先级进入不同的流队列，从而实现对用户的不同业务的差分服务。优先级映射请参见**配置优先级映射**。

操作步骤

步骤1 （可选）配置流队列的WRED模板及相关拥塞避免参数。

1. 执行命令**system-view**，进入系统视图。
2. 执行命令**flow-wred-profile** *flow-wred-profile-name*，创建流队列WRED模板或进入已经创建的流队列WRED模板视图。

   缺省情况下，系统预定义了一个名为default的流队列WRED模板，该模板不支持修改和删除。
3. 执行命令**color** { **green** | **yellow** | **red** } **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*，配置WRED丢弃的上下限以及丢弃概率。
4. （可选）执行命令**queue-depth** *queue-depth-value*，配置流队列的长度。
5. 执行命令**quit**，退出流队列WRED模板视图。

   说明

   缺省default模板中WRED丢弃的上下限以及丢弃概率均为100，若用户需要调整各流队列的WRED丢弃参数实现拥塞避免则需要选择上述配置，否则流队列将引用系统预定义名为default的流队列WRED模板。

步骤2 配置流队列模板及相关参数，包括拥塞管理，流量整形和流队列WRED模板。

1. 执行命令**flow-queue-profile** *flow-queue-profile-name*，创建流队列模板或进入已经创建的流队列模板视图。

   缺省情况下，系统预定义了一个名为default的流队列模板，该模板不支持修改和删除。

2. 执行命令**qos queue** *queue-index* { { **pq** | **wfq weight** *weight-value* } | { **shaping** { *shaping-value* | **shaping-percentage** *shaping-percentage-value* } } | { **flow-wred-profile** *flow-wred-profile-name* } }*，配置流队列的调度方式、流量整形速率以及流队列WRED模板。

   如果未指定流队列WRED模板，则使用缺省的default模板。

----结束

10.6.2 （可选）配置流队列到端口队列的映射

背景信息

通过配置流队列到端口队列的映射，可以灵活的控制流队列中某一服务等级的业务流量进入端口队列的某一服务等级队列，实现对不同用户的同一业务流量的差分服务。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**flow-mapping-profile** *flow-mapping-profile-name*，创建流映射模板或进入已经创建的流映射模板视图。

缺省情况下，系统预定义了一个名为default的流映射模板，该模板不支持删除和修改。

步骤3 执行命令**map flow-queue** *flow-queue-index* **to port-queue** *port-queue-index*，配置流队列与端口队列的映射关系。

如果想要调整流队列与端口队列的映射关系，则选择上述配置，否则用户队列将引用系统预定义的名为default的流映射模板。

----结束

10.6.3 配置用户队列

背景信息

通过配置用户队列，可以为不同的用户配置不同的流量整形速率，从而实现为高优先级的用户提供更高的带宽。

如果不是用户认证授权场景，要将不同用户的流量通过ACL进行区分（比如源、目的MAC地址，源、目的IP地址，VLAN ID等），那么请执行操作步骤1～3，对匹配规则的用户队列报文进行流量整形，并引用流队列和流映射模板实现HQoS。

如果是有线无线用户认证授权场景，那么请执行操作步骤1、4、5、6和7，通过RADIUS服务器和业务方案授权的方式，实现HQoS调度。

说明

仅X1E和X6H系列单板支持操作步骤3和5。

仅S12700E支持操作步骤6。

仅S12700E的X6H单板支持操作步骤4和7。

X6H单板不支持引用流映射模板。

前置任务

执行操作步骤1～3前，请配置相应的ACL规则。

执行操作步骤1、4、5、6和7前，请配置WLAN基本业务和NAC。其中，操作步骤6和7仅支持使用统一模式部署NAC功能。

- WLAN基本业务的详细配置请参见《S12700, S12700E V200R023C00 配置指南-WLAN-AC配置》中的“WLAN基本业务配置”。
- NAC的详细配置请参见《S12700, S12700E V200R023C00 配置指南-用户接入与认证配置》中的“NAC配置（统一模式）”和“NAC配置（传统模式）”。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**interface** *interface-type interface-number*，进入接口视图。

步骤3 根据配置的ACL规则类型按照需要选择如下配置：

- 执行命令**traffic-user-queue outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name* | **flow-mapping-profile** *flow-mapping-profile-name*] *，对匹配单个ACL规则的用户队列报文进行流量整形，并引用流队列和流映射模板实现HQoS。
- 执行命令**traffic-user-queue outbound acl** { *l2-acl* | **name** *acl-name* } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name* | **flow-mapping-profile** *flow-mapping-profile-name*] *，对同时匹配二层ACL和三层ACL规则的用户队列报文进行流量整形，并引用流队列和流映射模板实现HQoS。
- 执行命令**traffic-user-queue outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } **acl** { *l2–acl* | **name** *acl-name* } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name* | **flow-mapping-profile** *flow-mapping-profile-name*] *，对同时匹配二层ACL和三层ACL规则的用户队列报文进行流量整形，并引用流队列和流映射模板实现HQoS。

步骤4 （可选）在AP上线前，开启AC下行到AP的流量整形功能。

1. 执行命令**wlan**，进入WLAN视图。
2. 执行命令**ap auto-shaping enable**，开启AC下行到AP的流量整形功能。

   缺省情况下，设备关闭AC下行到AP的流量整形功能。对于配置本命令前已经上线的AP，本命令不生效。
3. 执行命令**quit**，返回系统视图。

步骤5 在QoS模板中创建用户队列，实现HQoS调度。该功能通过RADIUS服务器授权RADIUS属性实现，使用编号为26-17的华为RADIUS扩展属性HW-Subscriber-QoS-Profile，设备侧需要进行如下配置：

说明

无线用户中，仅数据转发方式为隧道转发且获取地址后的IPv4用户支持授权属性HW-Subscriber-QoS-Profile。

已经被授权属性HW-Subscriber-QoS-Profile的用户，不支持通过重认证方式删除该授权。

1. 执行命令**qos-profile name** *profile-name*，创建QoS模板并进入QoS模板视图，或进入已经存在的QoS模板视图。

   缺省情况下，未配置任何QoS模板。

2. 执行命令**user-queue** { **pir** *pir-value* | **flow-queue-profile** *flow-queue-profile-name* | **flow-mapping-profile** *flow-mapping-profile-name* }*，创建用户队列实现HQoS调度。

   如果需要配置自定义的流队列模板和流映射模板，则需要先执行命令**flow-queue-profile**和**flow-mapping-profile**，如果使用缺省的default模板则无需配置。

3. 执行命令**quit**，返回系统视图。

步骤6 （可选）通过业务方案授权，重标记报文的内部优先级。在SAC模板中配置基于用户ACL的重标记内部优先级，使设备根据重标记后的优先级对匹配ACL的报文进行调度。

1. 执行命令**sac-profile name** *profile-name*，创建SAC模板并进入SAC模板视图，或进入已经存在的SAC模板视图。

   缺省情况下，设备未配置任何SAC模板。

2. 执行命令**acl** { *ucl-number* | **name** *acl-name* } **remark local-precedence** *local-precedence-value*，配置基于用户ACL的重标记内部优先级。

   缺省情况下，SAC模板中没有配置基于用户ACL的重标记内部优先级。

3. 执行命令**quit**，返回到系统视图。
4. 执行命令**aaa**，进入AAA视图。
5. 执行命令**service-scheme** *service-scheme-name*，创建一个业务方案并进入业务方案视图。

   缺省情况下，设备中没有创建业务方案。

6. 执行命令**sac-profile** *profile-name*，将SAC模板绑定到业务方案中。
7. 执行命令**quit**，返回到AAA视图。

步骤7 （可选）通过业务方案授权，指定用户为VIP用户或普通用户。

1. 执行命令**aaa**，进入AAA视图。
2. 执行命令**service-scheme** *service-scheme-name*，创建一个业务方案并进入业务方案视图。

   缺省情况下，设备中没有创建业务方案。

3. 执行命令**priority** *priority-value*，在业务方案中配置用户的优先级。

   缺省情况下，用户的优先级为0。若配置用户的优先级为1，则表示VIP用户；若配置用户的优先级为0，则表示普通用户。

4. 执行命令**quit**，返回到AAA视图。
5. 执行命令**quit**，返回系统视图。

----结束

10.6.4 检查 HQoS 配置结果

操作步骤

- 执行命令**display flow-wred-profile** [**name** *flow-wred-profile-name* | **all**]，查看流队列WRED模板的配置信息。
- 执行命令**display flow-queue-profile** [**name** *flow-queue-profile-name* | **all**]，查看流队列模板的配置信息。
- 执行命令**display flow-mapping-profile** [**name** *flow-mapping-profile-name* | **all**]，查看流映射模板的配置信息。
- 执行命令**display traffic-applied** [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]，查看用户队列的配置信息。

----结束

10.7 维护 HQoS

10.7.1 查看用户队列流量统计信息

背景信息

设备上配置用户队列实现HQoS后，用户需要了解用户队列中各个流队列报文通过和被丢弃的情况时，可以根据用户队列匹配的ACL规则选择相应的命令查看其流量统计信息。

操作步骤

- 执行命令**display traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl** { *bas-acl* | *adv-acl* } [**acl** { *l2-acl* | **name** *acl-name* }]，查看用户队列的流量统计信息。
- 执行命令**display traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl** *l2-acl* [**acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }]，查看用户队列的流量统计信息。
- 执行命令**display traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl name** *name-acl* [**acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* }]，查看用户队列的流量统计信息。
- 执行命令**display traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* }，查看用户队列的流量统计信息。

----结束

10.7.2 清除用户队列流量统计信息

背景信息

当需要对用户队列的流量信息重新进行统计时，可以根据用户队列匹配的ACL规则在用户视图下执行以下命令，清除之前的统计信息。

须知

清除用户队列的流量统计信息后，以前的统计信息将无法恢复，请于清除之前仔细确认。

操作步骤

步骤1 执行命令**reset traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl** { *bas-acl* | *adv-acl* } [**acl** { *l2-acl* | **name** *acl-name* }]，清除用户队列的流量统计信息。

步骤2 执行命令**reset traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl** *l2-acl* [**acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }]，清除用户队列的流量统计信息。

步骤3 执行命令**reset traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl name** *acl-name* [**acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* }]，清除用户队列的流量统计信息。

步骤4 执行命令**reset traffic-user-queue statistics interface** *interface-type interface-number* **outbound acl ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* }，清除用户队列的流量统计信息。

----结束

10.8 HQoS 配置举例

10.8.1 配置 HQoS 示例（基于 ACL 配置用户队列）

组网需求

网络中有多个用户，每个用户都有语音，视频和数据三种不同的业务，其携带的802.1p优先级分别为6、5、2。现在需要优先保证语音业务的带宽，其次是视频业务，最后是数据业务。配置需求如表10-6和表10-7所述。

由于带宽有限，除了需要区分不同业务的优先级之外还需要针对不同的用户进行流量整形，为多个用户提供不同的带宽，配置需求如表10-8所述。

表 10-6 流队列拥塞避免配置参数

业务类型	颜色	阈值下限（%）	阈值上限（%）	丢弃概率
语音	绿	80	100	10

业务类型	颜色	阈值下限（%）	阈值上限（%）	丢弃概率
视频	黄	60	80	20
数据	红	40	60	40

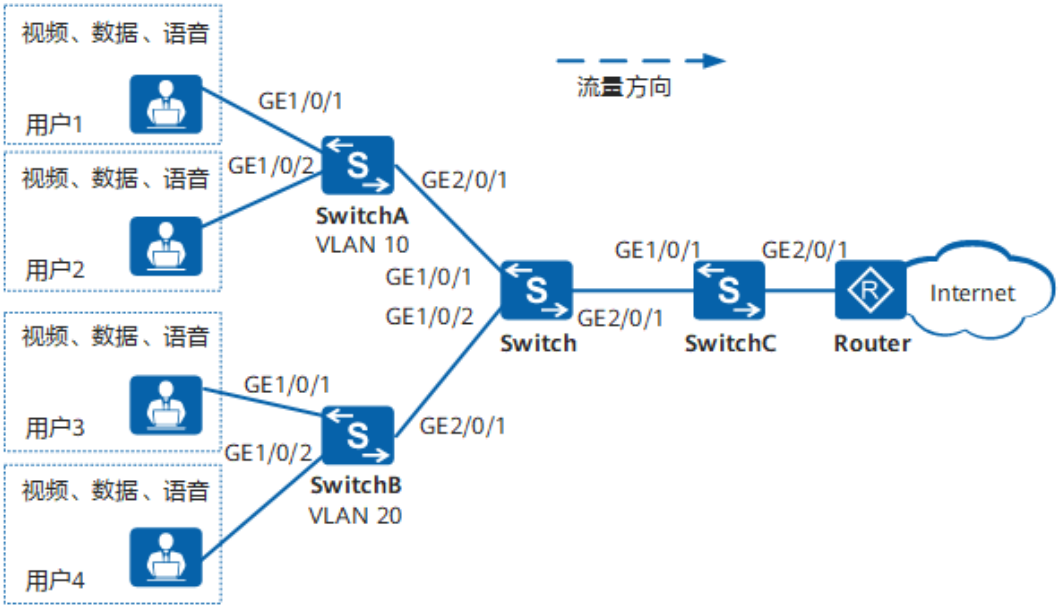
表 10-7 流队列拥塞管理配置参数

业务类型	服务等级
语音	EF
视频	AF3
数据	AF1

表 10-8 用户队列流量整形配置参数

用户	峰值带宽
属于VLAN10的用户	8000kbit/s
属于VLAN20的用户	5000kbit/s

图 10-5 配置 HQoS 组网图



配置思路

采用如下的思路配置HQoS：

1. 创建VLAN，并配置各接口，使用户能够通过Switch访问网络。
2. 在Switch上配置创建并配置DiffServ域，将802.1p优先级映射为PHB行为并为报文着色，并在Switch入接口上绑定DiffServ域。
3. 在Switch上配置流队列WRED模板和流队列模板及相关参数，以实现为不同的业务提供不同的调度优先级，丢弃参数及流量整形参数。
4. 在Switch上配置ACL规则，通过VLAN区分来自不同用户的数据流量。
5. 在Switch上配置用户队列及流量整形参数，通过引用流队列WRED模板和流队列模板实现HQoS。

操作步骤

步骤1 创建VLAN并配置各接口

在SwitchA上创建VLAN10，配置SwitchA上接口GE1/0/1、GE1/0/2的接口类型为Access，并加入VLAN10，配置接口GE2/0/1的接口类型为Trunk，并加入VLAN10。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type access
[SwitchA-GigabitEthernet1/0/1] port default vlan 10
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type access
[SwitchA-GigabitEthernet1/0/2] port default vlan 10
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 2/0/1
[SwitchA-GigabitEthernet2/0/1] port link-type trunk
[SwitchA-GigabitEthernet2/0/1] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet2/0/1] quit
```

在SwitchB上创建VLAN20，配置SwitchB上接口GE1/0/1、GE1/0/2的接口类型为Access，并加入VLAN20，配置接口GE2/0/1的接口类型为Trunk，并加入VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] vlan batch 20
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type access
[SwitchB-GigabitEthernet1/0/1] port default vlan 20
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type access
[SwitchB-GigabitEthernet1/0/2] port default vlan 20
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 2/0/1
[SwitchB-GigabitEthernet2/0/1] port link-type trunk
[SwitchB-GigabitEthernet2/0/1] port trunk allow-pass vlan 20
[SwitchB-GigabitEthernet2/0/1] quit
```

在SwitchC上创建VLAN10和VLAN20，配置SwitchC上接口GE1/0/1的接口类型为Trunk，并加入VLAN10和VLAN20，配置接口GE2/0/1的接口类型为Trunk，并加入VLAN10和VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] vlan batch 10 20
[SwitchC] interface gigabitethernet 1/0/1
```



```
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk allow-pass vlan 10 20
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface gigabitethernet 2/0/1
[SwitchC-GigabitEthernet2/0/1] port link-type trunk
[SwitchC-GigabitEthernet2/0/1] port trunk allow-pass vlan 10 20
[SwitchC-GigabitEthernet2/0/1] quit
```

在Switch上创建VLAN10和VLAN20，将接口GE1/0/1、GE1/0/2和GE2/0/1的接入类型分别配置为trunk，并分别将接口GE1/0/1加入VLAN10，GE1/0/2加入VLAN20，GE2/0/1加入VLAN 10、VLAN 20。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk allow-pass vlan 20
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] port link-type trunk
[Switch-GigabitEthernet2/0/1] port trunk allow-pass vlan 10 20
[Switch-GigabitEthernet2/0/1] quit
```

步骤2 配置优先级映射

创建DiffServ域ds1，将802.1p优先级6、5、2分别映射为服务等级EF、AF3、AF1，并分别将报文标记为绿色，黄色和红色。

```
[Switch] diffserv domain ds1
[Switch-dsdomain-ds1] 8021p-inbound 6 phb ef green
[Switch-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow
[Switch-dsdomain-ds1] 8021p-inbound 2 phb af1 red
[Switch-dsdomain-ds1] quit
```

在Switch入接口GE1/0/1和GE1/0/2上绑定DiffServ域。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] trust upstream ds1
[Switch-GigabitEthernet1/0/1] trust 8021p inner
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] trust upstream ds1
[Switch-GigabitEthernet1/0/2] trust 8021p inner
[Switch-GigabitEthernet1/0/2] quit
```

步骤3 配置流队列WRED模板及参数

在Switch上配置流队列WRED模板wred1，并配置wred1的三色报文参数。

```
[Switch] flow-wred-profile wred1
[Switch-flow-wred-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[Switch-flow-wred-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[Switch-flow-wred-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[Switch-flow-wred-wred1] quit
```

步骤4 配置流队列模板及参数

在Switch上配置流队列模板flow1引用流队列WRED模板wred1，并配置各服务等级的调度参数。

```
[Switch] flow-queue-profile flow1
[Switch-flow-queue-flow1] qos queue 5 pq flow-wred-profile wred1
[Switch-flow-queue-flow1] qos queue 3 wfq weight 20 flow-wred-profile wred1
```



```
[Switch-flow-queue-flow1] qos queue 1 wfq weight 10 flow-wred-profile wred1
[Switch-flow-queue-flow1] quit
```

步骤5 配置ACL规则

在Switch上配置ACL4001和ACL4002，并分别配置匹配VLAN10和VLAN20的rule规则。

```
[Switch] acl number 4001
[Switch-acl-L2-4001] rule 1 permit vlan-id 10
[Switch-acl-L2-4001] quit
[Switch] acl number 4002
[Switch-acl-L2-4002] rule 1 permit vlan-id 20
[Switch-acl-L2-4002] quit
```

步骤6 配置用户队列及参数

在Switch上配置基于ACL4001和ACL4002的用户队列，并引用流队列模板flow1。

```
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] traffic-user-queue outbound acl 4001 pir 8000 flow-queue-profile flow1
[Switch-GigabitEthernet2/0/1] traffic-user-queue outbound acl 4002 pir 5000 flow-queue-profile flow1
[Switch-GigabitEthernet2/0/1] quit
[Switch] quit
```

步骤7 验证配置结果

查看流队列WRED模板的配置信息，包括流队列WRED模板名称以及红、黄、绿三色报文的丢弃上下限和最大丢弃概率。

```
<Switch> display flow-wred-profile name wred1
Flow-wred-profile[1]: wred1
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
-------------------------------------------------------------------
```

查看流队列模板的配置信息，包括流队列模板名称以及WFQ调度的权重。

```
<Switch> display flow-queue-profile name flow1
Flow-queue-profile[1]: flow1
Queue Schedule(Weight) Shaping        flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     PQ             None           default
1     WFQ(10)        None           wred1
2     PQ             None           default
3     WFQ(20)        None           wred1
4     PQ             None           default
5     PQ             None           wred1
6     PQ             None           default
7     PQ             None           default
-----------------------------------------------------------------------
```

查看用户队列的流量统计信息。

```
<Switch> display traffic-user-queue statistics interface gigabitethernet 2/0/1 outbound acl 4001
------------------------------------------------------------------------------
 Interface: GigabitEthernet2/0/1
------------------------------------------------------------------------------
    Queue ID      |                Statistics information
------------------------------------------------------------------------------
        0         |         packets: pass:                   4,127
                  |                  drop:           2,798,787,076
                  |          bytes:  pass:                 610,796
                  |                  drop:         414,220,487,248
------------------------------------------------------------------------------
```



```
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    1       |  packets: pass:                 4,127
            |           drop:             5,597,436,717
            |  bytes:   pass:                   610,796
            |           drop:           828,420,634,116
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    2       |  packets: pass:                     0
            |           drop:                     0
            |  bytes:   pass:                     0
            |           drop:                     0
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    3       |  packets: pass:                 4,127
            |           drop:             5,597,436,713
            |  bytes:   pass:                   610,796
            |           drop:           828,420,633,524
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    4       |  packets: pass:                 4,127
            |           drop:             2,798,716,293
            |  bytes:   pass:                   610,796
            |           drop:           414,210,011,364
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    5       |  packets: pass:                 4,127
            |           drop:             2,798,716,294
            |  bytes:   pass:                   610,796
            |           drop:           414,210,011,512
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    6       |  packets: pass:                     0
            |           drop:                     0
            |  bytes:   pass:                     0
            |           drop:                     0
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    7       |  packets: pass:             1,119,509,460
            |           drop:             1,679,210,961
            |  bytes:   pass:           165,687,400,080
            |           drop:           248,523,222,228
--------------------------------------------------------------------------------
<Switch> display traffic-user-queue statistics interface gigabitethernet 2/0/1 outbound acl 4002
--------------------------------------------------------------------------------
 Interface: GigabitEthernet2/0/1
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    0       |  packets: pass:                 4,125
            |           drop:                 5,218,026
            |  bytes:   pass:                   610,500
            |           drop:                 772,267,848
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
    1       |  packets: pass:                 4,125
            |           drop:                10,440,178
            |  bytes:   pass:                   610,500
            |           drop:             1,545,146,344
--------------------------------------------------------------------------------
  Queue ID  |              Statistics information
--------------------------------------------------------------------------------
```



```
  2       |          packets: pass:                    0
          |                  drop:                    0
          |         bytes:   pass:                    0
          |                  drop:                    0
-------------------------------------------------------------------------------
  Queue ID    |                Statistics information
-------------------------------------------------------------------------------
  3       |          packets: pass:                4,125
          |                  drop:           10,440,178
          |         bytes:   pass:              610,500
          |                  drop:        1,545,146,344
-------------------------------------------------------------------------------
  Queue ID    |                Statistics information
-------------------------------------------------------------------------------
  4       |          packets: pass:                4,125
          |                  drop:            5,218,027
          |         bytes:   pass:              610,500
          |                  drop:          772,267,996
-------------------------------------------------------------------------------
  Queue ID    |                Statistics information
-------------------------------------------------------------------------------
  5       |          packets: pass:                4,125
          |                  drop:            5,218,027
          |         bytes:   pass:              610,500
          |                  drop:          772,267,996
-------------------------------------------------------------------------------
  Queue ID    |                Statistics information
-------------------------------------------------------------------------------
  6       |          packets: pass:                    0
          |                  drop:                    0
          |         bytes:   pass:                    0
          |                  drop:                    0
-------------------------------------------------------------------------------
  Queue ID    |                Statistics information
-------------------------------------------------------------------------------
  7       |          packets: pass:            2,092,988
          |                  drop:            3,129,165
          |         bytes:   pass:          309,762,224
          |                  drop:          463,116,420
-------------------------------------------------------------------------------
```

----结束

配置文件

- SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 10
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 10
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- SwitchB的配置文件

```
#
sysname SwitchB
```



```
#
vlan batch 20
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 20
#
interface GigabitEthernet1/0/2
 port link-type access
 port default vlan 20
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
```

- SwitchC的配置文件

```
#
sysname SwitchC
#
vlan batch 10 20
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
#
return
```

- Switch的配置文件

```
#
sysname Switch
#
vlan batch 10 20
#
diffserv domain ds1
 8021p-inbound 2 phb af1 red
 8021p-inbound 5 phb af3 yellow
 8021p-inbound 6 phb ef green
#
acl number 4001
 rule 1 permit vlan-id 10
acl number 4002
 rule 1 permit vlan-id 20
#
flow-wred-profile wred1
 color green low-limit 80 high-limit 100 discard-percentage 10
 color yellow low-limit 60 high-limit 80 discard-percentage 20
 color red low-limit 40 high-limit 60 discard-percentage 40
#
flow-queue-profile flow1
 qos queue 1 wfq weight 10 flow-wred-profile wred1
 qos queue 3 wfq weight 20 flow-wred-profile wred1
 qos queue 5 flow-wred-profile wred1
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 trust upstream ds1
 trust 8021p inner
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 trust upstream ds1
 trust 8021p inner
```



```
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10 20
 traffic-user-queue outbound acl 4001 pir 8000 flow-queue-profile flow1
 traffic-user-queue outbound acl 4002 pir 5000 flow-queue-profile flow1
#
return
```

相关信息

视频

S系列交换机HQoS特性介绍

10.8.2 配置有线无线用户授权 HQoS 示例

组网需求

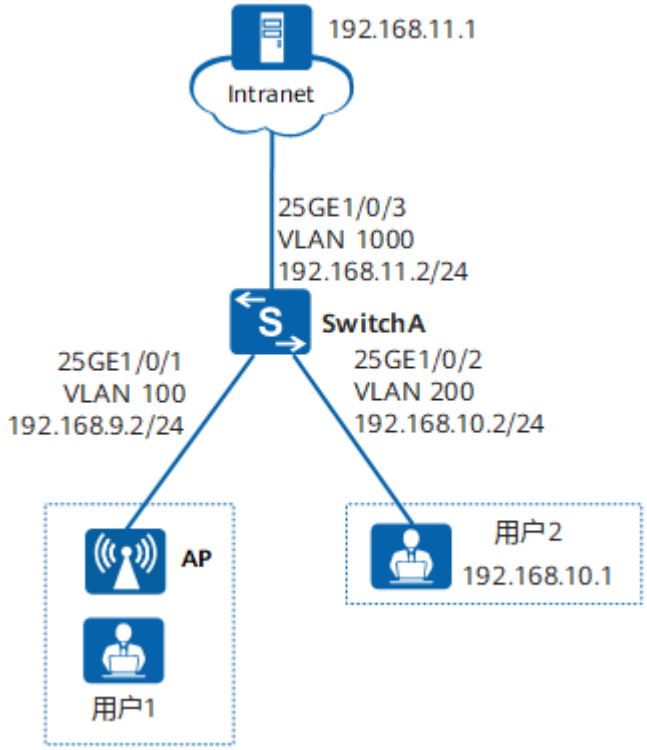
如图10-6所示，无线用户（用户1）通过SwitchA下接的AP接入网络，有线用户（用户2）通过SwitchA接入网络，用户均经过RADIUS服务器认证和授权后访问网络。每个用户都有语音、视频和文件传输三种不同的业务，其携带的802.1p优先级分别为6、5、2。由于带宽有限，现在需要通过在SwitchA部署HQoS，实现以下需求：

- 如果存在视频点播等业务，需要避免AP缓存溢出。
- 指定通过认证的用户为VIP用户。
- 已知用户2的IP地址为192.168.10.1，需要保证该有线用户发送和接收的报文始终得到优先调度。
- 优先保证语音业务的带宽，其次是视频业务，最后是文件传输业务。具体配置参数如表1所示。

表 10-9 流队列配置参数

业务类型	颜色	阈值下限（%）	阈值上限（%）	丢弃概率	服务等级
语音	绿	80	100	10	EF
视频	黄	60	80	20	AF3
文件传输	红	40	60	40	AF1

图 10-6 配置 HQoS 组网图



配置注意事项

- 仅S12700E的X6H系列单板支持本示例。
- 本示例主要介绍授权HQoS的相关配置，NAC和WLAN基本业务的配置这里不做相关说明。
  - 本示例仅支持使用统一模式部署NAC功能，详细配置过程请参见《 S12700, S12700E V200R023C00 配置指南-用户接入与认证 》 NAC配置（ 统一模式 ）。
  - WLAN基本业务的详细配置过程请参见《 S12700, S12700E V200R023C00 配置指南-WLAN-AC 》 WLAN基本业务配置。
- AC下行到AP的流量整形功能需要在AP上线前开启，否则相关配置将不生效。
- 无线用户中，仅数据转发方式为隧道转发且获取地址后的IPv4用户支持授权属性HW-Subscriber-QoS-Profile。
- 已经被授权属性HW-Subscriber-QoS-Profile的用户，不支持通过重认证方式删除该授权。

配置思路

采用如下的思路在SwitchA上配置HQoS：

1. 在AP上线前，开启AC下行到AP的流量整形功能。SwitchA通过和AP的协商，对转发给AP的流量进行整形。
2. 创建VLAN，并配置各接口，使用户能够通过SwitchA访问网络。
3. 通过业务方案授权，指定通过认证的用户为VIP用户，优先调度用户2收发的报文：

a. 配置SwitchA与RADIUS服务器的对接参数。
b. 配置AAA方案，指定认证、授权和计费方式。
c. 配置SAC模板，重标记用户2发送和接收的报文的内部优先级。
d. 将SAC模板绑定到业务方案中，并在业务方案中配置用户的优先级为1。
e. 在域下绑定AAA方案、业务方案和RADIUS服务器模板。

4. 通过QoS模板配置用户队列，通过RADIUS服务器授权相关RADIUS属性，实现HQoS调度：
   a. 配置DiffServ域，将802.1p优先级映射为PHB行为并为报文着色。
   b. 配置流队列模板及相关参数，以实现为不同的业务提供不同的调度优先级和丢弃参数。
   c. 在QoS模板中配置用户队列，在用户队列中引用流队列模板。
   d. 通过RADIUS服务器授权编号为26-17的华为RADIUS扩展属性HW-Subscriber-QoS-Profile。

操作步骤

步骤1 开启AC下行到AP的流量整形功能

为防止SwitchA转发给AP的突发流量引起AP缓存溢出，可以开启本功能，使SwitchA对转发给AP的流量进行整形，从而缓解AP的压力。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] wlan
[SwitchA-wlan-view] ap auto-shaping enable
[SwitchA-wlan-view] quit
```

步骤2 创建VLAN并配置各接口

创建VLAN100、VLAN200和VLAN1000。配置接口25GE1/0/1、25GE1/0/2和25GE1/0/3的接口类型为Access，并分别加入VLAN100、VLAN200和VLAN1000。

```
[SwitchA] vlan batch 100 200 1000
[SwitchA] interface 25ge 1/0/1
[SwitchA-25GE1/0/1] port link-type access
[SwitchA-25GE1/0/1] port default vlan 100
[SwitchA-25GE1/0/1] quit
[SwitchA] interface 25ge 1/0/2
[SwitchA-25GE1/0/2] port link-type access
[SwitchA-25GE1/0/2] port default vlan 200
[SwitchA-25GE1/0/2] quit
[SwitchA] interface 25ge 1/0/3
[SwitchA-25GE1/0/3] port link-type access
[SwitchA-25GE1/0/3] port default vlan 1000
[SwitchA-25GE1/0/3] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 192.168.9.2 24
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 200
[SwitchA-Vlanif200] ip address 192.168.10.2 24
[SwitchA-Vlanif200] quit
[SwitchA] interface vlanif 1000
[SwitchA-Vlanif1000] ip address 192.168.11.2 24
[SwitchA-Vlanif1000] quit
```

步骤3 配置业务方案授权

配置RADIUS服务器模板“tem_rad”，指定SwitchA与RADIUS服务器的对接参数。包括RADIUS认证服务器和RADIUS计费服务器的IP地址、端口号和共享密钥。


```
[SwitchA] radius-server template tem_rad
[SwitchA-radius-tem_rad] radius-server authentication 192.168.11.1 1812
[SwitchA-radius-tem_rad] radius-server accounting 192.168.11.1 1813
[SwitchA-radius-tem_rad] radius-server shared-key cipher YsHsjx_202206
[SwitchA-radius-tem_rad] quit
[SwitchA] radius-server authorization 192.168.11.1 shared-key cipher YsHsjx_202206
```

配置AAA方案，指定认证和计费方式均为RADIUS，计费时间间隔为15分钟。

```
[SwitchA] aaa
[SwitchA-aaa] authentication-scheme auth
[SwitchA-aaa-authen-auth] authentication-mode radius
[SwitchA-aaa-authen-auth] quit
[SwitchA-aaa] accounting-scheme acco
[SwitchA-aaa-accounting-acco] accounting-mode radius
[SwitchA-aaa-accounting-acco] accounting realtime 15
[SwitchA-aaa-accounting-acco] quit
[SwitchA-aaa] quit
```

重标记有线用户（用户2）发送和接收的报文的内部优先级。在SAC模板中配置基于用户ACL的重标记内部优先级，使设备根据重标记后的优先级对匹配ACL的报文进行调度。

```
[SwitchA] acl 6000
[SwitchA-acl-ucl-6000] rule permit ip source 192.168.10.1 0
[SwitchA-acl-ucl-6000] rule permit ip destination 192.168.10.1 0
[SwitchA-acl-ucl-6000] quit
[SwitchA] sac-profile name sac1
[SwitchA-sac-profile-sac1] acl 6000 remark local-precedence 7
[SwitchA-sac-profile-sac1] quit
```

创建业务方案，将SAC模板绑定到业务方案中，并在业务方案中配置用户的优先级为1。缺省情况下，用户的优先级为0，用户为普通用户。若配置用户的优先级为1，则用户为VIP用户。

```
[SwitchA] aaa
[SwitchA-aaa] service-scheme srvscheme1
[SwitchA-aaa-service-srvscheme1] sac-profile sac1
[SwitchA-aaa-service-srvscheme1] priority 1
[SwitchA-aaa-service-srvscheme1] quit
```

配置域“huawei.com”，在域下绑定AAA方案、业务方案和RADIUS服务器模板。

```
[SwitchA-aaa] domain huawei.com
[SwitchA-aaa-domain-huawei.com] authentication-scheme auth
[SwitchA-aaa-domain-huawei.com] accounting-scheme acco
[SwitchA-aaa-domain-huawei.com] radius-server tem_rad
[SwitchA-aaa-domain-huawei.com] service-scheme srvscheme1
[SwitchA-aaa-domain-huawei.com] quit
[SwitchA-aaa] quit
```

步骤4 通过QoS模板配置用户队列

配置优先级映射。创建DiffServ域ds1，将802.1p优先级6、5、2分别映射为服务等级EF、AF3、AF1，并分别将报文标记为绿色、黄色和红色。

```
[SwitchA] diffserv domain ds1
[SwitchA-dsdomain-ds1] 8021p-inbound 6 phb ef green
[SwitchA-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow
[SwitchA-dsdomain-ds1] 8021p-inbound 2 phb af1 red
[SwitchA-dsdomain-ds1] quit
[SwitchA] interface 25ge 1/0/1
[SwitchA-25GE1/0/1] trust upstream ds1
[SwitchA-25GE1/0/1] trust 8021p inner
[SwitchA-25GE1/0/1] quit
[SwitchA] interface 25ge 1/0/2
[SwitchA-25GE1/0/2] trust upstream ds1
[SwitchA-25GE1/0/2] trust 8021p inner
[SwitchA-25GE1/0/2] quit
```


配置流队列WRED模板wred1，并配置wred1的三色报文参数。

```
[SwitchA] flow-wred-profile wred1
[SwitchA-flow-wred-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[SwitchA-flow-wred-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[SwitchA-flow-wred-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[SwitchA-flow-wred-wred1] quit
```

配置流队列模板flow1引用流队列WRED模板wred1，并配置各服务等级的调度参数。

```
[SwitchA] flow-queue-profile flow1
[SwitchA-flow-queue-flow1] qos queue 5 pq flow-wred-profile wred1
[SwitchA-flow-queue-flow1] qos queue 3 wfq weight 20 flow-wred-profile wred1
[SwitchA-flow-queue-flow1] qos queue 1 wfq weight 10 flow-wred-profile wred1
[SwitchA-flow-queue-flow1] quit
```

在QoS模板中创建用户队列，在用户队列中引用流队列模板。

```
[SwitchA] qos-profile name qos1
[SwitchA-qos-qos1] user-queue flow-queue-profile flow1
[SwitchA-qos-qos1] quit
[SwitchA] quit
```

通过RADIUS服务器，为域“huawei.com”中认证成功的用户授权编号为26-17的华为RADIUS扩展属性HW-Subscriber-QoS-Profile。授权的属性值是QoS模板的名称qos1。

步骤5 验证配置结果

查看流队列WRED模板的配置信息，包括红、黄、绿三色报文的丢弃上下限和最大丢弃概率。

```
<SwitchA> display flow-wred-profile name wred1
Flow-wred-profile[1]: wred1
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
------------------------------------------------------------------------
```

查看流队列模板的配置信息，包括WFQ调度的权重。

```
<SwitchA> display flow-queue-profile name flow1
Flow-queue-profile[1]: flow1
Queue Schedule(Weight) Shaping        flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     PQ               None           default
1     WFQ(10)          None           wred1
2     PQ               None           default
3     WFQ(20)          None           wred1
4     PQ               None           default
5     PQ               None           wred1
6     PQ               None           default
7     PQ               None           default
------------------------------------------------------------------------
```

查看SAC模板配置信息，包括用户ACL的编号和对应的重标记内部优先级的值。

```
<SwitchA> display sac-profile name sac1
--------------------------
ACL Id   Local-precedence
--------------------------
 6000          7
--------------------------
Total: 1
```

查看业务方案配置信息，包括业务方案下用户的优先级。

```
<SwitchA> display service-scheme name srvscheme1
  service-scheme-name               : srvscheme1
  service-scheme-primary-dns        : -
  service-scheme-secondary-dns      : -
  service-scheme-adminlevel         : -
  service-scheme-dhcpgroup          : -
  service-scheme-ippool             : -
  service-scheme-primary-wins       : -
  service-scheme-secondary-wins     : -
  service-scheme-redirect-acl-id    : -
  service-scheme-v6-redirect-acl-id: -
  service-scheme-priority           : 1
  access-limit-username-maxnum      : -
  service-scheme-qosprofile         : -
  service-shceme-sacprofile         : -
  service-scheme-idlecut            : -
```

查看域的配置信息，包括域使用的认证方案、计费方案、业务方案和RADIUS服务器模板名称。

```
<SwitchA> display domain name huawei.com
  Domain-name                       : huawei.com
  Domain-index                      : 6
  Domain-state                      : Active
  Authentication-scheme-name        : auth
  Accounting-scheme-name            : acco
  Authorization-scheme-name         : -
  Service-scheme-name               : srvscheme1
  RADIUS-server-template            : tem_rad
  Accounting-copy-RADIUS-template : -
  HWTACACS-server-template          : -
  HACA-server-template              : -
  Push-url-address                  : -
  Accounting-DualStack-Separate     : -
  Flow-statistic                    : -
  Tariff-level                      : -
```

----结束

配置文件

SwitchA的配置文件

```
#
sysname SwitchA
#
vlan batch 100 200 1000
#
diffserv domain ds1
 8021p-inbound 2 phb af1 red
 8021p-inbound 5 phb af3 yellow
 8021p-inbound 6 phb ef green
#
radius-server template tem_rad
 radius-server shared-key cipher %^%#-_QJF_J/K7_x`[%C)+z)`rMaW,tdL8O6S%'BCcu@%^%#
 radius-server authentication 192.168.11.1 1812 weight 80
 radius-server accounting 192.168.11.1 1813 weight 80
radius-server authorization 192.168.11.1 shared-key cipher %^%#i7Y,+sQjQ<o,o4"gy+TNgGvt*`-
v#RW)B@Ri}!}3%^%#
#
acl number 6000
 rule 5 permit ip source 192.168.10.1 0
 rule 10 permit ip destination 192.168.10.1 0
#
sac-profile name sac1
 acl 6000 remark local-precedence 7
```



```
#
flow-wred-profile wred1
 color green low-limit 80 high-limit 100 discard-percentage 10
 color yellow low-limit 60 high-limit 80 discard-percentage 20
 color red low-limit 40 high-limit 60 discard-percentage 40
#
flow-queue-profile flow1
 qos queue 1 wfq weight 10 flow-wred-profile wred1
 qos queue 3 wfq weight 20 flow-wred-profile wred1
 qos queue 5 flow-wred-profile wred1
#
qos-profile name qos1
 user-queue flow-queue-profile flow1
#
aaa
 authentication-scheme auth
  authentication-mode radius
 accounting-scheme acco
  accounting-mode radius
  accounting realtime 15
 service-scheme srvscheme1
  priority 1
  sac-profile sac1
 domain huawei.com
  authentication-scheme auth
  accounting-scheme acco
  service-scheme srvscheme1
  radius-server tem_rad
#
interface Vlanif100
 ip address 192.168.9.2 255.255.255.0
#
interface Vlanif200
 ip address 192.168.10.2 255.255.255.0
#
interface Vlanif1000
 ip address 192.168.11.2 255.255.255.0
#
interface 25GE1/0/1
 port link-type access
 port default vlan 100
 trust upstream ds1
 trust 8021p inner
#
interface 25GE1/0/2
 port link-type access
 port default vlan 200
 trust upstream ds1
 trust 8021p inner
#
interface 25GE1/0/3
 port link-type access
 port default vlan 1000
#
return
```

