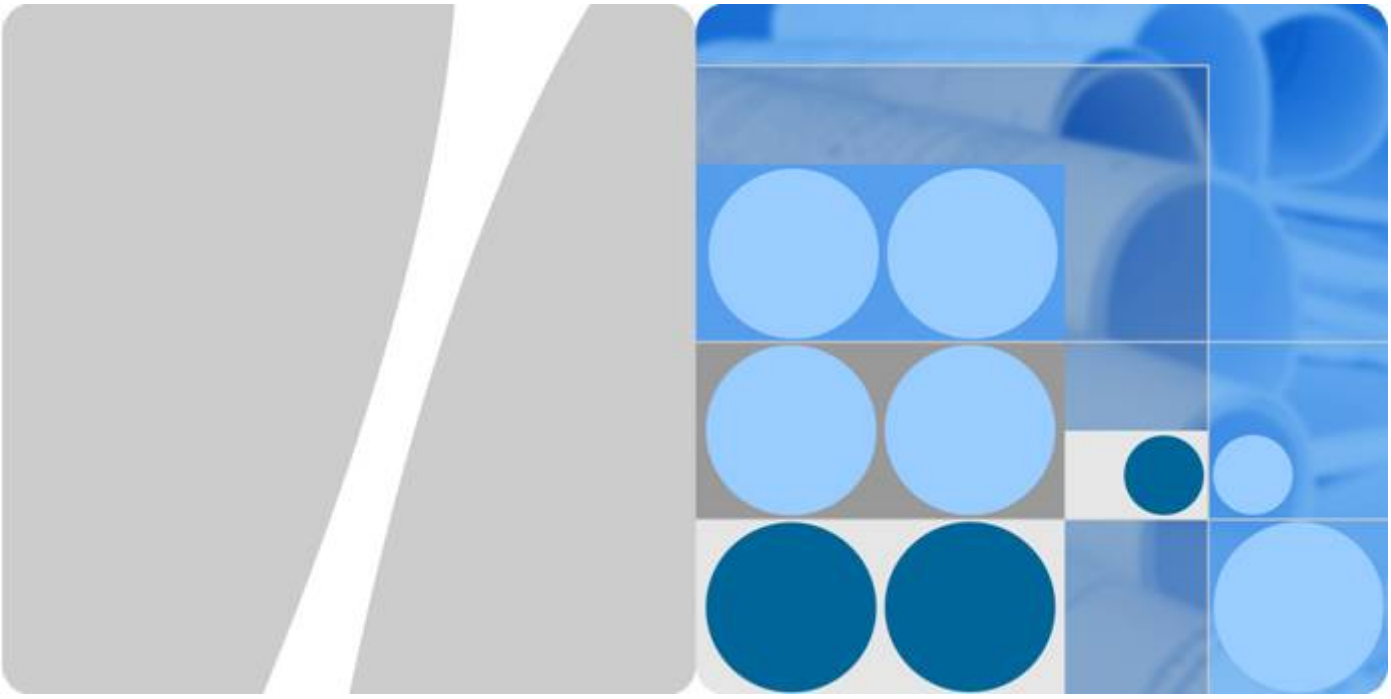


Huawei AR150&200 系列企业路由器

V200R002C00

配置指南-QoS

文档版本　02

发布日期　2012-03-30

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默示的声明或保证。

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： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档介绍了 AR150/200 中 QoS 的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了 QoS 的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 系统维护工程师

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
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从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。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 02 (2012-03-30)

相对于版本 01（2011-12-30）的变化如下：

修改：

- 1.5.5 检查配置结果

文档版本 01 (2011-12-30)

第一次正式发布。

目 录

1 QoS 配置

关于本章

介绍 AR150/200 各类接口通用的 QoS 功能：优先级映射、流量监管、流量整形、拥塞管理和拥塞避免以及 HQoS（Hierarchical Quality of Service）的配置方法和举例。

1.1 QoS 概述
QoS（Quality of Service）旨在针对网络的不同应用场景需求，为其提供不同的服务质量。

1.2 AR150/200 支持的 QoS 特性
介绍 QoS 特性在 AR150/200 中的支持情况。

1.3 配置优先级映射
AR150/200 将根据报文携带的优先级或端口优先级进行优先级映射，确定报文进入的队列和报文出设备时携带的优先级，从而提供差异化的服务。

1.4 配置流量监管
AR150/200 支持基于接口的流量监管和基于流的流量监管。

1.5 配置流量整形
流量整形实现报文的流量以均匀的速率向外发送，减少因超过承诺速率而被丢弃的报文。

1.6 配置拥塞管理
配置拥塞管理后，当网络中发生拥塞时，AR150/200 将按照配置好的调度策略决定报文转发时的处理次序。

1.7 配置拥塞避免
配置拥塞避免后，AR150/200 将根据 WRED 的配置信息丢弃超出流量范围的报文。

1.8 配置 HQoS
AR150/200 支持的 HQoS（Hierarchical Quality of Service）基于多级队列的层次化调度，可以实现对不同用户的不同业务流量的区分，提供更为精细化的服务质量。

1.9 维护 QoS
QoS 的维护通过查看或清除基于队列的流量统计信息来实现。

1.10 配置举例

通过示例介绍如何综合应用流量监管、流量整形、拥塞避免和拥塞管理。配置示例中包括组网需求、配置注意事项、配置思路等。

1.1 QoS 概述

QoS（Quality of Service）旨在针对网络的不同应用场景需求，为其提供不同的服务质量。

服务质量 QoS 用于评估服务方满足客户服务需求的能力，在 Internet 中，QoS 用于评估网络传送分组的服务能力。由于网络提供的服务是多样的，因此可以基于不同方面进行评估。通常所说的 QoS，是对分组投递过程中可为延迟、延迟抖动、丢包率等核心需求提供支持的服务能力的评估。

QoS 通过 Best Effort（尽力而为服务模型）、IntServ（综合服务模型）、DiffServ（区分服务模型）三种模式全局实现服务质量保证。

- Best Effort 模型是一个单一的服务模型，网络尽最大的可能性来发送报文，但对时延、可靠性等性能不提供任何保证。适合于绝大多数网络应用，如 FTP、E-Mail 等，它通过先入先出（FIFO）调度方式来实现。
- IntServ 模型是一个综合服务模型，它的特点是在发送报文前要先向网络提出申请。IntServ 模型常与组播应用结合，适用于需要保证带宽、低延迟的实时多媒体应用，如电视会议、视频点播等。
- DiffServ 模型是一种多服务模型，它可以满足不同的 QoS 需求，根据每个报文携带的优先级来提供特定的服务。可以用不同的方法来指定报文的 QoS，如 IP 报文的优先级（IP Precedence），报文的源地址和目的地址等。网络通过这些信息来进行报文的分类、流量整形、流量监管和队列调度。

1.2 AR150/200 支持的 QoS 特性

介绍 QoS 特性在 AR150/200 中的支持情况。

AR150/200 支持：

- 优先级映射
- 流量监管
- 流量整形
- 拥塞避免
- 拥塞管理
- HQoS

表 1-1 各功能的实现方式

名称	实现方式
优先级映射	接口的入方向或出方向均可应用。
流量监管	基于接口的流量监管，WAN 接口的入方向或出方向均可配置，LAN 接口仅可应用在接口的入方向上。 基于流的流量监管，接口的入方向或出方向均可应用。

名称	实现方式
流量整形	基于接口的流量整形，仅可应用在接口出方向。 基于队列的流量整形，仅可应用在接口出方向。 基于流的流量整形，仅可应用在 WAN 接口的出方向。
拥塞避免	基于队列的拥塞避免，仅可应用在 WAN 接口出方向。 基于流的拥塞避免，仅可应用在 WAN 接口的出方向。
拥塞管理	基于队列的拥塞管理，仅可应用在接口出方向。 基于流分类的拥塞管理，仅可应用在 WAN 接口的出方向。
HQoS	基于流的 HQoS，仅可应用在 WAN 接口的出方向。

优先级映射

不同的报文使用不同的 QoS 优先级，例如二层网络中一般根据 802.1p 优先级提供 QoS 服务，三层网络中一般根据 DSCP 优先级提供 QoS 服务。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标记的映射关系。

为了保证不同报文的服务质量，对于设备接收到的报文，用户可以根据报文携带的优先级（802.1p 优先级、DSCP 优先级）或端口缺省的 802.1p 优先级确定报文所进入的队列，并可以根据配置修改报文发送时所携带的优先级，以便下一设备根据报文的优先级提供相应的 QoS 服务。

AR150/200 按照映射后的 802.1p 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。AR150/200 的二层 FE 接口与其他接口不同，仅有 4 条队列，而其它接口下有 8 条队列，因此其对应关系也有所不同。AR150/200 的二层 FE 接口的 802.1p 优先级与各队列之间的对应关系如**表 1-2** 所述，其他接口的 802.1p 优先级与各队列之间的对应关系如**表 1-3** 所述：

表 1-2 802.1p 优先级与各队列之间的对应关系表

Dot1p	队列索引
0	0
1	0
2	1
3	1
4	2

Dot1p	队列索引
5	2
6	3
7	3

表 1-3 802.1p 优先级与各队列之间的对应关系表

Dot1p	队列索引
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

流量监管

流量监管（Traffic Policing）是通过对流量规格的监督，来限制流量及其资源使用的流控策略。

流量监管的典型应用是监督进入网络的某一流量的规格，把它限制在一个合理的范围之内，或对超出的部分流量进行“惩罚”，以保护网络资源。

流量监管广泛的用于监管进入因特网服务提供商（ISP）的网络流量。

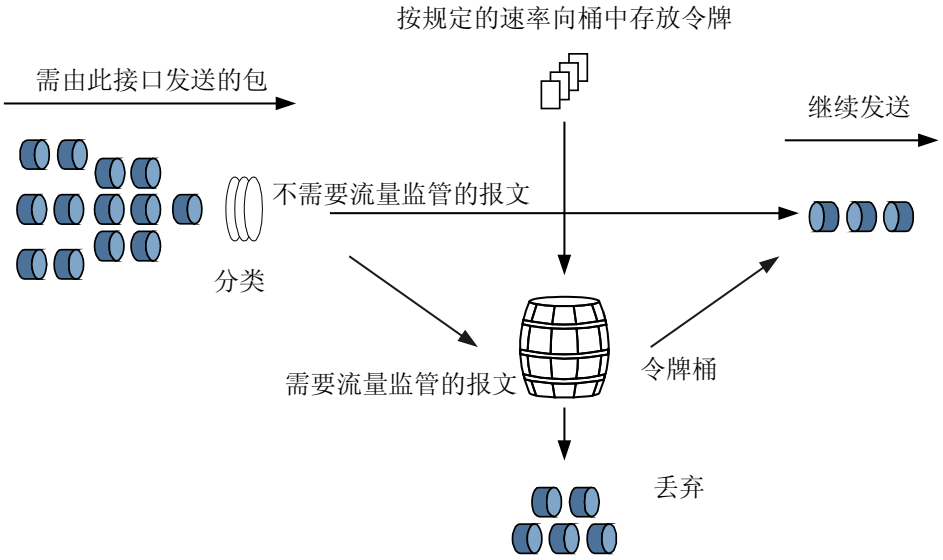
- 令牌桶与流量评估

  进行流量监管有一个前提条件，就是要判断流量是否超出了规格，然后才能根据评估结果实施调控策略。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（1 令牌=1bit），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。

图 1-1 用令牌桶评估流量



AR150/200 支持双令牌桶技术：

令牌桶参数包括：

- 承诺突发尺寸 CBS（Committed Burst Size）：即所谓的 C 桶，表示每次突发所允许的最大的流量尺寸，单位为 byte。
- 承诺信息速率 CIR（Committed Information Rate）：表示向 C 桶中放置令牌的速率，即 C 桶允许的流的平均速度，单位为 kbps。
- 过度突发尺寸 PBS（Peak Burst Size）：即所谓的 P 桶，表示每次突发所允许的超出 CBS 的最大的流量尺寸，单位为 byte。
- 峰值信息速率 PIR（Peak Information Rate）：表示向 P 桶中放置令牌的速率，即 P 桶允许的流的平均速度，单位为 kbps。

双令牌桶技术中，用户业务流量小于 CIR 的部分报文被标记为绿色，用户流量超出 PIR 的部分报文被标记为红色，超出 CIR 但小于 PIR 的部分报文被标记为黄色。

流量监管的动作包括通过、丢弃和改变优先级转发。缺省情况下，绿色、黄色报文被允许通过，红色报文被丢弃。

- AR150/200 支持的流量监管特性

  AR150/200 支持以下流量监管功能：

  - 基于接口的流量监管，可以对流入或流出某接口的业务流量进行流量控制。

    说明

    用户可以根据需要选择对接口下所有或部分业务流量进行流量监管，如：

    - 对接口下所有业务流量进行流量监管；
    - 对符合指定 ACL 规则的业务流量进行流量监管；
    - 对源、目的 IP 属于指定范围的业务流量进行流量监管。
  - 基于流的流量监管，可以对流入或流出接口的符合流分类规则的某类业务流量进行流量控制。

流量整形

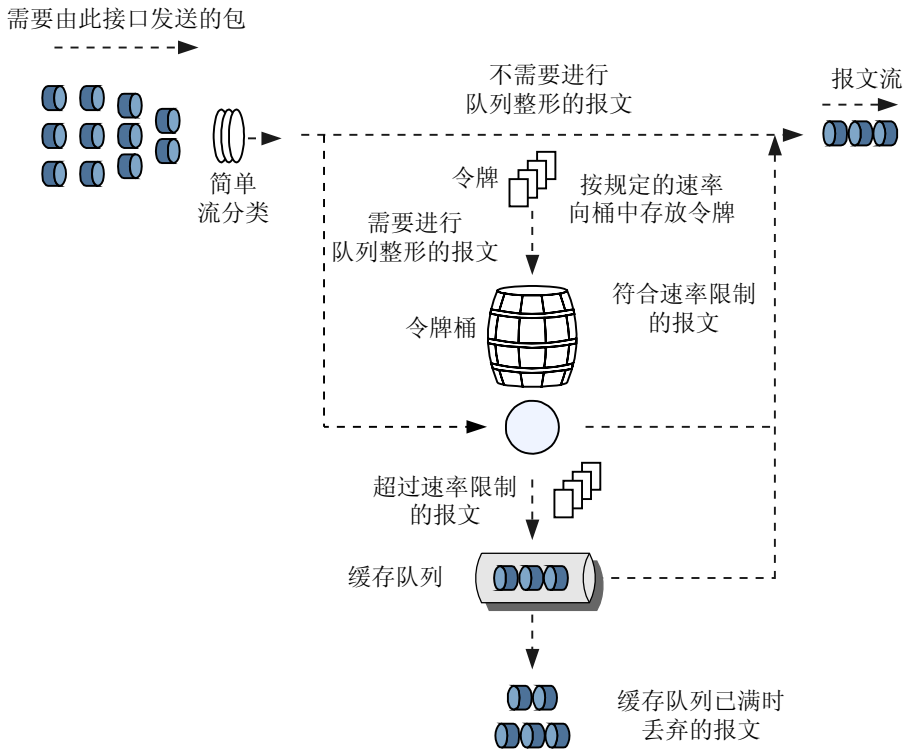
流量整形（Traffic Shaping）也是通过对流量规格的监督，来限制流量及其资源使用的流控策略。流量整形的流量评估也是通过令牌桶技术。

流量整形是一种主动调整流量输出速率的措施，一个典型应用是基于下游网络结点的流量监管指标来控制本地流量的输出。

- 流量整形与流量监管的区别

  流量整形与流量监管的主要区别在于，流量监管对不符合流量特性的报文直接丢弃，而流量整形对不符合流量规格的报文则是进行缓存——通常是将它们放入队列内，减少了报文的丢弃，如图 1-2 所示。在图 1-2 中，当令牌桶有足够令牌时，均匀地发送被缓存的报文，令牌不够时就继续缓存。当需要缓存的报文个数大于队列长度时报文因无法缓存而被丢弃。

  图 1-2 流量整形示意图

  正是由于流量整形将报文入缓存或队列，所以流量整形可能会增加延迟，而流量监管几乎不引入额外的延迟。

- AR150/200 支持的流量整形特性

  AR150/200 支持如下流量整形功能：

  - 基于接口或子接口的流量整形

    对接口或子接口上所有通过的报文进行流量整形。

  - 基于队列的流量整形

    对端口上某指定队列进行流量整形，从而可实现针对不同优先级报文的流量整形。

- 基于流的流量整形

  对端口上通过的某类报文进行流量整形，从而可实现针对符合流分类规则的报文的流量整形。

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量控制机制。

拥塞避免策略包括尾部丢弃（Tail-Drop）、随机早期检测 RED（Random Early Detection）、加权随机早期检测 WRED（Weighted Random Early Detection）等：

- 尾部丢弃

  传统的丢包策略采用尾部丢弃的方法，同等的对待所有的报文，不对服务等级进行区分。在拥塞发生期间，队列尾部的数据报文将被丢弃，直到拥塞解决。

  这种丢弃策略会引发 TCP 全局同步现象。所谓 TCP 全局同步现象，是指当队列同时丢弃多个 TCP 连接的报文时，将造成多个 TCP 连接同时进入拥塞避免和慢启动状态以降低并调整流量；而后这几个 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。

- RED

  RED 技术通过随机地丢弃报文，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。

  在 RED 技术的算法中，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，丢弃所有收到的报文。
  - 当队列的长度在阈值上限和阈值下限之间时，开始随机丢弃到来的报文。方法是为每个到来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，如果大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。

- WRED

  WRED 技术也是通过随机丢弃报文来避免 TCP 的全局同步现象，但该技术生成的随机丢弃参数是基于优先级的，它通过报文的不同优先级来区别丢弃策略，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。

AR150/200 的各级队列缺省配置均为尾部丢弃，支持基于队列的 WRED 和基于流的 WRED。

拥塞管理

当网络中间歇性的出现拥塞，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；如果任何时候都出现拥塞，则需要增加带宽。

拥塞管理一般采用队列调度技术，目前 AR150/200 采用的队列调度技术有：

- **PQ 调度**
- **WRR 调度**
- **DRR 调度**
- **WFQ 调度**
- **PQ+WRR/PQ+DRR/PQ+WFQ 调度**
- **CBQ 调度**

- PQ 调度

  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，将延迟敏感的关键业务放入高优先级队列，将非关键业务放入低优先级队列，从而确保关键业务被优先发送。

  PQ 调度的缺点是：拥塞发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

- 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。

  以端口有 8 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w7、w6、w5、w4、w3、w2、w1、w0），加权值表示获取资源的比重。例如：一个 100M 的端口，配置它的 WRR 队列调度算法的加权值为 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 5Mbit/s 带宽，避免了采用 PQ 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

  WRR 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。

  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。
  - 低延时需求业务（如语音）得不到及时调度。

- DRR 调度

  DRR（Deficit Round Robin）调度实现原理与 WRR 调度基本相同。

  DRR 与 WRR 的区别是：WRR 调度是按照报文个数进行调度，而 DRR 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，DRR 调度允许出现负权重，以保证长报文也能够得到调度。但下次轮循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 DRR 调度。

  DRR 调度避免了采用 PQ 调度时低优先级队列中的报文可能长时间得不到服务的缺点，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，DRR 调度也具有低延时需求业务（如语音）得不到及时调度的缺点。

- 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+DRR/PQ+WFQ 调度

PQ 调度和 WRR/DRR/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调度，而单纯采用 WRR/DRR/WFQ 调度时低延时需求业务得不到优先调度，“PQ+WRR/PQ+DRR/PQ+WFQ”调度方式则将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+DRR/PQ+WFQ 调度”调度方式，将重要的协议报文和有低延时需求的业务报文放入 PQ 队列中进行调度，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/DRR/WFQ 调度的各队列中，按照权值对各队列进行循环调度。

- CBQ 调度

  基于类的加权公平队列 CBQ（Class-based Queueing）是对 WFQ 功能的扩展，为用户提供了定义类的支持。CBQ 首先根据 IP 优先级或者 DSCP 优先级、输入接口、IP 报文的五元组等规则来对报文进行分类，然后让不同类别的报文进入不同的队列。对于不匹配任何类别的报文，送入系统定义的缺省类。

  CBQ 提供三类队列：

  - EF 队列：满足低时延业务

    EF 队列是一个具有高优先级的队列，一个或多个类的报文可以被设定进入 EF 队列，不同类别的报文可设定占用不同的带宽。在调度出队的时候，若 EF 队列中有报文，则总是优先发送 EF 队列中的报文，直到 EF 队列中没有报文时，或者超过为 EF 队列配置的最大预留带宽时才调度发送其他队列中的报文。

    由于 EF 队列中的报文一般是语音报文（VoIP），采用的是 UDP 报文，所以没有必要采用 WRED 的丢弃策略，采用尾丢弃策略即可。

  - AF 队列：满足需要带宽保证的关键数据业务

    每个 AF 队列分别对应一类报文，用户可以设定每类报文占用的带宽。在系统调度报文出队的时候，按用户为各类报文设定的带宽将报文出队发送，可以实现各个类的队列的公平调度。当接口有剩余带宽时，AF 队列按照权重分享剩余带宽。同时，在接口拥塞的时候，仍然能保证各类报文得到用户设定的最小带宽。

    对于 AF 队列，当队列的长度达到队列的最大长度时，缺省采用尾丢弃的策略，但用户还可以选择用 WRED 丢弃策略。

  - BE 队列：满足不需要严格 QoS 保证的尽力发送业务

    当报文不匹配用户设定的所有类别时，报文被送入系统定义的缺省类。虽然允许为缺省类配置 AF 队列，并配置带宽，但是更多的情况是为缺省类配置 BE 队列。BE 队列使用 WFQ 调度，使所有进入缺省类的报文进行基于流的队列调度。

    对于 BE 队列，当队列的长度达到队列的最大长度时，缺省采用尾丢弃的策略，但用户还可以选择用 WRED 丢弃策略。

HQoS

传统的 QoS 基于接口进行流量调度，单个接口只能区分业务优先级，无法区分用户。只要属于同一优先级的流量，使用同一个接口队列，彼此之间竞争同一个队列资源。因此，传统的 QoS 无法对接口上多个用户的多个流量进行区分服务。

随着网络用户数量的持续增长和网络业务的不断丰富，用户都希望能够提供区分用户和用户业务的服务，以获得更好的服务质量和更多的利润。HQoS（Hierarchical Quality of Service）基于多级队列实现层次化调度，不仅区分了业务，也区分了用户。既能够提供精细化的服务质量保证，又能够从整体上节约网络运行维护成本。

- HQoS 支持的队列

  HQoS 基于队列实现层次化调度，目前在 AR150/200 上支持三级队列：Level3 流队列 FQ（Flow Queue）、Level2 用户队列 SQ（Subscriber Queue）、 Level1 端口队

列 PQ（Port Queue）。三级队列以树状结构汇聚，流队列为叶子节点，端口队列为根结构。报文作层次化调度时，首先进入叶子节点，经过多级调度后，从根结点发送出去。

- HQoS 的实现方式

  AR150/200 支持的嵌套策略提供了 HQoS 的层次化配置模型。

  流策略嵌套是指一个 QoS 策略中包含另一个 QoS 策略，即父策略的行为（动作）是一个子策略。使用流策略嵌套时，对于命中流分类的某一类报文，除了执行父策略中定义的行为外，还由子策略再对该类流量进行分类，执行子策略中定义的行为。

  父策略区分网络中不同用户,即命中父策略的流分类的报文进入同一个用户队列。

  子策略区分用户的不同业务，即命中父策略的流分类后再次命中子策略的流分类的报文进入同一个流队列。

- HQoS 支持的调度方式

  HQoS 通过分级的方式，来实现更加精细化的调度，为用户 QoS 业务层面提供丰富的业务支撑。调度器的层次与应用的拓扑结构相对应。

  AR150/200 提供了三级调度器，即流队列调度器、用户队列调度器和端口队列调度器。流队列调度器和用户队列调度器都支持 PQ、WFQ、PQ+WFQ 调度。端口队列调度器使用轮询调度 RR（Round Robin）方式。

  以企业用户的 HQoS 部署为例，企业用户主要有三种业务：语音通讯（VoIP）、视频会议（VC）和数据业务（DATA），每个用户队列对应一个企业用户，每个流队列对应一种业务。通过部署 HQoS，可以实现：

  - 控制单个企业用户三种业务之间的流量调度
  - 控制单个企业用户三种业务的总带宽
  - 控制多个企业用户之间的带宽分配
  - 控制多个企业用户的总带宽

1.3 配置优先级映射

AR150/200 将根据报文携带的优先级或端口优先级进行优先级映射，确定报文进入的队列和报文出设备时携带的优先级，从而提供差异化的服务。

1.3.1 建立配置任务

在配置优先级映射前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

对于来自上游设备的报文，用户可以根据报文携带的优先级（802.1p 优先级或 DSCP 优先级）或端口优先级确定报文所进入的队列，并可以根据配置修改报文发送出去时所携带的优先级，以便下游设备根据报文的优先级提供相应的 QoS 服务。

- 配置信任报文携带的 DSCP 优先级时，AR150/200 根据优先级映射关系将 DSCP 优先级映射到 802.1p 优先级，确定报文所进入的队列，并对报文优先级值进行修改。
- 配置信任报文携带的 802.1p 优先级或使用端口优先级时，AR150/200 直接根据 802.1p 值，确定报文所进入的队列，并对报文优先级值进行修改。

前置任务

在配置基于简单流分类的优先级映射之前，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
- 配置相关接口的 IP 地址和路由协议，保证路由互通

数据准备

在配置优先级映射之前，需要准备以下数据：

序号	数据
1	端口的类型和编号
2	端口优先级
3	端口信任的报文优先级
4	输入优先级值和映射后的输出优先级值

1.3.2 配置端口信任的报文优先级

配置端口信任的报文优先级后，AR150/200 将根据指定的优先级进行映射。

背景信息

AR150/200 提供三种优先级信任模式：

- 信任报文的 802.1p 优先级
  - 对于带 VLAN Tag 的报文，根据报文的 802.1p 优先级确定报文所进入的队列，并修改报文的优先级值。
  - 对于不带 VLAN Tag 的报文，根据端口的缺省 802.1p 优先级确定报文所进入的队列，并修改报文的优先级值。
- 信任报文的 DSCP 优先级

  根据报文的 DSCP 优先级映射到 802.1p 优先级，确定报文所进入的队列，并按照优先级映射表修改报文的优先级值。
- 使用端口优先级

  根据端口优先级映射到本地优先级，确定报文所进入的队列，并按照优先级映射表修改报文的优先级值。

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*[.*subinterface-number*]，进入接口视图或子接口视图。

步骤 3 执行命令 **trust** { **8021p** | **dscp** } [**override**]，配置端口信任的报文优先级。

缺省情况下，使用端口优先级。

----结束

1.3.3 配置端口优先级

端口优先级是可配置的，缺省值为 0。

背景信息

在 VLAN 帧的 Tag 字段中有三个 Bit 用来记录帧的 802.1p 优先级，该优先级用于为 QoS 差分服务提供参考依据。

以下情况，会使用到端口的优先级值：

接口配置	收到报文是否带有 VLAN Tag	处理方式
缺省配置（使用端口优先级）	否	根据端口优先级查找对应的 802.1p 优先级到各优先级映射表，修改报文的优先级，按照修改后的 802.1p 优先级将报文入队列。
缺省配置（使用端口优先级）	是	根据端口优先级查找对应的 802.1p 优先级到各优先级映射表，修改报文的优先级，按照修改后的 802.1p 优先级将报文入队列。
trust 8021p override	否	根据端口优先级查找 802.1p 优先级到各优先级映射表，修改报文的优先级，按照修改后的 802.1p 优先级将报文入队列。
trust 8021p	否	根据端口优先级查找 802.1p 优先级到各优先级映射表，修改报文的优先级，按照修改后的 802.1p 优先级将报文入队列。

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。

----结束

1.3.4 配置优先级映射表

优先级映射表支持 802.1p、DSCP 优先级映射之间的相互映射。

背景信息

AR150/200 根据报文自带的优先级或端口缺省优先级进行优先级映射，各优先级之间的映射关系可以在优先级映射表中进行配置。

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 **qos map-table** { **dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp** }，进入优先级映射表视图。

步骤 3 执行命令 **input** { *input-value1* [**to** *input-value2*] } &<1-10> **output** *output-value*，配置优先级映射表中的映射关系。

----结束

1.3.5 检查配置结果

完成优先级映射的配置，可查看全局的优先级映射关系。

前提条件

已经完成优先级映射配置。

操作步骤

- 执行 **display qos map-table [dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp**]命令，查看当前的各优先级间的映射关系。

----结束

1.4 配置流量监管

AR150/200 支持基于接口的流量监管和基于流的流量监管。

1.4.1 建立配置任务

在配置流量监管前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果不限制用户发送的业务流量，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。

- 基于接口的流量监管，可以对流入或流出某接口的业务流量进行流量控制。

说明

用户可以根据需要选择对接口下所有或部分业务流量进行流量监管，如:

- 对接口下所有业务流量进行流量监管;
- 对符合指定 ACL 规则的业务流量进行流量监管;
- 对源、目的 IP 属于指定范围的业务流量进行流量监管。

- 基于流的流量监管，可以对流入或流出接口的符合流分类规则的某类业务流量进行流量控制。

前置任务

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
- 配置相关接口的 IP 地址和路由协议，保证路由互通

数据准备

在配置基于接口的流量监管之前，需要准备以下数据：

序号	数据
1	应用流量监管的接口和方向
2	流量监管参数：承诺信息速率、（可选）峰值信息速率、（可选）承诺突发尺寸、（可选）峰值突发尺寸、（可选）颜色、（可选）颜色模式

在配置基于流的流量监管之前，需要准备以下数据：

序号	数据
1	流分类名称及相关参数
2	流量监管行为名称及 CAR 参数：承诺信息速率、（可选）峰值信息速率、（可选）承诺突发尺寸、（可选）峰值突发尺寸、（可选）颜色、（可选）颜色模式
3	流策略名称及应用流策略的接口和方向（入方向或出方向）

1.4.2 配置基于接口的流量监管

在一个接口的出/入方向配置 CAR，限制进入或流出接口的流量速率。

背景信息

若需要对接口下出/入方向所有流量进行控制时，可以配置基于接口的流量监管，当报文的接收或发送速率不符合要求时，直接被丢弃。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*[.*subinterface-number*]，进入接口视图或子接口视图。

步骤 3 由于 LAN 侧和 WAN 侧接口的配置命令有所区别，选择执行下列命令，配置接口的流量监管。

- 对于 WAN 接口，执行命令 **qos car** { **inbound** | **outbound** } [**acl** *acl-number* | { **destination-ip-address range**| **source-ip-address range** } *start-ip-address* **to** *end-ip-address* [**per-address**]] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]，配置 WAN 接口的流量监管。

  缺省情况下，不进行接口的流量监管。

  说明

  配置 WAN 接口的流量监管时，若不指定 **cbs** 和 **pbs** 值:

  - 若不配置 *pir-value* 或 *pir-value* 与 *cir-value* 相等，则 *cbs-value* 为 *cir-value* 的 188 倍；*pbs-value* 为 *cir-value* 的 313 倍。
  - 若配置 *pir-value* 且 *pir-value* 与 *cir-value* 不相等，则 *cbs-value* 为 *cir-value* 的 125 倍；*pbs-value* 为 *pir-value* 的 125 倍。

  当 *cbs-value* 值小于当前部署业务中单个报文的字节数时，将导致这些报文被直接丢弃。

- 对于 LAN 接口，执行命令 **qos car** { **inbound cir** *cir-value* | { **inbound** | **outbound** } { **acl** *acl-number* | { **destination-ip-address range** | **source-ip-address range** } *start-ip-address* **to** *end-ip-address* [**per-address**] } **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] }，配置 LAN 接口的流量监管。

  缺省情况下，不进行接口的流量监管。

  说明

  AR150/200 LAN 侧接口仅支持对接口入方向进行流量监管。

----结束

1.4.3 配置基于流的流量监管

在流策略中配置流量监管后，可应用在多个接口上，实现对多个接口流入或流出的某类流量进行相同的速率限制。

背景信息

若需要对接口下出/入方向某类流量进行控制时，可以配置基于流的流量监管，相同的流策略可以在不同的接口下应用，当此类报文的接收或发送速率超过限制速率时，直接被丢弃。基于流的流量监管，可以通过复杂流分类，为不同业务提供更细致的差分服务。

操作步骤

步骤 1 定义流分类

AR150/200 支持根据报文中的二层信息、报文中的三层信息、ACL 进行流分类。请根据实际应用，选择合适的流分类规则，配置流分类，具体配置请参见**配置流分类**。

步骤 2 配置流行为

创建流行为，并为其配置流量监管 CAR 动作，具体配置请参见配置流行为中**配置流量监管**。

步骤 3 配置流策略

创建流策略，在流策略中关联流分类和动作，并在接口下应用流策略，具体配置请参见**配置流策略**。

----结束

1.4.4 检查配置结果

配置流量监管后，可查看 CAR 中的限速速率。

前提条件

已经完成流量监管的配置。

操作步骤

- 检查基于接口的流量监管配置结果
  完成配置后，在接口视图下执行命令 **display this**，查看接口下流量监管的配置情况。
- 检查基于流的流量监管配置结果
  - 执行命令 **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。
  - 执行命令 **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]，查看流分类的配置信息。
  - 执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
  - 执行命令 **display traffic-policy** *policy-name* **applied-record**，查看指定流量监管策略的应用记录信息。
- 查看接口上应用了流量监管后的报文统计信息
  - 执行命令 **display qos car statistics interface** *interface-type interface-number* { **inbound** | **outbound** }或 **display qos car statistics interface** { **virtual-template** *vt-number* **virtual-access** *va-number* | **dialer** *number* } { **inbound** | **outbound** }，查看接口上通过和丢弃报文的统计信息。

----结束

1.5 配置流量整形

流量整形实现报文的流量以均匀的速率向外发送，减少因超过承诺速率而被丢弃的报文。

1.5.1 建立配置任务

在配置流量整形前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果上下游网络的带宽不匹配，可在上游网络连接下游网络的出接口上配置流量整形功能，使流向下游网络的报文的速率满足下游网络的带宽要求，从而在一定程度上避免网络产生拥塞、丢包现象。AR150/200 支持以下几种流量整形：

- 基于接口的整形，对接口下所有的业务流量进行流量整形，使之以均匀的速率发送出去。
- 基于队列的整形，对接口下不同优先级队列配置不同的整形速率。
- 基于流的整形，对接口下符合流分类规则的不同类型的业务流量配置不同的整形速率。

可根据需要配置其中一种或两种整形方式，但是不可在同一接口上同时配置基于队列的流量整形和基于流的流量整形。

说明

如果同一接口下既配置基于队列的整形，也配置基于接口的整形，则接口整形的 *cir-value* 必须大于等于接口上所有队列整形的 *cir-value* 之和；否则，流量整形会出现异常现象，可能会造成某些高优先级队列得不到及时调度。

如果同一接口下既配置基于流的整形，也配置基于接口的整形，则接口整形的 cir-value 必须大于等于接口上所有基于流整形的 cir-value 之和；否则，流量整形会出现异常现象，可能会造成某些高优先级队列得不到及时调度。

当逻辑接口为 Dialer 接口、MP-Group 接口、VT 接口、VE 接口和 Tunnel 接口时，可以在逻辑接口或逻辑接口对应的物理接口上配置流量整形。只要逻辑接口上配置了流量整形、拥塞管理或拥塞避免中的任何一个或多个功能，则流量整形、拥塞管理或拥塞避免相关配置仅按照逻辑接口上的配置生效，物理接口上的配置不生效。

前置任务

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
- 配置相关接口的 IP 地址和路由协议，保证路由互通

数据准备

在配置基于接口的流量整形之前，需要准备以下数据：

序号	数据
1	应用流量整形的接口
2	端口整形参数：承诺信息速率、（可选）承诺突发尺寸

在配置基于队列的流量整形之前，需要准备以下数据：

序号	数据
1	应用流量整形的接口和队列
2	队列模板的名称
3	队列整形参数：承诺信息速率、（可选）承诺突发尺寸
4	应用队列模板的接口

在配置基于流的流量整形之前，需要准备以下数据：

序号	数据
1	流分类名称及相关参数
2	流量整形行为名称及 GTS 参数：承诺信息速率、（可选）承诺突发尺寸、（可选）峰值突发尺寸、（可选）队列长度
3	流策略名称及应用流策略的接口

1.5.2 配置基于接口的流量整形

通过配置接口流量整形，限制接口向外发送数据的速率。

背景信息

若需要对接口出方向所有流量进行控制时，可以配置基于接口的流量整形，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，再均匀的向外发送这些被缓存的报文，当缓存队列已满时，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 执行命令 **interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。

步骤 3 执行命令 **qos gts cir** *cir-value* [**cbs** *cbs-value*]，配置端口整形。

缺省情况下，不进行接口的流量整形。配置接口整形时，若不指定 **cbs** 值，*cbs-value* 为 *cir-value* 的 25 倍。

----结束

1.5.3 配置基于队列的流量整形

通过在队列模板中配置队列整形，启动指定端口队列的队列整形功能并设置整形参数。

背景信息

通过在接口下应用队列模板，可以实现针对各队列的流量整形。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。

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 queue-profile** *queue-profile-name*，创建一个队列模板，并进入队列模板视图。

步骤 3 执行命令 **queue** { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **length** { **bytes** *bytes-value* | **packets** *packets-value* }*，配置接口下各队列的长度。

缺省情况下，WAN 侧以 PQ 方式调度的队列，长度为 40960 个字节；WAN 侧以 WFQ 方式调度的队列，长度为 131072 个字节；LAN 侧以 PQ、DRR 和 WRR 方式调度的队列，长度为 5120 个字节。

说明

AR150/200 的二层 FE 接口不支持 **queue length** 配置。

步骤 4 执行命令 **queue** { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **gts cir** *cir-value* [**cbs** *cbs-value*]，配置队列整形。

缺省情况下，不进行队列的流量整形。配置队列整形时，若不指定 **cbs** 值，*cbs-value* 为 *cir-value* 的 25 倍。

步骤 5 执行命令 **quit**，退出队列模板视图。

步骤 6 执行命令 **interface** *interface-type interface-number*[*.subinterface-number*]，进入需要配置队列整形的接口视图或子接口视图。

步骤 7 执行命令 **qos queue-profile** *queue-profile-name*，在接口下应用队列模板。

----结束

1.5.4 配置基于流的流量整形

在流策略中配置流量整形后，可应用在多个接口上，实现对多个接口的某类流量进行相同速率的流量整形。

背景信息

若需要对接口下出方向的某类流量进行控制时，可以配置基于流的流量整形，相同的流策略可以在不同的接口下应用，当此类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，再均匀的向外发送这些被缓存的报文，当缓存队列已满时，报文将被丢弃。基于流的流量整形，可以通过复杂流分类，为不同业务提供更细致的差分服务。

操作步骤

步骤 1 定义流分类

AR150/200 支持根据报文中的二层信息、报文中的三层信息、ACL 进行流分类。请根据实际应用，选择合适的流分类规则，配置流分类，具体配置请参见**配置流分类**。

步骤 2 配置流行为

创建流行为，并为其配置流量整形 GTS 动作，具体配置请参见配置流行为中**配置流量整形**。

步骤 3 配置流策略

创建流策略，在流策略中关联流分类和动作，并在接口下应用流策略，具体配置请参见**配置流策略**。

----结束

1.5.5 检查配置结果

配置流量整形后，可查看配置的整形速率。

前提条件

已经完成流量整形的配置。

操作步骤

- 检查接口视图下的流量整形配置结果

  完成配置后，在接口视图下执行命令 **display this**，查看接口下流量整形的配置情况。
- 检查队列模板视图下的流量整形配置结果
  - 完成配置后，在接口视图下执行命令 **display this**，查看接口下绑定的队列模板。
  - 执行命令 **display qos queue-profile** [*queue-profile-name*]，查看队列模板的配置信息。
- 检查流行为视图下的流量整形配置结果
  - 执行命令 **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。
  - 执行命令 **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]，查看流分类的配置信息。
  - 执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
  - 执行命令 **display traffic-policy** *policy-name* **applied-record**，查看指定流量整形策略的应用记录信息。

----结束

1.6 配置拥塞管理

配置拥塞管理后，当网络中发生拥塞时，AR150/200 将按照配置好的调度策略决定报文转发时的处理次序。

1.6.1 建立配置任务

在配置拥塞管理前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当网络发生拥塞时，可以通过配置拥塞管理来实现如下功能：

- 均衡各类报文的延迟和延迟抖动。
- 关键业务（如视频业务、语音业务）的报文能够得到优先处理。
- 非关键业务（如 E-Mail）的报文，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。

AR150/200 支持基于队列的拥塞管理和基于流分类的拥塞管理：

- 基于队列的拥塞管理：当报文按照优先级映射进入接口下的队列后，可以通过队列模板为各队列配置不同的调度方式，使不同优先级业务获得不同等级的服务。
- 基于流分类的拥塞管理：AR150/200 为匹配流分类的报文提供 EF、AF、BE 三类队列，为匹配不同流分类的报文配置不同的调度方式，使不同类型的业务获得不同等级的服务。

说明

基于队列的拥塞管理与基于流分类的拥塞管理互斥，不可同时配置。

基于流分类的拥塞管理只能配置在 AR150/200 WAN 接口上，LAN 接口不支持此配置。

当逻辑接口为 Dialer 接口、MP-Group 接口、VT 接口、VE 接口和 Tunnel 接口时，可以在逻辑接口或逻辑接口对应的物理接口上配置拥塞管理。只要逻辑接口上配置了流量整形、拥塞管理或拥塞避免中的任何一个或多个功能，则流量整形、拥塞管理或拥塞避免相关配置仅按照逻辑接口上的配置生效，物理接口上的配置不生效。

前置任务

在配置拥塞管理之前，需要完成以下任务：

- 配置优先级映射
- 配置基于流分类的优先级重标记

数据准备

在配置基于队列的拥塞管理之前，需要准备以下数据：

序号	数据
1	应用拥塞管理的接口和队列
2	队列模板的名称
3	队列的调度模式
4	（可选）队列的长度
5	（可选）队列的权值

在配置基于流分类的拥塞管理之前，需要准备以下数据：

序号	数据
1	流分类名称及相关参数

序号	数据
2	拥塞管理行为名称及调度方式
3	流策略名称及应用流策略的接口

1.6.2 配置基于队列的拥塞管理

AR150/200 支持的队列调度模式包括：PQ、DRR、WFQ、WRR、PQ+DRR、PQ +WFQ、PQ+WRR。

背景信息

报文按照优先级映射进入接口下各个队列后，在从接口下发送出去时需要按照一定的规则进行调度。AR150/200 不同接口支持不同的调度模式，队列调度时，先调度 PQ 队列，多个 PQ 队列按优先级高低顺序进行调度。PQ 队列调度完成后，再对 DRR、WFQ 或 WRR 队列进行加权轮循调度。

表 1-4 各接口支持的调度模式

接口	调度模式
LAN 接口	● PQ ● DRR ● WRR ● PQ+DRR ● PQ+WRR **说明** AR150/200 的二层 FE 接口不支持 DRR 调度模式，仅支持: ● PQ ● WRR ● PQ+WRR
WAN 接口	● PQ ● WFQ ● PQ+WFQ

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 queue-profile** *queue-profile-name*，创建一个队列模板，并进入队列模板视图。

步骤 3 由于 LAN 侧和 WAN 侧接口支持的调度模式有所区别，选择执行下列命令，配置各队列的调度模式。

- 对于 WAN 接口，执行命令 **schedule** { { **pq** *start-queue-index* [**to** *end-queue-index*] } | { **wfq** *start-queue-index* [**to** *end-queue-index*] } }*，配置 WAN 接口下各队列的调度模式。
- 对于 LAN 接口，执行命令 **schedule** { { **pq** *start-queue-index* [**to** *end-queue-index*] } | { **drr** *start-queue-index* [**to** *end-queue-index*] } | { **wrr** *start-queue-index* [**to** *end-queue-index*] } }*，配置 LAN 接口下各队列的调度模式。

  缺省情况下，LAN 侧所有队列均采用 WRR 调度模式，WAN 侧所有队列均采用 WFQ 调度模式。

步骤 4 （可选）执行命令 **queue** { *start-queue-index* [**to** *end-queue-index*] } &<1－10> **length** { **bytes** *bytes-value* | **packets** *packets-value* }*，配置接口下各队列的长度。

缺省情况下，LAN 侧以 PQ、DRR 或 WRR 方式调度的队列，长度为 5120 个字节；WAN 侧以 PQ 调度的队列，长度为 40960 个字节；WAN 侧以 WFQ 方式调度的队列，长度为 131072 个字节。

说明

AR150/200 的二层 FE 接口不支持 **queue length** 配置。

步骤 5 （可选）执行命令 **queue** { *start-queue-index* [**to** *end-queue-index*] } &<1－10> **weight** *weight-value*，配置接口下各队列的权重。

缺省情况下，队列权重为 10。

说明

AR150/200 的二层 FE 接口不支持 **queue weight** 配置。

步骤 6 执行命令 **quit**，退出队列模板视图。

步骤 7 执行命令 **interface** *interface-type interface-number*[.*subinterface-number*]，进入需要配置拥塞管理的接口视图或子接口视图。

步骤 8 执行命令 **qos queue-profile** *queue-profile-name*，在接口下应用队列模板。

----结束

1.6.3 配置基于流分类的拥塞管理

配置流策略后，可应用在多个接口上，实现对多个接口的某类流量应用相同的队列调度方式。

背景信息

AR150/200 为命中流分类规则的数据报文提供了 3 类队列：

- 确保转发队列（AF）：可以保证在网络发送的业务流量没有超过最小可确保带宽的情况下，此队列中报文的丢失概率非常低。确保转发适用于流量较大，且需要被保证的业务。
- 加速转发队列（EF）：匹配规则的报文进入 EF 队列后，进行绝对优先级调度，仅当 EF 队列中的报文调度完毕后，才会调度其他队列中的报文。加速转发适用于需要保证低延时、低丢弃概率、确保带宽、且占用带宽不是很大的业务，例如语音报文。
- 尽力而为队列（BE）：与系统定义的缺省类 **default-class** 关联使用，未进入 AF 队列和 EF 队列的剩余报文进入 BE 队列。BE 队列使用 WFQ 算法调度，队列数越

多，带宽被分享的越公平，但是占用的队列资源相对也多。WFQ 调度的 BE 队列适用于那些对时延和丢包无特殊要求的业务，例如普通上网业务。

主接口或子接口上配置的基于流分类的拥塞管理（即 CBQ 调度），会与接口上的其他配置互斥：

CBQ 配置位置	是否可以配置队列模板（qos queue-profile（接口视图））	是否可以配置流量整形（qos gts）
主接口	主接口：否	主接口：是
	子接口：否	子接口：否
子接口	主接口：是	主接口：是
	子接口：否	子接口：是

操作步骤

步骤 1 配置流分类

AR150/200 支持根据报文中的二层信息、报文中的三层信息、ACL 进行流分类。请根据实际应用，选择合适的流分类规则，配置流分类，具体配置请参见**配置流分类**。

步骤 2 配置流行为

创建流行为，并为其配置基于流的队列调度，具体配置请参见配置流行为中**配置拥塞管理**。

步骤 3 配置流策略

创建流策略，在流策略中关联流分类和动作，并在接口下应用流策略，具体配置请参见**配置流策略**。

----结束

1.6.4 检查配置结果

配置拥塞管理后，可以查看指定接口上各队列的调度参数。

前提条件

已经完成拥塞管理的配置。

操作步骤

- 检查基于队列的拥塞管理配置结果
  - 完成配置后，在接口视图下执行命令 **display this**，查看接口下绑定的队列模板。
  - 执行命令 **display qos queue-profile** [*queue-profile-name*]，查看队列模板的配置信息。
- 检查基于流分类的拥塞管理配置结果

- 执行命令 **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。
- 执行命令 **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]，查看流分类的配置信息。
- 执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令 **display traffic-policy** *policy-name* **applied-record**，查看指定流量整形策略的应用记录信息。

----结束

1.7 配置拥塞避免

配置拥塞避免后，AR150/200 将根据 WRED 的配置信息丢弃超出流量范围的报文。

1.7.1 建立配置任务

在配置拥塞避免前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

当网络发生拥塞时，AR150/200 默认采用尾丢弃，即在拥塞发生期间，队列尾部的数据报文将被丢弃，直到拥塞解决。这种丢弃策略会引发 TCP 全局同步现象，影响链路利用率，配置 WRED 随机丢弃策略可以很好的避免这种现象，调整网络流量，解除网络过载。

AR150/200 支持基于队列的拥塞避免和基于流的拥塞避免：

- 基于队列的拥塞避免：通过在队列模板中为各队列绑定不同的丢弃模板，实现为各优先级队列配置不同的 WRED 参数，使不同优先级业务获得不同等级的服务。
- 基于流的拥塞避免：AR150/200 为流分类中的报文提供 3 种调度方式的队列，其中 EF 队列只能使用尾丢弃，AF 队列和 BE 队列可以通过在流行为中绑定丢弃模板，使不同优先级业务获得不同等级的服务。

说明

基于队列的拥塞避免与基于流的拥塞避免互斥，不可同时配置。

拥塞避免只能配置在 AR150/200 WAN 接口上，LAN 接口不支持此配置。

当逻辑接口为 Dialer 接口、MP-Group 接口、VT 接口、VE 接口和 Tunnel 接口时，可以在逻辑接口或逻辑接口对应的物理接口上配置拥塞避免。只要逻辑接口上配置了流量整形、拥塞管理或拥塞避免中的任何一个或多个功能，则流量整形、拥塞管理或拥塞避免相关配置仅按照逻辑接口上的配置生效，物理接口上的配置不生效。

前置任务

在配置拥塞避免之前，需要完成以下任务：

- 配置优先级映射
- 配置基于流分类的优先级重标记
- 配置拥塞管理

数据准备

在配置基于队列的拥塞避免之前，需要准备以下数据：

序号	数据
1	丢弃模板的名称和 WRED 参数
2	队列模板的名称
3	应用拥塞避免的接口和队列

在配置基于流的拥塞避免之前，需要准备以下数据：

序号	数据
1	丢弃模板的名称和 WRED 参数
2	流分类名称及相关参数
3	拥塞避免行为名称
4	流策略名称及应用流策略的接口

1.7.2 配置基于队列的 WRED

在 WAN 侧接口应用丢弃模板，可减少 WAN 侧口上的队列的拥塞。

背景信息

丢弃模板是队列各优先级 WRED 参数的集合，实现对绑定丢弃模板的队列的拥塞避免。

丢弃模板在队列模板中绑定后，还需要将队列模板在接口下绑定，才能使丢弃模板中配置的 WRED 参数在该接口下生效。

AR150/200 支持基于 DSCP 优先级的 WRED 和基于 IP 优先级的 WRED：

- IP 优先级分为 0 ～ 7，共 8 个等级。
- DSCP 优先级分为 0 ～ 63，共 64 个等级。
- DSCP 的 8 个等级对应 IP 优先级的同一个等级。

因此基于 DSCP 优先级配置 WRED 参数可以做到更为精细的划分，用户可以根据业务需要选择合适的配置。

说明

AR150/200 仅支持为 WAN 接口的队列模板中调度模式为 WFQ 的队列绑定丢弃模板。

操作步骤

步骤 1 配置丢弃模板

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **drop-profile** *drop-profile-name*，创建一个丢弃模板，并进入丢弃模板视图。
3. （可选）执行命令 **wred** { **dscp** | **ip-precedence** }，指定当前 WRED 丢弃模板基于 DSCP 优先级或 IP 优先级进行丢弃。
4. 选择执行下列命令，配置基于 DSCP 优先级或 IP 优先级的 WRED 参数。
   - 执行命令 **dscp** { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*，配置基于 DSCP 优先级的 WRED 参数。
   - 执行命令 **ip-precedence** { *ip-precedence-value1* [**to** *ip-precedence-value2*] } &<1-10> **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*，配置基于 IP 优先级的 WRED 参数。
5. 执行命令 **quit**，退出丢弃模板视图。

步骤 2 应用丢弃模板

1. 执行命令 **qos queue-profile** *queue-profile-name*，进入队列模板视图。

   此队列模板可以是新创建的，也可以是已创建的。队列模板下还可以根据需要配置队列调度方式、队列权重、队列长度、队列整形。
2. 执行命令 **schedule wfq** *start-queue-index* [**to** *end-queue-index*]，在队列模板中为指定队列配置 WFQ 调度模式。
3. 执行命令 **queue** { *start-queue-index* [**to** *end-queue-index*] } &<1－10> **drop-profile** *drop-profile-name*，在队列模板中为指定队列绑定丢弃模板。

   缺省情况下，所有队列未绑定丢弃模板，所有队列均采用尾丢弃。
4. 执行命令 **quit**，退出队列模板视图。
5. 执行命令 **interface** *interface-type interface-number*[*.subinterface-number*]，进入需要配置拥塞避免的接口视图或子接口视图。
6. 执行命令 **qos queue-profile** *queue-profile-name*，在接口下应用队列模板。

----结束

1.7.3 配置基于流的 WRED

在流策略上应用丢弃模板，可减少 AF 队列和 BE 队列的拥塞。

前提条件

已经配置了基于流分类的拥塞管理。

背景信息

丢弃模板是队列各优先级 WRED 参数的集合，实现对绑定丢弃模板的队列的拥塞避免。

丢弃模板在流行为中绑定后，将流行为与流分类在流策略下进行绑定，并在接口下应用流策略，才能使丢弃模板中配置的 WRED 参数在该接口下生效。

AR150/200 支持基于 DSCP 优先级的 WRED 和基于 IP 优先级的 WRED：

- IP 优先级分为 0 ～ 7，共 8 个等级。
- DSCP 优先级分为 0 ～ 63，共 64 个等级。
- DSCP 的 8 个等级对应 IP 优先级的同一个等级。

因此基于 DSCP 优先级配置 WRED 参数可以做到更为精细的划分，用户可以根据业务需要选择合适的配置。

说明

拥塞避免只能配置在 AR150/200 WAN 接口上，LAN 接口不支持此配置。

由于丢弃模板只能应用于 AF 队列和 BE 队列，所以配置基于流的拥塞避免前必须前配置基于流分类的拥塞管理。

操作步骤

步骤 1 配置丢弃模板

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **drop-profile** *drop-profile-name*，创建一个丢弃模板，并进入丢弃模板视图。
3. （可选）执行命令 **wred** { **dscp** | **ip-precedence** }，指定当前 WRED 丢弃模板基于 DSCP 优先级或 IP 优先级进行丢弃。
4. 选择执行下列命令，配置基于 DSCP 优先级或 IP 优先级的 WRED 参数。
   - 执行命令 **dscp** { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*，配置基于 DSCP 优先级的 WRED 参数。
   - 执行命令 **ip-precedence** { *ip-precedence-value1* [**to** *ip-precedence-value2*] } &<1-10> **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*，配置基于 IP 优先级的 WRED 参数。
5. 执行命令 **quit**，退出丢弃模板视图。

步骤 2 应用丢弃模板

1. 定义流分类

   AR150/200 支持根据报文中的二层信息、报文中的三层信息、ACL 进行流分类。请根据实际应用，选择合适的流分类规则，配置流分类，具体配置请参见**配置流分类**。

2. 配置流行为

   创建流行为，并为其配置基于流的拥塞避免，具体配置请参见配置流行为中**配置拥塞避免**。

3. 配置流策略

   创建流策略，在流策略中关联流分类和动作，并在接口下应用流策略，具体配置请参见**配置流策略**。

----结束

1.7.4 检查配置结果

配置拥塞避免后，可查看 WRED 模板的丢弃参数。

前提条件

已经完成拥塞避免的配置。

操作步骤

- 检查基于队列的拥塞避免配置结果
  - 完成配置后，在接口视图下执行命令 **display this**，查看接口下绑定的队列模板。
  - 在队列模板视图下执行命令 **display this**，查看队列模板绑定的丢弃模板。
  - 执行命令 **display drop-profile** [*drop-profile-name*]，查看丢弃模板的配置信息。
- 检查基于流的拥塞避免配置结果
  - 执行命令 **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。
  - 执行命令 **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]，查看流分类的配置信息。
  - 执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
  - 执行命令 **display traffic-policy** *policy-name* **applied-record**，查看指定流量整形策略的应用记录信息。

----结束

1.8 配置 HQoS

AR150/200 支持的 HQoS（Hierarchical Quality of Service）基于多级队列的层次化调度，可以实现对不同用户的不同业务流量的区分，提供更为精细化的服务质量。

1.8.1 建立配置任务

在配置 HQoS 前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

传统的 QoS 基于接口进行流量调度，单个接口只能区分业务优先级，无法区分用户。只要属于同一优先级的流量，使用同一个接口队列，彼此之间竞争同一个队列资源，无法对接口上多个用户的多个流量进行区分服务。

随着网络用户数量的持续增长和网络业务的不断丰富，用户都希望能够提供区分用户和用户业务的服务，以获得更好的服务质量和更多的利润。HQoS 基于多级队列实现层次化调度，不仅区分了业务，也区分了用户。既能够提供精细化的服务质量保证，又能够从整体上节约网络运行维护成本。

AR150/200 通过嵌套流策略实现 HQoS，即父策略的流行为是一个子策略，使用嵌套流策略时，各策略中允许配置的流分类和流行为如**表 1-5** 所示：

表 1-5 嵌套流策略支持的流分类和流行为

流策略	流分类	流行为
父策略	全部支持	（必选）配置基于流的流量整形 （必选）绑定子策略 （可选）配置流量统计
子策略	全部支持	以下 2 种流行为是互斥的，不可同时配置： ● 配置基于流的流量整形 ● 配置基于流分类的拥塞管理和拥塞避免 –（必选）配置基于流分类的拥塞管理 –（可选）配置基于流的拥塞避免

说明

AR150/200 仅支持在 WAN 接口的出方向配置 HQoS。

前置任务

在配置 HQoS 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
- 配置相关接口的 IP 地址和路由协议，保证路由互通
- 配置优先级映射
- 如果使用 ACL 作为流分类规则，配置相应的 ACL

数据准备

在配置 HQoS 之前，需要准备以下数据：

序号	数据
1	父流策略的流分类、流行为和流策略的名称及相关参数
2	子流策略的流分类、流行为和流策略的名称及相关参数
3	应用流策略的接口
4	（可选）基于接口的流量监管和流量整形参数

1.8.2 配置流策略

父流策略和子流策略的嵌套使用，可以实现区分用户和用户业务，提供更为精细的服务。

1.8.2.1 配置子流策略

子流策略可以区分用户的不同业务。

背景信息

AR150/200 子流策略的流行为中不可同时配置以下 2 类互斥的流行为：

- 基于流的流量整形
- 基于流分类的拥塞管理和拥塞避免

操作步骤

步骤 1 定义流分类

AR150/200 支持根据报文中的二层信息、报文中的三层信息、ACL 进行流分类。请根据实际应用，选择合适的流分类规则，配置流分类，具体配置请参见**配置流分类**。

步骤 2 配置流行为

创建流行为，根据实际应用，为其配置合适的动作，具体配置请参见**配置流行为**。

步骤 3 绑定流分类和流行为

创建子流策略，在子流策略中关联流分类和动作，具体配置请参见**配置流策略**。

----结束

1.8.2.2 配置父流策略

父流策略区分网络中不同用户,并进行基于用户的流量整形。

前提条件

已经完成**配置子流策略**。

背景信息

父流策略的流行为必须先配置 **gts（流行为视图）**，再配置子流策略，还可以选择配置流量统计功能。

操作步骤

步骤 1 定义流分类

请根据实际应用，选择合适的流分类规则，配置流分类，具体配置请参见**配置流分类**。

步骤 2 配置流行为

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。
3. 执行命令 **gts cir** *cir-value* [**cbs** *cbs-value* [**queue-length** *queue-length*]]，配置流量整形 GTS 动作。
4. 执行命令 **traffic-policy** *policy-name*,在流行为中绑定子流策略。
5. （可选）执行命令 **statistic enable**，使能流量统计功能。
6. 执行命令 **quit**，退出流行为视图。

步骤 3 绑定流分类和流行为

创建父流策略，在父流策略中关联流分类和动作，具体配置请参见**配置流策略**。

说明

父流策略和子流策略都支持 1024 个流分类和流行为的绑定。

父流策略的每一个流行为只能绑定一个子流策略，不同的流行为可以绑定不同的子流策略。

父流策略绑定的多组流分类和流行为中，各流分类的匹配规则不允许相同，若规则相同，即对同一类报文做不同的动作，导致出错。

----结束

1.8.2.3 应用流策略

配置的流策略只有在接口应用后才能生效。

背景信息

说明

AR150/200 仅支持在 WAN 接口的出方向上应用嵌套流策略。

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*[*.subinterface-number*]，进入接口视图或子接口视图。

步骤 3 执行命令 **traffic-policy** *policy-name* **outbound**，在接口或子接口的出方向上应用父流策略。

----结束

1.8.3 （可选）配置接口的流量监管

通过在接口的出方向配置 CAR，限制接口向外发送数据的速率，不引入额外的延迟。

背景信息

AR150/200 支持对流队列和端口队列进行流量监管。

- 子流策略中配置的 **car（流行为视图）**，是对流队列的流量进行控制，即对同一用户的不同业务配置不同的数据发送速率。
- 接口上配置的 **qos car**，是对端口下总流量进行控制，不区分用户和业务。

操作步骤

步骤 1 请根据实际应用，配置流量监管参数，具体配置请参见**配置基于接口的流量监管**。

----结束

1.8.4 （可选）配置接口的流量整形

通过在接口配置 GTS，限制接口向外发送数据的速率，可能会增加延迟。

背景信息

AR150/200 支持三级整形器，即流队列整形器、用户队列整形器和端口队列整形器。

- 子流策略中配置的 **gts（流行为视图）**，是对流队列的整形，即为同一用户的不同业务配置差异化的整形速率。
- 父流策略中配置的 **gts（流行为视图）**，是对用户队列的整形，即为不同用户配置差异化的整形速率。
- 接口上配置的 **qos gts**，是对端口下总流量进行整形，不区分用户和业务。

说明

若同一接口下配置了三级整形，则接口整形的 *cir-value* 必须大于等于接口和子接口上绑定的父策略中所有行为的 *cir-value* 之和，每个父策略中的 *cir-value* 必须大于等于子策略中所有行为的 *cir-value* 之和。

操作步骤

步骤 1 请根据实际应用，配置流量整形速率，具体配置请参见**配置基于接口的流量整形**。

----结束

1.8.5 检查配置结果

配置 HQoS 后，可以查看 HQoS 中配置的队列调度方式。

前提条件

已经完成 HQoS 的配置。

操作步骤

- 执行命令 **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。
- 执行命令 **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]，查看流分类的配置信息。
- 执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。
- 执行命令 **display traffic-policy** *policy-name* **applied-record**，查看指定流量整形策略的应用记录信息。
- 在接口视图下执行命令 **display this**，查看接口下流量监管和流量整形的配置情况。

----结束

1.9 维护 QoS

QoS 的维护通过查看或清除基于队列的流量统计信息来实现。

1.9.1 查看队列统计信息

队列统计信息中包含通过和丢弃的报文数等。

背景信息

用户需要了解接口下各队列是否有报文通过，是否有报文因为发生拥塞被丢弃时，可以查看接口下各队列的统计信息。

操作步骤

- 执行命令 **display qos queue statistics interface** *interface-type interface-number* [**queue** *queue-index*]或 **display qos queue statistics interface** { **virtual-template** *vt-number* **virtual-access** *va-number* | **dialer** *number* } [**queue** *queue-index*]，查看基于队列的流量统计信息。

----结束

1.9.2 清除队列统计信息

通过 **reset** 命令清除队列的统计信息。

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。

注意

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* [**queue** *queue-index*]或 **reset qos queue statistics interface** { **virtual-template** *vt-number* **virtual-access** *va-number* | **dialer** *number* } [**queue** *queue-index*]，清除接口上基于队列的流量统计信息。

----结束

1.10 配置举例

通过示例介绍如何综合应用流量监管、流量整形、拥塞避免和拥塞管理。配置示例中包括组网需求、配置注意事项、配置思路等。

1.10.1 配置优先级映射示例

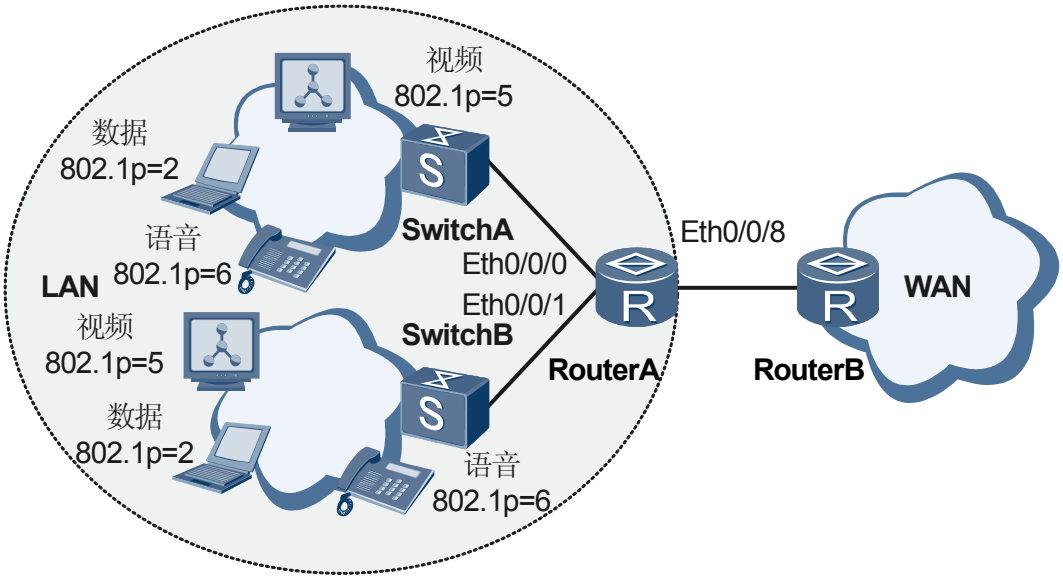
通过配置端口信任的报文优先级和优先级映射表后，AR150/200 根据指定的优先级确定报文所进入的队列并可以根据需要修改报文的优先级值，以提供差分服务。

组网需求

如图 1-3 所示，企业网内部 LAN 侧的语音、视频和数据业务通过 SwitchA 和 SwitchB 连接到 RouterA 的 Eth0/0/0 和 Eth0/0/1 上，并通过 RouterA 的 Eth0/0/8 接口连接到 WAN 侧网络。

不同业务的报文在 LAN 侧使用 802.1p 优先级进行标识，在 RouterA 上根据报文的 802.1p 优先级入队列，当报文从 Eth0/0/8 接口到达 WAN 侧时，需要根据报文的 DSCP 优先级提供差分服务，配置优先级映射表，可以根据报文的 802.1p 优先级修改报文中的 DSCP 优先级值。

图 1-3 配置优先级映射的组网图



配置思路

采用如下的思路配置优先级映射：

1. 在 RouterA 创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 RouterA 访问 WAN 侧网络。
2. 在 RouterA 上配置端口信任的报文优先级为信任报文的 802.1p 优先级。
3. 在 RouterA 上配置优先级映射表，修改 802.1p 优先级与 DSCP 优先级之间的映射关系，使设备能根据要求按照报文的 802.1p 优先级为其修改不同的 DSCP 优先级值。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 与 SwitchA 相连的接口所属 VLAN 编号为 20，VLANIF 20 的 IP 地址为 192.168.2.1/24，接口信任报文的 802.1p 优先级。
- RouterA 与 SwitchB 相连的接口所属 VLAN 编号为 30，VLANIF 30 的 IP 地址为 192.168.3.1/24，接口信任报文的 802.1p 优先级。
- RouterA 与 WAN 侧相连的接口 IP 地址为 192.168.4.1/24。
- RouterA 上 802.1p 优先级与 DSCP 优先级的映射关系：将 802.1p 优先级 2、5、6 映射为 DSCP 优先级 14、40、46。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 RouterA 上创建 VLAN 20、30。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 20 30
```

配置接口 Eth0/0/0 和 Eth0/0/1 为 Trunk 类型端口，并将 Eth0/0/0 加入 VLAN20，将 Eth0/0/1 加入 VLAN30。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] port link-type trunk
[RouterA-Ethernet0/0/0] port trunk allow-pass vlan 20
[RouterA-Ethernet0/0/0] quit
[RouterA] interface ethernet 0/0/1
[RouterA-Ethernet0/0/1] port link-type trunk
[RouterA-Ethernet0/0/1] port trunk allow-pass vlan 30
[RouterA-Ethernet0/0/1] quit
```

说明

请配置 SwitchA 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN20。

请配置 SwitchB 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN30。

创建 VLANIF 20、30，并为 VLANIF 20 配置 IP 地址 192.168.2.1/24，为 VLANIF 30 配置 IP 地址 192.168.3.1/24。

```
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 192.168.2.1 24
[RouterA-Vlanif20] quit
[RouterA] interface vlanif 30
[RouterA-Vlanif30] ip address 192.168.3.1 24
[RouterA-Vlanif30] quit
```

配置 Eth0/0/8 的 IP 地址为 192.168.4.1/24。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] ip address 192.168.4.1 24
[RouterA-Ethernet0/0/8] quit
```

说明

根据实际情况配置 RouterB，确保 RouterB 与 RouterA 间路由可达，具体步骤略。

步骤 2 配置优先级映射

配置 Eth0/0/0 和 Eth0/0/1 接口信任报文的 802.1p 优先级。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] trust 8021p
[RouterA-Ethernet0/0/0] quit
[RouterA] interface ethernet 0/0/1
[RouterA-Ethernet0/0/1] trust 8021p
[RouterA-Ethernet0/0/1] quit
```

配置优先级映射关系。

```
[RouterA] qos map-table dot1p-dscp
[RouterA-maptbl-dot1p-dscp] input 2 output 14
[RouterA-maptbl-dot1p-dscp] input 5 output 40
[RouterA-maptbl-dot1p-dscp] input 6 output 46
```

步骤 3 验证配置结果

查看 RouterA 上的优先级映射信息。

```
<RouterA> display qos map-table dot1p-dscp
Input Dot1p      DSCP
-------------------
 0               0
 1               8
 2               14
 3               24
 4               32
 5               40
 6               46
 7               56
```

查看 RouterA 接口的配置信息。

```
<RouterA> system-view
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] display this
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 trust 8021p
#
return
[RouterA-Ethernet0/0/0] quit
[RouterA] interface ethernet 0/0/1
[RouterA-Ethernet0/0/1] display this
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 trust 8021p
#
return
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 20 30
#
qos map-table dot1p-dscp
  input 2 output 14
  input 6 output 46
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type trunk
```

```
 port trunk allow-pass vlan 20
 trust 8021p
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 trust 8021p
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
#
return
```

1.10.2 配置流量监管示例

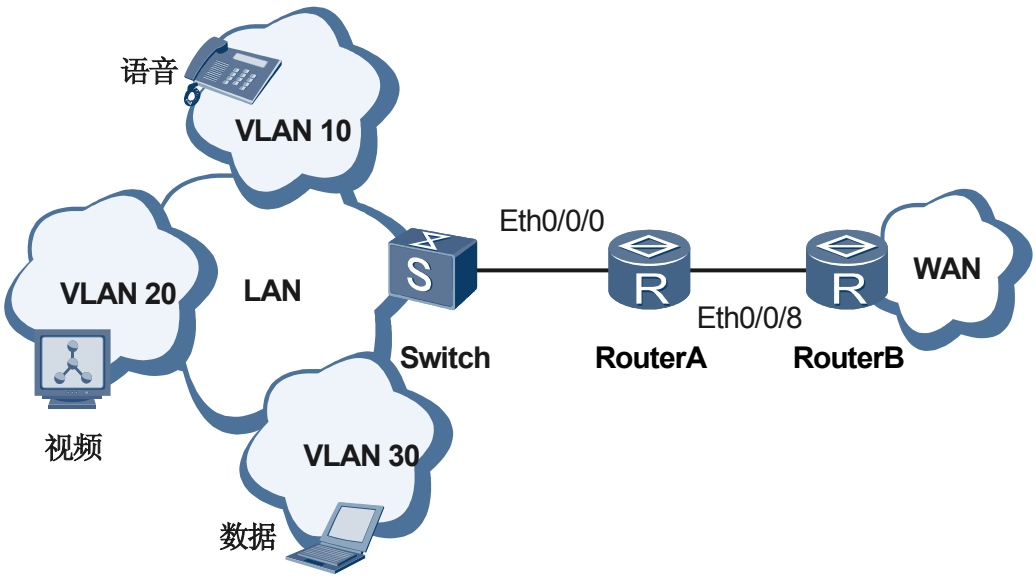
通过配置基于接口的流量监管，为不同用户提供不同的带宽服务；通过配置基于流的流量监管，对同一用户的不同业务设置不同的 CAR 参数，提供不同的带宽服务。

组网需求

如图 1-4 所示，企业网内部 LAN 侧的语音、视频和数据业务对应的 VLAN ID 分别为 10、20、30，并通过 Switch 连接到 RouterA 的 Eth0/0/0 上，通过 RouterA 的 Eth0/0/8 接口连接到 WAN 侧网络。

在 RouterA 上需要对不同业务的报文分别进行基于流的流量监管，以将各业务流量控制在一个合理的范围之内，保证各业务的带宽要求；并对接口 Eth0/0/0 入方向的所有流量进行基于接口的流量监管，控制单个企业用户的总流量在一个合理范围之内。

图 1-4 配置流量监管的组网图



配置思路

采用如下的思路配置流量监管：

1. 在 RouterA 创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 RouterA 访问 WAN 侧网络。

2. 在 RouterA 上配置基于 VLAN ID 进行流分类的匹配规则。
3. 在 RouterA 上配置流行为，对来自企业网内部的不同业务报文进行流量监管。
4. 在 RouterA 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 RouterA 与 Switch 连接的接口入方向上。
5. 在 RouterA 与 Switch 连接的接口入方向上配置基于接口的流量监管，对来自该企业网内部的所有报文进行流量监管。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 与 Switch 相连的接口允许 VLAN 10、VLAN 20、VLAN 30 的报文通过，VLANIF 10 的 IP 地址为 192.168.1.1/24，VLANIF 20 的 IP 地址为 192.168.2.1/24，VLANIF 30 的 IP 地址为 192.168.3.1/24。
- RouterA 与 WAN 侧相连的接口 IP 地址为 192.168.4.1/24。
- 匹配不同业务流的流分类名称。
- 不同业务流的流量监管参数：
  - 语音：CIR 为 256kbit/s，CBS 为 48128byte，PBS 为 80128byte。
  - 视频：CIR 为 4000kbit/s，CBS 为 752000byte，PBS 为 1252000byte。
  - 数据：CIR 为 2000kbit/s，CBS 为 376000byte，PBS 为 626000byte。
- 企业用户的总带宽参数：CIR 为 10000kbit/s。
- 需要应用流策略的接口类型、方向和编号:RouterA 上接口 Eth0/0/0 的入方向。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 RouterA 上创建 VLAN 10、20、30。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 10 20 30
```

配置接口 Eth0/0/0 为 Trunk 类型端口，并允许 VLAN 10、VLAN 20、VLAN 30 的报文通过。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] port link-type trunk
[RouterA-Ethernet0/0/0] port trunk allow-pass vlan 10 20 30
[RouterA-Ethernet0/0/0] quit
```

说明

请配置 Switch 与 RouterA 对接的接口为 Trunk 类型接口，并允许 VLAN 10、VLAN 20、VLAN 30 的报文通过。

创建 VLANIF 10、20、30，并为 VLANIF 10 配置 IP 地址 192.168.1.1/24，并为 VLANIF 20 配置 IP 地址 192.168.2.1/24，为 VLANIF 30 配置 IP 地址 192.168.3.1/24。

```
[RouterA] interface vlanif 10
[RouterA-Vlanif10] ip address 192.168.1.1 24
[RouterA-Vlanif10] quit
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 192.168.2.1 24
[RouterA-Vlanif20] quit
[RouterA] interface vlanif 30
[RouterA-Vlanif30] ip address 192.168.3.1 24
[RouterA-Vlanif30] quit
```

配置 Eth0/0/8 的 IP 地址为 192.168.4.1/24。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] ip address 192.168.4.1 24
[RouterA-Ethernet0/0/8] quit
```

说明

根据实际情况配置 RouterB，确保 RouterB 与 RouterA 间路由可达，具体步骤略。

步骤 2 配置流分类

在 RouterA 上创建流分类 c1 ～ c3，对来自企业的不同业务流按照其 VLAN ID 进行分类。

```
[RouterA] traffic classifier c1
[RouterA-classifier-c1] if-match vlan-id 10
[RouterA-classifier-c1] quit
[RouterA] traffic classifier c2
[RouterA-classifier-c2] if-match vlan-id 20
[RouterA-classifier-c2] quit
[RouterA] traffic classifier c3
[RouterA-classifier-c3] if-match vlan-id 30
[RouterA-classifier-c3] quit
```

步骤 3 配置流量监管行为

在 RouterA 上创建流行为 b1 ～ b3，对来自企业的不同业务流进行流量监管,并使能流量统计功能。

```
[RouterA] traffic behavior b1
[RouterA-behavior-b1] car cir 256 cbs 48128 pbs 80128
[RouterA-behavior-b1] statistic enable
[RouterA-behavior-b1] quit
[RouterA] traffic behavior b2
[RouterA-behavior-b2] car cir 4000 cbs 752000 pbs 1252000
[RouterA-behavior-b2] statistic enable
[RouterA-behavior-b2] quit
[RouterA] traffic behavior b3
[RouterA-behavior-b3] car cir 2000 cbs 376000 pbs 626000
[RouterA-behavior-b3] statistic enable
[RouterA-behavior-b3] quit
```

步骤 4 配置流量监管策略并应用到接口上

在 RouterA 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 Eth0/0/0 入方向上，对来自企业的不同业务报文进行基于流的流量监管。

```
[RouterA] traffic policy p1
[RouterA-trafficpolicy-p1] classifier c1 behavior b1
[RouterA-trafficpolicy-p1] classifier c2 behavior b2
[RouterA-trafficpolicy-p1] classifier c3 behavior b3
[RouterA-trafficpolicy-p1] quit
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] traffic-policy p1 inbound
```

步骤 5 配置基于接口的流量监管

在 RouterA 的接口 Eth0/0/0 入方向上配置基于接口的流量监管，控制单个企业用户的总流量在一个合理范围之内。

```
[RouterA-Ethernet0/0/0] qos car inbound cir 10000
[RouterA-Ethernet0/0/0] quit
```

步骤 6 验证配置结果

查看流分类的配置信息。

```
[RouterA] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: OR
    Rule(s) : if-match vlan-id 20

   Classifier: c3
    Operator: OR
    Rule(s) : if-match vlan-id 30

   Classifier: c1
    Operator: OR
    Rule(s) : if-match vlan-id 10
```

查看流策略的配置信息。

```
[RouterA] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: OR
     Behavior: b1
      Committed Access Rate:
        CIR 256 (Kbps), PIR 0 (Kbps), CBS 48128 (byte), PBS 80128 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      statistic: enable

   Classifier: c2
    Operator: OR
     Behavior: b2
      Committed Access Rate:
         CIR 4000 (Kbps), PIR 0 (Kbps), CBS 752000 (byte), PBS 1252000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      statistic: enable

   Classifier: c3
    Operator: OR
     Behavior: b3
      Committed Access Rate:
       CIR 2000 (Kbps), PIR 0 (Kbps), CBS 376000 (byte), PBS 626000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      statistic: enable
```

查看在接口上应用的流策略信息。

```
[RouterA] display traffic policy statistics interface ethernet 0/0/0 inbound

 Interface: Ethernet0/0/0
 Traffic policy inbound: p1
 Rule number: 3
 Current status: OK!
Item                          Sum(Packets/Bytes)            Rate(pps/bps)
-------------------------------------------------------------------------------
Matched                                    0/                          0/
                                           0                           0
  +--Passed                                0/                          0/
                                           0                           0
  +--Dropped                               0/                          0/
                                           0                           0
```

```
    +--Filter                    0/                    0/
                                 0                     0
    +--CAR                       0/                    0/
                                 0                     0
 +--Queue Matched                 0/                     0/
                                 0                     0
    +--Enqueued                  0/                    0/
                                 0                     0
    +--Discarded                 0/                    0/
                                 0                     0
  +--Car                         0/                    0/
                                 0                     0
    +--Green packets             0/                    0/
                                 0                     0
    +--Yellow packets            0/                    0/
                                 0                     0
    +--Red packets               0/                    0/
                                 0                     0
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 10 20 30
#
traffic classifier c1 operator or
 if-match vlan-id 10
traffic classifier c2 operator or
 if-match vlan-id 20
traffic classifier c3 operator or
 if-match vlan-id 30
#
traffic behavior b1
 car cir 256 cbs 48128 pbs 80128 green pass yellow pass red discard
 statistic enable
traffic behavior b2
 car cir 4000 cbs 752000 pbs 1252000 green pass yellow pass red discard
 statistic enable
traffic behavior b3
 car cir 2000 cbs 376000 pbs 626000 green pass yellow pass red discard
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
 qos car inbound cir 10000
 traffic-policy p1 inbound
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
```

```
#
return
```

1.10.3 配置流量整形示例

通过配置基于接口的流量整形，对接口下同一用户的所有业务流量进行流量整形，使之以均匀的速率发送出去；通过配置基于队列的流量整形，对同一用户的不同业务设置不同的 GTS 参数，提供不同的带宽服务。

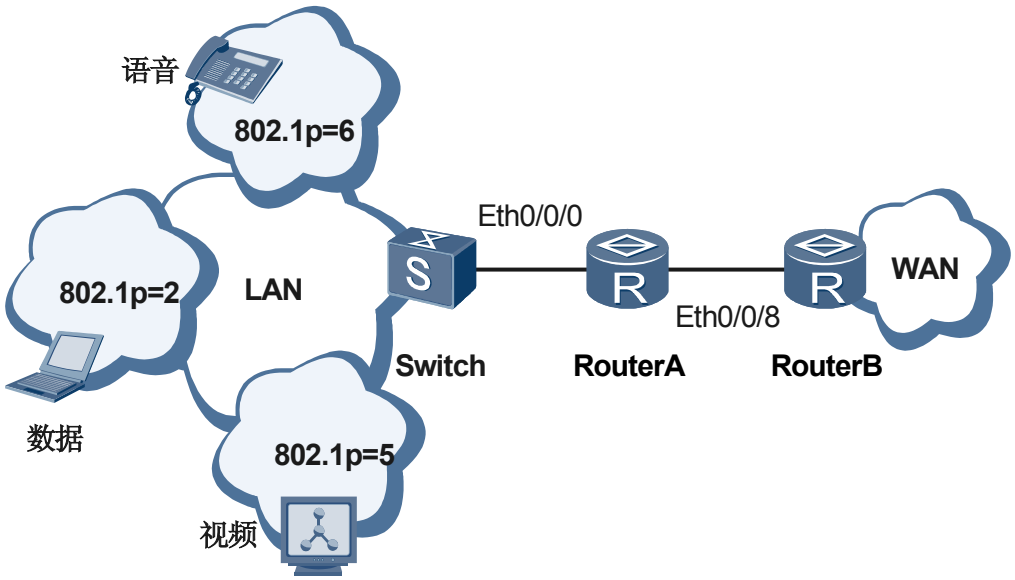
组网需求

如图 1-5 所示，企业网内部 LAN 侧的语音、视频和数据业务通过 Switch 连接到 RouterA 的 Eth0/0/0 上，并通过 RouterA 的 Eth0/0/8 接口连接到 WAN 侧网络。

不同业务的报文在 LAN 侧使用 802.1p 优先级进行标识，在 RouterA 上根据报文的 802.1p 优先级入队列，当报文从 Eth0/0/8 接口到达 WAN 侧时可能会发生带宽抖动。为了减少带宽抖动，同时保证各类业务带宽要求，现要求如下：

- 端口保证带宽为 8000kbit/s。
- 语音保证带宽为 256kbit/s，承诺突发尺寸为 6400byte。
- 视频保证带宽为 4000kbit/s,承诺突发尺寸为 100000byte。
- 数据保证带宽为 2000kbit/s，承诺突发尺寸为 50000byte。

图 1-5 配置流量整形的组网图



配置思路

采用如下的思路配置流量整形：

1. 在 RouterA 上创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 RouterA 访问 WAN 侧网络。
2. 在 RouterA 上配置端口信任的报文优先级为信任报文的 802.1p 优先级。
3. 在 RouterA 上配置基于接口的流量整形，限制端口带宽。

4. 在 RouterA 上配置基于队列的流量整形，限制语音、视频、数据三类业务的带宽。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 与 Switch 相连的接口所属 VLAN 编号为 10，VLANIF 10 的 IP 地址为 192.168.1.1/24，接口信任报文的 802.1p 优先级。
- RouterA 与 WAN 侧相连的接口 IP 地址为 192.168.4.1/24。
- 基于接口的流量整形速率。
- 基于队列的流量整形速率。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 RouterA 上创建 VLAN 10。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan 10
```

配置接口 Eth0/0/0 为 Trunk 类型端口，并将 Eth0/0/0 加入 VLAN10。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] port link-type trunk
[RouterA-Ethernet0/0/0] port trunk allow-pass vlan 10
[RouterA-Ethernet0/0/0] quit
```

说明

请配置 Switch 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN10。

创建 VLANIF 10，并为 VLANIF 10 配置 IP 地址 192.168.1.1/24。

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

配置 Eth0/0/8 的 IP 地址为 192.168.4.1/24。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] ip address 192.168.4.1 24
[RouterA-Ethernet0/0/8] quit
```

说明

根据实际情况配置 RouterB，确保 RouterB 与 RouterA 间路由可达，具体步骤略。

步骤 2 配置端口信任的报文优先级

配置 Eth0/0/0 接口信任报文的 802.1p 优先级。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] trust 8021p
[RouterA-Ethernet0/0/0] quit
```

步骤 3 配置基于接口的流量整形

在 RouterA 上配置基于接口的流量整形，将端口速率限制在 8000kbit/s。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] qos gts cir 8000
[RouterA-Ethernet0/0/8] quit
```

步骤 4 配置基于队列的流量整形

在 RouterA 上创建队列模板 qp1，配置队列 0 ～ 5 的调度方式为 WFQ，队列 6 ～ 7 的调度方式为 PQ；配置队列 6、队列 5 和队列 2 的承诺信息速率分别为 256kbit/s、4000kbit/s、2000kbit/s，承诺突发尺寸分别为 6400byte、100000byte 和 50000byte。

```
[RouterA] qos queue-profile qp1
[RouterA-qos-queue-profile-qp1] schedule pq 6 to 7 wfq 0 to 5
[RouterA-qos-queue-profile-qp1] queue 6 gts cir 256 cbs 6400
[RouterA-qos-queue-profile-qp1] queue 5 gts cir 4000 cbs 100000
[RouterA-qos-queue-profile-qp1] queue 2 gts cir 2000 cbs 50000
[RouterA-qos-queue-profile-qp1] quit
```

在 RouterA 的接口 Eth0/0/8 上应用队列模板 qp1。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] qos queue-profile qp1
```

步骤 5 验证配置结果

查看 RouterA 接口的配置信息。

```
[RouterA-Ethernet0/0/8] display this
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile qp1
 qos gts cir 8000 cbs 200000
#
return
```

查看在接口上应用的队列模板信息。

```
[RouterA-Ethernet0/0/8] quit
[RouterA] display qos queue-profile qp1
Queue-profile: qp1
Queue  Schedule  Weight  Length(Bytes/Packets) GTS(CIR/CBS)
------------------------------------------------------------------
0      WFQ       10                -/-              -/-
1      WFQ       10                -/-              -/-
2      WFQ       10                -/-          2000/50000
3      WFQ       10                -/-              -/-
4      WFQ       10                -/-              -/-
5      WFQ       10                -/-          4000/100000
6      PQ        -                 -/-           256/6400
7      PQ        -                 -/-              -/-
```

----结束

配置文件

- RouterA 的配置文件

```
 sysname RouterA
#
 vlan 10
#
qos queue-profile qp1
  queue 2 gts cir 2000 cbs 50000
  queue 5 gts cir 4000 cbs 100000
  queue 6 gts cir 256 cbs 6400
  schedule wfq 0 to 5 pq 6 to 7
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
```

```
 trust 8021p
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile qp1
 qos gts cir 8000 cbs 200000
#
return
```

1.10.4 配置拥塞管理和拥塞避免综合示例

通过配置拥塞避免和拥塞管理，AR150/200 为不同优先级的报文提供不同的服务，保证用户对于高优先级、低延迟业务的服务要求。

组网需求

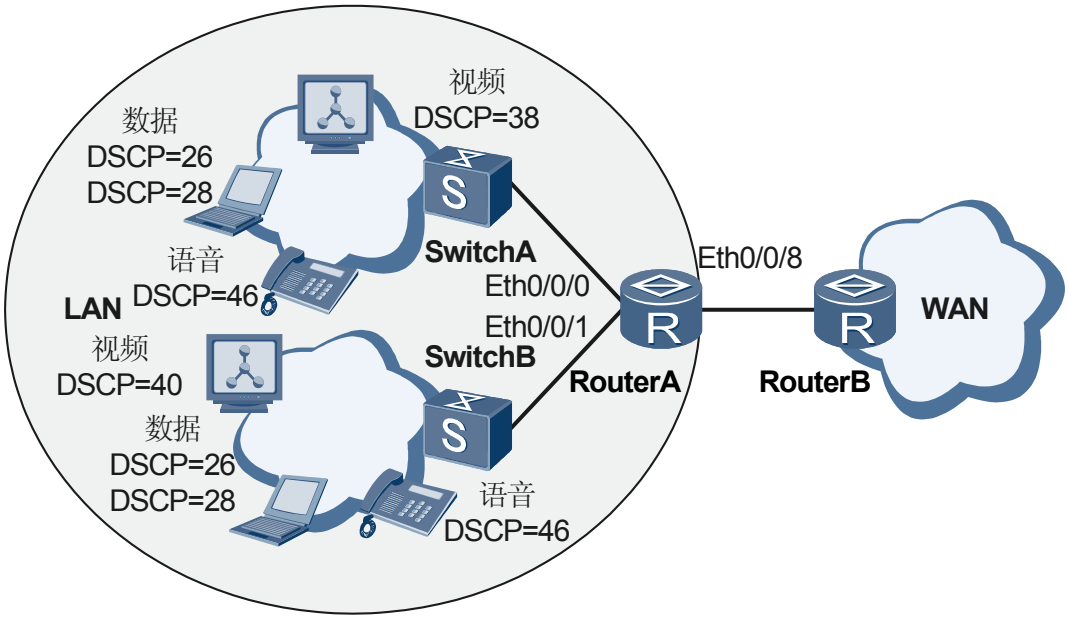
如图 1-6 所示，企业网内部 LAN 侧的语音、视频和数据业务通过 SwitchA 和 SwitchB 连接到 RouterA 的 Eth0/0/0 和 Eth0/0/1 上，并通过 RouterA 的 Eth0/0/8 接口连接到 WAN 侧网络。

各类报文被 SwitchA 和 SwitchB 打上不同的 DSCP 优先级，语音、视频和数据分别为 ef、cs5、af32 和 af31，在 RouterA 上根据报文的 DSCP 优先级入队列，由于 RouterA 的接口 Eth0/0/0 和 Eth0/0/1 的速率大于接口 Eth0/0/8 的速率，在接口 Eth0/0/8 出方向处可能会发生拥塞。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，配置需求如下表所述：

表 1-6 拥塞避免配置参数

业务类型	DSCP 优先级	队列索引	调度方式	丢弃方式
语音	46	5	PQ	尾丢弃
视频	38	4	WFQ	WRED： ● 阈值下限(%)：60 ● 阈值上限(%)：80 ● 丢弃概率(%)：20
数据	28 26	3	WFQ	WRED： ● DSCP=28 – 阈值下限(%)：50 – 阈值上限(%)：70 – 丢弃概率(%)：30 ● DSCP=26 – 阈值下限(%)：40 – 阈值上限(%)：60 – 丢弃概率(%)：40

图 1-6 配置拥塞避免和拥塞管理的组网图



配置思路

采用如下的思路配置：

1. 在 RouterA 创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 RouterA 访问 WAN 侧网络。
2. 在 RouterA 上配置端口信任的报文优先级为信任报文的 DSCP 优先级。
3. 创建丢弃模板，并配置基于 DSCP 优先级的 WRED 参数。
4. 创建队列模板，并配置各队列的调度模式和丢弃方式。
5. 在 RouterA 与 WAN 侧网络连接的接口出方向上应用队列模板，实现拥塞避免和拥塞管理。

数据准备

为完成此配置示例，需准备如下的数据：

- RouterA 与 SwitchA 相连的接口所属 VLAN 编号为 20，VLANIF 20 的 IP 地址为 192.168.2.1/24，接口信任报文的 DSCP 优先级。
- RouterA 与 SwitchB 相连的接口所属 VLAN 编号为 30，VLANIF 30 的 IP 地址为 192.168.3.1/24，接口信任报文的 DSCP 优先级。
- RouterA 与 WAN 侧相连的接口 IP 地址为 192.168.4.1/24。
- WRED 丢弃模板名及 WRED 参数。
- 队列模板名及调度方式。
- 应用队列模板的接口编号。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 RouterA 上创建 VLAN 20、30。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 20 30
```

配置接口 Eth0/0/0 和 Eth0/0/1 信任报文的 DSCP 优先级，均为 Trunk 类型端口，并将 Eth0/0/0 加入 VLAN20，将 Eth0/0/1 加入 VLAN30。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] trust dscp
[RouterA-Ethernet0/0/0] port link-type trunk
[RouterA-Ethernet0/0/0] port trunk allow-pass vlan 20
[RouterA-Ethernet0/0/0] quit
[RouterA] interface ethernet 0/0/1
[RouterA-Ethernet0/0/1] trust dscp
[RouterA-Ethernet0/0/1] port link-type trunk
[RouterA-Ethernet0/0/1] port trunk allow-pass vlan 30
[RouterA-Ethernet0/0/1] quit
```

说明

请配置 SwitchA 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN20。

请配置 SwitchB 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN30。

创建 VLANIF 20、30，并为 VLANIF 20 配置 IP 地址 192.168.2.1/24，为 VLANIF 30 配置 IP 地址 192.168.3.1/24。

```
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 192.168.2.1 24
[RouterA-Vlanif20] quit
[RouterA] interface vlanif 30
[RouterA-Vlanif30] ip address 192.168.3.1 24
[RouterA-Vlanif30] quit
```

配置 Eth0/0/8 的 IP 地址为 192.168.4.1/24。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] ip address 192.168.4.1 24
[RouterA-Ethernet0/0/8] quit
```

说明

根据实际情况配置 RouterB，确保 RouterB 与 RouterA 间路由可达，具体步骤略。

步骤 2 创建丢弃模板

在 RouterA 上创建 WRED 丢弃模板 data 和 video。

```
[RouterA] drop-profile data
[RouterA-drop-profile-data] wred dscp
 Info: Weight type has changed to DSCP.
[RouterA-drop-profile-data] dscp 28 low-limit 50 high-limit 70 discard-percentage 30
[RouterA-drop-profile-data] dscp 26 low-limit 40 high-limit 60 discard-percentage 40
[RouterA-drop-profile-data] quit
[RouterA] drop-profile video
[RouterA-drop-profile-video] wred dscp
 Info: Weight type has changed to DSCP.
[RouterA-drop-profile-video] dscp 38 low-limit 60 high-limit 80 discard-percentage 20
[RouterA-drop-profile-video] quit
```

步骤 3 创建队列模板

在 RouterA 上创建队列模板 queue-profile1，并配置各队列的调度模式和丢弃方式。

```
[RouterA] qos queue-profile queue-profile1
[RouterA-qos-queue-profile-queue-profile1] schedule pq 5 wfq 4 to 3
[RouterA-qos-queue-profile-queue-profile1] queue 4 drop-profile video
[RouterA-qos-queue-profile-queue-profile1] queue 3 drop-profile data
[RouterA-qos-queue-profile-queue-profile1] quit
```

步骤 4 应用队列模板

在 RouterA 的接口 Eth0/0/8 上应用队列模板。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] qos queue-profile queue-profile1
```

步骤 5 验证配置结果

查看 RouterA 接口的配置信息。

```
[RouterA-Ethernet0/0/8] display this
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile queue-profile1
#
return
```

查看在接口上应用的队列模板信息。

```
[RouterA-Ethernet0/0/8] quit
[RouterA] display qos queue-profile queue-profile1
Queue-profile: queue-profile1
Queue  Schedule  Weight  Length(Bytes/Packets) GTS(CIR/CBS)
------------------------------------------------------------------
3      WFQ       10                -/-             -/-
4      WFQ       10                -/-             -/-
5      PQ        -                 -/-             -/-
```

查看队列模板中绑定的丢弃模板。

```
[RouterA] qos queue-profile queue-profile1
[RouterA-qos-queue-profile-queue-profile1] display this
#
qos queue-profile queue-profile1
  queue 3 drop-profile data
  queue 4 drop-profile video
  schedule wfq 3 to 4 pq 5
#
return
```

查看在接口上应用的 WRED 丢弃模板信息。

```
[RouterA-qos-queue-profile-queue-profile1] quit
[RouterA] display drop-profile video
Drop-profile[2]: video
DSCP              Low-limit   High-limit  Discard-percentage
------------------------------------------------------------------
0(default)        30          100         10
1                 30          100         10
2                 30          100         10
3                 30          100         10
4                 30          100         10
5                 30          100         10
6                 30          100         10
7                 30          100         10
8(cs1)            30          100         10
9                 30          100         10
10(af11)          30          100         10
11                30          100         10
12(af12)          30          100         10
13                30          100         10
14(af13)          30          100         10
```

```
15                30            100           10
16(cs2)           30            100           10
17                30            100           10
18(af21)          30            100           10
19                30            100           10
20(af22)          30            100           10
21                30            100           10
22(af23)          30            100           10
23                30            100           10
24(cs3)           30            100           10
25                30            100           10
26(af31)          30            100           10
27                30            100           10
28(af32)          30            100           10
29                30            100           10
30(af33)          30            100           10
31                30            100           10
32(cs4)           30            100           10
33                30            100           10
34(af41)          30            100           10
35                30            100           10
36(af42)          30            100           10
37                30            100           10
38(af43)          60             80           20
39                30            100           10
40(cs5)           30            100           10
41                30            100           10
42                30            100           10
43                30            100           10
44                30            100           10
45                30            100           10
46(ef)            30            100           10
47                30            100           10
48(cs6)           30            100           10
49                30            100           10
50                30            100           10
51                30            100           10
52                30            100           10
53                30            100           10
54                30            100           10
55                30            100           10
56(cs7)           30            100           10
57                30            100           10
58                30            100           10
59                30            100           10
60                30            100           10
61                30            100           10
62                30            100           10
63                30            100           10
-------------------------------------------------------------------
[RouterA] display drop-profile data
Drop-profile[1]: data
DSCP              Low-limit   High-limit  Discard-percentage
-------------------------------------------------------------------
0(default)        30            100           10
1                 30            100           10
2                 30            100           10
3                 30            100           10
4                 30            100           10
5                 30            100           10
6                 30            100           10
7                 30            100           10
8(cs1)            30            100           10
9                 30            100           10
10(af11)          30            100           10
11                30            100           10
12(af12)          30            100           10
13                30            100           10
14(af13)          30            100           10
```

```
15                30          100         10
16(cs2)           30          100         10
17                30          100         10
18(af21)          30          100         10
19                30          100         10
20(af22)          30          100         10
21                30          100         10
22(af23)          30          100         10
23                30          100         10
24(cs3)           30          100         10
25                30          100         10
26(af31)          40          60          40
27                30          100         10
28(af32)          50          70          30
29                30          100         10
30(af33)          30          100         10
31                30          100         10
32(cs4)           30          100         10
33                30          100         10
34(af41)          30          100         10
35                30          100         10
36(af42)          30          100         10
37                30          100         10
38(af43)          60          80          20
39                30          100         10
40(cs5)           30          100         10
41                30          100         10
42                30          100         10
43                30          100         10
44                30          100         10
45                30          100         10
46(ef)            30          100         10
47                30          100         10
48(cs6)           30          100         10
49                30          100         10
50                30          100         10
51                30          100         10
52                30          100         10
53                30          100         10
54                30          100         10
55                30          100         10
56(cs7)           30          100         10
57                30          100         10
58                30          100         10
59                30          100         10
60                30          100         10
61                30          100         10
62                30          100         10
63                30          100         10
-----------------------------------------------------------------
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
 vlan batch 20 30
#
drop-profile data
wred dscp
  dscp af31 low-limit 40 high-limit 60 discard-percentage 40
  dscp af32 low-limit 50 high-limit 70 discard-percentage 30
#
drop-profile video
wred dscp
  dscp af43 low-limit 60 high-limit 80 discard-percentage 20
```

```
#
qos queue-profile queue-profile1
  queue 3 drop-profile data
  queue 4 drop-profile video
  schedule wfq 3 to 4 pq 5
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 trust dscp
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 trust dscp
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile queue-profile1
#
return
```

1.10.5 配置 HQoS 示例

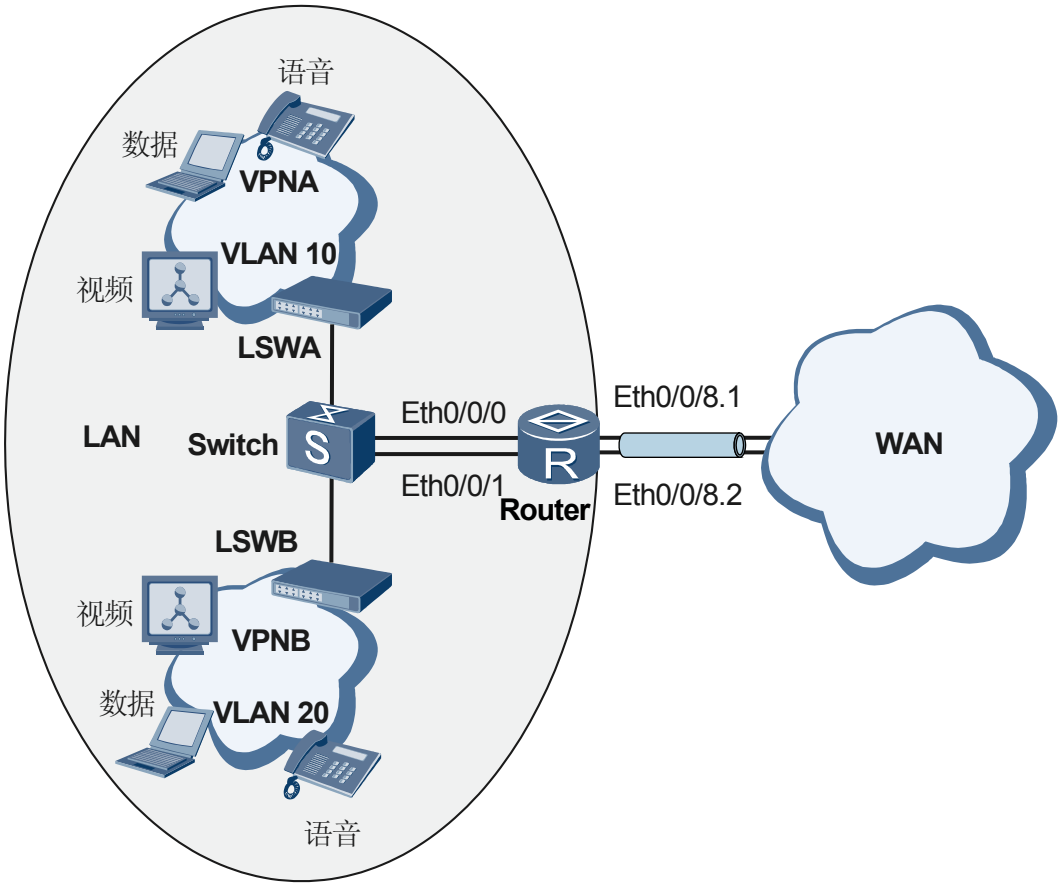
通过配置 HQoS，AR150/200 同时满足对不同优先级的业务报文和不同优先级的用户提供有差别的服务，保证用户对于高优先级、低延迟业务的服务要求。

组网需求

如图 1-7 所示，VPNA 和 VPNB 是两个部门，通过交换机连接到 Router，并通过 Router 的 Eth0/0/8 接口上的两个子接口与总部连接。每个部门有各自的业务流，包括语音、视频和数据。

各类报文被 Switch 打上不同的 DSCP 优先级，语音、视频和数据分别为 ef、af21 和 af11，现要求各部门有各自的保证带宽，并且能共享端口的最大带宽；对于不同的业务流，语音报文要保证优先发送，视频、数据报文要保证带宽。

图 1-7 配置 HQoS 的组网图



配置思路

采用如下的思路配置流量整形：

1. 创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 Router 访问 WAN 侧网络。
2. 在 Router 上配置端口信任的报文优先级为信任报文的 DSCP 优先级。
3. 在 Router 上配置 VPNA 和 VPNB 的子流策略，基于 DSCP 优先级进行流分类，语音报文入 EF 队列，视频和数据报文进入 AF 队列，并绑定丢弃模板。
4. 在 Router 上配置父流策略，基于 VLAN ID 进行流分类，对来自不同 VLAN 的报文进行流量整形， 并为其绑定相应的子流策略。
5. 在 Router 与 WAN 侧网络连接的接口出方向上应用父流策略，实现对不同用户的不同业务流量的区分，提供更为精细化的服务质量。

数据准备

为完成此配置例，需准备如下的数据：

- Router 与 Switch 相连的接口 Eth0/0/0 允许 VLAN 10 的报文通过，VLANIF 10 的 IP 地址为 192.168.1.1/24，接口信任报文的 DSCP 优先级。

- Router 与 Switch 相连的接口 Eth0/0/1 允许 VLAN 20 的报文通过，VLANIF 20 的 IP 地址为 192.168.2.1/24，接口信任报文的 DSCP 优先级。
- Router 与 WAN 侧相连的接口 Eth0/0/8 的 IP 地址为 192.168.3.1/24，其子接口 Eth0/0/8.1 控制 VLAN 为 10，封装方式为 dot1q，IP 地址为 192.168.4.1/24，子接口 Eth0/0/8.2 控制 VLAN 为 20，封装方式为 dot1q，IP 地址为 192.168.5.1/24。
- WRED 丢弃模板名及 WRED 参数：

模板名称	DSCP	丢弃下限	丢弃上限	最大丢弃概率
video	18	80%	95%	60%
data	10	70%	85%	60%

- 子流策略和父流策略的流分类、流行为和流策略名称。
- 不同业务流的队列类型、带宽分配和丢弃方式：
  - 语音：EF 队列，最大允许带宽占接口可用带宽的 5%，使用尾丢弃。
  - 视频：AF 队列，可确保的带宽占接口可用带宽的 60%，使用 WRED 丢弃模板。
  - 数据：AF 队列，可确保的带宽占接口可用带宽的 30%，使用 WRED 丢弃模板。
- 各部门的保证带宽：
  - VPNA:30Mbit/s。
  - VPNB:20Mbit/s。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 Router 上创建 VLAN 10、20。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

配置接口 Eth0/0/0 为 Trunk 类型端口，并将 Eth0/0/0 加入 VLAN10。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port link-type trunk
[Router-Ethernet0/0/0] port trunk allow-pass vlan 10
[Router-Ethernet0/0/0] quit
```

配置接口 Eth0/0/1 为 Trunk 类型端口，并将 Eth0/0/1 加入 VLAN20。

```
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port link-type trunk
[Router-Ethernet0/0/1] port trunk allow-pass vlan 20
[Router-Ethernet0/0/1] quit
```

说明

请配置 Switch 与 Router 对接的接口为 Trunk 类型接口，并分别加入 VLAN10、VLAN20。

创建 VLANIF 10、20，并为 VLANIF 10 配置 IP 地址 192.168.1.1/24，为 VLANIF 20 配置 IP 地址 192.168.2.1/24。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 192.168.1.1 24
[Router-Vlanif10] quit
[Router] interface vlanif 20
```

```
[Router-Vlanif20] ip address 192.168.2.1 24
[Router-Vlanif20] quit
```

配置 Eth0/0/8 的 IP 地址为 192.168.3.1/24。

```
[Router] interface ethernet 0/0/8
[Router-Ethernet0/0/8] ip address 192.168.3.1 24
[Router-Ethernet0/0/8] quit
```

配置 Ethernet0/0/8.1 的控制 VLAN 为 10，封装方式为 dot1q，IP 地址为 192.168.4.1/24，配置 Ethernet0/0/8.2 的控制 VLAN 为 20，封装方式为 dot1q，IP 地址为 192.168.5.1/24。

```
[Router] interface ethernet 0/0/8.1
[Router-Ethernet0/0/8.1] ip address 192.168.4.1 24
[Router-Ethernet0/0/8.1] control-vid 1 dot1q-termination
[Router-Ethernet0/0/8.1] dot1q termination vid 10
[Router-Ethernet0/0/8.1] quit
[Router] interface ethernet 0/0/8.2
[Router-ethernet 0/0/8.2] ip address 192.168.5.1 24
[Router-ethernet 0/0/8.2] control-vid 2 dot1q-termination
[Router-ethernet 0/0/8.2] dot1q termination vid 20
[Router-ethernet 0/0/8.2] quit
```

步骤 2 配置端口信任的报文优先级

配置 Eth0/0/0 和 0/0/1 接口信任报文的 DSCP 优先级。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] trust dscp
[Router-Ethernet0/0/0] quit
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] trust dscp
[Router-Ethernet0/0/1] quit
```

步骤 3 配置 VPNA 和 VPNB 的子流策略

在 Router 上创建流分类 data、video 和 voice，对来自企业的不同业务流按照其 DSCP 优先级进行分类。

```
[Router] traffic classifier data
[Router-classifier-data] if-match dscp af11
[Router-classifier-data] quit
[Router] traffic classifier video
[Router-classifier-video] if-match dscp af21
[Router-classifier-video] quit
[Router] traffic classifier voice
[Router-classifier-voice] if-match dscp ef
[Router-classifier-voice] quit
```

在 Router 上创建 WRED 丢弃模板 data 和 video。

```
[Router] drop-profile data
[Router-drop-profile-data] wred dscp
[Router-drop-profile-data] dscp 10 low-limit 70 high-limit 85 discard-percentage 60
[Router-drop-profile-data] quit
[Router] drop-profile video
[Router-drop-profile-video] wred dscp
[Router-drop-profile-video] dscp 18 low-limit 80 high-limit 95 discard-percentage 60
[Router-drop-profile-video] quit
```

在 Router 上创建流行为 data、video 和 voice，为来自企业的不同业务流配置拥塞管理和拥塞避免。

```
[Router] traffic behavior data
[Router-behavior-data] queue af bandwidth pct 30
[Router-behavior-data] drop-profile data
[Router-behavior-data] quit
```

```
[Router] traffic behavior video
[Router-behavior-video] queue af bandwidth pct 60
[Router-behavior-video] drop-profile video
[Router-behavior-video] quit
[Router] traffic behavior voice
[Router-behavior-voice] queue ef bandwidth pct 5
[Router-behavior-voice] quit
```

在 Router 上定义 VPNA 和 VPNB 的子流策略。

```
[Router] traffic policy vpna-sub
[Router-trafficpolicy-vpna-sub] classifier voice  behavior voice
[Router-trafficpolicy-vpna-sub] classifier video  behavior video
[Router-trafficpolicy-vpna-sub] classifier data  behavior  data
[Router-trafficpolicy-vpna-sub] quit
[Router] traffic policy vpnb-sub
[Router-trafficpolicy-vpnb-sub] classifier voice  behavior voice
[Router-trafficpolicy-vpnb-sub] classifier video  behavior video
[Router-trafficpolicy-vpnb-sub] classifier data  behavior  data
[Router-trafficpolicy-vpnb-sub] quit
```

步骤 4 配置父流策略

在 Router 上创建流分类 vpna 和 vpnb，对来自企业的不同业务流按照其 VLAN ID 进行分类。

```
[Router] traffic classifier vpna
[Router-classifier-vpna] if-match vlan-id 10
[Router-classifier-vpna] quit
[Router] traffic classifier vpnb
[Router-classifier-vpnb] if-match vlan-id 20
[Router-classifier-vpnb] quit
```

在 Router 上创建流行为 vpna 和 vpnb，对来自不同 VLAN 的报文进行流量整形，并为其绑定相应的子流策略。

```
[Router] traffic behavior vpna
[Router-behavior-vpna] gts cir 20000 cbs 500000 queue-length 50
[Router-behavior-vpna] traffic-policy vpna-sub
[Router-behavior-vpna] quit
[Router] traffic behavior vpnb
[Router-behavior-vpnb] gts cir 30000 cbs 750000 queue-length 50
[Router-behavior-vpnb] traffic-policy vpnb-sub
[Router-behavior-vpnb] quit
```

在 Router 上定义父流策略。

```
[Router] traffic policy enterprise
[Router-trafficpolicy-enterprise] classifier vpna behavior vpna
[Router-trafficpolicy-enterprise] classifier vpnb behavior vpnb
[Router-trafficpolicy-enterprise] quit
```

步骤 5 应用父流策略

在 Router 的接口 Eth0/0/8 出方向上应用父流策略。

```
[Router] interface ethernet 0/0/8
[Router-Ethernet0/0/8] traffic-policy enterprise outbound
```

步骤 6 验证配置结果

查看 Router 接口的配置信息。

```
[Router-Ethernet0/0/8] display this
#
interface Ethernet0/0/8
 ip address 192.168.3.1 255.255.255.0
 traffic-policy enterprise outbound
```

```
#
return
```

查看在接口上应用的流策略信息。

```
[Router-Ethernet0/0/8] quit
[Router] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: enterprise
   Classifier: vpna
    Operator: OR
     Behavior: vpna
      General Traffic Shape:
        CIR 20000 (Kbps), CBS 500000 (byte)
        Queue length 50 (Packets)
      Traffic-policy:
        Traffic-policy vpna-sub

   Classifier: vpnb
    Operator: OR
     Behavior: vpnb
      General Traffic Shape:
        CIR 30000 (Kbps), CBS 750000 (byte)
        Queue length 50 (Packets)
      Traffic-policy:
        Traffic-policy vpnb-sub

  Policy: vpna-sub
   Classifier: voice
    Operator: OR
     Behavior: voice
      Expedited Forwarding:
        Bandwidth 5 (%)
        Queue Length: 64 (Packets) 131072 (Bytes)

   Classifier: video
    Operator: OR
     Behavior: video
      Assured Forwarding:
        Bandwidth 60 (%)
        Drop Method: WRED
        Drop-profile: video

   Classifier: data
    Operator: OR
     Behavior: data
      Assured Forwarding:
        Bandwidth 30 (%)
        Drop Method: WRED
        Drop-profile: data

  Policy: vpnb-sub
   Classifier: voice
    Operator: OR
     Behavior: voice
      Expedited Forwarding:
        Bandwidth 5 (%)
        Queue Length: 64 (Packets) 131072 (Bytes)

   Classifier: video
    Operator: OR
     Behavior: video
      Assured Forwarding:
        Bandwidth 60 (%)
        Drop Method: WRED
        Drop-profile: video

   Classifier: data
    Operator: OR
     Behavior: data
```

```
    Assured Forwarding:
      Bandwidth 30 (%)
      Drop Method: WRED
      Drop-profile: data
```

查看在接口上应用的 WRED 丢弃模板信息。

```
[Router] display drop-profile video
Drop-profile[1]: video
DSCP              Low-limit   High-limit  Discard-percentage
------------------------------------------------------------------
0(default)        30          100         10
1                 30          100         10
2                 30          100         10
3                 30          100         10
4                 30          100         10
5                 30          100         10
6                 30          100         10
7                 30          100         10
8(cs1)            30          100         10
9                 30          100         10
10(af11)          30          100         10
11                30          100         10
12(af12)          30          100         10
13                30          100         10
14(af13)          30          100         10
15                30          100         10
16(cs2)           30          100         10
17                30          100         10
18(af21)          80           95         60
19                30          100         10
20(af22)          30          100         10
21                30          100         10
22(af23)          30          100         10
23                30          100         10
24(cs3)           30          100         10
25                30          100         10
26(af31)          30          100         10
27                30          100         10
28(af32)          30          100         10
29                30          100         10
30(af33)          30          100         10
31                30          100         10
32(cs4)           30          100         10
33                30          100         10
34(af41)          30          100         10
35                30          100         10
36(af42)          30          100         10
37                30          100         10
38(af43)          30          100         10
39                30          100         10
40(cs5)           30          100         10
41                30          100         10
42                30          100         10
43                30          100         10
44                30          100         10
45                30          100         10
46(ef)            30          100         10
47                30          100         10
48(cs6)           30          100         10
49                30          100         10
50                30          100         10
51                30          100         10
52                30          100         10
53                30          100         10
54                30          100         10
55                30          100         10
56(cs7)           30          100         10
57                30          100         10
```

```
58                  30          100         10
59                  30          100         10
60                  30          100         10
61                  30          100         10
62                  30          100         10
63                  30          100         10
-----------------------------------------------------------------
[Router] display drop-profile data
Drop-profile[2]: data
DSCP                Low-limit   High-limit  Discard-percentage
-----------------------------------------------------------------
0(default)          30          100         10
1                   30          100         10
2                   30          100         10
3                   30          100         10
4                   30          100         10
5                   30          100         10
6                   30          100         10
7                   30          100         10
8(cs1)              30          100         10
9                   30          100         10
10(af11)            70           85         60
11                  30          100         10
12(af12)            30          100         10
13                  30          100         10
14(af13)            30          100         10
15                  30          100         10
16(cs2)             30          100         10
17                  30          100         10
18(af21)            30          100         10
19                  30          100         10
20(af22)            30          100         10
21                  30          100         10
22(af23)            30          100         10
23                  30          100         10
24(cs3)             30          100         10
25                  30          100         10
26(af31)            30          100         10
27                  30          100         10
28(af32)            30          100         10
29                  30          100         10
30(af33)            30          100         10
31                  30          100         10
32(cs4)             30          100         10
33                  30          100         10
34(af41)            30          100         10
35                  30          100         10
36(af42)            30          100         10
37                  30          100         10
38(af43)            30          100         10
39                  30          100         10
40(cs5)             30          100         10
41                  30          100         10
42                  30          100         10
43                  30          100         10
44                  30          100         10
45                  30          100         10
46(ef)              30          100         10
47                  30          100         10
48(cs6)             30          100         10
49                  30          100         10
50                  30          100         10
51                  30          100         10
52                  30          100         10
53                  30          100         10
54                  30          100         10
55                  30          100         10
56(cs7)             30          100         10
57                  30          100         10
```

```
58                  30          100         10
59                  30          100         10
60                  30          100         10
61                  30          100         10
62                  30          100         10
63                  30          100         10
------------------------------------------------------------
```

----结束

配置文件

- Router 的配置文件

```
 sysname Router
#
 vlan batch 10 20
#
drop-profile data
wred dscp
   dscp af11 low-limit 70 high-limit 85 discard-percentage 60
#
drop-profile video
wred dscp
  dscp af21 low-limit 80 high-limit 95 discard-percentage 60
#
traffic classifier vpna operator or
 if-match vlan-id 10
traffic classifier video operator or
 if-match dscp af21
traffic classifier vpnb operator or
 if-match vlan-id 20
traffic classifier data operator or
 if-match dscp af11
traffic classifier voice operator or
 if-match dscp ef
#
traffic behavior vpna
 gts cir 20000 cbs 500000 queue-length 50
 traffic-policy vpna-sub
traffic behavior video
 queue af bandwidth pct 60
 drop-profile video
traffic behavior vpnb
 gts cir 30000 cbs 750000 queue-length 50
 traffic-policy vpnb-sub
traffic behavior data
 queue af bandwidth pct 30
 drop-profile data
traffic behavior voice
 queue ef bandwidth pct 5
#
traffic policy enterprise
 classifier vpna behavior vpna
 classifier vpnb behavior vpnb
traffic policy vpna-sub
 classifier voice behavior voice
 classifier video behavior video
 classifier data behavior data
traffic policy vpnb-sub
 classifier voice behavior voice
 classifier video behavior video
 classifier data behavior data
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
```

```
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
 trust dscp
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
 trust dscp
#
interface Ethernet0/0/8
 ip address 192.168.3.1 255.255.255.0
 traffic-policy enterprise outbound
#
interface Ethernet0/0/8.1
 control-vid 1 dot1q-termination
 dot1q termination vid 10
 ip address 192.168.4.1 255.255.255.0
#
interface Ethernet0/0/8.2
 control-vid 2 dot1q-termination
 dot1q termination vid 20
 ip address 192.168.5.1 255.255.255.0
#
return
```

2 流策略配置

关于本章

流策略配置介绍了流分类、流行为、流策略的配置方法和配置示例。

2.1 流策略概述
流策略即将用户流量分类，并对每个分类指定一个流行为。AR150/200 中流策略提供了模块化的配置思路，流分类和流行为都通过模板来定义，简化了配置逻辑。

2.2 AR150/200 支持的流策略特性
AR150/200 中的流策略支持多种条件的流分类以及多种动作的流行为。

2.3 配置流分类
流分类是配置流策略的前提条件，需要先区分出用户流量再继续后续的配置。

2.4 配置流行为
配置流行为即为符合流分类规则的流量指定后续动作，是配置流策略的前提条件。在AR150/200 中针对流分类可实施的流行为包括禁止/允许、重标记、重定向、流量监管、流量整形、流量统计、队列调度。

2.5 配置流策略
配置完流分类和流行为后需要将流分类与流行为绑定，并应用在接口上。

2.6 维护流策略
如果已经使能了流量统计功能，可以查看和清除基于流的流量统计信息。

2.7 配置举例
通过示例介绍如何应用流策略。配置示例中包括组网需求、配置注意事项、配置思路等。

2.1 流策略概述

流策略即将用户流量分类，并对每个分类指定一个流行为。AR150/200 中流策略提供了模块化的配置思路，流分类和流行为都通过模板来定义，简化了配置逻辑。

流策略提供了一组模板化的命令行配置方式，目的是将基于 ACL 的 QoS 配置和命令整合在一起，包含三个要素：

- 流分类器（traffic classifier）
- 流行为（traffic behavior）
- 流策略（traffic policy）

流分类器

流分类器用来定义一组流量匹配规则，来对报文进行分类。

分类器中规则之间的关系分为：and 或者 or，默认关系为 or。

- and：报文只有匹配了所有的规则，设备才认为报文属于这个类。
- or：报文只要匹配了类中的一个规则，设备就认为报文属于这个类。

流行为

流行为用来定义针对报文所做的 QoS 动作。进行复杂流分类是为了有区别地提供服务，它必须与某种流量控制或资源分配行为关联起来才有意义。

流策略

流策略是将分类器和流行为关联后形成的完整的 QoS 策略。

2.2 AR150/200 支持的流策略特性

AR150/200 中的流策略支持多种条件的流分类以及多种动作的流行为。

流分类

- 传统流分类

  传统流分类器与 ACL 都有分类匹配的功能，但是却又不同于 ACL。二者之间的最主要区别在于流分类器只有分类匹配一个作用，而没有表明对符合分类的流做出什么动作，而 ACL 本身是为了进行访问控制，所以附带有 deny 和 permit 的动作。而且二者所匹配的范围不同，流分类器所能匹配的流范围大于 ACL，可以说 ACL 中的匹配范围是流分类器中的一个子集。比如流分类器可以匹配入接口，ACL 则不支持。

  分类规则见**表 2-1**：

表 2-1 复杂流分类的分类规则

层级	分类规则
二层	● VLAN 报文外层 Tag 的 ID 信息 ● VLAN 报文内层 Tag 的 ID 信息 ● VLAN 报文外层 Tag 的 802.1p 优先级 ● VLAN 报文内层 Tag 的 802.1p 优先级 ● 源 MAC 地址 ● 目的 MAC 地址 ● 基于二层封装的协议字段 ● FR DE ● FR DLCI ● ATM PVC ● ACL 4000 ～ 4999
三层	● IP 报文的 DSCP 优先级 ● IP 报文的 IP 优先级 ● IP 协议类型（即 IPv4 协议） ● ACL 2000 ～ 3999
四层	● RTP 端口号 ● TCP 报文的 TCP SYN 标志
其他	● 入接口

- 基于 SAC 的流分类器

  智能应用控制 SAC（Smart Application Control）是一个智能的应用识别与分类引擎，利用 DPI（Deep Packet Inspection）深度报文检测技术，对报文中的第 4 ～ 7 层内容和一些动态协议(如 HTTP、FTP、RTP)进行检测和识别，根据分类结果实施精细化 QoS 策略控制。SAC 特征库包含 SAC 能识别的全部应用协议。

  说明

  SAC 功能使用 License 授权，缺省情况下，设备的 SAC 功能受限无法使用。如果需要使用 SAC 功能，请联系华为办事处申请并购买如下 License，

  - AR150&200 安全业务增值包

流行为

在 AR150/200 中可实施的流行为包括禁止/允许、重标记、重定向、流量监管、流量整形、流镜像、流量统计、队列调度：

- 禁止/允许

  禁止/允许是最简单的流控动作。AR150/200 通过对报文的通过或丢弃处理，来达到控制网络流量的目的。

- 重标记

重标记是对报文的优先级字段进行设置。在不同的网络中报文使用不同的优先级字段，例如 VLAN 网络使用 802.1p，IP 网络使用 ToS。因此需要 AR150/200 可以针对不同的网络对报文的优先级进行重标记。

通常网络的边界节点设备需要对进入的报文进行优先级重标记。网络内部的节点设备按照边界节点所标记的优先级提供相应等级的 QoS 服务，或者按自己的标准重新进行标记。

- 重定向

  重定向是指将不按报文原始的目的地址进行路由转发，而是将报文重定向到指定的下一跳地址。

  通过重定向可以实现策略路由。这种策略路由是静态的，当配置中的下一跳不可用时，系统将按原来的转发路径转发报文。

- 流量监管

  流量监管就是一种通过对流量规格的监督，来限制流量及其资源使用的流控动作。通过流量监管，可以控制某个流的规格，对于超过规格的流量，可以采取丢弃、重标记颜色、重标记优先级或其他的 QoS 措施。

- 流量整形

  流量整形也是通过对流量规格的监督，来限制流量及其资源使用的流控动作。它是一种主动调整流的输出速率的流控措施，通常是为了使流量适配下游设备可供给的网络资源，避免不必要的报文丢弃和拥塞。流量整形通过限制流出某一网络的某一连接的流量，使这类报文以比较均匀的速度向外发送。

- 流镜像

  流镜像，即将指定的数据报文复制到用户指定的目的地，以进行网络检测和故障排除。请参见《*Huawei AR150&200 系列 企业路由器 配置指南-设备管理*》中“配置流镜像”部分。

- 流量统计

  流量统计用于统计指定业务流的数据报文，它统计的是设备中转发的数据报文中匹配已定义的复杂流分类规则的数据信息。

  流量统计本身不是 QoS 控制措施，但可以和其他 QoS 动作组合使用，以提高网络和报文的安全性。

- 队列调度

  包括 EF、AF、WFQ 队列调度模式，流量整形（TS），WRED 等与队列相关机制的配置。请参见 **AR150/200 支持的 QoS 特性**中拥塞管理中的“CBQ”。

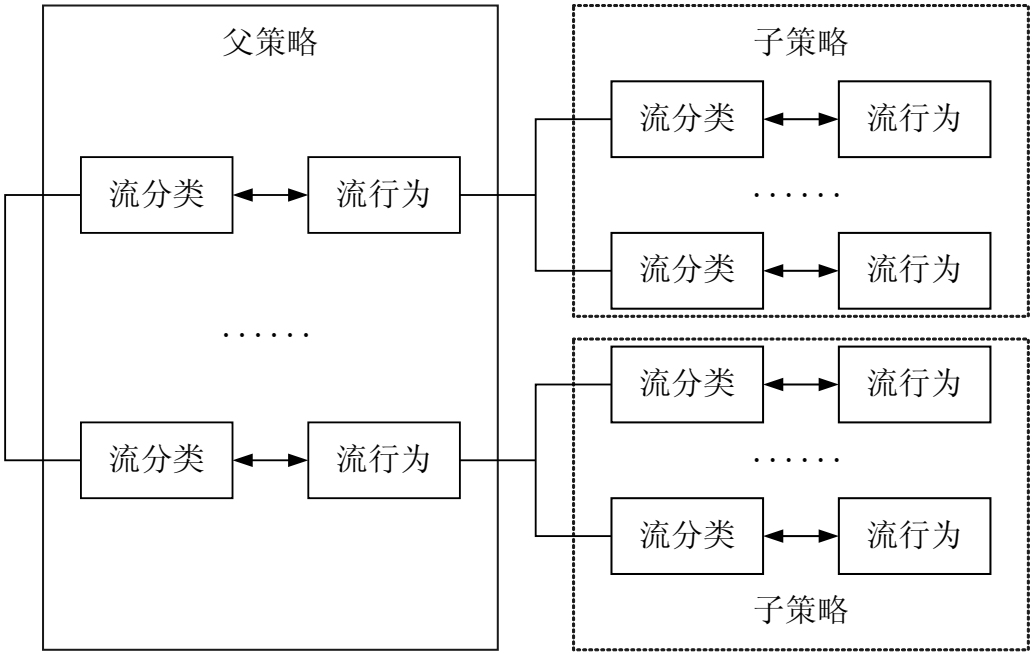
流策略

用户可以通过流策略将指定的流分类和流行为绑定起来，然后在接口上应用流策略，从而实现 QoS 功能。AR150/200 支持在 LAN 接口、WAN 接口或 WAN 子接口应用流策略。

流策略嵌套

流策略嵌套是指一个 QoS 策略中包含另一个 QoS 策略，如**图 2-1** 所示，即父策略的行为（动作）是一个子策略。使用流策略嵌套时，对于命中流分类的某一类报文，除了执行父策略中定义的行为外，还由子策略再对该类流量进行分类，执行子策略中定义的行为。

图 2-1 流策略嵌套示意图



AR150/200 支持两层策略嵌套，子策略下面不能再有嵌套。

嵌套策略提供了 HQoS 的层次化配置模型，只能应用在 WAN 接口的出方向。

2.3 配置流分类

流分类是配置流策略的前提条件，需要先区分出用户流量再继续后续的配置。

2.3.1 建立配置任务

在配置流分类前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

对于进入设备的各种流量，可以对其进行分类以提供差别服务。AR150/200 支持以下流分类：

- 传统流分类

  对于进入设备的各种流量，可以根据报文的 VLAN ID、802.1p 值、源 MAC、目的 MAC、二层封装的协议字段、FR DE、FR DLCI、ATM PVC、ACL 4000 ～ 4999 等二层信息，报文的 DSCP 优先级、IP 优先级、协议类型、ACL 2000 ～ 3999 等三层信息，报文的 RTP 端口号、TCP 报文的 TCP SYN 标志等四层信息以及报文的入接口等参数进行分类。

- 基于 SAC(Smart Application Control)的流分类

使用 DPI(Deep Packet Inspection)深度报文检测技术，对报文中第 4 ～ 7 层的内容和一些动态协议(如 HTTP、FTP、RTP)进行检测和识别，通过对报文进行深度的识别和分类，识别网络中运行的协议和应用。

流分类必须与流行为绑定，才能形成完整的流策略，单独配置流分类是没有意义的。

前置任务

在配置流分类之前，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
- 配置相关接口的 IP 地址和路由协议，保证路由互通
- 如果使用 ACL 作为流分类规则，配置相应的 ACL
- SAC 特征库文件已经上传到设备，保存在设备的存储介质中

数据准备

在配置流分类之前，需要准备以下数据：

序号	数据
1	流分类名称及相关的参数
2	SAC 特征库文件的名称和存储路径

2.3.2 （可选）配置 SAC 功能

SAC 可以对企业的网络流量进行更细粒度调控，避免网络带宽被非关键业务占用，保障关键业务带宽。

2.3.2.1 配置 SAC 特征库

要使用 SAC 功能，必须进行 SAC 使能和加载 SAC 特征库。特征库包含有 SAC 所支持的全部应用协议。

前提条件

SAC 特征库文件已经上传到设备，保存在设备的存储介质中。

背景信息

执行 **sac enable signature** 后需要间隔 20 秒才能执行 **sac update signature** 或 **undo sac enable**。

执行 **sac update signature** 后需要间隔 20 秒才能执行 **undo sac enable** 或再次执行 **sac update signature**。

执行 **undo sac enable** 后需要间隔 20 秒才能执行 **sac enable signature**。

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 **sac enable signature** *signature-name*，使能 SAC 功能，并加载特征库文件。

缺省情况下，不使能 SAC 功能。

说明

指定特征库名称时，若未指定完整的路径时，默认为当前路径。即使特征库加载成功，但是在恢复配置时可能会出错，因此要求用户输入完整的路径和名称。

步骤 3 （可选）执行命令 **sac update signature** *signature-name*，更新特征库文件。

----结束

2.3.2.2 配置 SAC 协议组

为方便用户使用应用协议进行分类管理，AR150/200 提供 SAC 协议组配置。

前提条件

SAC 特征库已经加载。

背景信息

AR150/200 最多可以配置的 SAC 协议组个数为 32 个，一个 SAC 协议组中最多可以包含 32 个应用协议。

缺省情况下，系统未创建任何 SAC 协议组。

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 **sac protocol-group** *protocol-group*，创建一个 SAC 协议组，进入 SAC 协议组视图。

步骤 3 执行命令 **app-protocol** *protocol-name*，将指定应用协议加入当前 SAC 协议组。

----结束

2.3.2.3 配置基于 SAC 的流量统计

在指定接口或子接口下配置基于 SAC 的流量统计，可以自动发现 DPI 引擎可以识别的流量，进行统计分析。

前提条件

SAC 特性库已经加载。

背景信息

AR150/200 对经过的流量进行识别、分类、统计，把流量统计数据上报给网管系统，网管记录上报的数据，可以分析业务应用及带宽分布情况，形成统计报表，网络管理员可以根据统计流量分析，做出相应的业务决策，保障关键业务带宽，限制垃圾流量。

接口上基于不同 SAC 应用协议的报文统计信息的数据是累积的，如果需要重新开始统计，可将原有统计信息清除，重新开始统计。

缺省情况下，不使能接口的 SAC 的统计功能。

操作步骤

- 使能接口的 SAC 的统计功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。
  3. 执行命令 **sac protocol-statistic enable**，使能接口的 SAC 的统计功能。
- 清除接口的 SAC 的统计信息
  1. 在接口视图下执行命令 **reset sac protocol-statistic** { **protocol** *protocol-name* | **all** } **interface** *interface-type interface-number* 或 **reset sac protocol-statistic** { **protocol** *protocol-name* | **all** } **interface virtual-template** *vt-number* **virtual-access** *va-number*，清除指定接口上基于不同 SAC 应用协议的报文统计信息。

----结束

2.3.2.4 检查配置结果

配置 SAC 功能后，可查看 SAC 相关的配置信息和统计信息。

前提条件

已经完成 SAC 功能配置。

操作步骤

- 执行命令 **display sac information**，查看当前设备的 SAC 相关配置信息。
- 执行命令 **display sac protocol-group** [*protocol-group*]，查看设备上配置的 SAC 协议组。
- 执行命令 **display sac protocol-list**，查看当前设备支持的 SAC 协议列表。
- 执行命令 **display sac protocol-statistic** { **protocol** *protocol-name* | **top-n** *number* | **all** } **interface** *interface-type interface-number* [**inbound** | **outbound**]或 **display sac protocol-statistic** { **protocol** *protocol-name* | **top-n** *number* | **all** } **interface virtual-template** *vt-number* **virtual-access** *va-number* [**inbound** | **outbound**]，查看接口上基于不同 SAC 应用协议的报文统计信息。

----结束

2.3.3 定义流分类

定义流分类，可以将符合一定规则的报文作为一类，对匹配同一流分类的报文进行相同的处理。

前提条件

如果要定义基于应用协议的匹配规则，必须使能 SAC 功能并加载特征库。

如果要定义基于 SAC 协议组的匹配规则，必须使能 SAC 功能、加载特征库且配置了 SAC 协议组。

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 **traffic classifier** *classifier-name* [**operator** { **and** | **or** }]，创建一个流分类，进入流分类视图。

- **and** 表示流分类中各规则之间关系为“逻辑与”，即报文必须匹配流分类中所有的非 ACL 规则以及其中一条 ACL 规则才能命中。
- **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规则即可命中。

缺省情况下，流分类中各规则之间的关系为“逻辑或”。

步骤 3 定义流分类中的匹配规则。能定义的匹配规则如下：

- 定义基于 VLAN 报文 802.1p 优先级的匹配规则，执行命令 **if-match 8021p** *8021p-value* &<1-8>。
- 定义基于 QinQ 报文内层 802.1p 优先级的匹配规则，执行命令 **if-match cvlan-8021p** *8021p-value* &<1-8>。
- 定义基于 ACL 的匹配规则，执行命令 **if-match acl** { *acl-number* | *acl-name* }。

  说明

  使用 ACL 作为流分类规则，必须先配置相应的 ACL 规则，AR150/200 支持:

  - 基本 ACL，具体配置请参见配置基本 ACL。
  - 高级 ACL，具体配置请参见配置高级 ACL。
  - 二层 ACL，具体配置请参见配置二层 ACL。
- 定义基于所有报文的匹配规则，执行命令 **if-match any**。

  说明

  流分类中同时配置 **if-match any** 和其他规则时，报文流只匹配 **if-match any** 规则，而忽略其他规则。
- 定义基于目的 MAC 地址匹配规则，执行命令 **if-match destination-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]。
- 定义基于源 MAC 地址的匹配规则，执行命令 **if-match source-mac** *mac-address* [**mac-address-mask** *mac-address-mask*]。
- 定义基于 FR 报文中的 DLCI 信息的匹配规则，执行命令 **if-match dlci** *start-dlci-number* [**to** *end-dlci-number*]。
- 定义基于 FR 报文中的 DE 标志位的匹配规则，执行命令 **if-match fr-de**。
- 定义基于 IP 报文 DSCP 优先级的匹配规则，执行命令 **if-match dscp** *dscp-value* &<1-8>。
- 定义基于 IP 报文 IP 优先级的匹配规则，执行命令 **if-match ip-precedence** *ip-precedence-value* &<1-8>。

  说明

  不能在一个逻辑关系为“与”的流分类中同时配置 **if-match dscp** 和 **if-match ip-precedence**。
- 定义基于入接口的匹配规则，执行命令 **if-match inbound-interface** *interface-type interface-number*
- 定义基于以太网帧头中协议类型字段的匹配规则，执行命令 **if-match l2-protocol** { **arp** | **ip** | **rarp** | *protocol-value* }。
- 定义基于报文三层协议类型的匹配规则，执行命令 **if-match protocol ip**。

- 定义基于 ATM 报文中的 PVC 信息的匹配规则，执行命令 **if-match pvc** *vpi-number*/*vci-number*。
- 定义基于 RTP 端口号的匹配规则，执行命令 **if-match rtp start-port** *start-port-number* **end-port** *end-port-number*。
- 定义基于 TCP 报文 SYN Flag 的匹配规则，执行命令 **if-match tcp syn-flag** *syn-flag* &<1-6>。
- 定义基于 VLAN ID 匹配规则，执行命令 **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]。
- 定义基于 QinQ 报文内层 VLAN ID 的匹配规则，执行命令 **if-match cvlan-id** *start-cvlan-id* [**to** *end-cvlan-id*]。
- 定义基于应用协议的匹配规则，执行命令 **if-match app-protocol** *protocol-name* [**time-range** *time-name*]。

  说明

  当流分类中包含 **if-match app-protocol** 时，流分类各规则之间的关系必须是 **or**。
- 定义基于 SAC 协议组的匹配规则，执行命令 **if-match protocol-group** *protocol-group* [**time-range** *time-name*]。

  说明

  当流分类中包含 **if-match protocol-group** 时，流分类各规则之间的关系必须是 **or**。

----结束

2.3.4 检查配置结果

配置流分类后，可查看流分类信息。

前提条件

已经完成流分类的配置。

操作步骤

步骤 1 执行命令 **display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*]，查看流分类的配置信息。

----结束

2.4 配置流行为

配置流行为即为符合流分类规则的流量指定后续动作，是配置流策略的前提条件。在 AR150/200 中针对流分类可实施的流行为包括禁止/允许、重标记、重定向、流量监管、流量整形、流量统计、队列调度。

2.4.1 建立配置任务

在配置流行为前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

流行为用来定义针对报文所做的 QoS 动作。进行复杂流分类是为了有区别地提供服务，它必须与某种流量控制或资源分配行为关联起来才有意义。

流分类必须与流行为绑定，才能形成完整的流策略，单独配置流行为是没有意义的。

包含不同流行为的流策略在 AR150/200 可以应用的接口和方向有所不同，具体情况如表 2-2：

表 2-2 包含各流行为的流策略的应用限制

流策略包含的流行为	应用限制
禁止/允许 重标记 流量监管 流量统计	无应用限制
重定向	LAN/WAN 接口入方向
流量整形 拥塞管理 拥塞避免 绑定子策略	WAN 接口出方向

前置任务

在配置流行为之前，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
- 配置相关接口的 IP 地址和路由协议，保证路由互通

数据准备

在配置流行为之前，需要准备以下数据：

序号	数据
1	流行为名称及相关的参数

2.4.2 配置禁止或允许动作

AR150/200 的访问控制功能由流策略实现，可以通过允许/禁止的策略来实现防火墙过滤。

背景信息

通过配置禁止或允许动作，AR150/200 将禁止或允许符合流分类规则的报文通过，从而控制网络流量。

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 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 请根据实际需要进行如下配置：

- 执行命令 **permit**，配置允许动作。
- 执行命令 **deny**，配置禁止动作。

说明

- 如果配置了 **deny** 动作，则符合流分类规则的报文都会丢弃，流动作 **deny** 和其他流动作互斥，所以不能再配置其它动作（流量统计除外）。
- 如果配置了 **permit** 动作，则对符合流分类规则的报文采取的动作进行逐条匹配。

----结束

2.4.3 配置重定向

通过配置重定向，将符合流分类规则的报文重定向到指定的下一跳地址。

背景信息

通过在流行为中配置重定向，可以实现策略路由功能。

包含重定向动作的流策略只能在接口的入方向上应用。

如果设备上没有指定的下一跳 IP 地址对应的 ARP 表项，设备会触发 ARP 学习，如果一直学习不到 ARP，则报文按原始路径转发，如果设备上有或学习到了此 ARP 表项，则按照指定的 IP 进行报文转发。

NQA（Network Quality Analysis）是网络故障诊断和定位的有效工具，配置 NQA 与重定向联动功能，可以在网络链路出现故障时，实现路由快速切换，保障用户数据流量正常转发：

- 当 NQA 检测到与目的 IP 可达时，按照指定的 IP 进行报文转发，即重定向生效。
- 当 NQA 检测到与目的 IP 不可达时，系统将按原来的转发路径转发报文，即重定向不生效。

说明

NQA 测试例必须为 ICMP 类型，具体配置请参见《*Huawei AR150&200 系列 企业路由器 配置指南-网络管理*》中“NQA 配置”部分的配置 ICMP 测试、配置测试例的通用参数。

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 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **redirect ip-nexthop** *ip-address* [**track nqa** *admin-name test-name*]，将符合流分类的报文重定向到下一跳，并配置重定向与 NQA 测试例联动。

----结束

2.4.4 配置重标记

通过配置重标记，AR150/200 对符合流分类规则的报文的指定字段进行设置，如 VLAN 报文的 802.1p 优先级、IP 报文的 DSCP、FR 报文的 DE 标志位和内部优先级。

背景信息

重标记报文某些字段，将不会影响当前设备对报文的 QoS 处理，仅会影响下游设备对报文的 QoS 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 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 请根据实际需要进行如下配置：

- 执行命令 **remark 8021p** *8021p-value*，将符合流分类的报文重新标记 802.1p 优先级。
- 执行命令 **remark cvlan-8021p** *8021p-value*，将符合流分类的 QinQ 报文重新标记内层 802.1p 优先级的值。
- 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 fr-de** *fr-de-value*，将符合流分类的 FR 报文重新标记 DE 标志位。
- 执行命令 **remark local-precedence** *local-precedence-value*，将符合流分类的重新标记本地优先级。

  说明

  如果在流行为中配置了 **remark 8021p**、**remark dscp**、**remark mpls-exp**，未配置 **remark local-precedence**，则报文中的本地优先级会被标记为 0。

----结束

2.4.5 配置流量监管

流量监管就是一种通过对流量规格的监督，来限制流量及其资源使用的流量控制动作。

背景信息

通过配置流量监管，AR150/200 对符合流分类规则的报文的流量进行监督，对于超过规格的流量，可以采取丢弃、重标记颜色、重标记服务级别。

说明

当承诺突发尺寸 *cbs-value* 值小于当前部署业务中单个报文的字节数时，将导致这些报文被直接丢弃。

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 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **car cir** { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**green** { **discard** | **pass** [**remark-8021p** *8021p-*

precedence | **remark-dscp** *dscp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-precedence* | **remark-dscp** *dscp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-precedence* | **remark-dscp** *dscp-value*] }]，配置流量监管动作。

配置 **share** 参数即对流做共享 CAR，使绑定了同一流行为的流分类中的所有的规则共享 CAR 参数，系统将这些流聚合在一起做 CAR。

----结束

2.4.6 配置流量整形

流量整形也是通过对流量规格的监督，来限制流量及其资源使用的流量控制动作。

背景信息

流量整形是一种主动调整流的输出速率的流量控制措施，通常是为了使流量适配下游设备可供给的网络资源，避免不必要的报文丢弃和拥塞。流量整形通过限制流出某一网络的某一连接的流量，使这类报文以比较均匀的速度向外发送。

说明

包含此流行为的流策略只能应用在 AR150/200 WAN 接口出方向上。

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 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **gts cir** *cir-value* [**cbs** *cbs-value* [**queue-length** *queue-length*]]，配置流量整形动作。

----结束

2.4.7 配置拥塞管理

AR150/200 为命中流分类规则的数据报文提供了 3 类队列：AF、EF、BE。

背景信息

AR150/200 为命中流分类规则的数据报文提供了 3 类队列：

- 确保转发队列（AF）：可以保证在网络发送的业务流量没有超过最小可确保带宽的情况下，此队列中报文的丢失概率非常低。确保转发适用于流量较大，且需要被保证的业务。
- 加速转发队列（EF）：匹配规则的报文进入 EF 队列后，进行绝对优先级调度，仅当 EF 队列中的报文调度完毕后，才会调度其他队列中的报文。 加速转发适用于需要保证低延时、低丢弃概率、确保带宽、且占用带宽不是很大的业务，例如语音报文。
- 尽力而为队列（BE）：与系统定义的缺省类 **default-class** 关联使用，未进入 AF 队列和 EF 队列的剩余报文进入 BE 队列。BE 队列使用 WFQ 算法调度，队列数越多，带宽被分享的越公平，但是占用的队列资源相对也多。WFQ 调度的 BE 队列适用于那些对时延和丢包无特殊要求的业务，例如普通上网业务。

说明

包含此流行为的流策略只能应用在 AR150/200 WAN 接口出方向上。

虽然允许为缺省类 **default-class** 配置 AF 队列，并配置带宽，但是更多的情况是为缺省类配置 BE 队列。

- 当缺省类 **default-class** 与 AF 队列关联使用时:
  - AF 队列和 EF 队列带宽之和不得超过接口带宽的 100%；
  - 各 AF 队列按照权重分享剩余带宽（可用带宽减去 EF 队列占用带宽后的剩余资源）。
- 当缺省类 **default-class** 与 BE 队列关联使用时:
  - 系统默认为 BE 队列分配的带宽为接口可用带宽的 10%；
  - AF 队列和 EF 队列带宽之和不得超过接口带宽的 99%；
  - 各 AF 队列和 BE 队列按照权重分享剩余带宽（可用带宽减去 EF 队列占用带宽后的剩余资源）。

系统按照用户为各队列配置的带宽换算队列的权重，为各队列分配带宽。

假设接口带宽和用户配置如表 2-3 所示：

表 2-3 拥塞管理配置参数示例

接口带宽	用户配置
100M	EF 队列：最大带宽为接口带宽的 50%
	AF 队列：最小带宽为 30M
	BE 队列：**default-class** 与 BE 队列关联使用，系统默认为其分配带宽为接口可用带宽的 10%

系统首先保证 EF 队列的带宽，AF 队列和 BE 队列按照权重分享剩余带宽：

- EF 队列带宽为 100M×50%=50M
- AF 队列：BE 队列=30M：（100M×10%）=30M：10M=3：1
- 剩余带宽为 100M－50M=50M
- AF 队列和 BE 队列按照 3：1 的权重分享剩余带宽：
  - AF 队列带宽为 50M×[3/(3+1)]=37.5M
  - BE 队列带宽为 50M×[1/(3+1)]=12.5M

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 **traffic behavior** *behavior-name*，创建一个流行为，并进入流行为视图。

步骤 3 请根据实际需要，选择执行下列命令，配置队列的调度方式：

- 执行命令 **queue af bandwidth** { *bandwidth* | **pct** *percentage* }，配置符合要求的某一类报文进入 AF 队列，并配置可确保的最小带宽。
- 执行命令 **queue ef bandwidth** { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] }，配置符合要求的某一类报文进入 EF 队列，并配置允许的最大带宽。

- 执行命令 **queue wfq** [**queue-number** *total-queue-number*]，配置缺省类报文进入使用 WFQ 方式调度的 BE 队列，并配置队列的总数。

步骤 4 （可选）执行命令 **queue-length** { **bytes** *bytes-value* | **packets** *packets-value* }*，配置队列的最大长度。

----结束

2.4.8 配置拥塞避免

配置基于流的拥塞避免，设置具有不同优先级的报文的丢弃高低门限以及最大丢弃概率。

背景信息

丢弃模板是队列各优先级 WRED 参数的集合，实现对绑定丢弃模板的队列的拥塞避免。

丢弃模板在流行为中绑定后，将流行为与流分类在流策略下进行绑定，并在接口下应用流策略，才能使丢弃模板中配置的 WRED 参数在该接口下生效。

说明

包含此流行为的流策略只能应用在 AR150/200 WAN 接口出方向上。

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 **traffic behavior** *behavior-name*，进入流行为视图。

说明

此流行为必须已经配置了 **queue af** 或 **queue wfq**。

步骤 3 执行命令 **drop-profile** *drop-profile-name*，在流行为中绑定已创建的丢弃模板。

说明

丢弃模板必须已经创建，并配置各优先级的 WRED 参数。

----结束

2.4.9 绑定子流策略

AR150/200 支持为流行为绑定一个子流策略，通过流策略嵌套实现更为精细化的 HQoS 服务。

背景信息

流策略嵌套是指一个 QoS 策略中包含另一个 QoS 策略，即父策略的行为（动作）是一个子策略。使用流策略嵌套时，对于命中流分类的某一类报文，除了执行父策略中定义的行为外，还由子策略再对该类流量进行分类，执行子策略中定义的行为。

AR150/200 支持两层策略嵌套，子策略下面不能再有嵌套。

只有子流策略和父流策略符合**表 2-4** 所示嵌套流策略的要求时，才能在父流策略中成功绑定子流策略。

表 2-4 嵌套流策略支持的流分类和流行为

流策略	流分类	流行为
父策略	全部支持	（必选）配置基于流的流量整形 （必选）绑定子策略 （可选）配置流量统计
子策略	全部支持	以下 2 种流行为是互斥的，不可同时配置： ● 配置基于流的流量整形 ● 配置基于流分类的拥塞管理和拥塞避免 －（必选）配置基于流分类的拥塞管理 －（可选）配置基于流的拥塞避免

说明

包含此流行为的流策略只能应用在 AR150/200 WAN 接口出方向上。

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 **traffic behavior** *behavior-name*，进入流行为视图。

说明

此流行为必须已经配置了 **gts（流行为视图）**。

步骤 3 执行命令 **traffic-policy** *policy-name*,在流行为中绑定子流策略。

说明

被绑定的子流策略必须是已经配置好的。

----结束

2.4.10 配置流量统计

通过配置流量统计，AR150/200 将对符合流分类规则的报文进行流量统计。

背景信息

接口下应用流策略后的报文统计信息，可以帮助用户了解应用流策略后报文通过和被丢弃的统计情况，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。

缺省情况下，未使能流策略的统计功能，必须先在流行为中使能该功能才能通过 **display traffic policy statistics** 命令查看相应统计信息。

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 **traffic behavior** *behavior-name*，创建一个流行为，进入流行为视图。

步骤 3 执行命令 **statistic enable**，使能流量统计功能。

----结束

2.4.11 检查配置结果

配置流行为后，可查看流行为信息。

前提条件

已经完成流行为的配置。

操作步骤

- 执行命令 **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]，查看流行为的配置信息。

----结束

2.5 配置流策略

配置完流分类和流行为后需要将流分类与流行为绑定，并应用在接口上。

应用环境

流分类提供了有区别地进行服务的前提和基础，流行为用来定义针对某类报文所做的 QoS 动作，只有将流分类和流行为关联起来才能形成完整的 QoS 策略。AR150/200 支持在 LAN 接口、WAN 接口或子接口应用 QoS 策略，更方便的配置 QoS 功能。

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。

前置任务

在配置流策略之前，需要完成以下任务：

- 配置流分类
- 配置流行为

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 **traffic policy** *policy-name*，创建流策略并进入流策略视图。

步骤 3 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，在策略中关联流分类和动作。

步骤 4 执行命令 **quit**，退出流策略视图。

步骤 5 执行命令 **interface** *interface-type interface-number*[*.subinterface-number*]，进入接口视图或子接口视图。

步骤 6 执行命令 **traffic-policy** *policy-name* { **inbound** | **outbound** }，在接口或子接口的入方向或出方向应用流策略。

----结束

检查配置结果

执行命令 **display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]，查看流策略的配置信息。

执行命令 **display traffic-policy** *policy-name* **applied-record**，查看指定流策略的应用记录信息。

2.6 维护流策略

如果已经使能了流量统计功能，可以查看和清除基于流的流量统计信息。

2.6.1 查看流策略统计信息

流策略统计信息中包含通过和丢弃的报文数等。

背景信息

用户需要了解接口下应用指定流策略后报文通过和被丢弃的情况时，可以查看接口下流策略的统计信息。

查看基于流的流量统计信息时，策略必须存在且已经包含流量统计动作。

操作步骤

步骤 1 执行命令 **display traffic policy statistics interface** *interface-type interface-number* [**pvc** *vpi-number/vci-number* | **dlci** *dlic-number*] { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]或 **display traffic policy statistics interface** { **virtual-template** *vt-number* **virtual-access** *va-number* | **dialer** *number* } { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]，查看指定接口应用流策略后的统计信息。

----结束

2.6.2 清除流策略统计信息

通过 **reset** 命令清除基于流的统计信息。

背景信息

当需要对接口上基于流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。

清除基于流的流量统计信息时，策略必须存在且已经包含流量统计动作。

注意

清除接口上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

步骤 1 执行命令 **reset traffic policy statistics interface** *interface-type interface-number* { **inbound** | **outbound** }或 **reset traffic policy statistics interface** { **virtual-template** *vt-number* **virtual-access** *va-number* | **dialer** *number* } { **inbound** | **outbound** }，清除接口上基于流的流量统计信息。

----结束

2.7 配置举例

通过示例介绍如何应用流策略。配置示例中包括组网需求、配置注意事项、配置思路等。

2.7.1 配置重标记示例

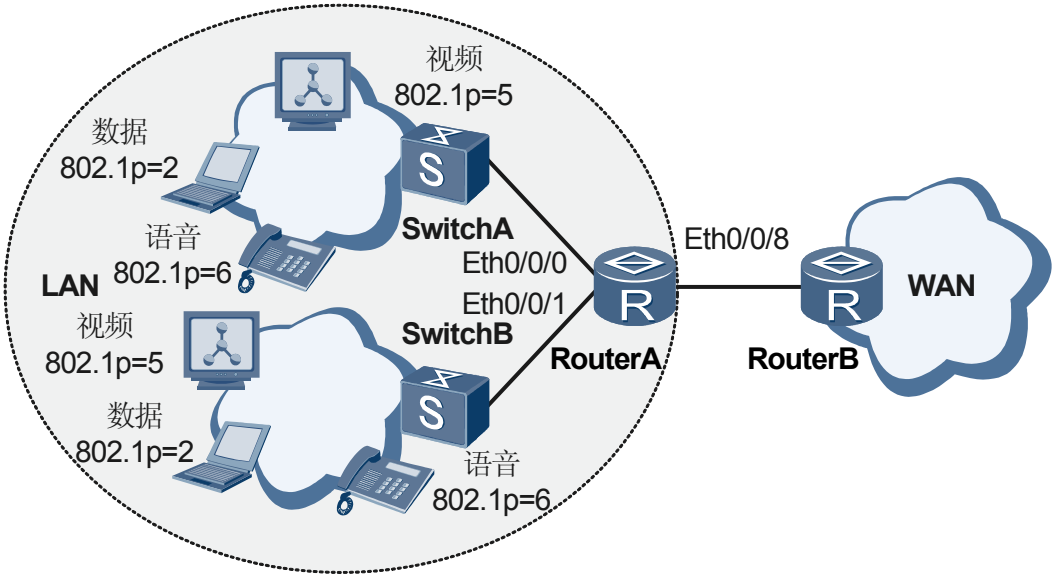
通过配置重标记，对具有不同 802.1p 优先级的报文重标记不同的 DSCP 优先级，以提供差分服务。

组网需求

如图 2-2 所示，企业网内部 LAN 侧的语音、视频和数据业务通过 SwitchA 和 SwitchB 连接到 RouterA 的 Eth0/0/0 和 Eth0/0/1 上，并通过 RouterA 的 Eth0/0/8 接口连接到 WAN 侧网络。

不同业务的报文在 LAN 侧使用 802.1p 优先级进行标识，当报文从 RouterA 的 Eth0/0/8 接口到达 WAN 侧时，需要根据报文的 DSCP 优先级提供差分服务，通过重标记，可以根据报文的 802.1p 优先级为其标记相应的 DSCP 优先级。

图 2-2 配置重标记的组网图



配置思路

采用如下的思路配置基于复杂流分类的优先级重标记：

1. 在 RouterA 上创建 VLAN、VLANIF，并配置各接口，使企业用户能通过 RouterA 访问 WAN 侧网络。
2. 在 RouterA 上配置流分类，基于 802.1p 优先级对报文进行匹配。
3. 在 RouterA 上配置流行为，重标记报文的 DSCP 优先级。
4. 在 RouterA 上配置流策略，绑定已经配置好的流行为和流分类，并应用到接口 Eth0/0/0 和 Eth0/0/1 入方向上。

数据准备

为完成此配置例，需准备如下的数据：

- RouterA 与 SwitchA 相连的接口所属 VLAN 编号为 20，VLANIF 20 的 IP 地址为 192.168.2.1/24。
- RouterA 与 SwitchB 相连的接口所属 VLAN 编号为 30，VLANIF 30 的 IP 地址为 192.168.3.1/24。
- RouterA 与 WAN 侧相连的接口 IP 地址为 192.168.4.1/24。
- 802.1p 优先级分别为 2、5、6 的数据、视频和语音报文重标记后的 DSCP 优先级为 15、40、50。
- 需要应用流策略的接口类型、方向和编号：RouterA 上接口 Eth0/0/0 和 Eth0/0/1 的入方向。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 RouterA 上创建 VLAN 20、30。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 20 30
```

配置接口 Eth0/0/0 和 Eth0/0/1 为 Trunk 类型端口，并将 Eth0/0/0 加入 VLAN20，将 Eth0/0/1 加入 VLAN30。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] port link-type trunk
[RouterA-Ethernet0/0/0] port trunk allow-pass vlan 20
[RouterA-Ethernet0/0/0] quit
[RouterA] interface ethernet 0/0/1
[RouterA-Ethernet0/0/1] port link-type trunk
[RouterA-Ethernet0/0/1] port trunk allow-pass vlan 30
[RouterA-Ethernet0/0/1] quit
```

说明

请配置 SwitchA 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN20。

请配置 SwitchB 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN30。

创建 VLANIF 20、30，并为 VLANIF 20 配置 IP 地址 192.168.2.1/24，为 VLANIF 30 配置 IP 地址 192.168.3.1/24。

```
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 192.168.2.1 24
[RouterA-Vlanif20] quit
[RouterA] interface vlanif 30
[RouterA-Vlanif30] ip address 192.168.3.1 24
[RouterA-Vlanif30] quit
```

配置 Eth0/0/8 的 IP 地址为 192.168.4.1/24。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] ip address 192.168.4.1 24
[RouterA-Ethernet0/0/8] quit
```

说明

根据实际情况配置 RouterB，确保 RouterB 与 RouterA 间路由可达，具体步骤略。

步骤 2 配置流分类

在 RouterA 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。

```
[RouterA] traffic classifier c1
[RouterA-classifier-c1] if-match 8021p 2
[RouterA-classifier-c1] quit
[RouterA] traffic classifier c2
[RouterA-classifier-c2] if-match 8021p 5
[RouterA-classifier-c2] quit
[RouterA] traffic classifier c3
[RouterA-classifier-c3] if-match 8021p 6
[RouterA-classifier-c3] quit
```

步骤 3 配置流行为

在 RouterA 上创建并配置流行为 b1、b2、b3，重标记用户报文的优先级。

```
[RouterA] traffic behavior b1
[RouterA-behavior-b1] remark dscp 15
[RouterA-behavior-b1]  quit
[RouterA] traffic behavior b2
[RouterA-behavior-b2] remark dscp 40
[RouterA-behavior-b2] quit
[RouterA] traffic behavior b3
[RouterA-behavior-b3] remark dscp 50
[RouterA-behavior-b3] quit
```

步骤 4 配置流策略并应用到接口上

在 RouterA 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 Eth0/0/0 和 Eth0/0/1 的入方向上，对报文进行重标记。

```
[RouterA] traffic policy p1
[RouterA-trafficpolicy-p1] classifier c1 behavior b1
[RouterA-trafficpolicy-p1] classifier c2 behavior b2
[RouterA-trafficpolicy-p1] classifier c3 behavior b3
[RouterA-trafficpolicy-p1] quit
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] traffic-policy p1 inbound
[RouterA-Ethernet0/0/0] quit
[RouterA] interface ethernet 0/0/1
[RouterA-Ethernet0/0/1] traffic-policy p1 inbound
[RouterA-Ethernet0/0/1] quit
[RouterA] quit
```

步骤 5 验证配置结果

查看流分类的配置信息。

```
<RouterA> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: OR
    Rule(s) : if-match 8021p 5

   Classifier: c3
    Operator: OR
    Rule(s) : if-match 8021p 6

   Classifier: c1
    Operator: OR
    Rule(s) : if-match 8021p 2
```

查看流策略的配置信息。

```
<RouterA> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: OR
     Behavior: b1
      Marking:
        Remark DSCP 15

   Classifier: c2
    Operator: OR
     Behavior: b2
      Marking:
        Remark DSCP cs5

   Classifier: c3
    Operator: OR
     Behavior: b3
      Marking:
        Remark DSCP 50
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
```

```
#
 vlan batch 20 30
#
traffic classifier c3 operator or
 if-match 8021p 6
traffic classifier c2 operator or
 if-match 8021p 5
traffic classifier c1 operator or
 if-match 8021p 2
#
traffic behavior b3
 remark dscp 50
traffic behavior b2
 remark dscp cs5
traffic behavior b1
 remark dscp 15
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p1 inbound
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p1 inbound
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
#
return
```

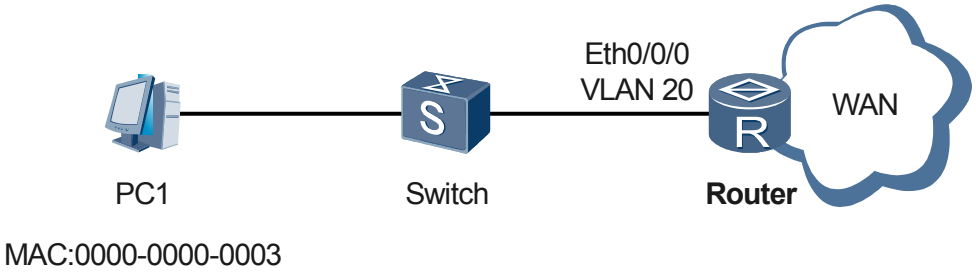
2.7.2 配置流量统计示例

通过配置流量统计，对具有特定源 MAC 地址的报文进行流量统计。

组网需求

如图 2-3 所示,PC1 的 MAC 地址为 0000-0000-0003，它通过交换机连接在 Router 的 Eth0/0/0 端口上。现要求 Router 对源 MAC 为 0000-0000-0003 的报文进行流量统计。

图 2-3 配置流量统计的组网图



配置思路

采用如下的思路配置基于复杂流分类的流量统计：

1. 配置各接口，实现 Router 与 Switch、PC1 互通。
2. 配置 ACL 规则，匹配源 MAC 为 0000-0000-0003 的报文。
3. 配置流分类，匹配规则为上述 ACL 规则。
4. 配置流行为，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 Eth0/0/0 入方向，对该接口收到的源 MAC 为 0000-0000-0003 的报文进行流量统计。

数据准备

为完成此配置示例，需准备如下的数据：

- Router 与 Switch 相连的接口所属 VLAN 编号为 20。
- ACL 规则编号为 4000。
- 流分类的名称为 c1。
- 流行为的名称为 b1。
- 流策略的名称为 p1。

操作步骤

步骤 1 创建 VLAN 并配置各接口

创建 VLAN20。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 20
[Router-vlan20] quit
```

配置接口 Eth0/0/0 为 Trunk 类型端口，并将 Eth0/0/0 加入 VLAN20。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port link-type trunk
[Router-Ethernet0/0/0] port trunk allow-pass vlan 20
[Router-Ethernet0/0/0] quit
```

说明

请配置 Switch 与 Router 对接的接口为 Trunk 类型接口，并加入 VLAN20。

请配置 Switch 与 PC1 对接的接口为 Access 类型接口，并加入 VLAN20。

步骤 2 配置 ACL 规则

在 Router 上创建编码为 4000 的二层 ACL，匹配源 MAC 为 0000-0000-0003 的报文。

```
[Router] acl 4000
[Router-acl-L2-4000] rule permit source-mac 0000-0000-0003 ffff-ffff-ffff
[Router-acl-L2-4000] quit
```

步骤 3 配置流分类

在 Router 上创建流分类 c1，匹配规则为 ACL 4000。

```
[Router] traffic classifier c1
[Router-classifier-c1] if-match acl 4000
[Router-classifier-c1] quit
```

步骤 4 配置流行为

在 Router 上创建流行为 b1，并配置流量统计动作。

```
[Router] traffic behavior b1
[Router-behavior-b1] statistic enable
[Router-behavior-b1] quit
```

步骤 5 配置流策略并应用到接口上

在 Router 上创建流策略 p1，将流分类和对应的流行为进行绑定。

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

将流策略 p1 应用到接口 Ethernet0/0/0。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] traffic-policy p1 inbound
[Router-Ethernet0/0/0] quit
[Router] quit
```

步骤 6 验证配置结果

查看 ACL 规则的配置信息。

```
<Router> display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 permit source-mac 0000-0000-0003
```

查看流分类的配置信息。

```
<Router> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Operator: OR
    Rule(s) : if-match acl 4000
```

查看流策略的配置信息。

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

查看流量统计信息。

```
<Router> display traffic policy statistics interface Ethernet 0/0/0 inbound

 Interface: Ethernet0/0/0 Traffic policy inbound:
p1
 Rule number: 1
 Current status: OK!
Item                          Sum(Packets/Bytes)            Rate(pps/bps)
-------------------------------------------------------------------------------
Matched                                    0/                            0/
                                           -                             -
  +--Passed                                0/                            0/
                                           -                             -
  +--Dropped                               0/                            0/
                                           -                             -
```

```
    +--Filter                    0/                    0/
                                 -                     -
    +--CAR                       0/                    0/
                                 -                     -
  +--Queue Matched               0/                     0/
                                 0                     0
    +--Enqueued                  0/                    0/
                                 0                     0
    +--Discarded                 0/                    0/
                                 0                     0
   +--Car                        0/                    0/
                                 -                     -
    +--Green packets             0/                    0/
                                 -                     -
    +--Yellow packets            0/                    0/
                                 -                     -
    +--Red packets               0/                    0/
                                 -                     -
```

----结束

配置文件

- Router 的配置文件

```
#
 sysname Router
#
 vlan batch 20
#
acl number 4000
 rule 5 permit source-mac 0000-0000-0003
#
traffic classifier c1 operator or
 if-match acl 4000
#
traffic behavior b1
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p1 inbound
#
return
```

2.7.3 配置禁止 BT 下载示例

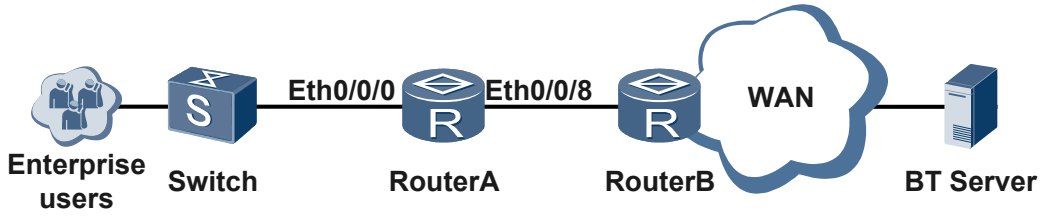
通过配置基于 SAC 的流分类，实现禁止 BT 下载，对企业的网络流量进行细粒度调控，避免带宽被非关键业务占用。

组网需求

如图 2-4 所示，企业内部用户通过交换机连接到 RouterA 的 Eth0/0/0，并通过 RouterA 的 Eth0/0/8 接口连接到 WAN 侧网络。

现在要求在 RouterA 上通过配置基于 SAC 的流分类，禁止企业用户进行 BT 下载。

图 2-4 配置禁止 BT 下载的组网图



配置思路

采用如下的思路配置禁止 BT 下载：

1. 配置各接口，使企业用户能通过 RouterA 访问 WAN 侧网络。
2. 配置 SAC 功能。
3. 配置流分类，匹配规则为匹配 BT 应用协议。
4. 配置流行为，禁止符合流分类规则的报文通过。
5. 配置流策略，绑定上述流分类和流行为，并应用到相应的接口。

数据准备

为完成此配置示例，需准备如下的数据：

- RouterA 与 Switch 相连的接口 Eth0/0/0 所属 VLAN 编号为 20，VLANIF 20 的 IP 地址为 192.168.2.1/24。
- RouterA 与 WAN 侧相连的接口 Eth0/0/8IP 地址为 192.168.4.1/24。
- SAC 特征库文件的名称和存储路径：**flash:/sacrule.dat**。
- 流分类的名称为 **c1**，匹配规则为匹配 BT 应用协议。
- 流行为的名称为 **b1**，动作为 **deny**。
- 流策略的名称为 **p1**，应用在接口 Eth0/0/8 和 VLANIF 20 的入方向上。

操作步骤

步骤 1 创建 VLAN 并配置各接口

在 RouterA 上创建 VLAN 20。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan 20
```

配置接口 Eth0/0/0 为 Trunk 类型端口，并将 Eth0/0/0 加入 VLAN 20。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] port link-type trunk
[RouterA-Ethernet0/0/0] port trunk allow-pass vlan 20
[RouterA-Ethernet0/0/0] quit
```

说明

请配置 Switch 与 RouterA 对接的接口为 Trunk 类型接口，并加入 VLAN 20。

创建 VLANIF 20，并为 VLANIF 20 配置 IP 地址 192.168.2.1/24。

```
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 192.168.2.1 24
[RouterA-Vlanif20] quit
```

配置 Eth0/0/8 的 IP 地址为 192.168.4.1/24。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] ip address 192.168.4.1 24
[RouterA-Ethernet0/0/8] quit
```

说明

根据实际情况配置 RouterB，确保 RouterB 与 RouterA 间路由可达，具体步骤略。

步骤 2 配置 SAC 功能

在 RouterA 使能 SAC 功能，并加载特征库文件。

```
[RouterA] sac enable signature flash:/sacrule.dat
Info: SAC enable successful.
```

说明

SAC 特征库文件已经上传到设备，保存在设备的 flash 上。

使能接口 Eth0/0/8 和 VLANIF 20 基于 SAC 的流量统计功能。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] sac protocol-statistic enable
[RouterA-Ethernet0/0/8] quit
[RouterA] interface vlanif 20
[RouterA-Vlanif20] sac protocol-statistic enable
[RouterA-Vlanif20] quit
```

步骤 3 配置流分类

在 RouterA 上创建流分类 **c1**，匹配 BT 应用协议。

```
[RouterA] traffic classifier c1
[RouterA-classifier-c1] if-match app-protocol bittorrent
[RouterA-classifier-c1] quit
```

步骤 4 配置流行为

在 RouterA 上创建流行为 **b1**，禁止匹配指定规则的报文流通过。

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

步骤 5 配置流策略并应用到接口上

在 RouterA 上创建流策略 **p1**，将流分类和对应的流行为进行绑定。

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

将流策略 **p1** 应用到接口 Eth0/0/8 和 VLANIF 20 入方向。

```
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] traffic-policy p1 inbound
[RouterA-Ethernet0/0/8] quit
[RouterA] interface vlanif 20
[RouterA-Vlanif20] traffic-policy p1 inbound
[RouterA-Vlanif20] quit
```

步骤 6 验证配置结果

查看 RouterA 接口的配置信息。

```
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] display this
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
#
return
[RouterA-Ethernet0/0/0] quit
[RouterA] interface vlanif 20
[RouterA-Vlanif20] display this
#

interface
Vlanif20
 ip address 192.168.2.1
255.255.255.0
 sac protocol-statistic
enable
 traffic-policy p1
inbound
#

return
[RouterA-Vlanif20] quit
[RouterA] interface ethernet 0/0/8
[RouterA-Ethernet0/0/8] display this
#
interfaceEthernet0/0/8
 ip address 192.168.4.1 255.255.255.0
 sac protocol-statistic enable
 traffic-policy p1 inbound
#
return
[RouterA-Ethernet0/0/8] quit
```

查看在接口上应用的流策略的配置信息。

```
[RouterA] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: OR
     Behavior: b1
      Deny
```

查看流分类 **c1** 的配置信息。

```
[RouterA] display traffic classifier user-defined c1
  User Defined Classifier Information:
   Classifier: c1
    Operator: OR
    Rule(s) : if-match app-protocol name bittorrent
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
vlan batch 20
#
 sac enable signature flash:/sacrule.dat
#
traffic classifier c1 operator or
 if-match app-protocol bittorrent
#
```

```
traffic behavior b1
 deny
#

traffic policy p1
 classifier c1 behavior b1
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
 sac protocol-statistic
enable
 traffic-policy p1
inbound
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface Ethernet0/0/8
 ip address 192.168.4.1 255.255.255.0
 sac protocol-statistic enable
 traffic-policy p1 inbound
#
return
```